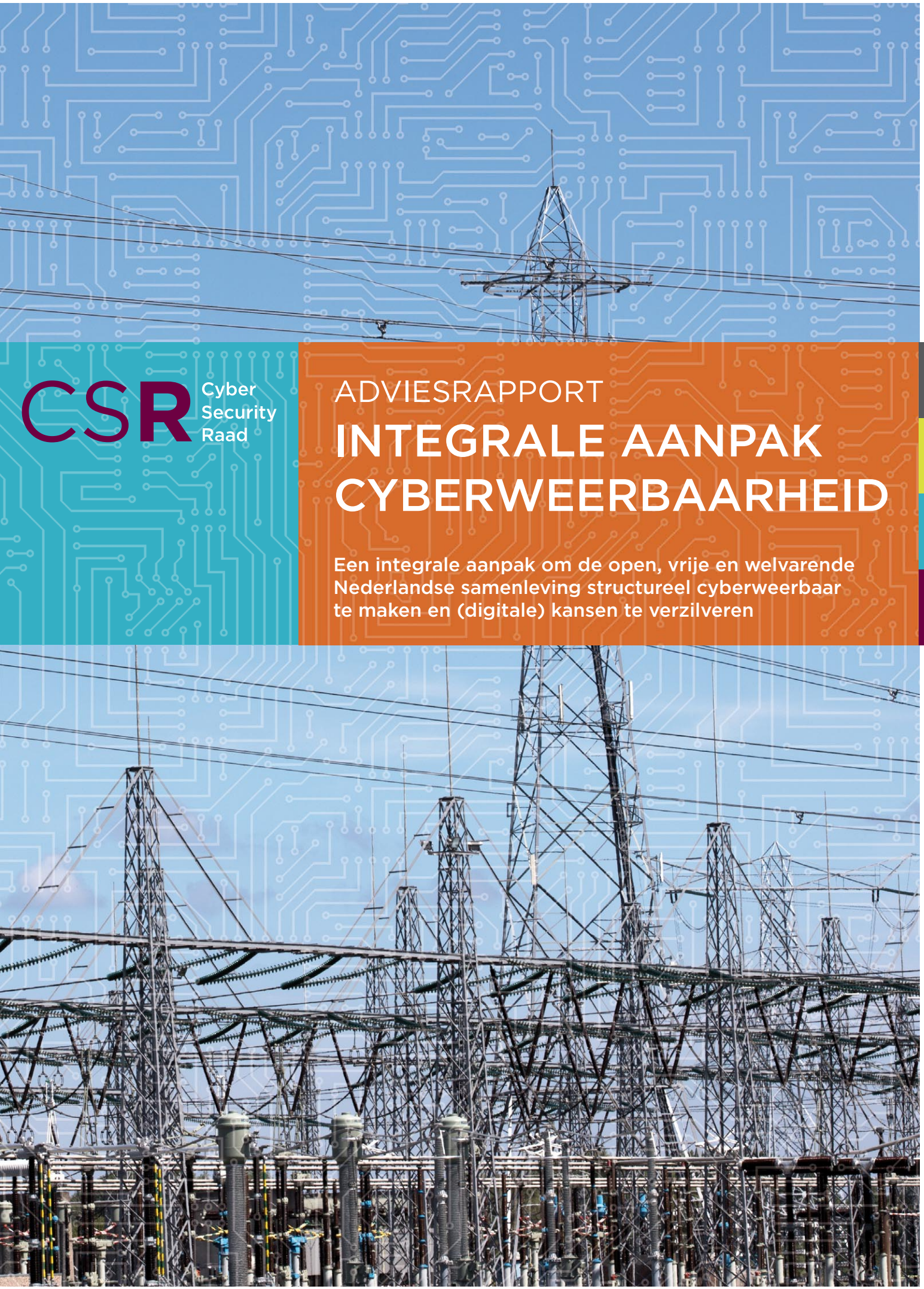


CSR Cyber Security Raad

ADVIESRAPPORT

INTEGRALE AANPAK CYBERWEERBAARHEID

Een integrale aanpak om de open, vrije en welvarende Nederlandse samenleving structureel cyberweerbaar te maken en (digitale) kansen te verzilveren

Foto omslag: Jeroen de Bakker

INHOUDSOPGAVE

Foto: Jeroen de Bakker

SAMENVATTING

Dit adviesrapport van de Cyber Security Raad (hierna de raad) heeft als doel om op basis van een grondige analyse van de huidige staat van de cyberweerbaarheid van de Nederlandse samenleving concrete adviezen te geven, met daaraan gekoppeld de benodigde investeringen gedurende de komende kabinetsperiode die leiden tot verbeterde cyberweerbaarheid van de Nederlandse samenleving. De totaal benodigde minimale investeringen van de vijf speerpunten komen uit op minimaal € 833 miljoen voor de aankomende kabinetsperiode. Deze investeringen zijn aanvullend op de huidige (structurele) investeringen in cyberweerbaarheid. Aanleiding voor dit adviesrapport is het verzoek van de (nu demissionair) minister van Justitie en Veiligheid[1] om een advies uit te brengen over de benodigde investeringen in cyberweerbaarheid door het nieuwe kabinet. Voorbeelden van tekortschietende cyberweerbaarheid verschijnen bijna dagelijks in het nieuws. Het datalek bij de GGD (opstapeling van cyberrisico's), de aanval op de Universiteit van Maastricht (ransomware) en de Citrix-kwetsbaarheid zijn recente voorbeelden van de maatschappelijke impact van onvoldoende cyberweerbaarheid.

Het belang van cyberweerbaarheid

De toename in cyberincidenten in de laatste jaren is voornamelijk te verklaren op basis van twee ontwikkelingen: de Nederlandse digitaliseringsambitie en toenemende cyberdreigingen. De Nederlandse overheid, economie en samenleving digitaliseert steeds verder. Deze digitalisering draagt direct bij aan een open, vrije en welvarende samenleving. Deze digitalisering is door COVID-19 in een versnelling gekomen waarbij de informatiebeveiliging geen gelijke tred hield. Het risico is dus in absolute en relatieve zin toegenomen. Voor het behoud van de open, vrije en welvarende samenleving is het noodzakelijk om de cyberweerbaarheid in Nederland te versterken aan de hand van een aantal gerichte investeringen. Het maatschappelijk belang van een cyberweerbare overheid, samenleving en economie wordt ook voor een deel erkend door politieke partijen in Nederland. In de verkiezingsprogramma's voor de aankomende verkiezingen hebben de meeste partijen een standpunt ingenomen om de cyberweerbaarheid van Nederland te versterken.

Permanente cyberdreigingen

Om de weerbaarheid te kunnen vergroten, moet deze in samenhang worden bezien met de dreiging en de te beschermen belangen. Cyberdreigingen voor de Nederlandse samenleving zijn permanent aanwezig. In het Cybersecuritybeeld Nederland (CSBN) 2020, gepubliceerd door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), wordt geconcludeerd dat net als in 2019 de digitale dreiging een permanent karakter heeft en dat cyberincidenten kunnen leiden tot maatschappij-ontwrichtende schade. Recente criminele cyberaanvallen en uitval van systemen hebben duidelijke maatschappelijke gevolgen gehad voor de overheid, het bedrijfsleven en burgers.[2]

1 Verzoekbrief NCTV, advies evaluatie NCSA en investeringen nieuw kabinet, d.d. 4 maart 2020
2 Nationaal Coördinator Terrorismebestrijding en Veiligheid, Cybersecuritybeeld Nederland 2020

Naast het CSBN 2020 hebben de NCTV, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) recent het Dreigingsbeeld Statelijke Actoren 2020[3] gepubliceerd. Hierin wordt geconcludeerd dat de verschillende nationale veiligheidsbelangen kwetsbaar zijn en door statelijke actoren substantieel bedreigd en aangetast worden. Ook is er sprake van economische spionageactiviteiten, die met name zijn gericht op Nederlandse topsectoren en kennisinstellingen. Economische activiteiten zoals investeringen in en samenwerking bij de ontwikkeling van sensitieve technologieën vormen een dreiging, omdat kennis- en technologieoverdracht die vanuit het oogpunt van nationale veiligheid ongewenst is kan plaatsvinden en omdat (ongewenste) strategische afhankelijkheid kan ontstaan. Wanneer er in dit rapport gesproken wordt over weerbaarheid tegen cyberdreigingen, dan wordt hierbij gerefereerd naar alle dreigingen die in deze beide rapporten worden genoemd.

De internationale positie van Nederland

In navolging van bovenstaande ontwikkelingen hebben landen om ons heen voorgenomen investeringen in cyberweerbaarheid in de afgelopen jaren versneld. De investeringsambitie (genormaliseerd voor BBP) van deze landen is significant hoger dan de Nederlandse ambitie in de Nederlandse Cybersecurity Agenda[4] (€ 95 miljoen). Zo is de Belgische investeringsambitie 14 keer zo hoog dan de Nederlandse. De investeringsambitie van Denemarken en het Verenigd Koninkrijk ligt respectievelijk 9% en 56% hoger. Van de buitenlandse ambities is niet inzichtelijk hoe deze worden besteed en in welke mate deze worden waargemaakt. Onderzoek laat zien dat Nederland voor 2018 geen investeringsvoorsprong heeft opgebouwd die de verschillen in investeringsambities verklaren[5]. Nederland raakt dus mogelijk op achterstand wanneer er geen versnelling wordt ingezet door de komende regering. In veiligheidstermen betekent ‘achterlopen’ dat het relatieve risico toeneemt omdat (cyber)criminaliteit de weg van de minste weerstand kiest. Meer details over het benchmarkonderzoek zijn opgenomen in bijlage 2[6].

Huidige cyberweerbaarheid moet verder worden versterkt

In de afgelopen jaren is door overheid, bedrijfsleven en wetenschap veel tijd en middelen geïnvesteerd in cyberweerbaarheid. Echter is op dit moment de cyberweerbaarheid in Nederland nog niet overal afdoende om de toenemende dreigingen het hoofd te bieden. Daarom zijn additionele inzet en investering vereist in de komende jaren. De cyberweerbaarheidsketen in Nederland bestaat uit vijf kerncomponenten, zoals in Figuur 1 is uitgebeeld. De keten beslaat zowel componenten die direct bijdragen aan cyberweerbaarheid zoals veilige producten en diensten, als componenten die randvoorwaardelijk zijn voor succesvol verbeteren van de cyberweerbaarheid, zoals regie en kennisontwikkeling. De cyberweerbaarheidsketen bestaat uit de volgende componenten (zie ook Figuur 1):

1. Regie op cyberweerbaarheid: overkoepelende coördinatie op activiteiten, heldere verantwoordelijkheden, en een dekkend stelsel van informatieknooppunten.
2. Kennis, onderzoek en ontwikkeling: het continue verbeteren van kennis, expertise en bewustzijn op het gebied van cybersecurity. Hieronder valt ook onderzoek en innovatie om toegang tot innovatieve producten en diensten te bevorderen.
3. Veilige producten en diensten voor burgers, bedrijfsleven en overheid: zorgdragen voor de maximale beveiliging van producten en diensten, zodat burgers en bedrijven kunnen vertrouwen op hetgeen zij afnemen en gebruiken in hun dagelijks leven of bedrijfsprocessen.
4. Veilige vitale processen en infrastructuur: het beveiligen van vitale processen om de kans en impact van disruptieve gebeurtenis als gevolg van cyberaanvallen zo veel mogelijk te voorkomen en de schade ervan te beperken.
5. Toezicht, handhaving en bescherming: de drie kerntaken van de overheid op dit gebied; opsporing en vervolging van cybercriminaliteit, inlichtingen verzamelen over digitale dreigingen en bescherming van de digitale ruimte en tegengaan en bestrijding van nationale cybercrises.

3 Algemene Inlichtingen- en Veiligheidsdienst, Militaire Inlichtingen- en Veiligheidsdienst en Nationaal Coördinator Terrorismebestrijding en Veiligheid, Dreigingsbeeld Statelijke Actoren 2020

4 Nederlandse Cybersecurity Agenda, Ministerie van Justitie en Veiligheid (2018).

5 *Global Cybersecurity Index (CGI)* (2018) en *Dutch Investments in ICT and Cybersecurity: Putting it in Perspective*, The Hague Centre for Strategic Studies (2016).

6 Zie bijlage 2 voor het benchmarkonderzoek

Figuur 1 **Cyberweerbaarheidsketen**

Bij het bovenstaande is digitale strategische autonomie in cybersecurity een doorsnijdend thema[7]. Cybersecurity wordt dus ook nadrukkelijk gezien vanuit soevereiniteitsperspectief. Dit verband komt in dit rapport bij elk speerpunt terug. Met uitzondering van benodigde investeringen voor het implementeren en uitvoeren van een toetsingskader voor digitale autonomie (zie sectie 1.4), zijn specifieke investeringen op dit vlak niet in dit rapport meegenomen. Dit betekent dat de investeringen die benodigd zijn om de (gerichte) adviezen omtrent autonomie uit te voeren niet meegenomen zijn in de begroting en er bijvoorbeeld nog investeringen benodigd zijn voor het realiseren van de drie basisvoorzieningen[8].

Voor alle componenten binnen de cyberweerbaarheidsketen geldt dat de defensieve, offensieve en inlichtingen cybercapaciteiten binnen Defensie (incl. MIVD en KMar), de AIVD, het NCSC de politie en het OM[9] een essentiële bijdrage leveren, bijvoorbeeld door middel van het inzichtelijk maken en delen van dreigingen en concrete informatie daaromtrent en de afschrikwekkende werking (deterrence) voortkomend uit de offensieve capaciteiten. De investeringen uit dit rapport kunnen niet los worden gezien van benodigde investeringen in de digitale slagkracht en digitale overheid. Investeren in de inlichtingendiensten is vrijwel gelijk aan investeren in zowel zicht op de dreiging als in deterrence. Het budget van deze diensten valt weliswaar buiten de scope van dit advies: de intensivering van de inlichtingentaak op het terrein van cybersecurity is van wezensbelang voor de verhoging de cyberweerbaarheid van Nederland

Huidige staat

Voor elk van de componenten voor de cyberweerbaarheidsketen wordt zowel op nationaal als op EU-niveau belangrijke activiteiten ondernomen ter verbetering van de cyberweerbaarheid. Echter, op dit moment is de cyberweerbaarheidsketen in Nederland niet op alle punten even sterk, wat maakt dat er lacunes en gebreken ontstaan waardoor de cyberweerbaarheid van Nederland op diverse onderdelen zwakheden vertoont. Ook is de dreiging in de afgelopen vier jaar aanzienlijk toegenomen. Op bijna dagelijkse basis zien we criminele en statelijke actoren daar gebruik van maken. Nederland moet het been bijtrekken, ook om te voorkomen dat het achter Europese ontwikkelingen aanloopt. Deze tekortkoming vereisen additionele inzet en investering. Uit het onderzoek blijkt dat de grootste problemen die op dit moment worden geconstateerd in de Nederlandse cyberweerbaarheidsketen de volgende zijn:

De coördinatie op de cyberweerbaarheidsketen en informatiedeling daarbinnen kan beter

Het cybersecuritylandschap kenmerkt zich door versnippering. Een duidelijke gezamenlijke nationale cyberweerbaarheidsstrategie, op basis van een gedegen risico inschatting, gemaakt door voorgenoemde diensten, ontbreekt. Departementen werken nog onvoldoende samen en cruciale dreigingsinformatie wordt om diverse redenen niet gedeeld. Er is nog geen proactieve aanpak om bedreigingen van digitale autonomie te anticiperen of tijdig af te weren[10]. Er kan beter gebruik gemaakt worden van het brede spectrum van middelen en processen om cyberweerbaarheid actief en geïntegreerd aan te pakken.

7 Onderzoeksrapport 'Nederlandse strategische autonomie en cybersecurity', Paul Timmers en Freddy Dezeure, januari 2021 (een onderzoek uitgevoerd in opdracht van de Cyber Security Raad)
8 De drie basisvoorzieningen zijn een soevereiniteit-respecterende cloud, veilige digitale communicatie en postkwantumcryptografie
9 In navolging van onder andere de Wet Computercriminaliteit III
10 Onderzoeksrapport 'Nederlandse strategische autonomie en cybersecurity', Paul Timmers en Freddy Dezeure, januari 2021 (een onderzoek uitgevoerd in opdracht van de Cyber Security Raad)

Organisaties hebben onvoldoende dreigingsinformatie tot hun beschikking, waardoor zij qua beveiliging achter de feiten aanlopen, kwetsbaarheden over het hoofd zien of niet weten dat zij (potentieel) doelwit of slachtoffer van een dreigingsactor zijn. In het algemeen ontbreekt het besef bij bedrijven en burgers dat de kans groot is slachtoffer te worden zonder doelwit te zijn.

Cyberweerbaarheid van veel organisaties is nog onvoldoende op orde

Regelmatig is bij organisaties de cybersecurityvolwassenheid onvoldoende op orde, mede doordat de basis IT- en beveiligingshygiëne niet op orde is waardoor ook basale dreigingen niet gepareerd of gedetecteerd kunnen worden. Dit geldt ook voor organisaties die onderdeel zijn van vitale processen. Doordat eigen beveiliging (en die van gebruikte diensten en producten) nog te weinig op het benodigde niveau is, en organisaties vaak zelfs niet in staat zijn basale dreigingen te weren, loopt ook de opsporing vol met meer zaken dan zij aankan. Bedrijven en burgers kunnen onvoldoende vertrouwen op veiligheid van hard- en software die zij inkopen. Het is niet duidelijk welke eisen zij moeten stellen aan diensten om te bepalen of die veilig genoeg zijn voor hun gebruik.

Bestrijding van misbruik van onze digitale infrastructuur wordt nog in beperkte mate over de volle breedte van de keten gedaan, waardoor voor sommige fenomenen alleen strafrechtelijk ingrijpen wordt toegepast.

Opsporing en vervolging heeft te weinig capaciteit en expertise, en processen zijn onvoldoende geoptimaliseerd voor de taak waar zij voor staat

Er is onvoldoende zicht op belangrijke trends waar opsporing en vervolging op in zou kunnen grijpen en informatie wordt beperkt gedeeld tussen opsporing en vervolging en andere delen in de cyberweerbaarheidsketen. Daarnaast komt de informatie die potentieel voortkomt uit deze taak, onvoldoende ten goede aan preventie. Bovendien neemt het aantal slachtoffers van cybercrime toe en is er onvoldoende kennis en capaciteit bij de politie en het OM.

Onvoldoende investeringen in onderzoek, onderwijs en innovatie

Er wordt onvoldoende in Nederlands cyberweerbaarheid-onderzoek, onderwijs en innovatie geïnvesteerd. Dit heeft als gevolg dat Nederlands wetenschappelijk en maatschappelijk cybertalent vertrekt naar het buitenland (*braindrain*) wat verder bijdraagt aan het huidige tekort aan voldoende gekwalificeerde specialisten in het cybersecuritydomein.

Advies: Integrale aanpak cyberweerbaarheid

Cyberweerbaarheid is een complex probleem wat in alle lagen van onze samenleving geadresseerd moet worden. Om de volgende regering te ondersteunen bij het integraal versterken van de cyberweerbaarheid presenteert de raad vijf concrete speerpunten. Deze speerpunten vormen aanvullende adviezen op eerder uitgebrachte adviezen van de raad, waar in wisselende mate opvolging aan is gegeven. Deze adviezen en bijbehorende kosten zullen uitgebreid in dit rapport worden behandeld. Daarmee wordt antwoord gegeven op het verzoek van de (nu demissionair) minister van Justitie en Veiligheid[11] waarmee dit onderzoek is geïnitieerd.

11 Verzoekbrief NCTV, advies evaluatie NCSA en investeringen nieuw kabinet, d.d. 4 maart 2020

Figuur 2


(1) Regie op cyberweerbaarheid
Ontwikkel een gemeenschappelijke koers op het gebied van cybersecurity
• Realiseer een effectieve, strategische geïntegreerde aanpak vanuit het digitale soevereiniteitsperspectief.
• Ontwikkel een gedragen nationale cyberweerbaarheids-strategie.
Verbeter informatiedelingscapaciteiten en ondersteuning
• Optimaliseer het landelijk Dekkend Stelsel Informatie-knooppunten.
• Pas juridische beperkingen voor het delen dreigings-informatie aan.
(5) Veilige producten en diensten voor burgers, bedrijfsleven en overheid
Zorgplicht voor cybersecurity van hard- en software
• Draag bij aan het invoeren van EU-richtlijnen m.b.t. zorgplicht en het toezicht hierop.
• Investeer in een systeem van co-regulering.
• Sluit een cyberverzekeringssysteem aan op de co-regulering.
Ondersteuning burgers en mkb bij cyberveilig gedrag
• Zet een monitor voor besmette IoT-apparaten op.
• Investeer in bewustwordings-campagnes voor het belang veilige producten.
• Voer een labeling-systeem in.
(2) Weerbare vitale processen en infrastructuur
Cyberweerbaarheid versnellings-fonds
• Zet een cyberweerbaarheids-versnellingsfonds voor vitale aanbieders op.
Versterkt toezicht op vitale processen
• Herzie het onderscheid vitale/niet vitale organisaties.
• Bouw de capaciteit en expertise van toezichthouders verder op.
Aansluiting bij Europese initiatieven en ondersteuning
• Sluit aan bij (supply chain) beveiliging- en autonomie initiatieven op EU-niveau.
(4) Cybercrimetoezicht, -handhaving en -bescherming
Inzichtelijker maken van cybercrime
• Zet een cybercrimemonitor op.
• Investeer in het stimuleren van melding en aangifte doen.
• Breng bestaande initiatieven samen m.b.t. bieden handelings-perspectieven burgers.
Structurele investering aanpak cybercrime
• Investeer in slagkracht OM.
• Investeer in digitale vaardigheden, middelen en data gedreven werken politie en KMar.
• Investeer in initiatieven voor het ontsnappen uit cybercriminaliteit.
• Herzie/herformuleer de wettelijke rol van hostingbedrijven.
(3) Kennis, onderzoek en innovatie
Cybersecurity-onderzoek en innovatie
• Transformeer het *Samenwerkings-platform 'cybersecurity kennis en innovatie'* naar een centraal cybersecurity-onderzoeks- en innovatie-ecosysteem.
Stimulans wetenschappelijk onder-zoek en innovatie
• Maak meer financiële middelen vrij voor cybersecurity-onderzoek en innovatie.
Voldoende gekwalificeerde specialisten
• Stel een nationale cybersecurity workforce-strategie op.
• Haal digitale geletterdheid uit het totaal van de curriculum-herziening.
• Zet een stimuleringsprogramma cybersecurity voor docenten.
• Zet '*life long learning*' pro-gramma's op voor cybersecurity-talent en -professionals.

De investeringen die nodig zijn om deze adviezen te realiseren zijn hieronder samengevat. Deze investeringen zijn aanvullend op huidige (structurele) investeringen in cyberweerbaarheid.

Speerpunt	Structurele investering (afgerond, per jaar)	Eenmalige investering (afgerond, 2021-2024)
Regie op samenwerking en informatiedeling	€ 24 miljoen	-
Weerbare vitale processen	€ 19 miljoen	€ 155 miljoen
Versterking onderzoek en onderwijs	€ 35 miljoen	€ 47 miljoen
Realiseren van cybercrime handhavingsketen	€ 108 miljoen	€ 30 miljoen
Zorgplicht van leveranciers voor veilige producten en diensten voor burgers, bedrijfsleven en overheid	€ 8 miljoen	€ 6 miljoen
Totaal	**€ 194 miljoen per jaar**	**€ 238 miljoen**
Totale investeringen komende kabinetsperiode (2021-2024)[12]	**€ 833 miljoen**	

De totaal benodigde minimale investeringen van de vijf speerpunten komen uit op minimaal € 833 miljoen voor de aankomende kabinetsperiode. Deze investeringen moeten *bovenop* de huidige structurele investeringen in cyberweerbaarheid worden gedaan. Dit betreft een kostenindicatie. Er zijn noodzakelijkerwijs aannames gedaan die vooruitlopen op de adviezen, waarbij andere realisaties van de adviezen ook mogelijk zijn.

Voor dit onderzoek is gekeken naar de volledige keten van organisaties en activiteiten die bijdragen aan de cyberweerbaarheid van Nederland. Binnen deze keten heeft de raad vijf speerpunten vastgesteld. Voor dit rapport ligt de focus binnen de handhavingsketen op het tegengaan van cybercrime. Dat wil niet zeggen dat investeringen in de versterking van andere domeinen niet nodig of belangrijk zijn. Voorbeelden hiervan zijn investeringen specifiek gericht op het tegengaan van statelijke dreigingen, offensieve en defensieve cybercapaciteiten binnen Defensie en cyberdiplomatie. Investeringen buiten deze vijf speerpunten zijn geen onderdeel van dit advies maar dienen uitdrukkelijk wel in ogenschouw genomen te worden. Daarmee is de verwachting dat de totale benodigde investeringen in cyberweerbaarheid hoger zijn dan in dit rapport worden beschreven.

Uniciteit van het advies

Nog niet eerder is in Nederland op zo'n integrale manier onderzoek gedaan naar benodigde verbeteringen en investeringen in cyberweerbaarheid. Het onderzoek heeft focus gelegd op de vijf meest urgente speerpunten. Door haar unieke samenstelling met raadsleden uit de overheid, het bedrijfsleven en de wetenschap, is de raad bij uitstek in staat om te borgen dat het advies in afstemming is met de wensen en benodigdheden van deze drie domeinen. Daarnaast heeft de raad zich bij het uitvoeren van dit onderzoek en het opstellen van adviesrapport laten ondersteunen door (onafhankelijke) onderzoekers en cybersecurity-experts van Deloitte. Dit team heeft gedurende een half jaar diepgaand (internationaal) onderzoek gedaan naar de huidige staat van cyberweerbaarheid (en investeringen) in Nederland en deze vergeleken met landen om ons heen. De raad bouwt met de adviezen voort op deze onderzoeken en heeft het Deloitte-team vervolgens gevraagd om de adviezen door te rekenen. Het resultaat is een gedegen, onafhankelijk en toepasbaar advies om Nederland structureel cyberweerbaar te maken.

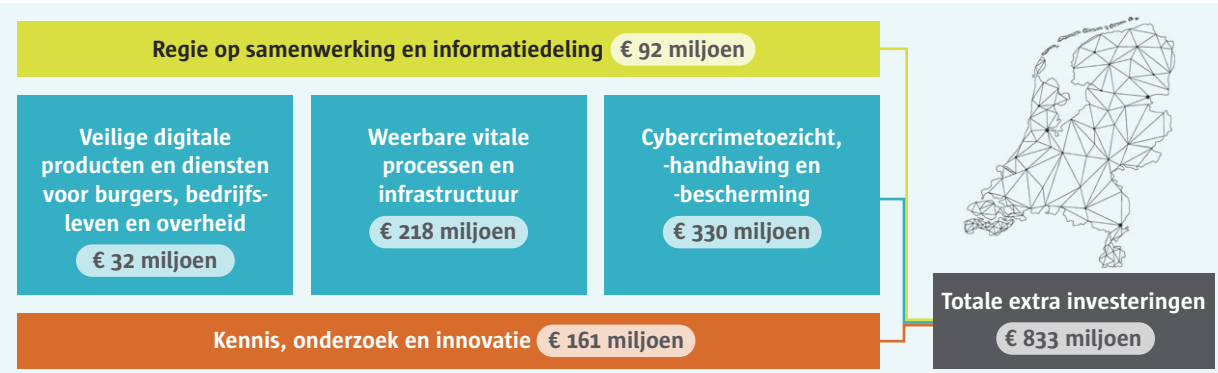
Het rapport is zo geschreven dat de volgende regering concrete handvatten krijgt om de adviezen uit te voeren. Per speerpunt is aangegeven wie de belangrijkste stakeholders zijn, op welke initiatieven voortgebouwd kan worden en welke (structurele) investeringen er ieder jaar nodig zijn in de komende vier jaar.

12 Om tot een totaal van de kosten over de regeerperiode te komen, is rekening gehouden met hoe structurele kosten zich over de vier jaar zullen ontwikkelen. Details hierover zijn opgenomen in de detailbudgetten bij elk speerpunt in dit rapport.

Tot slot

Bovenstaande zaken zijn niet nieuw. De raad en andere organen hebben de afgelopen jaren meerdere adviezen opgesteld waarin deze en andere knelpunten en benodigde maatregelen worden beschreven. Deze adviezen zijn soms niet of slechts ten dele uitgevoerd. Nederland moet een veilige, open en welvarende samenleving blijven en afgewogen keuzes kunnen maken ten behoeve van haar eigen (Europese) digitale autonomie. Digitalisering biedt veel economische en maatschappelijke kansen die alleen kunnen worden verzilverd als Nederland digitaal weerbaar is. Het is van belang om de cyberweerbaarheidsketen integraal te versterken. Om dit te realiseren zal er in samenhang in de navolgende speerpunten moeten worden geïnvesteerd. Publiek-private samenwerking is daarbij randvoorwaardelijk voor een effectieve aanpak, aangezien de schaarse kennis en expertise over vele partijen verspreid zijn. Publiek, privaat en wetenschap hebben elkaar nodig om tot oplossingen te komen.

Figuur 3 **Benodigde extra investeringen in de Nederlandse cyberweerbaarheidsketen 2021-2024**



Verbeteren van regie op samenwerking en informatiedeling

Realiseer een effectieve vorm van regie op samenwerking, inclusief één nationale cyberweerbaarheidsstrategie
€ 10 miljoen

Verbeter informatiedelingscapaciteiten om beter te kunnen reageren op (acute) cyberdreigingen
€ 82 miljoen

Veilige digitale producten en diensten voor burgers, bedrijfsleven en overheid

Zorgplicht voor veilige hard- en software om burgers en bedrijven te beschermen tegen cybercrime
€ 25 miljoen

Ondersteun burgers en mkb bij cyberveilig gedrag om bewustzijn en handelingsbekwaamheid te vergroten
€ 7 miljoen

Verbeteren van de weerbaarheid van vitale processen en infrastructuur

Cyberweerbaarheidsfonds voor vitale aanbieders om versterking gelijke tred te laten houden met toenemende dreigingen
€ 150 miljoen

Versterken van toezicht om weerbaarheid van vitale processen beter te controleren en waar nodig bij te sturen
€ 68 miljoen

Realiseren van een sterkere cybercrime-handhavingsketen

Inzichtelijker maken van cybercrime om de handhavingsketen (kosten)effectiever in te richten
€ 14 miljoen

Structureel investeren in de bestrijding van cybercrime om de maatschappelijke impact te verkleinen en vertrouwen van burgers te versterken
€ 316 miljoen

Versterken van kennis, onderzoek en innovatie

Stimuleren van onderzoek en innovatie om hoogwaardige cyberweerbaarheid-diensten en -producten te ontwikkelen
€ 48 miljoen

Investeren in wetenschappelijk onderzoek om deze in Nederland te verbeteren en 'cyber-braindrain' tegen te gaan
€ 81 miljoen

Zorgdragen voor Voldoende gekwalificeerde cyberweerbaarheidsspecialisten voor de Nederlandse overheid en bedrijfsleven
€ 32 miljoen

Foto: Jeroen de Bakker

INTRODUCTIE

Achtergrond en aanpak

De raad heeft zich ten doel gesteld om na de Tweede Kamerverkiezingen van maart 2021 te komen met een advies voor de integrale aanpak voor de cyberweerbaarheid van Nederland. In 2020 heeft de raad in een urgentieverklaring aangegeven dat om de cyberweerbaarheid van ons land te verhogen regie op samenwerking, meerjarenprogrammering en een dekkende financiering noodzakelijk zijn. Ook ontbreekt het in de huidige aanpak aan voldoende aandacht voor digitale autonomie. Digitale autonomie raakt het hart van onze rechtsstaat en samenleving, daarom benadert de raad in dit advies cyberweerbaarheid vanuit het soevereiniteitsperspectief. Aanleiding voor dit advies is het verzoek van de minister van Justitie en Veiligheid om advies te geven over de benodigde investeringen in cyberweerbaarheid door het nieuwe kabinet.

Met ondersteuning van Deloitte heeft de raad onderzoek uitgevoerd naar de huidige staat van de Nederlandse cyberweerbaarheid om hierover aan het nieuwe kabinet een gedegen en integraal advies te kunnen geven. Dit rapport bevat de uitkomsten van het uitgevoerde onderzoek en de adviezen die de raad op basis daarvan aan het kabinet doet. Voor alle adviezen is een inschatting gemaakt van de kosten die komen kijken bij het uitvoeren van elk advies, zodat de volgende regering deze kan opnemen in het regeerakkoord en de begroting.

Op basis van eerder uitgebrachte rapporten van diverse instanties, input vanuit alle raadsleden en inzicht van het onderzoeksteam in de Nederlandse cyberweerbaarheid is inzichtelijk gemaakt op welke terreinen in Nederland momenteel wordt gewerkt aan het verbeteren van deze weerbaarheid. Daarbij is ook een vergelijking gemaakt tussen de investeringen in Nederland op dit terrein over de afgelopen vier jaar, en die in een aantal met Nederland vergelijkbare landen. Deze inzichten zijn met de raad afgestemd, waarna een vijftal speerpunten adviezen zijn geformuleerd. Elk advies is tenslotte nader uitgewerkt om te bepalen wat de benodigde acties zijn en welke kosten daarmee (naar schatting) gemoeid zijn. Bovendien is een analyse uitgevoerd om vast te stellen wat de te verwachten baten van elk advies zijn. De resultaten van het bovenstaande zijn gebundeld in dit adviesrapport.

Scope van het onderzoek

Voor dit onderzoek is gekeken naar de volledige keten van organisaties en activiteiten die bijdragen aan de cyberweerbaarheid van Nederland, zoals in de introductie is beschreven. Binnen deze keten heeft de raad vijf speerpunten vastgesteld. Voor dit rapport ligt de focus binnen de handhavingsketen op het tegengaan van cybercrime. Dat wil niet zeggen dat investeringen in de versterking van andere domeinen niet nodig of belangrijk zijn. Voorbeelden hiervan zijn investeringen specifiek gericht op het tegengaan van statelijke dreigingen, offensieve cybercapaciteiten binnen Defensie en cyberdiplomatie. Investeringen buiten deze vijf speerpunten zijn geen onderdeel van dit advies maar dienen uitdrukkelijk wel in ogenschouw genomen te worden. Daarmee is de verwachting dat de totale benodigde investeringen in cyberweerbaarheid hoger zijn dan in dit rapport worden beschreven.

De informatiebeveiliging van (IT-)middelen van overheidsorganisaties zelf vallen niet direct binnen de scope van dit onderzoek. Benodigde investeringen om deze informatiebeveiliging te verbeteren, zijn dus ook niet opgenomen in dit rapport. Deze investeringen vallen onder de bedrijfsvoering van overheidsorganisaties. Benodigde investeringen worden daarom via de reguliere begroting van deze organisaties geborgd. Aanbevelingen met betrekking tot het versterken van de weerbaarheid van vitale processen en het invoeren zorgplicht kunnen wel een indirect effect hebben.

Permanente cyberdreigingen

Om de weerbaarheid te kunnen vergroten, moet deze in samenhang worden bezien met de dreiging en de te beschermen belangen. Cyberdreigingen voor de Nederlandse samenleving zijn permanent aanwezig. In het Cybersecuritybeeld Nederland (CSBN) 2020, gepubliceerd door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), wordt geconcludeerd dat net als in 2019 de digitale dreiging een permanent karakter heeft en dat cyberincidenten kunnen leiden tot maatschappij-ontwrichtende schade. Recente criminele cyberaanvallen en uitval van systemen hebben duidelijke maatschappelijke gevolgen gehad voor de overheid, het bedrijfsleven en burgers.[13] Naast het CSBN 2020 hebben de NCTV, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) recent het Dreigingsbeeld Statelijke Actoren 2020[14] gepubliceerd. Hierin wordt geconcludeerd dat de verschillende nationale veiligheidsbelangen kwetsbaar zijn en door statelijke actoren substantieel bedreigd en aangetast worden. Ook is er sprake van economische spionageactiviteiten, die met name zijn gericht op Nederlandse topsectoren en kennisinstellingen. Economische activiteiten zoals investeringen in en samenwerking bij de ontwikkeling van sensitieve technologieën vormen een dreiging, omdat kennis- en technologieoverdracht die vanuit het oogpunt van nationale veiligheid ongewenst is kan plaatsvinden en omdat (ongewenste) strategische afhankelijkheid kan ontstaan. Wanneer er in dit rapport gesproken wordt over weerbaarheid tegen cyberdreigingen, dan wordt hierbij gerefereerd naar alle dreigingen die in deze beide rapporten worden genoemd.

13 Nationaal Coördinator Terrorismebestrijding en Veiligheid, Cybersecuritybeeld Nederland 2020.

14 Algemene Inlichtingen- en Veiligheidsdienst, Militaire Inlichtingen- en Veiligheidsdienst en Nationaal Coördinator Terrorismebestrijding en Veiligheid, Dreigingsbeeld Statelijke Actoren 2020

Structuur van het rapport

In dit adviesrapport worden vijf investeringsspeerpunten beschreven voor het volgende kabinet. Voor ieder speerpunt wordt de onderstaande structuur aangehouden bij de beschrijving:

1. **Introductie van het speerpunt en beschrijving van huidige stand van zaken**
   Per speerpunt wordt beschreven wat de huidige stand van zaken is. Dit wordt gedaan door huidige initiatieven en behaalde resultaten binnen de context van ieder speerpunt te beschrijven.

2. **Adviezen**
   Vervolgens wordt beschreven welke maatregelen aanvullend op de huidige stand van zaken wordt geadviseerd. Dit aanvullende advies wordt beschreven op basis van eerder uitgebrachte adviesbrieven van de raad en additionele adviezen die de leden en het onderzoeksteam van Deloitte hebben geformuleerd tijdens het 'Onderzoek investeringen cyberweerbaarheid'.

3. **Verwachte baten en kosten van het aanvullende advies**
   Voor dit aanvullende advies worden vervolgens de verwachte baten en kosten beschreven. De kosten worden geraamd op basis van vergelijkbare cybermaatregelen in de twaalf benchmarklanden[15] (bijvoorbeeld het opzetten van een onderzoek-ecosysteem) of voorbeelden van vergelijkbare niet-cybermaatregelen in Nederland (bijvoorbeeld investeringen in deltawerken).

Vasstellen van benodigde investeringen

Om vast te stellen wat de benodigde investeringen per speerpunt zijn, is op basis van de adviezen die de raad bij elk speerpunt heeft gegeven, een inschatting gemaakt van de kosten. Omdat de adviezen aan de nieuw te vormen regering zijn gericht, zijn de kosten voor de komende vier jaar ingeschat. Uiteraard moeten bij die implementatie in de regel nog diverse keuzes gemaakt worden, die ook invloed kunnen hebben op de daadwerkelijke uitvoeringskosten. Per investering is in dit rapport toegelicht hoe de schatting tot stand is gekomen.

In het rapport wordt onderscheid gemaakt tussen structurele en eenmalige investeringen. Structurele investeringen zijn gedefinieerd als alle jaarlijks terugkerende kosten voor bijvoorbeeld werknemers, een product of een systeem. Voor structurele kosten voor werknemers gaat dit onderzoek uit van € 150.000 euro per persoon per jaar, inclusief facilitaire kosten. Er wordt uitgegaan van de volgende opbouw van deze structurele kosten: 50% in het eerste jaar, 75% in het tweede jaar (vanwege verdere opbouwtijd) en 100% in het derde en vierde jaar. Onder eenmalige investeringen vallen kosten voor ontwikkeling of levering van niet-verbruikbare onderdelen van een product of systeem, zoals investeringsfondsen of bewustwordingscampagnes. Uitgangspunt is dat eenmalige investeringen aan het einde van de kabinetsperiode worden geëvalueerd en opnieuw worden vastgesteld.

15 Zie bijlage 2 voor de uitkomsten van het Integrale Aanpak Cyberweerbaarheid benchmark onderzoek.

Foto: Jeroen de Bakker

SPEERPUNT 1

REGIE OP SAMENWERKING EN INFORMATIEDELING

Introductie en huidige staat

Voor regie op cyberweerbaarheid en informatiedeling wordt in Nederland gebruikgemaakt van een decentraal bestuursmodel. De verantwoordelijkheid voor het versterken van de cyberweerbaarheid is verdeeld over meerdere ministeries, departementen en organisaties[16] (zie ook bijlage 1 voor een overzicht van het cyberweerbaarheid stakeholderveld). De nationale regiefunctie in het cybersecurity-domein wordt niet optimaal uitgevoerd en cyberweerbaarheidsinitiatieven en -investeringen en ook het wettelijke kader worden niet optimaal ingezet. Daarnaast is een toegewijde cyber-informatiedelingscapaciteit om structureel relevante (dreigings-) informatie[17] te kunnen genereren en te delen met belanghebbende Nederlandse organisaties een belangrijk onderdeel van dit speerpunt. De informatie-uitwisseling moet snel worden verbeterd voor bijvoorbeeld de informatiepositie van een groot deel van het (non-vitale) Nederlandse bedrijfsleven en inzicht in de patronen in cyberaanvallen en cybercrime. De volgende paragrafen zetten uiteen welke acties al binnen dit domein zijn ondernomen.

Gemeenschappelijke koers op het gebied van cyberweerbaarheid

Cybersecurity is voor het huidige kabinet een topprioriteit[18] waarbij onder andere afgesproken is de integrale publiek-private aanpak van cybersecurity te gaan versterken door structurele en adaptieve risicobeheersing in te zetten[19]. Ondanks deze belofte en lopende initiatieven is door onvoldoende daadwerkelijke politieke aandacht de regie op samenwerking en informatiedeling op het gebied van cybersecurity nog niet op het noodzakelijke niveau. Dit wordt versterkt door toenemende dreigingen, waardoor deze regie op samenwerking en informatiedeling nog sneller tot stand moet komen.

De Nederlandse Cybersecurity Agenda (NCSA) wordt momenteel geëvalueerd op basis van volledigheid, realisatie en impact op de Nederlandse cyberweerbaarheid[20]. Er zijn naast de NCSA meerdere cybersecurity en cybercrime (deel)strategieën opgesteld door de Rijksoverheid en decentrale overheden die decentraal worden uitgevoerd. Er is nog onvoldoende een gemeenschappelijke visie en koers die onderling tussen de diverse stakeholders goed afgestemd en gedragen is. Zo ontbreken meetbare doelstellingen en resultaten, worden taken en verantwoordelijkheden om maatregelen te realiseren onvoldoende belegd, en wordt niet aangegeven hoe de investeringen moeten worden ingezet. Voorafgaand aan de NCSA is geen nulmeting uitgevoerd waardoor het lastig is om vast te stellen of investeringen daadwerkelijk verandering tot gevolg hebben.

16 Cybersecurity A State-of-the-art Review: Phase 2 Final report, WODC (2020)
17 Bijvoorbeeld: Indicators of Compromise, kwetsbaarheden, etc.
18 Nederlandse Cybersecurity Agenda, Ministerie van Justitie en Veiligheid (2018)
29 Voortgang Nederlandse Cybersecurity Agenda, Ministerie van Justitie en Veiligheid (2019)
20 De evaluatie wordt uitgevoerd door Dialogic in opdracht van het WODC.
Bron: https://www.dialogic.nl/2020/10/28/evaluatie-nederlandse-cybersecurity-agenda/

Tot slot besteed de NCSA onvoldoende aandacht aan het behouden van zeggenschap over de toekomst van de Nederlandse economie, maatschappij en democratie waar die toenemend bedreigd worden door gebrek aan cyberweerbaarheid (d.i., digitale strategische autonomie en cybersecurity)[21]. Dit leidt tot het ontbreken van de (mogelijkheid van) centrale regie op prioriteitsstellingen en investeringen in cyberweerbaarheid.

De in 2018 opgerichte Cybersecurity Alliantie (CSA) draagt bij aan de realisatie van de NCSA-doelstellingen met het opleveren van kortlopende concrete projecten[22]. Deze projecten worden vrijwillig door partijen uit de private-en publieke sector co-gefinancierd en uitgevoerd. De CSA is een goed voorbeeld van publiek-private samenwerking maar beschikt in de praktijk niet altijd over voldoende capaciteiten en financiering om intensief bij te kunnen dragen aan de realisatie van doelstellingen. De scope van de CSA is voornamelijk gericht op het cybersecurity-domein, waardoor er bijvoorbeeld niet wordt gewerkt aan het versterken van handhaving en opsporing vanuit een cybersecurity oogpunt.

Er is een digitale crisisstructuur ingericht onder regie van de NCTV[23], en er worden ISIDOOR-oefeningen uitgevoerd waaraan publieke en private partners de gezamenlijke aanpak, coördinatie, en samenwerking bij een cybercrisis testen[24]. De keerzijde van de ISIDOOR-oefening is dat de frequentie laag is (uitgevoerd in 2015 en 2017) en dat enkel de overheid en partijen uit de vitale infrastructuur hier onderdeel van uitmaken.

Informatiedelingscapaciteiten

Een van de belangrijkste instrumenten om de cyberweerbaarheid van organisaties en burgers te verhogen, is hen snel te informeren wanneer hun IT-systemen kwetsbaarheden vertonen of gehackt zijn. In het voorzien van deze informatie spelen de inlichtingendiensten, politie, OM en het NCSC een belangrijke rol. Zonder sterke inlichtingenpositie zijn de Nederlandse overheid, het bedrijfsleven en burgers onmogelijk in staat om zich tijdig te weren tegen cyberdreigingen. Momenteel wordt onder coördinatie van het ministerie van Justitie en Veiligheid (JenV) gewerkt aan het verwezenlijken van het Landelijk Dekkend Stelsel van informatieknooppunten[25]. Als onderdeel hiervan is het bestaande stelsel van samenwerkingsverbanden deels versterkt en uitgebreid (waaronder de capaciteit van het NCSC)[26] en zijn het Nationaal Detectie Netwerk (NDN) en het Digital Trust Center (DTC) hierbij aangesloten. Het stelsel is echter nog steeds niet volledig dekkend: dreigingsinformatie wordt nog onvoldoende snel en gericht gedeeld waardoor organisaties binnen de overheid en het bedrijfsleven niet alle relevante informatie tot hun beschikking hebben om (geavanceerde) cyberdreigingen te weren. Een voorbeeld hiervan is dat het NCSC op dit moment geen incidentinformatie deelt met de belangrijkste schakelorganisaties waardoor kritieke incidentinformatie de getroffen bedrijven en burgers[27] niet bereikt. Dit komt voornamelijk door de juridische beperkingen die (te) veel tijd vragen om te worden geïdentificeerd en opgelost. Het tempo waarin organisaties als Objectief Kenbaar Tot Taak (OKTT) (kunnen) worden aangewezen is te laag[28]; momenteel zijn nog slechts vier organisaties als OKTT aangewezen[29].

21 Onderzoeksrapport 'Nederlandse strategische autonomie en cybersecurity', Paul Timmers en Freddy Dezeure, januari 2021 (een onderzoek uitgevoerd in opdracht van de Cyber Security Raad). In de NCSA wordt digitale autonomie maar twee keer zijdelings genoemd.

22 https://ecp.nl/project/cybersecurity-alliantie/

23 Als onderdeel hiervan bestaat het Interdepartementaal Afstemmingsoverleg (IAO) dat de link verzorgt tussen o.a. het OM, het NCC en Departementale Coördinatiecentra (DCC's), die op hun beurt communicatie onderhouden met NCSC, Rijksdiensten en vitale aanbieders.

24 Nationaal Coördinator Terrorismebestrijding en Veiligheid Pieter-Jaap Aalbersberg: 'Oefenen, oefenen en nog eens oefenen!' – Waterspiegel, Vereniging van Exploitanten van Waterleidingbedrijven in Nederland (2020)

25 De Cyber Security Raad heeft hier in 2017 een advies over uitgebracht: CSR Advies 'Naar een landelijk dekkend stelsel van informatieknooppunten, advies inzake informatie-uitwisseling met betrekking tot cybersecurity en cybercrime', CSR Advies 2017, nr. 2.

26 Voortgang Nederlandse Cybersecurity Agenda, Ministerie van Justitie en Veiligheid (2019). Tevens is een voorbeeld van een samenwerkingsverband tussen private en publieke sector Brainport Eindhoven: dit is een innovatie ecosysteem waarin informatie met betrekking tot sleuteltechnologieën wordt uitgewisseld.

27 Burgers krijgen een melding van hun internetaanbieder als een van hun apparaten is geïnfecteerd. Internetaanbieders verzorgen deze melding op basis van informatie die met hen gedeeld wordt over IP-adressen in hun netwerk waarop geïnfecteerde apparaten zijn gesignaleerd. Voor veel internetaanbieders loopt het ontvangen van deze informatie via AbuseHub, de 'abuse information exchange' die is opgericht door aanbieders om hun gebruikers te kunnen informeren en beschermen.

28 Daarbij moet de kanttekening worden gemaakt dat organisaties niet altijd (al) geschikt zijn om OKTT te worden. Zo moet er veel geregeld worden, zoals privacy beleid en rechtspersoonlijkheid.

29 De NBIP (Nationale Beheersorganisatie Internet Providers), het Cyberweerbaarheidscentrum Brainport, de Abuse Information Exchange (AbuseHub), en Cyberveilig Nederland. Bronnen: Informatie-uitwisseling landelijk dekkend stelsel cybersecurity – eindrapport, WODC (2020) en https://cyberveilignederland.nl/cyberveilig-nederland-aangewezen-als-oktt-door-ncsc-en-nctv/

Ten slotte wordt het belang van Information Sharing and Analysis Centres (ISAC's) steeds breder erkend en zijn voor de meeste grote sectoren inmiddels ISAC's opgericht[30]. Het NCSC stimuleert vitale sectoren ISAC's op te stellen en biedt hiervoor onder andere in samenwerking met TNO een ontwikkelmodel en praktische inrichtingstips[31].

Er is voor alle vitale sectoren een platform beschikbaar waar informatie kan worden uitgewisseld[32], alhoewel de inrichting en volwassenheid van deze ISAC's vrijblijvend is en per sector verschilt. Daarnaast wordt er nog beperkt gewerkt aan de opbouw van ISAC's buiten vitale sectoren om, zoals in de topsectoren[33], terwijl deze interessante, en soms kwetsbare, doelwitten voor o.a. statelijke actoren kunnen zijn.

Standpunten en eerdere adviezen van de raad

De raad is van mening dat een integrale aanpak van onze cyberweerbaarheid hoge prioriteit moet krijgen. Regie op samenwerking, meerjarenprogrammering en dekkende financiering zijn noodzakelijk om de cyberweerbaarheid in ons land structureel op het gewenste niveau te houden. Om binnen het cybersecurityweerbaarheid domein de nationale regiefunctie optimaal uit te kunnen voeren en over de verschillende beleidsterreinen prioriteiten in de uitvoering te kunnen stellen, moet een effectieve vorm van regie op samenwerking worden ontwikkeld. Daarvoor is het ook noodzakelijk duidelijkheid te creëren in de rollen en verantwoordelijkheden, en het afstemmen van werkgebieden en mandaten binnen de overheid. Dit draagt bij aan een optimale nationale regiefunctie op het gebied van cyberweerbaarheid. De raad is van mening dat ook meer in het algemeen (overheids-)partijen tijdens cyberincidenten in voldoende mate bijeen moeten worden gebracht, zodat gezamenlijk de nodige acties en maatregelen kunnen worden genomen. Snel betrouwbare en begrijpelijke informatie delen vormt het fundament van onze cyberweerbaarheid. Aandacht moet daarbij ook uitgaan naar operationele technologie (OT); OT wordt onder andere gebruikt voor besturing van (fysieke) meet- en regelsystemen, zoals in de drinkwatersector, transport en energie die een essentiële rol spelen in de veiligheid van onze vitale infrastructuur.

Aanvullende adviezen van de raad

Ontwikkel een gedragen nationale cyberweerbaarheidsstrategie

Ontwikkel een gedragen nationale cyberweerbaarheidsstrategie en meerjarenprogramma waarin nationale ambities, integrale prioriteiten, uitvoeringsinitiatieven en inzet van investeringen worden vastgelegd. Waarborg dat deze nationale strategie wordt opgesteld in samenwerking en samenspraak met de voornaamste belanghebbenden binnen de overheid en dat hierbij ook afstemming wordt gezocht met het bedrijfsleven en de wetenschap. Een belangrijk fundament voor de nationale cyberweerbaarheidsstrategie is de dreigingsinformatie die wordt verzameld door de verschillende organisaties binnen de overheid (bijvoorbeeld vanuit de NCTV, NCSC, AIVD, MIVD, politie en OM) en (waar mogelijk) het bedrijfsleven (bijvoorbeeld het Anti-Abuse Netwerk). Ook moet bijzondere aandacht worden besteed aan de wijze waarop deze strategie aansluit bij relevante nationale strategieën zoals de Nederlandse Digitaliseringsstrategie en relevante internationale strategieën zoals de recent gepubliceerde cybersecurity-strategie van de Europese Commissie[34], en Nederlandse ambities op bijvoorbeeld het vlak van digitale autonomie. Daarnaast moet aandacht besteed worden aan de samenwerking tussen de rijksoverheid, lokale overheden, het bedrijfsleven en de wetenschap. In deze samenwerking moet bijvoorbeeld gekeken worden naar welke private initiatieven gestimuleerd kunnen worden vanuit de overheid. Denk verder bijvoorbeeld ook aan het vaststellen van een acceptabele frequentie van de voorgenoemde ISIDOOR-oefeningen om de gezamenlijke aanpak, coördinatie, en samenwerking bij een cybercrisis-testen. Zorg voor voldoende capaciteit om deze strategie op te stellen, te onderhouden en voortgang op de gestelde doelen te bewaken.

30 Een nooit gelopen race, Rathenau Instituut (2017)

31 Samenwerking in een ISAC, Nationaal Cyber Security Centrum (2020)

32 Er wordt ook op Europees niveau geïnvesteerd in de inrichting van ISAC's. Zo wordt er gewerkt aan ISAC's in kritische sectoren als de zorg en de maritieme en watersector. Nederland heeft hierin een leidende rol met een combinatie van publieke en private partijen. Bron: ENISA kiest Capgemini Invent en TNO voor ISAC-uitbreiding, Consultancy.nl (https://www.consultancy.nl/nieuws/27766/enisa-kiest-capgemini-invent-en-tno-voor-isac-uitbreiding), 2020

33 Topsectoren, hoe en waarom?, Topsectoren (2015)

34 The EU's Cybersecurity Strategy for the Digital Decade, European Commission, 2020

Het voeren van een nationale cyberweerbaarheidsstrategie draagt bij aan gecentraliseerde prioriteitsstellingen en verdelingen van investeringen in cyberweerbaarheid. Dit stelt de overheid in staat om beter toekomstgericht te werk te gaan en adequaat te reageren op nieuwe bedreigingen en kansen (bijvoorbeeld voortkomend uit het gebruik van nieuwe technologie en in de context van digitale autonomie). Naast het opstellen van deze strategie, dient er ook capaciteit te zijn om de uitvoering en voortgang van prioriteiten te bewaken.

Realiseer een effectieve vorm van regie op samenwerking

Om de cyberweerbaarheid integraal te verbeteren is het noodzakelijk om een betere regie op samenwerking te voeren. Regie op samenwerking tussen overheid, bedrijfsleven en wetenschap draagt zorg voor het harmoniseren van (nationale) cyberweerbaarheidsinitiatieven en -investeringen, en vergroot daarmee de effectiviteit, samenhang en slagkracht van deze initiatieven. Publiek-private samenwerking is daarbij randvoorwaardelijk voor een effectieve aanpak, aangezien de schaarse kennis en expertise over vele partijen verspreid zijn. Publiek, privaat en wetenschap hebben elkaar nodig om tot oplossingen te komen. De regievorm moet voldoende slagkracht en mandaat hebben om de nationale regiefunctie uit te voeren en over de verschillende beleidsterreinen prioriteiten in de uitvoering te kunnen stellen. Het moet uitgaan van een gedragen nationaal besturingsmodel voor cyberweerbaarheid waarin werkgebieden en mandaten binnen overheid zijn afgestemd, zonder overlap en hiaten. Vanuit deze regie kan ook de eerdergenoemde nationale cyberweerbaarheid strategie en uitvoeringsagenda worden opgesteld, waarmee de Nederlandse cyberweerbaarheidsambitie wordt gesteld en integrale prioriteiten, uitvoeringsinitiatieven en investeringen welke nodig zijn om de ambitie te realiseren worden vormgegeven. Door centrale prioriteitstelling komen de investeringen in cyberweerbaarheid daarmee per definitie tot een hoger rendement. Een belangrijk uitgangspunt hierbij is dat de regievoering primair faciliterend moet zijn aan de uitvoering, bijvoorbeeld door samenwerking te faciliteren waardoor meer bereikt kan worden tegen dezelfde investeringen dan wanneer stakeholders individueel te werk gaan. Belanghebbenden in het cyberweerbaarheidsdomein, zoals ministeries, voeren vanuit de eigen expertise en wettelijke mandaten regie over initiatieven en investeringen binnen het eigen domein, maar doen dit wel binnen de kaders en prioriteiten die gesteld zijn op nationaal niveau.

De regie moet er bovendien voor zorgen dat concrete en realistische doelen voor digitale autonomie bereikt worden met samenhangende maatregelen[35]. Op de lange termijn resulteert dit in een proactieve aanpak om bedreigingen van digitale autonomie te anticiperen of tijdig af te weren. Dit vergt dat verschillende beleidsterreinen en belangen hecht met elkaar worden verbonden, met sturing vanaf het *hoogste niveau* (*Whole-of-Government*). Cybersecurity vanuit soevereiniteitsperspectief dient dus *chefsache* te zijn. De voorgestelde regie op samenwerking kan meerdere actuele thema's met urgentie oppakken om de Nederlandse strategische autonomie in verband met cybersecurity te versterken. Zonder digitale strategische autonomie kunnen we geen zeggenschap houden over toekomst in economie, maatschappij en democratie. Het CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity', dat parallel aan dit adviesrapport is ontwikkeld, benoemt de concrete stappen om te komen tot een integrale aanpak van digitale autonomie waar cyberweerbaarheid in het geding is.

Strategische regie en samenwerking: oprichting van interdepartementale strategische overlegkoepel

Cyberweerbaarheid is chefsache, er dient daarom op het juiste niveau richting aan gegeven te worden. Daartoe dient er in het nieuwe kabinet een ministeriële onderraad digitale zaken te worden ingesteld, waar cyberweerbaarheid integraal aan de orde wordt gesteld. De ambtelijke ondersteuning vindt plaats via de instelling van een op te richten interdepartementaal strategische overlegkoepel cyberweerbaarheid. Richt deze koepel op vanuit een 'whole of government' aanpak, met afgevaardigden van de ministeries, in structurele afstemming met decentrale overheden. Door deze koepel moet met hoge prioriteit op korte termijn één nationale cyberweerbaarheid strategie worden opgesteld. In deze strategie worden prioriteiten gesteld in de uitvoering en financiering de strategie, als kader voor cyberweerbaarheidsplannen. Hierbij wordt structureel samengewerkt en afgestemd met (vertegenwoordigers uit) het bedrijfsleven en de wetenschap vanuit de 'triple helix' gedachte. De overlegkoepel rapporteert naar de nieuw in te stellen ministeriele onderraad Digitale Zaken over de voortgang op de nationale cyberweerbaarheidsstrategie. Uitvoerende organisaties behouden hun eigen mandaat en verantwoordelijkheden.

35 Privacybeschermende Cloud wordt hier als voorbeeld gebruikt. Andere voorbeelden zijn landsbrede veilige digitale communicatie en robuuste en langdurige encryptie en vertrouwensdiensten, zie ook: Onderzoeksrapport 'Nederlandse strategische autonomie en cybersecurity', Paul Timmers en Freddy Dezeure, januari 2021 (een onderzoek uitgevoerd in opdracht van de Cyber Security Raad).

Verder verkennen van structurele strategische regie en operationele samenwerking

Daarmee zijn we er nog niet. Het oprichten van de strategische overlegkoepel is op korte termijn een eerste goede stap naar betere regie op samenwerking. Zo snel mogelijk dient echter ook uitgewerkt te worden hoe overheid, wetenschap en bedrijfsleven ook op tactisch en operationeel niveau kunnen samenwerken en hoe zij allen structureel kunnen bijdragen aan de nationale cyberweerbaarheidsstrategie. De raad benadrukt daarom met klem dat naast de instelling van de overlegkoepel direct ook een verkenning moet worden uitgevoerd naar de beste inrichting voor die samenwerking.

Verbeter informatiedelingscapaciteiten en ondersteuning

Om de informatiedelingscapaciteiten rondom cyberweerbaarheid in Nederland te verbeteren, is het noodzakelijk om op korte termijn voor een landelijk dekkend stelsel van informatieknooppunten (LDS) te zorgen, zodat alle Nederlandse bedrijven en organisaties over de benodigde informatie kunnen beschikken[36]. Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) heeft uitgebreid onderzoek gedaan naar het LDS en de verschillende aanbevelingen in het eindrapport *'Informatie-uitwisseling landelijk dekkend stelsel cybersecurity'* gepubliceerd[37]. Een van deze aanbevelingen is om de NCSC-restinformatie[38] via het DTC te laten delen met niet-vitale organisaties en samenwerkingsverbanden. Om dit te kunnen realiseren is het nodig dat het DTC de OKTT-status verkrijgt[39] en dat het DTC en de samenwerking tussen het DTC en het bedrijfsleven verder wordt versterkt. Ook is het van belang dat deze aanbevelingen worden opgevolgd om het stelsel te realiseren. Via dit stelsel kan ook dreigingsinformatie worden gedeeld, bijvoorbeeld voortkomend uit analyses van de AIVD en MIVD. Dit geeft organisaties een beter inzicht in de maatregelen die genomen kunnen worden. Ondersteun de opbouw van ISAC's buiten vitale sectoren om (zoals in topsectoren, vanwege het belang en het hoge dreigingsprofiel van deze sectoren) en maak deze ISAC's onderdeel van het LDS. Sluit ook het virtueel steunpunt OT aan, welke wordt beschreven in het volgende speerpunt.

Daarnaast adviseert de raad om op korte termijn een structurele (juridische) oplossing te vinden voor juridische obstakels met betrekking tot het delen van dreigingsinformatie[40]. Huidige juridische beperkingen op het delen van herleidbare vertrouwelijke informatie en persoonsgegevens (zoals de AVG en huidige wet politiegegevens) staan het structureel delen van dreigingsinformatie met publieke en private partijen in de weg.

Toetsingskader digitale autonomie

De bewustwording van het belang van strategische autonomie in cybersecurity dient op alle relevante niveaus van de Nederlandse overheid, politiek, bedrijfsleven en academica te worden verhoogd. In het parallel ontwikkelde CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity' wordt geadviseerd om een toetsingskader digitale autonomie cybersecurity te implementeren, een toetsingskader dat wordt voorgesteld in het rapport.[41] Het voorgestelde toetsingskader stelt gebruikers in staat om te beoordelen of de overheid moet interveniëren om de Nederlandse strategische autonomie te versterken, en op welke manier dit moet worden gerealiseerd. De raad zal een voorstel voor een 'Handreiking toepassing toetsingskader digitale autonomie' beschikbaar maken.

36 Zij bijlage 2 voor buitenslandse voorbeelden informatiedelingscapaciteiten

37 Informatie-uitwisseling landelijk dekkend stelsel cybersecurity – eindrapport, Dialogic Innovatie en Interactie, Eindhoven University of Technology, WODC (2020).

38 Het NCSC heeft niet de taak om informatie te zoeken buiten zijn primaire doelgroep: Rijksoverheid en vitaal. Met 'restinformatie' wordt gedoeld op informatie die het NCSC uit hoofde van onderzoek ten behoeve van die doelgroep in zijn bezit heeft, maar die relevant is voor niet-vitale partijen.

39 OKTT staat voor een organisatie die 'Objectief Kenbaar Tot Taak' heeft om dreigingsinformatie te delen met het publiek of andere organisaties (Informatie-uitwisseling landelijk dekkend stelsel cybersecurity – eindrapport, Dialogic Innovatie en Interactie, Eindhoven University of Technology, WODC (2020)).

40 Zie CSR Adviesbrief inzake het versneld delen van incidentinformatie, CSR Advies 2021, nr. 2

41 Onderzoeksrapport 'Nederlandse strategische autonomie en cybersecurity', Paul Timmers en Freddy Dezeure, januari 2021 (een onderzoek uitgevoerd in opdracht van de Cyber Security Raad)

Baten van de aanvullende adviezen

Nationale cyberweerbaarheidsstrategie

Het ontwikkelen van een gedragen nationale cyberweerbaarheidsstrategie zorgt voor een betere interdepartementale samenwerking, coördinatie, prioriteitstelling en budgetverdeling op het gebied van cyberweerbaarheid. Dit zal de samenwerking in het hele netwerk van organisaties (zowel publiek, privaat als wetenschap) verbeteren en bijdragen aan het realiseren van een integrale aanpak. Een integrale aanpak vergroot vervolgens de slagkracht en stelt de betrokken partijen in staat om te bepalen welke initiatieven de grootste bijdrage leveren aan de cyberweerbaarheid van Nederland, en welke inzet van middelen op deze initiatieven nodig zijn. Dit leidt daarmee tot de effectievere inzet van middelen, in het bijzonder op weerbaarheidsinitiatieven die individuele organisaties of sectorale ketens overstijgen, en voorkomt daarnaast overlappende initiatieven.

Regie op samenwerking

Het op de lange termijn realiseren van een strategische overlegkoepel cyberweerbaarheid zorgt ervoor dat er gecoördineerd regie wordt gevoerd over alle cyberweerbaarheid-initiatieven. Hierdoor wordt (onder anderen door informatiedeling) de samenhang en samenwerking tussen strategische cyberweerbaarheid-initiatieven versterkt, en worden de afzonderlijke initiatieven en middelen effectiever en beter ingezet. Nederland kan hierdoor gerichter en slagvaardiger te werk gaan om de cyberweerbaarheid doorlopend te verbeteren. Het oprichten van de koepel vraagt bovendien om weinig bestuurlijke verandering ten opzichte van huidige situatie en vergt een relatief kleine investering en ingreep, waarmee het al op korte termijn leidt tot een effectievere investering van tijd en middelen. De strategische overlegkoepel cyberweerbaarheid kan in de tussentijd ook bijdragen aan het verbeteren van de Nederlandse digitale autonomie doordat verschillende beleidsterreinen en belangen hecht met elkaar worden verbonden, met sturing vanaf het hoogste niveau (*'Whole-of-Government'*)[42]. Een integrale aanpak zal hierbij meer baten opleveren voor de Nederlandse digitale autonomie[43].

Verbeter informatiedelingscapaciteiten en ondersteuning

Het verbeteren van de informatiedelingscapaciteiten draagt direct bij aan de cyberweerbaarheid van *alle* organisaties, door hen in staat te stellen zich beter tegen dreigingsactoren te beschermen, zowel preventief als reactief. Voorwaarde is wel dat de informatie een voedingsbodem moet hebben bij de organisaties. Veel kleinere bedrijven zijn onvoldoende in staat om te acteren op dreigingsinformatie. Door te investeren in preventie kunnen cyberincidenten worden voorkomen. Daarnaast is het belangrijk bedrijven een handelingsperspectief te bieden wanneer zij getroffen worden door cyberincidenten. Van onbewust onbekwaam naar bewust bekwaam vereist het vergroten van *awareness* en *capacitybuilding*. Veel bedrijven, waaronder mkb-bedrijven, zijn onvoldoende in staat om te acteren op dreigingsinformatie en hebben behoefte aan ondersteuning bij het nemen van maatregelen. Om bedrijven te helpen hun beveiliging beter op orde te krijgen en te houden wordt structureel geïnvesteerd in de ontwikkeling en het structureel onderhoud van hulpmiddelen en tools die dat ondersteunen. Het DTC moet hiervoor worden versterkt. Een netwerkbenadering met publiek-private samenwerking biedt de beste kansen om de weerbaarheid van het Nederlandse bedrijfsleven op een hoger niveau te brengen.

Kosten van de aanvullende adviezen

De geschatte investeringen voor de periode 2021-2024 om de aanvullende adviezen te realiseren zijn opgenomen in de volgende tabel. De onderbouwing van de inschatting wordt daaronder verder uiteengezet.

42 Onderzoeksrapport 'Nederlandse strategische autonomie en cybersecurity', Paul Timmers en Freddy Dezeure, januari 2021 (een onderzoek uitgevoerd in opdracht van de Cyber Security Raad)

43 Deze baten worden verder uitgewerkt in het Onderzoeksrapport 'Nederlandse strategische autonomie en cybersecurity', Paul Timmers en Freddy Dezeure, januari 2021 (een onderzoek uitgevoerd in opdracht van de Cyber Security Raad)

Advies	2021	2022	2023	2024 (structureel)	Eenmalige investering (2021-2024)	Totaal (2021-2024)
Realiseren een effectieve vorm van regie op samenwerking en ontwikkelen een gemeenschappelijke koers op het gebied van cybersecurity	€ 800.000	€ 1.100.000	€ 1.500.000	€ 1.500.000	-	**€ 4.900.000**
Verbeteren van informatiedelings-capaciteiten en ondersteuning	€ 20.200.000	€ 20.400.000	€ 20.550.000	€ 20.550.000	-	**€ 81.700.000**
Uitvoering toetsingskader digitale autonomie	€ 800.000	€ 1.100.000	€ 1.500.000	€ 1.500.000	-	**€ 4.900.000**
Structurele, eenmalige en totale investeringen komende kabinetsperiode (2021-2024)				**€ 23.550.000**		**€ 91.500.000**

Nationale cyberweerbaarheidsstrategie en regie op samenwerking

Voor het realiseren en onderhouden van een nationale cyberweerbaarheidsstrategie, het opzetten en organiseren van de strategische overlegkoepel en het verkennen en begeleiden van verdere regie op samenwerking wordt aangenomen dat structureel 10 fte nodig zijn.

Verbeter informatiedelingscapaciteiten en ondersteuning

Voor het optimaliseren en onderhouden van een Landelijk Dekkend Stelsel van Informatieknooppunten, en ook het bewerkstellingen van een structurele (juridische) oplossing voor het delen van dreigingsinformatie wordt aangenomen dat structureel 5 fte nodig zijn.

Investeer daarnaast structureel € 8 miljoen in het DTC ter versterking van de uitbouw van de informatiedienst en van het netwerk van samenwerkingsverbanden met bedrijven om te komen tot een landelijk dekkend stelsel van informatieknooppunten voor cybersecurity.

De rol van het NCSC als nationaal cybersecurity-knooppunt wordt steeds belangrijker terwijl de beschikbare middelen achterblijven. Om informatiedeling en weerbaarheidsadviezen voor organisaties binnen en buiten de vitale infrastructuur mogelijk te maken, is versterking van het NCSC nodig. Onder meer voor het vergroten van de capaciteit om verkregen dreigingsinformatie te ontvangen, te duiden en te delen met schakelorganisaties, zoals het DTC. Ook de samenwerking met andere operationele partijen moet verder worden uitgebouwd. Daarnaast dient de sector-overstijgende expertise bij het NCSC over risicoanalyses, strategische afhankelijkheden en informatiedeling te worden uitgebouwd. Het gaat dan om het versterken NCSC, uitbreiden NDN en doorontwikkelen LDS. Voor deze versterking is structureel € 11,8 miljoen per jaar nodig.

Uitvoering toetsingskader digitale autonomie

Het Onderzoeksrapport 'Nederlandse strategische autonomie en cybersecurity'[44], schatten de benodigde investering voor de implementatie en uitvoering van het toetsingskader op minimaal € 5 miljoen over een periode van vier jaar. Er volgen mogelijk nog kosten uit het daadwerkelijk uitvoeren van interventies die voortvloeien uit het gebruik van het toetsingskader. Deze kosten vallen buiten de scope van dit rapport[45].

44 Onderzoeksrapport 'Nederlandse strategische autonomie en cybersecurity', Paul Timmers en Freddy Dezeure, januari 2021 (een onderzoek uitgevoerd in opdracht van de Cyber Security Raad)

45 In de regie is budget voorzien voor de toepassing van het toetsingskader voor digitale strategische autonomie. De verwachting is dat het benodigde budget voor de implementatie van de prioriteiten voor digitale strategische autonomie (dat aanzienlijk is) komt uit al voorziene ICT-investeringen van de overheid die met meer coherentie en synergie gebruikt gaan worden, EU-budgetten voor O&O en 'digitaal' waarop een sterker strategisch beroep gedaan zal worden, en recent voorgestelde nieuwe Nederlandse en Europese fondsen voor innovatie en herstel. Dit volgt uit het Onderzoeksrapport 'Nederlandse strategische autonomie en cybersecurity', Paul Timmers en Freddy Dezeure, januari 2021 (een onderzoek uitgevoerd in opdracht van de Cyber Security Raad).

Foto: Jeroen de Bakker

SPEERPUNT 2

WEERBARE VITALE PROCESSEN

Introductie en huidige staat

Nederland moet kunnen vertrouwen op de veiligheid en weerbaarheid van de vitale processen. Vitale processen[46] zijn processen die een essentiële dienst leveren zoals stroomvoorziening, telecommunicatie en betalingsverkeer, en waarvan verstoring door cyberaanvallen direct ontwrichtende effecten kunnen hebben op de maatschappij en een bedreiging vormt voor de nationale veiligheid. Kenmerkend is dat vitale processen vaak van elkaar afhankelijk zijn waardoor een incident in het ene proces ook het andere proces ernstig kan verstoren. Denk hierbij aan de uitval van energievoorziening dat ook directe gevolgen heeft voor de warmwatervoorziening, het openbare vervoer, en leven ondersteunende apparatuur in ziekenhuizen. Een deel van vitale processen is afhankelijk van betrouwbare informatietechnologie (IT), maar een groot deel ook van zogenaamde operationele technologie (OT). De impact van een cyberincident in vitale processen manifesteert zich daardoor ook snel in de fysieke wereld, met alle veiligheidsconsequenties van dien. Een andere zorg is dat veel vitale aanbieders gebruik maken van verouderde OT-systemen; in het verleden bestond OT uit op zichzelf staande systemen waar tijdens het verbinden van deze systemen met IT vaak geen rekening met cybersecurity is gehouden, en beveiligingsupdates zijn niet altijd (tijdig) beschikbaar. Kortom, de weerbaarheid van de IT en OT van vitale processen tegen cyberdreigingen is essentieel om Nederland nu en in de toekomst met vertrouwen te digitaliseren. De drie onderstaande paragrafen lichten toe welke initiatieven er momenteel binnen dit domein lopen.

Sectorale veiligheidsraamwerken en -eisen voor OT en IT

Cybersecurityrisico's binnen OT in vitale processen ontstaan vaak uit verouderde technologie en verouderde besturingssystemen, omdat ze niet voldoende afgeschermd zijn van de kwetsbare bedrijfs-IT. Beheer en beveiliging van IT en OT wordt vaak door verschillende teams met verschillende werkprocessen en kennis gedaan[47]. De beveiliging van OT vereist daarom een significant andere aanpak ten opzichte van 'reguliere' cybersecurity, en het onderscheid tussen OT en IT is van belang bij de aanpak. Daarnaast wordt vanwege de uniciteit van de OT-omgevingen en -systemen binnen de verschillende sectoren vaak op basis van door organisaties zelf bepaalde doelen en normen ingericht. Dit gebeurt momenteel veelal ad-hoc en er zijn geen gedeelde (minimale) weerbaarheidsdoelstellingen.

46 Raadpleeg https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen voor een overzicht van vitale processen

47 Cybersecurity – A State-of-the-art Review: Phase 2, Wetenschappelijk Onderzoek- en Documentatiecentrum, 2020

Ook erkennen en behandelen partijen in de vitale sector (in zowel de private als publieke sector) elkaar nog niet genoeg als ketenpartners en ontbreekt daarmee structurele samenwerking op het gebied van cyberweerbaarheid[48]. Momenteel streeft iedere vitale partij nog binnen het eigen deel naar weerbaarheid terwijl betere samenwerking ten aanzien van ketenveiligheid een grotere bijdrage levert dan de som der delen. Ook wordt kennis over de beveiliging van OT niet breed genoeg gedeeld met partijen buiten de vitale sector, terwijl het gebruik van OT niet beperkt is tot de vitale sector.

Een belangrijke stap die hierin is gezet, is dat de Wet beveiliging netwerk- en informatiediensten (Wbni) eind 2018 in werking is getreden. De Wbni is de Nederlands implementatie van de Europese Network and Information Security (NIS) Directive. De Wbni bevat voor (voornamelijk) vitale aanbieders regels op het vlak van zorgplicht voor cybersecurity en eisen voor het melden van cybersecurityincidenten[49]. De Europese Commissie heeft na publieke consultatie van experts erkend dat de huidige NIS verbeterd moet worden, onder andere als gevolg van veranderingen in het dreigingslandschap, inconsistenties in toepassing tussen EU-landen en verdergaande digitalisering die een groter deel van de samenleving raakt[50]. Daarom is de NIS 2 voorgesteld, waarin onder andere zowel nieuwe maatregelen als ook nieuwe vitale sectoren worden voorgesteld[51]. De nieuwe NIS 2 zal door de Nederlandse overheid vertaald moeten worden naar een nieuwe Wbni.

Inhaalslag met verbeterprogramma's

Om vitale processen goed te beveiligen moeten bij veel organisaties IT- en OT-systemen beter beveiligd worden. Hier zijn vaak (omvangrijke) verbeterprogramma's voor nodig. Zo zijn er op dit moment binnen specifieke sectoren programma's bezig om de cyberweerbaarheid te vergroten, zoals het programma Beveiligd Werken Rijkswaterstaat (BWR) binnen de vitale sector Keren en Beheren[52]. De meeste vitale processen omvatten zowel publieke als private organisaties, met zeer wisselende mate van volwassenheid waar het hun eigen cyberweerbaarheid betreft. Om tot volledig weerbare vitale processen te komen zijn daarom maatregelen binnen deze organisaties nodig, door bijvoorbeeld directe investeringen en het versterken van toezicht.

Toezicht op vitale sectoren

Cybersecurity in vitale sectoren kan in de praktijk onvoldoende afgedwongen worden, zowel voor IT als OT. De Wbni legt een zorgplicht (treffen van beveiligingsmaatregelen) op aan Aanbieders van Essentiele Diensten (AED's). Het Agentschap Telecom, de Nederlandse Bank, de Inspectie Leefomgeving en Transport (ILT) en de Inspectie Gezondheidszorg en Jeugd (IGJ)[53] zijn aangewezen om toezicht op de cybersecurity van deze AED's te houden. Bij het niet naleven van de zorgplicht kan een toezichthouder een AED een bindende aanwijzing geven en indien nodig zelfs een bestuurlijke boete opleggen. Het is daarmee een belangrijke stok achter de deur om verdere verbeteringen in cyberweerbaarheid van vitale sectoren. Op dit moment is een aantal betrokken toezichthouders nog onvoldoende in staat om toe te zien op de naleving van de Wbni. Zo moet het ILT, dat toezicht moet houden op de vitale sectoren vervoer en levering en distributie van drinkwater, haar toezicht rol in het kader van de Wbni, inclusief kennis, expertise en inspectieproces, in 2021 nog verder opbouwen[54], en heeft de IGJ, omdat het op dit moment nog geen toezicht hoeft te houden bij gebrek aan AED's in de zorg, ook nog geen capaciteit opgebouwd op dit vlak. Zonder effectief toezicht kan niet goed in kaart worden gebracht hoe weerbaar vitale sectoren zijn, en zijn AED's niet goed aan te spreken op het nakomen van hun zorgplicht als ze achterblijven.

48 Informatie-uitwisseling tussen vitale aanbieders is essentieel om de cybersecurityvolwassenheid van de vitale processen in hun geheel te verhogen. Dit is in speerpunt 1 in meer detail uitgewerkt.

49 Er wordt in de Wbni onder andere onderscheid gemaakt tussen Aanbieders van Essentiële Diensten (AED's) en Andere Aangewezen Vitale Aanbieders (AAVA's). Deze verschillen in de mate waarin rechten en plichten van de Wbni op ze van toepassing zijn.

50 Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, Europese Commissie (2020)

51 Proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, European Commission, 2020

52 Digitale dijkverzwaring: cybersecurity en vitale waterwerken, Algemene Rekenkamer. Bron: (https://www.rekenkamer.nl/publicaties/rapporten/2019/03/28/digitale-dijkverzwaring-cybersecurity-en-vitale-waterwerken), 2019

53 Binnen de sector gezondheidszorg zijn nog geen AED's aangewezen.

54 ILT-brede risicoanalyse (IBRA) 2020, Inspectie Leefomgeving en Transport (2020).

Standpunten en eerdere adviezen van de raad

De cyberweerbaarheid van OT van vitale aanbieders moet op het vereiste niveau worden gebracht dat passend en proportioneel is gelet op de dreigingen en risico's. Vitale sectoren moeten zonder uitzondering beschikken over een eigen sectoraal OT-controleraamwerk. Waar nodig wordt het toezicht proportioneel versterkt. De raad is voorstander van een actieve invulling van toezicht binnen de wettelijke kaders (Wbni). Hierbij is het van belang dat voor iedereen duidelijk is hoe dit toezicht is geregeld en welke consequenties er zijn verbonden aan het schenden van regels. Alle betrokken stakeholders, waaronder het Nationaal Cyber Security Centrum (NCSC), de (sectorale) toezichthouders, en de beheerders van OT binnen de vitale sectoren moeten daarom over voldoende kennis beschikken om met elkaar en met andere lande de dialoog aan te gaan. De raad pleit ervoor om naast de reguliere wijze van informatie-uitwisseling binnen het in het eerste speerpunt genoemde landelijk dekkend stelsel van informatieknooppunten, 'trusted channels' te realiseren voor het delen van gerubriceerde (dreigings-)informatie door alle overheidsinstanties (NCTV, AIVD/MIVD, NCSC en toezichthouders) met individuele beheerders binnen vitale sectoren.

De raad adviseert ook een (virtueel) steunpunt OT in te richten. Het steunpunt heeft onder andere tot doel de beheerders van OT te ondersteunen bij hun inkoopproces met relevante kennis op het terrein van cybersecurity en het verzamelen en delen van meldingen van kwetsbaarheden van leveranciers en beheerders. Hierbij moet het steunpunt zich aansluiten bij het Landelijk Dekkend Stelsel van informatieknooppunten. In Duitsland zijn afspraken tussen overheid en OT-leveranciers vastgelegd in een Charter-of-Trust. Ook dit zou het steunpunt tot taak moeten hebben. Het steunpunt dient daarnaast juridische obstakels te identificeren bij het delen van informatie over OT. Alle relevante cybersecurity-informatie moet gedeeld kunnen worden om handelingsperspectief te bieden aan bijvoorbeeld OT-beheerders.

Aanvullende adviezen van de raad

Opzetten cyberweerbaarheid-versnellingsfonds voor vitale aanbieders

Het verbeteren van de beveiliging van vitale aanbieders is niet een eenmalige exercitie, maar vereist doorlopende aandacht en investeringen. Daarom moeten er gerichte en structurele investeringen komen om de beschikbaarheid van voldoende financiële en personele slagkracht te waarborgen waarmee binnen vijf jaar de benodigde cybersecurityinitiatieven binnen vitale sectoren gerealiseerd kunnen worden. Het opzetten van een versnellingsfonds, eventueel met eigen bijdrage en/of resultaatsverplichting, moet vitale aanbieders waar nodig de middelen bieden om deze inhaalslag onder eigen verantwoordelijkheid te bewerkstelligen. Zo zou een dergelijk fonds dit soort investeringen kunnen stimuleren door een bepaalde mate van cofinanciering en een 'groot-helpt- klein-principe', naast andere voorwaarden die overwogen kunnen worden om de impact zo groot mogelijk te kunnen laten zijn. Om de resultaatsverplichting te toetsen is het wenselijk om een 'Plan, Do, Check, Act' mechanisme onderdeel te laten uitmaken van het versnellingsfonds; vitale aanbieders die van het fonds gebruik maken kunnen bijvoorbeeld verplicht worden periodieke dreigings-gebaseerde toetsingen uit te voeren om te valideren dat zij met hun fonds hun cyberweerbaarheid hebben verbeterd.

Sluit aan bij Europese initiatieven en ondersteuning

In EU-verband is het nodig aan te sluiten bij supply chain beveiligingsinitiatieven zoals voorgesteld in onder andere de eerste contouren van de NIS2 richtlijn en voorbereid in de 5G aanbeveling. Hierbij past ook het coherent versterken van cyberweerbaarheid in het licht van strategische autonomie. Bijvoorbeeld, vitale aanbieders zullen in toenemende mate op cloud-infrastructuur bouwen. Een aantal onder hen zal als 'launching customer' de positie van Nederland in de komende generatie van cloud kunnen gaan versterken, met name op het vlak van betrouwbaarheid van data en processen die beheerd worden door cloud-leveranciers van buiten de EU. Hierbij kan ook beroep gedaan worden op EU-ondersteuning.

Versterkt toezicht op vitale processen

Toezichthouders zijn op dit moment vaak nog niet volwassen genoeg om effectief toezicht te houden op organisaties in het kader van de Wbni. Bij sommige toezichthouders, zoals de ILT en in de toekomst IGJ, moet de toezichts-competentie nog vrijwel volledig opgebouwd worden. Om die reden moet ten eerste voor alle toezichthouders een algemene doelvolwassenheid afgestemd worden en moeten waar nodig nadere implementatieplannen opgesteld en uitgevoerd worden om de toezichthouders op termijn op dat niveau te krijgen. Streef in de wijze waarop toezicht wordt gehouden waar mogelijk naar uniformiteit (bijvoorbeeld bij rapportage over weerbaarheid naar verantwoordelijke ministers en de relevante Tweede Kamercommissie) en waar nodig naar uniciteit (om te borgen dat het toezicht aansluit op de unieke kenmerken van een sector, zoals bijvoorbeeld een type OT-systemen).

Een onderdeel van effectief toezichthouderschap moet zijn dat toezichthouders erop toezien dat aanbieders (eventueel door middel van het inschakelen van externe partijen) regelmatig de cyberweerbaarheid van de organisatie toetsen door middel van zogenaamde ethische hacks, op basis van gerichte dreigingsinformatie[55]. Dit is een aanpak die uniform kan worden toegepast in de verschillende sectoren en tegelijkertijd rekening houdt met de uniciteit. Deze competentie kan voor vitale aanbieders ontwikkeld worden.

Op dit moment kan met de Wbni alleen de zorgplicht (om 'kansen en gevolgen van digitale incidenten te verkleinen'[56]) bij AED's afgedwongen worden. Het type organisaties dat als AED aangewezen is, is beperkt[57]. Hierdoor is de zorgplicht op veel organisaties niet van toepassing terwijl die wel als vitaal voor de Nederlandse samenleving gekenmerkt kunnen worden. Denk hierbij bijvoorbeeld aan aanbieders in de zorgsector. Herzie daarom welke organisaties als AED aangemerkt zouden moeten worden. Voor de herziening van soorten organisaties die onder de zorgplicht van de Wbni vallen moet aangesloten worden op de door de Europese Unie opgestelde NIS 2-richtlijn[58].

Baten van de aanvullende adviezen

Opzetten cyberweerbaarheidsversnellingsfonds voor vitale aanbieders

De NCTV stelt dat verstoring of uitval van vitale processen tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Het doel van het cyberweerbaarheidsversnellingsfonds is om vitale aanbieders waar nodig van extra slagkracht en voldoende financiële middelen te voorzien om te waarborgen dat het versterken van de cyberweerbaarheid gelijke tred houdt met de toenemende cyberdreigingen (denk hierbij aan spionage en sabotage door bijvoorbeeld statelijke actoren). De organisaties blijven nadrukkelijk zelf verantwoordelijk voor het verbeteren van de cyberweerbaarheid van de eigen IT- en OT-systemen en moeten deze ook voornamelijk zelf financieren, en er worden randvoorwaarden gedefinieerd om gebruik te kunnen maken van het fonds. Dit zal de kans van slagen van een gerichte cyberaanval op Nederlandse vitale aanbieders met als doel het verstoren of laten uitvallen van vitale processen verlagen. Bovendien kan op de lange termijn kennis worden opgedaan over onder andere nog effectievere manieren om de cyberweerbaarheid van vitale aanbieders te verhogen; door hier bijvoorbeeld onderzoekers aan te koppelen kan deze kennis verder worden ontwikkeld en ook in andere sectoren worden toegepast.

Versterken van toezicht op vitale processen

Met versterkt toezicht op vitale processen krijgen toezichthouders actueel inzicht in hoe de vitale sectoren en AED's ervoor staan qua cybersecurityvolwassenheid, inclusief mogelijke structurele problemen. Dit stelt toezichthouders in staat om beter en tijdig in te grijpen (zoals het geven van bindende aanwijzingen en het opleggen van sancties) als het cybersecurityniveau van een AED niet op het gewenste niveau is. Hierdoor wordt op de lange termijn het lerend vermogen van een vitaal proces verbeterd en wordt controle gehouden over het benodigde weerbaarheidsniveau. Daarnaast maakt deze investering het bijsturen op het weerbaarheidsniveau mogelijk, bijvoorbeeld wanneer nieuwe dreigingen daar aanleiding toe geven. Door toezichthouderschap waar mogelijk (in de basis) uniform in te richten, met name in de wijze waarop het weerbaarheidsniveau wordt vastgesteld en gerapporteerd, is het mogelijk om op nationaal niveau de weerbaarheid van verschillende vitale processen met elkaar te vergelijken en waar nodig additioneel te investeren vanuit de Rijksoverheid.

55 Een vergelijkbare aanpak, Threat Based Ethical Red-Teaming (TIBER), wordt met succes gebruikt in de bankensector.

56 https://www.ncsc.nl/over-ncsc/wettelijke-taak

57 Het Besluit beveiliging netwerk- en informatiesystemen specificeert onder andere welke organisaties AED en AAVA zijn.

58 Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade, European Commission, 2020.

Kosten van de aanvullende adviezen

De geschatte investeringen voor de periode 2021-2024 om de aanvullende adviezen te realiseren zijn opgenomen in de volgende tabel. De onderbouwing van de inschatting wordt daaronder verder uiteengezet.

Advies	2021	2022	2023	2024 (structureel)	Eenmalige investering (2021-2024)	Totaal (2021-2024)
Richt een (virtueel) steunpunt OT in	€ 600.000	€ 900.000	€ 1.250.000	€ 1.250.000	-	€ 4.000.000
Zet een cyberweerbaarheids versnellingsfonds voor vitale aanbieders op -	-	-	-	-	€ 150.000.000	**€ 150.000.000**
Bouw benodigde capaciteit en expertise op voor toezichthouders Wbni	€ 9.000.000	€ 13.500.000	€ 18.000.000	€ 18.000.000	€ 5.000.000	**€ 63.500.000**
Structurele, eenmalige en totale investeringen komende kabinetsperiode (2021-2024)				**€ 19.250.000**	**€ 155.000.000**	**€ 217.500.000**

Richt een (virtueel) steunpunt OT in

Om te bepalen welke investering vereist is om een steunpunt OT tot stand te brengen is er gekeken naar de Duitse investering van de *'Bundesamt für Sicherheit in der Informationstechnik (BSI)'*, welke wordt geschat op 8 fte. Vanwege het belang van fysieke veiligheid met betrekking tot OT in Nederland wordt er uitgegaan van eenzelfde investering en wordt aangenomen dat voor de komende vier jaar structureel 8 fte nodig zijn.

Zet een cyberweerbaarheidsversnellingsfonds voor vitale aanbieders op

Door € 150 miljoen beschikbaar te stellen in een versnellingsfonds levert de overheid een directe bijdrage aan het beveiligen van organisaties binnen vitale sectoren. De organisaties blijven nadrukkelijk zelf verantwoordelijk voor het verbeteren van de cyberweerbaarheid van de eigen IT- en OT-systemen en moeten deze ook voornamelijk zelf financieren. Het doel van het cyberweerbaarheidsversnellingsfonds is om verbeterprogramma's waar nodig van extra slagkracht te voorzien om te waarborgen dat het versterken van de cyberweerbaarheid gelijke tred houdt met de toenemende cyberdreigingen. Dit bedrag hoort na het einde van de kabinetsperiode te worden herzien.

Bouw benodigde capaciteit en expertise op voor toezichthouders Wbni

Om tot een inschatting van de benodigde investeringen voor het versterken van toezicht op vitale sectoren te komen is de huidige cybertoezicht capaciteit van de DNB als uitgangspositie genomen. De jaarlijkse kosten voor cybertoezicht van de DNB worden op basis van industriekennis van Deloitte geschat op circa € 3 miljoen per jaar. Het uitgangspunt is dat deze vereiste investering voor alle toezichthouders op de Wbni ongeveer gelijk is. Daarnaast wordt in acht genomen dat in de NIS 2 acht nieuwe sectoren worden toegevoegd (bijvoorbeeld Voedsel). Aangenomen wordt dat daardoor twee additionele toezichthouder wordt belast met cybertoezicht (bijvoorbeeld de NVWA), waarmee het totaal op 6 toezichthouders komt. Tot slot wordt aangenomen dat voor iedere toezichthouder buiten de DNB investeringen nodig zijn om op het juiste volwassenheidsniveau te komen. Deze worden op € 1 miljoen per toezichthouder geraamd. Het herijken van het onderscheid van tussen vitale - en niet vitale organisaties binnen de Wbni wordt beschouwd als onderdeel van het versterken van effectief toezicht op vitale sectoren.

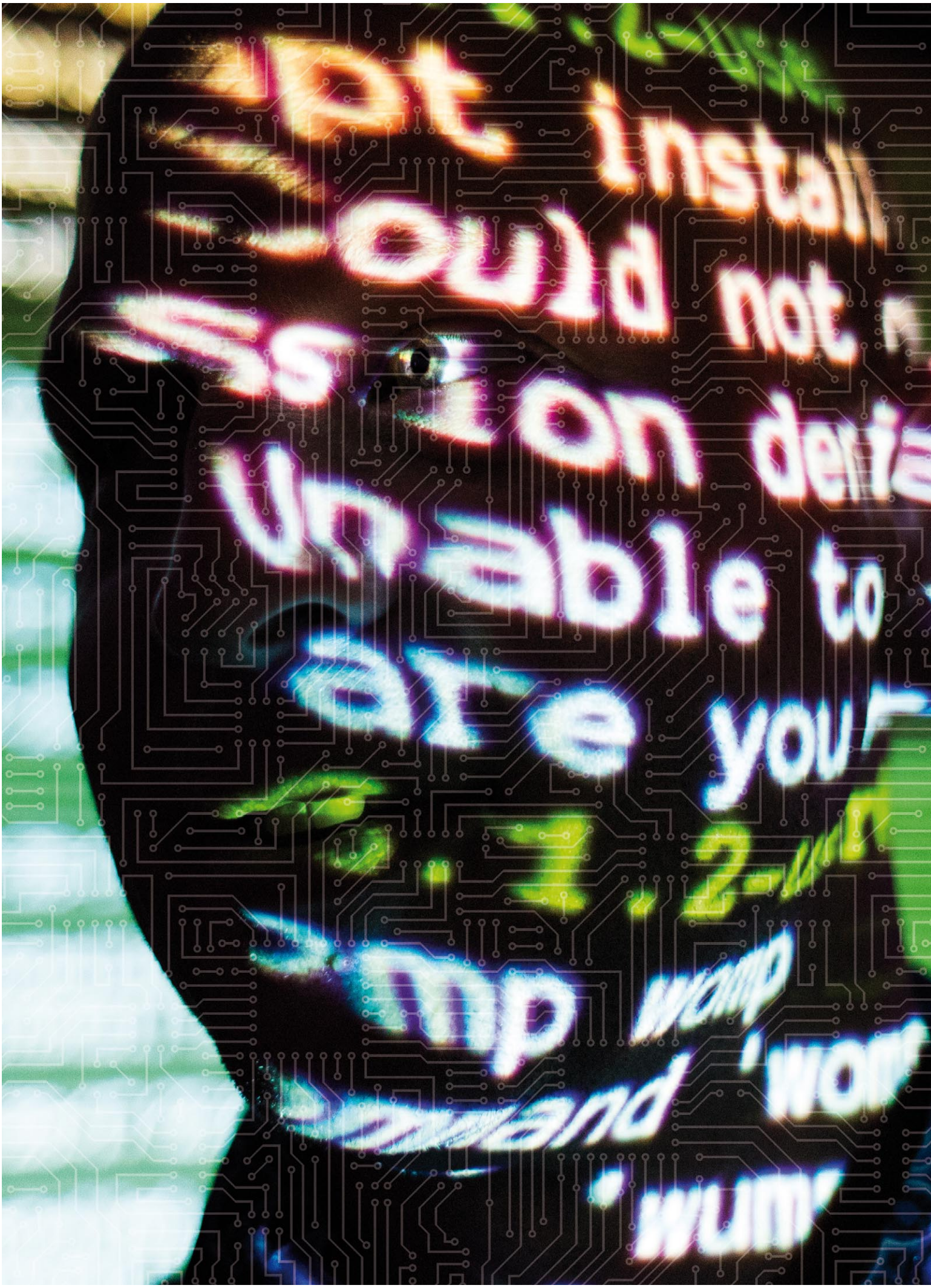


Foto: Jeroen de Bakker

SPEERPUNT 3

VERSTERKING ONDERZOEK EN ONDERWIJS

Introductie en huidige staat

Het doel van dit speerpunt is om te bewerkstelligen dat Nederland een concurrerende kenniseconomie blijft. Om dit te bereiken moet ons land (in de wetenschappelijke wereld en private-en publieke sector) beschikken over een sterke kennispositie op het gebied van cybersecurity en cybercrime. Een sterke kennispositie betekent niet alleen een sterke academische sector, maar ook de beschikbaarheid van hoogwaardige cybersecurity- en cybercrime-kennis in de kern van private organisaties en de overheid. Op deze manier wordt niet enkel fundamenteel en toegepast wetenschappelijk onderzoek versterkt, maar resulteert dit ook in een beter beleid, strategie en de uitvoering hiervan. Bovendien moest ons land de valorisatie van genoemde kennis en onderzoek stimuleren, bewust innoveren in technieken die de cyberweerbaarheid vergroten en professionals met de benodigde digitale vaardigheden opleiden en behouden. Nederland is nu in veel gevallen afhankelijk van landen die andere (geopolitieke) belangen kunnen hebben, doordat veel diensten en producten die in Nederland worden afgenomen buiten Europa worden ontwikkeld en geproduceerd. Daarnaast wordt er onvoldoende geïnvesteerd in fundamenteel en toegepast wetenschappelijk cybersecurityonderzoek, is er sprake van een *braindrain* van waardevolle cybersecuritykennis naar het buitenland en een tekort aan voldoende gekwalificeerde specialisten. Als resultaat is het noodzakelijk om in te zetten op de versterking van cybersecurity-gerelateerd onderzoek en onderwijs, zodat de cyberweerbaarheid van Nederland in de toekomst op het juiste niveau kan komen. De drie onderstaande paragrafen lichten toe welke initiatieven er momenteel binnen dit domein lopen.

Cybersecurity-onderzoek en -innovatie

In februari 2021 is het Samenwerkingsplatform ‘cybersecurity kennis en innovatie’ van start gegaan. Dit publiek-privaat samenwerkingsplatform (dat onder de verantwoordelijkheid van het Ministerie van Economische Zaken en Klimaat valt) zet zich in voor kennis en innovatie op het gebied van cybersecurity, wat moet bijdragen aan een ‘veiliger, slimmer, digitaal autonoom en economisch sterker Nederland’ door vraag, aanbod en financiering voor cybersecurity-onderwijs, onderzoek, innovatie en toepassing effectief bij elkaar te brengen[59]. Hiermee is Nederland in staat om internationaal leidende cybersecurity-expertise te genereren, zorg te dragen voor voldoende goed opgeleide cybersecurityspecialisten en effectieve toepassing van Nederlandse innovatieve producten en diensten. Het platform zal een thematische aanpak hanteren die gericht is op het teweegbrengen van veranderingen om voorgenoemde doelen te bereiken en in juli 2020 is een inrichtingsplan van het samenwerkingsplatform opgeleverd[60]. Het platform zal verder bouwen op het werk van dcypher en er wordt sinds oktober 2020 gewerkt aan inhoudelijke agendering van het platform[61].

59 Samenwerkingsplatform cybersecurity’, Advies Kwartiermakers versie 1.0 (2020)
60 Realisatiefase Samenwerkingsplatform ‘cybersecurity kennis en innovatie’, Ministerie van Economische Zaken en Klimaat (2020)
61 Kamerbrief Realisatiefase Samenwerkingsplatform ‘cybersecurity kennis en innovatie’ (2020)

Cybersecurity-onderzoek en -innovatie zullen ook de digitale autonomie van Nederland in cybersecurity versterken. Dit betekent een langetermijnperspectief waarbij kennis systematisch opgebouwd wordt en de innovatie en bedrijvigheid die hieruit voortkomt – waar die van belang is voor strategische autonomie - voor Nederland en haar strategische partners behouden blijft of ingezet wordt om wereldwijde belangen te realiseren. Dat betekent een weloverwogen inzet, ook van onderzoek en ontwikkeling, in internationale samenwerking (zoals in standaardisatie) en in de EU. Er is daarnaast een aantal onderzoeksagenda's opgesteld door verschillende organisaties die richting geven aan onderzoek dat kan helpen Nederlandse organisaties weerbaarder te maken tegen cybersecuritydreigingen. Voorbeelden hiervan zijn de Onderzoeksagenda 2019-2022 van het NCSC, de Nationale Cyber Security Research Agenda (NCSRA) en De Kennis- en innovatieagenda Veiligheid, die zich deels richt op cybersecurity.

Tot slot heeft het ministerie van Defensie in samenwerking met andere partijen onderzoek gedaan naar de oprichting van een Cyber Innovation Hub[62]. Deze hub heeft als doel de in Nederland gevestigde cyberkennis en-kunde te versterken en innovaties en experimenten te faciliteren door met verschillende partijen vanuit de private-en publieke sector samen te werken[63]. Voorlopig richt de hub zich uitsluitend op het defensiedomein maar in de toekomst is het streven om deze focus te verbreden.

Stimulering wetenschappelijk onderzoek

Het voorgenoemde Samenwerkingsplatform 'cybersecurity kennis en innovatie zal zich inzetten voor het terugdringen van versnippering in financiering voor cybersecurity-onderwijs, onderzoek, innovatie en toepassing daarvan. Het dient daarbij vooral als ondersteuning bij het verkrijgen van structurele financiering vanuit bestaande fondsen. Ook hier zal het platform zich richten op nader te bepalen thema's. Volgens de huidige plannen zal het platform geen eigen middelen hebben om onderzoek te financieren, waardoor partijen die onderdeel uitmaken van het platform volledig afhankelijk zullen zijn van het vermogen van Samenwerkingsplatform Cybersecurity om externe financiering te regelen.

Daarnaast wordt in Nederland onder andere via het Small Business Innovation Research (SBIR)-instrument, Topconsortia voor Kennis en Innovatie (TKI), de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) en doelfinancieringsprogramma's geïnvesteerd in cybersecurity gerelateerd innovatie en onderzoek[64].

Voldoende gekwalificeerde specialisten

Het Samenwerkingsplatform 'cybersecurity kennis en innovatie' zal zich inzetten voor het verhogen van het aantal goed opgeleide cybersecurityspecialisten in Nederland. Zoals eerder aangegeven zal de focus voornamelijk liggen op het creëren en borgen van hoogwaardig cybersecurity-onderwijs op universiteiten en hogescholen.

Het voormalige platform dcypher heeft zich ingezet voor het in kaart brengen van het Nederlandse landschap voor hoger onderwijs en onderzoek op het vlak van cybersecurity. Deze kaart is te vinden op de website van dcypher maar is niet meer geüpdatet sinds de opheffing van het platform op 1 oktober 2020. Tevens heeft dcypher in 2020 de Nederlandse Cybersecurity Educatie Agenda gepubliceerd; deze agenda bevat een roadmap met een lijst van interventies[65] in het (hoger) cybersecurity-onderwijs die partijen in de wetenschap en in de publieke en private sector kunnen realiseren om zowel op korte als lange termijn structurele verbeteringen in cybersecurity onderwijs kunnen bewerkstelligen[66]. In de roadmap zijn echter geen specifieke acties gekoppeld aan partijen die deze voor een bepaalde tijd moeten realiseren.

62 Voortgang Nederlandse Cybersecurity Agenda, Ministerie van Justitie en Veiligheid (2019)

63 https://securitytalent.nl/nl/vacatures/kwartiermaker-cyber-innovation-hub

64 Naar schatting is de afgelopen 8 jaar gemiddeld € 7,5 miljoen euro geïnvesteerd. Bron: Samenwerkingsplatform cybersecurity – Advies Kwartiermakers (versie 1.0) (2020)

65 Interventies bestaan onder andere uit het bevorderen van de instroom van cybertalent naar het Nederlandse cybersecurity-onderwijs, en het stimuleren van gevorderde studenten om te kiezen voor een cybersecurity loopbaan in Nederland.

66 https://www.dcypher.nl/nationale-cyber-security-educatie-agenda-gepubliceerd

Ook werkt de Nederlandse overheid aan het verbeteren van de digitale geletterdheid van jongeren door onder andere de curriculum kerndoelen[67] (voor het basis-en voortgezet onderwijs) te herzien en cybersecurity hieraan toe te voegen; naar verwachting wordt dit proces in 2022 afgerond, waarna de wettelijke verankering van de kerndoelen zal plaatsvinden[68].

Ook is in 2019 de Human Capital Agenda Security door The Hague Security Delta gepubliceerd. Het doel van deze agenda is om de mismatch op de cybersecurity arbeidsmarkt aan te pakken door vraag en aanbod van cybersecurityspecialisten beter op elkaar aan te sluiten[69]. Een soortgelijk initiatief is de Roadmap Human Capital 2020-2030 voor Nederlandse topsectoren; de missie van de roadmap is een 'toekomstbestendige beroepsbevolking als voorwaarde voor een florerende economie en een positieve maatschappelijke dynamiek'[70]. Er wordt benadruk dat het noodzakelijk is om te investeren in kennis en vaardigheden van mensen om met cybersecurity om te kunnen gaan[71], wat op den duur bijdraagt aan een toekomstbestendige beroepsbevolking. Daarnaast is er een Human Capital Agenda voor ICT van de Dutch Digital Delta, die met verschillende initiatieven aan de bredere vraag naar ICT-professionals probeert te voldoen[72].

Daarnaast heeft eind 2019 de Minister van Onderwijs, Cultuur en Wetenschap een nota met potentiële oplossingen voor het terugdringen van het docententekort (in technische opleidingen) in ontvangst genomen[73].

Standpunten en eerdere adviezen van de raad

De raad ziet graag een samenleving die innovatief en ondernemend is, maar die ook weerbaar is tegen de risico's die de grote afhankelijkheid van ICT met zich meebrengt. Dit brengt met zich mee dat Nederland moet beschikken over een krachtige kennispositie en voldoende en juist gekwalificeerde cybersecurity professionals. Nederlandse jongeren moeten goed zijn voorbereid op de digitale toekomst door middel van een geïntegreerde aanpak in het onderwijs die ervoor zorgt dat digitale geletterdheid en cybersecurity onderdeel worden van het curriculum. Er dient bovendien bewust geïnventariseerd te worden welke startups, technologie, kennis en infrastructuur van strategisch belang zijn, waardoor inzichtelijk wordt gemaakt wanneer verkoop aan of vertrek naar het buitenland nadelig kan zijn voor de Nederlandse strategische positie. Gezien de grote belangen die op het spel staan, zal Nederland bewust en zo snel mogelijk hier een positie over moeten innemen.

67 Curriculum.nu heeft in samenwerking met verschillende partijen bouwstenen opgeleverd voor de herziening van het curriculum: 'digitaal samenleven', 'technologisch burgerschap', 'van data naar informatie', 'digitale data', en 'veiligheid en privacy in de digitale wereld'. Raadpleeg https://www.curriculum.nu/bouwstenen/voor meer informatie.

68 Kamerbrief met kabinetsreactie op verbetervoorstellen voor curriculum basisonderwijs en voortgezet onderwijs, Ministerie van Onderwijs, Cultuur en Wetenschap (9 december, 2019).

69 https://www.thehaguesecuritydelta.com/news/newsitem/1283-launched-human-capital-agenda-security-2019-2022

70 Samen aan de slag – roadmap Human Capital Topsectoren 2020-2023, negen topsectoren, dutch digital delta en Platform Talent voor Technologie (2019)

71 Arbeidsmarktonderzoek ICT met topsectoren: naar een digitaal vaardiger beroepsbevolking (2019). Bron: https://www.caict.nl/wp-content/uploads/2019/09/190703-Eindrapport-Arbeidsmarktonderzoek-ICT-met-topsectoren-Berenschot-kwalitatief-1.pdf

72 https://dutchdigitaldelta.nl/hca-ict

73 https://www.cybersecurityraad.nl/actueel/nieuws/2019/09/06/minister-ocw-neemt-nota-oplossingsrichtingen-terugdringen-docententekort-in-ontvangst

Aanvullende adviezen van de raad

Cybersecurity-onderzoek en -innovatie

Om nieuwe ideeën te ontwikkelen en ook realiteit te laten worden is er een centraal cybersecurity onderzoeks- en innovatie-ecosysteem nodig waarin fundamenteel onderzoek, vraag en aanbod worden samengebracht[74]. De thematische aanpak van het Samenwerkingsplatform 'cybersecurity, kennis en innovatie' resulteert in het mogelijk buitensluiten van partijen die onderzoek doen naar, en kennisbehoefte hebben aan, cybersecuritygebieden die niet onder deze thematische aanpak vallen. Bovendien richt de Cyber Innovation Hub zich voorlopig alleen op het defensie domein, waardoor de partijen die geen onderdeel van dit domein uitmaken geen gebruik kunnen maken van de cyberkennis-en kunde die hier wordt gegenereerd. Daarnaast laten voorbeelden uit het buitenland zien dat er ruimte is om een centraal ecosysteem breder in te vullen: zo heeft het Singaporese Cyber Security Agency het *Innovation Cybersecurity Ecosystem @ Block71* opgericht. Hier worden cybersecurity startups van een vroeg tot lanceerstadium begeleid met een pre-accelerator bootcamp, een accelerator training programma en een launch-voorbereidingsprogramma[75], waarbij een deel van dit programma door de Singaporese overheid wordt gefinancierd. Ook is Belgische overheid van plan om met het *Centrum voor Cyber Security* een *Cyber Security Greenhouse* op te zetten om innovatieve cyberoplossingen en businessmodellen te ontwikkelen[76].

Er dient dus in Nederland een centrale organisatie te worden ingericht die alle partijen en bestaande Nederlandse cybersecurity ecosystemen-en hubs voor onderzoek en kennisbehoeftes op het gebied van cybersecurity samenbrengt (niet alleen geselecteerd thema's of specifieke partijen), van waaruit integrale regie gevoerd kan worden, en die kennisvalorisatie beter kan sturen. Hiermee wordt op de lange termijn bijgedragen aan het verhogen van de cyberweerbaarheid van de gehele Nederlandse maatschappij (en niet enkel één domein). Het Samenwerkingsplatform 'cybersecurity kennis en innovatie' zou hier bijvoorbeeld voor kunnen worden ingezet. Dit vereist wel dat er ook begeleiding aan onderzoekstrajecten zal worden aangeboden, en er wordt geholpen om nieuwe ontwikkelingen naar de markt te brengen. Daarbij moet ook gedacht worden over hoe een transitie naar de markt versnelt kan worden. Een fysieke locatie en digitale infrastructuur om samenwerking te bevorderen en onderzoekers en startups een werkomgeving te bieden biedt hierbij uitkomst.

Ook moet de overheid een interdepartementale rol als *launching customer* van het centrale onderzoeks-en innovatie-ecosysteem met betrekking tot cybersecurity en cybercrime aannemen om direct innovatieve oplossingen in te kunnen zetten ten behoeve van de nationale cyberweerbaarheid. De Cyber Innovation Hub van het ministerie van Defensie is hier een mooi voorbeeld van.

Stimulering wetenschappelijk onderzoek

Om onze nationale behoefte aan eigen hoogwaardige expertise te kunnen vervullen is het noodzakelijk om cybersecuritykennis in eigen land te ontwikkelen en voor ons zelf beschikbaar te houden. Om dit te kunnen doen is het van belang dat Nederland beschikt over fundamenteel en toegepast wetenschappelijk onderzoek dat is toegespitst op het verbeteren van de nationale cyberweerbaarheid. Een oplossing is om vanuit de overheid meer financiële middelen beschikbaar te stellen voor fundamenteel en toegepast cybersecurityonderzoek met bestaande fondsen en doelfinancieringsprogramma's[77]; vervolgens kunnen deze fondsen en doelfinancieringsprogramma's zij beslissen aan welke projecten de financiële middelen worden toebedeeld[78].

74 Mazzucato, M. (2015). De ondernemende staat: waarom de markt niet zonder overheid kan. Nieuw Amsterdam

75 https://www.csa.gov.sg/programmes/ice71

76 Zie bijlage 2 voor meer toelichting. Bron: Building a Cyber Resilient and Trusted Belgium – Cyber Security Themes for the Strategic Investment Pact 2030 (Centre for Cyber Security Belgium)

77 Denk aan organisaties zoals het Small Business Innovation Research (SBIR)-instrument, Topconsortia voor Kennis en Innovatie (TKI), en de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO).

78 De financiële middelen kunnen worden toebedeeld aan cybersecurityonderzoek waar momenteel in Nederland behoefte aan is. Deze onderwerpen staan onder andere omschreven in de Nationale Cyber Security Research Agenda (NCSRA-III). Bron: https://www.dcypher.nl/sites/default/files/uploads/documents/NCSRA-III_0.pdf

Deze middelen kunnen ook worden ingezet om onderzoek en innovatie op het gebied van cybersecurity door marktpartijen te ondersteunen, jaarlijks (PhD) studenten[79] die onderzoek doen naar cybersecurity[80] op te leiden, of om wetenschappers te voorzien van internationale marktconforme en competitieve lonen en beloningsstructuren zodat zij niet naar het buitenland vertrekken. Ook is het mogelijk om de middelen beschikbaar te stellen aan het voorgenoemde centrale cybersecurity-onderzoeks- en innovatie-ecosysteem, waarbij het verantwoordelijk wordt gesteld voor het coördineren en toebedelen van het geld aan gewenste onderwerpen en initiatieven. Hierbij is het mogelijk om een gerichte beleidsrelatie in cybersecurity met de Europese Unie aan te gaan zodat de in het algemeen sterke positie van Nederland in Europese onderzoeks- en innovatie-financiering ook in cybersecurity wordt verzekerd. Denk bijvoorbeeld aan met de eventuele aansluiting van dit fonds op EU-initiatieven en in met EU-bondgenoten te investeren in cybersecurity-onderzoek en onderwijs om de cyberweerbaarheid van zowel Nederlandse als de EU te versterken. Nederland kan hier een actieve rol in spelen.

Voldoende gekwalificeerde specialisten

Om ervoor te zorgen dat Nederland nu en in de toekomst over voldoende gekwalificeerde specialisten beschikt dat bijdraagt aan de verhoging van de cyberweerbaarheid, is het noodzakelijk om vanuit de overheid een nationale *cybersecurity workforce* strategie op te stellen[81]. Deze strategie omschrijft onder andere de ambitie met betrekking tot de Nederlandse werkende bevolking in het cybersecurity domein, de benodigde cybersecurity kennis en vaardigheden en welke interventies nodig zijn om deze ambitie te realiseren[82]. Deze strategie zal zowel de overheid als de publieke en private partijen in staat stellen om initiatieven te prioriteren die ertoe leiden dat Nederland over voldoende gekwalificeerde specialisten in het cybersecuritydomein beschikt, en daarmee op de lange termijn zowel de huidige als toekomstige Nederlandse cyberweerbaarheid kunnen garanderen.

Ook moet de zij-instroom en bijzonder hoogleraarschappen vanuit het bedrijfsleven worden gestimuleerd en moeten docenten op het vlak van ICT worden opgeleid om het tekort aan cybersecurity-kennis in het onderwijs terug te dringen – dit kan verwezenlijkt worden met het ontwikkelen van stimuleringsprogramma's[83].

De curriculumherziening[84] voor het basis-en voortgezet onderwijs loopt op dit moment, maar kan nog een aantal jaren duren. Vanwege de urgentie om digitale geletterdheid op te nemen in het huidige curriculum van scholieren, is het belangrijk dit onderwerp uit deze algemene herziening te trekken. Zo kan het curriculum voor digitale geletterdheid afzonderlijk behandeld worden en sneller in het onderwijs geïmplementeerd worden.

Tot slot dient er geïnvesteerd te worden in 'life long learning' trainingsprogramma's waarin nieuwe en ervaren ICT-, cybercrime- en cybersecurityprofessionals, data scientists, onderzoekers en werknemers binnen de wetenschap en de publieke sector hun vaardigheden kunnen bijhouden en op de hoogte blijven van nieuwe ontwikkelingen in het cyberdomein. Daarnaast kunnen de 'life long learning' trainingsprogramma's een grote bijdrage leveren aan de kennispositie van de overheid op het gebied van cybersecurity en cybercrime– een verbeterde en relevante kennispositie van overheidsmedewerkers houdt in dat er betere keuzes worden gemaakt op het gebied van de actieve ontwikkeling van strategie, beleid, wetgeving, en investeringen, (toekomstige) technologie en infrastructuur. Daarnaast zullen zowel de voorgenoemde stimuleringsprogramma's als de 'life long learning' trainingsprogramma's op de lange termijn bijdragen aan het terugdringen van het huidige tekort van voldoende gekwalificeerde specialisten in de wetenschap en de publieke- en private sector.

79 Hogescholen en universiteiten kunnen ook met door hun uitgevoerde cybersecurity-onderzoek bijdragen aan de ontwikkeling van diensten en producten die in Nederland breed inzetbaar kunnen zijn.

80 Een voorbeeld van een onderzoeksonderwerp dat wetenschappelijke aandacht vereist is de impact van geavanceerde technologieën, zoals kwantumtechnologie, op cybersecurity.

81 Cybersecurity A State-of-the-art Review: Phase 2 Final report, WODC (2020)

82 Het is noodzakelijk dat tijdens het opstellen en uitvoeren van de workforce strategie de 'lessons learned' van voorgaande campagnes en pogingen om zorg te dragen voor voldoende gekwalificeerde specialisten worden meegenomen. Dit heeft als doel het verhogen van de kans dat de doelstellingen van de workforce strategie worden gerealiseerd. Denk hierbij aan voorgaande campagnes waar bijvoorbeeld meer vrouwen en jongeren werden gestimuleerd om te gaan werken in de technische sector.

83 Dit kan bijvoorbeeld gerealiseerd worden door een flexibel aannamebeleid bij universiteiten ten aanzien van parttime docenten uit het bedrijfsleven en het opstellen van een gezamenlijk opleidingsprogramma, of het formeren van een multidisciplinair team dat universiteiten actief ondersteunt bij het snel vinden van gekwalificeerde specialisten en de benodigde middelen. Deze middelen horen ook door cybersecurity-gerelateerde studies te worden ingezet om aan de toenemende vraag te kunnen voldoen.

84 Curriculum.nu heeft in samenwerking met verschillende partijen bouwstenen opgeleverd voor de herziening van het curriculum: 'digitaal samenleven', 'technologisch burgerschap', 'van data naar informatie', 'digitale data', en 'veiligheid en privacy in de digitale wereld'. Raadpleeg https://www.curriculum.nu/bouwstenen/voor meer informatie.

Baten van de aanvullende adviezen

Stimuleren van cybersecurity-onderzoek en innovatie

Het transformeren van het Samenwerkingsplatform 'cybersecurity kennis en innovatie' naar een centraal cybersecurity-onderzoeks- en innovatie-ecosysteem stelt verschillende Nederlandse partijen in staat om hun cybersecuritytalent en kennis te bundelen om zodoende in eigen land hoogwaardige cybersecuritydiensten en -producten te ontwikkelen en te produceren. Dit ecosysteem kan als startpunt worden gebruikt voor de opbouw van een Nederlandse cybersecurity-maakindustrie. De unieke cybersecuritykennis en -oplossingen die uit dit ecosysteem voortvloeien kunnen vervolgens worden ingezet om de cyberweerbaarheid en digitale autonomie van Nederland te verhogen. Zo onderhoudt Nederland bijvoorbeeld de capaciteit om onafhankelijke validatie van buitenlandse oplossingen te kunnen leveren. Nederland wordt immers minder afhankelijk van landen (met mogelijk andere geopolitieke belangen) waar momenteel soortgelijke (cybersecurity) kennis en oplossingen worden afgenomen, en buiten Europa worden ontwikkeld en geproduceerd. Ook zal het centrale ecosysteem op de lange termijn deels de cybersecurity *braindrain* naar het buitenland tegengaan door wetenschappelijk- en maatschappelijk cybersecuritytalent de (momenteel nog afwezige) infrastructuur en begeleiding in eigen land aan te bieden.

Stimuleren van wetenschappelijk onderzoek

Bestaande fondsen en doelfinancieringsprogramma's voorzien van meer en structurele financiële middelen zal resulteren in een systematische toename van zowel de kwantiteit als kwaliteit van het in Nederland uitgevoerde fundamenteel en toegepaste cybersecurity-onderzoek. De unieke cybersecuritykennis en -kunde van wetenschappers kan vervolgens door partijen in de publieke en private sector gebruikt worden om eventuele dreigingen of kwetsbaarheden beter te herkennen en zich beter tegen cybercrime- en aanvallen te beschermen. De systematische toename in cybersecuritykennis draagt ook bij aan het vermogen van Nederland om de academische cybersecuritycompetentie te blijven onderhouden en de *braindrain* van cybertalent naar het buitenland terug te dringen; wetenschappelijk- en maatschappelijk cybersecuritytalent hoeft niet meer naar het buitenland voor financiering uit te wijken, waar vaak internationale marktconforme en competitievere lonen worden aangeboden en meer geld voor cybersecurity-gerelateerd onderzoek beschikbaar wordt gemaakt[85]. Op den duur zullen deze factoren bijdragen aan het imago van Nederland als voorloper op het gebied van wetenschappelijk cybersecurity-onderzoek, wat mogelijk ook buitenlands cybertalent zal aantrekken en behouden.

Zorgdragen voor voldoende gekwalificeerde specialisten

Het bestaan van voldoende gekwalificeerd cybersecurityspecialisten resulteert in de verhoging van de Nederlandse cyberweerbaarheid met de doorstroom van specialisten naar de Nederlandse private- en publieke sector. Hier kunnen specialisten hoogwaardige cybersecuritykennis toepassen om verschillende sectoren in staat te stellen zich beter tegen cyberaanvallen te beschermen. De verhoging van voldoende Nederlands gekwalificeerde (cybersecurity)-specialisten zal op de lange termijn ook meer buitenlands cybersecuritytalent aantrekken om in Nederland te komen werken. Bovendien zullen de structurele investeringen in cybersecurity kennisontwikkeling en onderwijs ook op den duur het bewustzijn van de Nederlandse samenleving op het gebied van cybersecurity verhogen, wat direct bijdraagt aan de cyberweerbaarheid van Nederland. Dit is ook van toepassing op de verbetering van de kennispositie van de overheid op het gebied van cybersecurity – dit stelt de overheid beter in staat om effectieve aan cyberweerbaarheid gerelateerde strategieën, beleidsstukken, en wetgeving op te stellen, wat op de lange termijn leidt tot de verhoging van de Nederlandse cyberweerbaarheid.

Kosten van de aanvullende adviezen

De geschatte investeringen voor de periode 2021-2024 om de aanvullende adviezen te realiseren zijn opgenomen in de volgende tabel. De onderbouwing van de inschatting wordt daaronder verder uiteengezet. Ondanks dat deze investeringen in dit rapport als eenmalige investeringen worden geduid is het nadrukkelijk van belang dat er ook na de komende kabinetsperiode in wordt voorzien. Het is immers noodzakelijk om structureel in cybersecurity-onderzoek en innovatie te blijven investeren, om zowel de nationale cyberweerbaarheid op peil te kunnen houden als te kunnen verhogen.

85 Zie bijlage 2 voor buitenlandse voorbeelden van financiering cybersecurity wetenschap.

Advies	2021	2022	2023	2024 (structureel)	Eenmalige investering (2021-2024)	Totaal (2021-2024)
Transformeer het Samenwerkings-platform 'cybersecurity kennis en innovatie' tot een centraal ecosysteem	€ 5.000.000	€ 7.500.000	€ 10.000.000	€ 10.000.000	€ 15.000.000	€ 47.500.000
Investeer in cybersecurity-onderzoek en –onderwijs	€ 12.500.000	€ 18.800.000	€ 25.000.000	€ 25.000.000	-	€ 81.300.000
Stel een nationale 'cybersecurity workforce'-strategie op	€ 750.000	-	-	-	-	€ 750.000
Keur de curriculumherziening digitale geletterdheid versneld goed	-	-	-	-	€ 1.500.000	€ 1.500.000
Zet het specifieke 'life long learning'-programma op	-	-	-	-	€ 20.000.000	€ 20.000.000
Zet stimuleringsprogramma's op om het tekort aan cybersecurity-docenten in het onderwijs terug te brengen	-	-	-	-	€ 10.000.000	€ 10.000.000
Structurele, eenmalige en totale investeringen komende kabinetsperiode (2021-2024)				**€ 35.000.000**	**€ 46.500.000**	**€ 161.050.000**

Transformeer het Samenwerkingsplatform 'cybersecurity kennis en innovatie' naar een centraal cybersecurity-onderzoeks-en innovatie-ecosysteem

De noodzakelijke eenmalige investering om het huidige *Samenwerkingsplatform 'cybersecurity kennis en innovatie'* naar een centraal cybersecurity-onderzoeks- en innovatie-ecosysteem te transformeren bedraagt ongeveer € 15 miljoen[86]. Daarnaast zal een jaarlijkse structurele exploitatiebegroting van € 10 miljoen[87] worden geïnvesteerd. Hierin inbegrepen zijn kosten voor de organisatie (mensen), huur van ruimtes met inrichtingsmiddelen, uitvoering van kennisdisseminatie en begeleiding, communicatie en marketing en de doorontwikkeling van de digitale infrastructuur. Verder dienen de partners van het ecosysteem jaarlijks een beperkte vergoeding te betalen voor het gebruik van de beschikbare ruimte en tools aan de beheerder van het ecosysteem. Er zal over een kabinetsperiode van vier jaar in totaal ongeveer € 4.5 miljoen euro geïnvesteerd moeten worden in het opzetten van dit centraal onderzoeks-en innovatie-ecosysteem.

Maak financiële middelen vrij voor cybersecurityonderzoek en -innovatie

Voor het vrijmaken van meer financiële middelen voor cybersecurity-onderzoek, innovatie en ondersteuning van marktpartijen, wordt gekeken naar voorbeelden uit het buitenland. Zo wordt er vanuit de Belgische overheid jaarlijks € 8 miljoen[88] geïnvesteerd in cybersecurity-onderzoek en wordt er in Singapore jaarlijks circa € 2.5 miljoen[89] vrijgemaakt voor de financiering van Singaporese bedrijven die zich bezighouden met cybersecurity-innovatie.

86 Zie sectie 4.2 in https://www.kansenvoorwest2.nl/files/tno-financieringvanfieldlabs.pdf. Dit bedrag is bestemd voor zowel de oprichting als het onderhoud van het ecosysteem in het eerste jaar.

87 Zie sectie 4.3 in https://www.kansenvoorwest2.nl/files/tno-financieringvanfieldlabs.pdf. Dit bedrag is iets hoger ingeschat vanwege de complexiteit van het ecosysteem.

88 De Vlaamse regering zal jaarlijks 8 miljoen euro investeren in het versterken van cybersecurity-onderzoek, waarbij specifiek wordt ingezet op strategisch onderzoekscentra en universiteiten. Bron: https://www.vlaio.be/nl/andere-doelgroepen/vlaams-beleidsplan-cybersecurity/vlaams-beleidsplan-cybersecurity/vlaams

89 Met het Singaporese CSA Cybersecurity Co-Innovation and Development Fund kunnen bedrijven financiering ontvangen; in 2018 hebben 8 bedrijven elk 500.000 Singaporese dollars aan investeringen uit dit fonds ontvangen (dit komt neer op een jaarlijks bedrag van ~2.5 miljoen euro). Bron: https://www.tnb.vc/cybercall2019.

Omgerekend naar het Nederlandse BBP komen deze bedragen jaarlijks uit op circa € 15 miljoen[90] voor cybersecurity-onderzoek en circa € 10 miljoen ter ondersteuning van marktpartijen in Nederland. Hierbij wordt gebruik gemaakt van in Nederland bestaande fondsen en doelfinancieringsprogramma's waardoor bovengenoemde bedragen worden gecombineerd en het beschikbare fondsbedrag neerkomt op circa € 81 miljoen over een kabinetsperiode van vier jaar. Na deze kabinetsperiode is het nodig om het fonds te blijven voorzien van financiële middelen en het bedrag te herzien. Dit bedrag is jaarlijks gezien circa drie keer groter dan het huidige gemiddelde jaarlijkse bedrag (€ 7,5 miljoen) dat de afgelopen acht jaar in Nederland in cybersecurity-onderzoek en innovatie is geïnvesteerd[91].

Stel een nationale cybersecurity workforce-strategie op

Voor het opstellen van een nationale cybersecurity workforce-strategie wordt aangenomen dat de komende vier jaar eenmalig 5 fte moet worden ingezet, ervan uitgaande dat de strategie binnen één jaar is afgerond.

Versnel de goedkeuring voor de herziening van het curriculum digitale geletterdheid

Het versnellen van de goedkeuring van de herziening van het curriculum digitale geletterdheid vergt vooral daadkracht en samenwerking tussen de verschillende partijen. Om dit aan te jagen is er een éénmalige investering nodig om 5 fte 2 jaar te kunnen inzetten.

Zet specifieke 'life long learning' trainings- en stimuleringsprogramma's voor cybersecuritytalent en professionals

Kijkend naar het buitenland zien wij dat de Vlaamse overheid per jaar ongeveer € 3 miljoen investeert in cybersecurity-gerelateerde bewustmaking en in de versterking van opleidingsmodules voor universiteiten en hogescholen, waarbij extra aandacht wordt geschonken aan de permanente vorming hiervan[92]. Voor de berekening van de benodigde investeringen in de 'life long learning' trainings-en stimuleringsprogramma's wordt het voorgenoemde Vlaamse voorbeeld als basis gebruikt en wordt aangenomen dat dit bedrag overeenkomt met de benodigde investeringen voor het opzetten van deze trainings-en stimuleringsprogramma's. Door de voorgenoemde € 3 miljoen om te rekenen naar het Nederlandse BBP, zullen de totale investeringen over een kabinetsperiode van vier jaar oplopen tot ongeveer € 20 miljoen. Dit bedrag dient na de kabinetsperiode te worden herzien.

Zet stimuleringsprogramma's op om het tekort aan cybersecuritydocenten in het onderwijs terug te dringen

Uitgaand van het voorgenoemde Vlaamse voorbeeld en de daarbij behorende investeringen, zullen de totale investeringen voor het opzetten van stimuleringsprogramma's om het tekort aan cybersecuritydocenten in het onderwijs terug te dringen over een kabinetsperiode van vier jaar oplopen tot circa € 10 miljoen. Hier wordt aangenomen dat de gewenste cybersecuritydocenten populatie kleiner is dan 'life long learning' trainings-en stimuleringsprogramma's doelgroep, waardoor het bedrag lager is dan de voorgestelde € 20 miljoen voor het opzetten van de geadviseerde trainings-en stimuleringsprogramma's voor cybersecuritytalent en -professionals. Dit bedrag dient na de kabinetsperiode te worden herzien.

90 Dit is een verdubbeling van het gemiddelde bedrag dat jaarlijks in Nederland wordt geïnvesteerd in cybersecurity-onderzoek en innovatie (gemiddeld 7.5 miljoen via het SBIR-instrument, NWO, TKI en doelfinancieringsprogramma's in de afgelopen 8 jaar). Bron: Samenwerkingsplatform cybersecurity – Advies Kwartiermakers (versie 1.0) (2020)

91 Samenwerkingsplatform cybersecurity – Advies Kwartiermakers (versie 1.0) (2020)

92 https://www.vlaio.be/nl/andere-doelgroepen/vlaams-beleidsplan-cybersecurity/vlaams-beleidsplan-cybersecurity/vlaams

Foto: Jeroen de Bakker

SPEERPUNT 4

REALISEREN VAN CYBERCRIME-HANDHAVINGSKETEN

Introductie en huidige staat

De aanpak van cybercrime[93] is essentieel voor een weerbare Nederlandse maatschappij. Het doel van dit speerpunt is het creëren van een effectieve handhavingsketen om cybercrime te bestrijden, waarbij specifieke handhavingsacties bij partijen met het grootste handelingsvermogen worden belegd. Op dit moment is de nodige informatie over onrechtmatigheden (op bijvoorbeeld het internet) verspreid over vele partijen in zowel Nederland als het buitenland (publiek, privaat en academisch); dit wordt nog onvoldoende bij elkaar gebracht. Bovendien kan de overheid op dit moment daar nog maar in zeer beperkte mate tegen optreden door beperkte expertise en capaciteit[94]. Daarnaast brengt cybercrime nieuwe eigenschappen met zich waar momenteel de basisinfrastructuur voor ontbreekt om efficiënt om te gaan met veel voorkomende delicten. Ook de massaliteit van cybercrime – er kunnen makkelijk 10.000 slachtoffers zijn van een enkele misdaad – brengt nieuwe vraagstukken met zich mee. Ook heeft de burger op dit moment geen goed en volledig beeld van cybercrimerisico's en hoe daarmee omgegaan kan worden. Daarom is het noodzakelijk om het handelingsvermogen van de gehele handhavingsketen – preventie, verstoring, opsporing en vervolging – te vergroten en versterken. De twee onderstaande paragrafen lichten toe welke initiatieven er momenteel binnen dit domein lopen.

Het valt niet te ontkennen dat Nederland bedreigd wordt door cyberspionage en cyberaanvallen van statelijke actoren. Nederland zal ook moeten omgaan met extraterritoriale toegang tot gevoelige gegevens. Het systematisch en in samenwerking met (zowel nationale als internationale) strategische partners tegengaan van deze bedreigingen zal toenemend belangrijk worden. De AIVD, MIVD, NCSC, Defensie, OM en politie houden zicht op deze dreigingen. Daarnaast hebben de offensieve capaciteiten van Defensie (incl. MIVD), de AIVD en de Nationale Politie een afschrikwekkende werking (*deterrence*)[95]. Om Nederland te beschermen tegen schadelijke activiteiten van statelijke actoren zijn ook investeringen in de AIVD, MIVD, NCSC en Defensie noodzakelijk. Zoals reeds is benoemd in de introductie zijn deze extra investeringen niet in dit rapport opgenomen, maar dragen deze wel bij aan een goed zicht op de dreigingen, inzicht in weerbaarheid verhogende maatregelen en responscapaciteit.

93 Cybercrime is volgens de politie 'misdaad gepleegd met ICT, gericht op ICT' (Bron: https://www.politie.nl/themas/cybercrime.html). Dit onderzoek bedoelt bij het gebruik van het begrip cybercrime daarnaast cyber-enabled crime, waarbij digitale technieken worden ingezet voor het faciliteren van criminaliteit (bron: Uitwerking Veiligheidsagenda 2019 – 2022, Ministerie van Justitie en Veiligheid (2018)).

94 Zo worden er bijvoorbeeld nog beperkt marktpartijen ingeschakeld die de overheid kunnen helpen met het optreden tegen cybercrime, en wordt informatiedeling tussen marktpartijen (onderling) en o.a. politie en OM bemoeilijkt door wet- en regelgeving.

95 CSAM Hosting Monitor, TU Delft (2020)

Inzichtelijker maken van cybercrime

Het ministerie van Justitie en Veiligheid en de staatssecretaris van Economische Zaken en Klimaat hebben sinds 2018 een samenwerkingsverband met onder andere de Technische Universiteit Delft en een aantal hostingbedrijven. Als onderdeel van de nationale aanpak doet de TU Delft technisch onderzoek naar de hoeveelheid kinderporno die aangetroffen wordt op website die door Nederlandse hostingbedrijven gehost worden, en legt deze vast in de Child Sexual Abuse Material (CSAM) Monitor[96] Het ministerie van Justitie en Veiligheid gebruikt deze data om hostingbedrijven hierop aan te spreken. Daarnaast is het publiceren van de CSAM Hosting Monitor een vorm van 'naming en shaming'[97]. Dit zijn goede voorbeelden van hoe samenwerking kan helpen om cybercrime inzichtelijker te maken, maar slechts voor selectief aantal onderwerpen. Op dit gebied is meer inzet nodig om breder inzicht te krijgen in het effect van cybercrime en mogelijkheden voor effectieve bestrijding.

Structurele investering in aanpak van cybercrime

Er is in 2019 een eenmalige investering van € 30 miljoen gedaan die ten dele is gebruikt voor de integrale aanpak cybercrime[98]. Deze aanpak is een verzameling van maatregelen onder leiding van het ministerie van Justitie en Veiligheid dat zich onder andere richt op de versterking van opsporing en verstoring van criminele businessmodellen. Volgend uit afspraken in de Veiligheidsagenda zijn in 2019 de politie en het OM gestart met een eenheid-overstijgende aanpak van (cybercrime-)fenomenen en dadergroepen. Hiervoor zijn de cybercrimeteams van de politie met 145 fte uitgebreid. Deze teams werken in een landelijke structuur samen met Team High Tech Crime (THTC) en ondersteunen districtsrecherches en basisteams bij kennisopbouw voor de uitvoering van reguliere onderzoeken naar cybercrime. De Koninklijke Marechaussee is destijds niet meegenomen bij deze eenmalige investering, wat zorgt voor een zwakke schakel in de veiligheidsketen.

Naast deze aanpak wordt er meer aandacht besteedt aan opsporing van *bullet proof hosters*: hostingbedrijven die bewust criminaliteit faciliteren[99]. De ministeries van Justitie en Veiligheid en Economische Zaken en Klimaat werken met de politie en het OM aan maatregelen om het faciliteren van criminaliteit via hostingbedrijven tegen te gaan. Zo is in 2008 de 'Notice-and-Take-Down'-regeling ingevoerd. Hostingpartijen die onrechtmatige gegevens hosten en dat weten of horen te weten, kunnen hiervoor verantwoordelijk worden gehouden. Als iemand een melding maakt van deze gegevens moet het materiaal binnen twee tot tien dagen ontoegankelijk worden gemaakt, afhankelijk van de schade die het betrokkenen berokkent[100]. Bovendien is bekend gemaakt dat hostingsbedrijven die niet meewerken aan het verwijderen van kinderporno vanaf september 2020 op een zwarte lijst komen te staan, en mogelijk ook een boete of dwangsom opgelegd krijgen[101].

Naast inzicht krijgen in cybercrime is het ook noodzakelijk om daadkrachtig op te treden. De aanpak van cybercrime is op dit moment ad-hoc en vaak afhankelijk van eenmalige financiële investeringen. Daarnaast worden veel investeringen door organisaties op individuele basis gevraagd en mist daardoor een integrale aanpak van cybercrime die de gehele keten, van preventie tot opsporing en straf, op elkaar aansluit.

96 CSAM Hosting Monitor, TU Delft (2020)
97 Kamerbrief Voortgang aanpak online seksueel kindermisbruik en kindersekstoerisme, Ministerie van Justitie en Veiligheid (2020)
98 Kamerbrief Voortgang integrale aanpak van cybercrime, Ministerie van Justitie en Veiligheid (2019)
99 Kamerbrief Voortgang integrale aanpak van cybercrime, Ministerie van Justitie en Veiligheid (2020)
100 Notice and takedown, ICTRecht. Bron: (https://www.ictrecht.nl/kennis/factsheets/notice-en-takedown) (2020)
101 https://www.rijksoverheid.nl/documenten/toespraken/2020/06/09/speech-by-minister-of-justice-and-security-ferdinand-grapperhaus-on-eu-action-to-combat-child-sexual-abuse-9-june-2020

Standpunten en eerdere adviezen van de raad

Wat cybercrime precies is, hoeveel schade het veroorzaakt en hoe groot de omvang van het probleem is, is niet altijd duidelijk. Daarnaast wordt bestaande kennis onvoldoende gedeeld tussen handhavings- en private partners. Hierdoor is het lastiger om effectief te handhaven op de verschillende vormen waarin cybercrime zich uit, zoals het hosten van kinderporno, georganiseerde criminaliteit en malware. Daarom heeft de raad geadviseerd dat Nederland ervoor zorgt dat cybercrime beter inzichtelijk wordt en de publiek-private aanpak op dit terrein versterkt. De politie en het OM dienen de publiek-private samenwerking te structureren en intensiveren om de informatiepositie met betrekking tot cybercrime te versterken. Daarnaast dient het ministerie van Economische Zaken en Klimaat en brancheorganisaties het bedrijfsleven aan te sporen bewuster te worden van cybersecurityrisico's en -dreigingen, deze onderling beter te delen en vaker melding en aangifte te doen van cybercrime. Tot slot heeft de raad ook geadviseerd om datalekmeldingen bij de Autoriteit Persoonsgegevens voor wetenschappelijk en statistisch onderzoek beschikbaar te stellen[102]. Het doel is om preventieve informatie op te halen en daarmee persoonsgegevens beter tegen cybercriminelen te beveiligen.

Aanvullende adviezen van de raad

Inzichtelijker maken van cybercrime

Er wordt nog onvoldoende geïnvesteerd in publiek-private samenwerking om inzichtelijker te maken waar cybercrime zoal uit bestaat, hoe groot de omvang is, en welke actoren vaak slachtoffer worden. Zo is het nodig een monitor op te zetten die gevoed wordt door overheidsinformatie (zoals dreigingsbeelden van NCSC) en private informatie (zoals meldingen van kwetsbaarheden, onveilige websites). Zo'n monitor kan overheid, private organisaties en burgers een volledig beeld van cybercrime bieden. Daarnaast moet worden onderzocht welke rol het Centraal Bureau voor de Statistiek en/of Autoriteit Persoonsgegevens kunnen spelen in het opzetten en beheren van de monitor.

Het is daarbij van belang dat er meer data verkregen wordt over cybercrime. Om melding en aangifte doen voor het bedrijfsleven eenvoudiger te maken is het nodig om een gerichte campagne op te zetten waarbij bedrijven en particulieren op praktische wijze gestimuleerd worden om melding en aangifte te doen van cybercrime. Denk hierbij aan het op de hoogte stellen van burgers en bedrijven van het gemak en het bestaan van digitaal melding en aangifte doen met het gebruik van DigiD[103], en het onderzoeken van andere methoden waarmee het makkelijker wordt om melding en aangifte te doen.

Naast het aanvullen en centraliseren van informatie over cybercrime is het ook belangrijk bevindingen effectief en actiegericht te communiceren. Er is op dit moment geen entiteit die op het vlak van cybercrime een belangrijke kennisbron van burger en samenleving is en ons handelingsvermogen vergroot. Daarom is het van belang dat bestaande initiatieven worden samengebracht in een entiteit die de burger en de samenleving handelingsperspectieven biedt op het gebied van cybercrime.

Een monitor met publieke en private informatie met betrekking tot cybercrime, het stimuleren van bedrijven en particulieren om melding en aangifte te doen tegen cybercrime en het samenbrengen van initiatieven in één entiteit dragen in grote mate bij aan het meer inzichtelijker maken van cybercrime en het realiseren van de handhavingsketen.

Structurele investering in aanpak van cybercrime

De incidentele investeringen in de aanpak van cybercrime moeten worden omgezet naar gerichte en structurele investeringen. Hierbij dient specifiek geïnvesteerd te worden in de slagkracht (capaciteit, kennis en kunde) van het Openbaar Ministerie en de KMar, omdat de cybercapaciteit van beide op dit moment achterblijven ten opzichte van de capaciteit van onder anderen de politie[104].

102 CSR Advies 'Beschikbaar stellen datalekmeldingen voor onderzoeksdoeleinden', CSR Advies 2020, nr. 1
103 https://www.politie.nl/nieuws/2017/juli/21/00-gemakkelijker-aangifte-doen-met-digid-app.html
104 Kamerbrief Voortgang integrale aanpak van cybercrime, Ministerie van Justitie en Veiligheid (2020)

Het is ook noodzakelijk om de fenomeengerichte aanpak van de politie en de KMar te versterken, zodat deze kan meegroeien met de stijging van de toenemende criminele dreigingen en de politie en de KMar in staat worden gesteld om cybercriminaliteit succesvol aan te pakken[105]. Een succesvolle fenomeengerichte aanpak vergt dat structureel geïnvesteerd wordt in het instrumenteren en digitaal vaardig maken van de politieorganisaties middels het aanbieden van opleidingen, tools en het versterken van teams; zo worden bestaande medewerkers gefaciliteerd om effectief om te kunnen gaan met cybercrime en digitale criminaliteit. Hieronder valt ook de versterking van het samenwerkingsverband tussen publieke en private partijen die ad hoc en structureel op verschillende niveaus samenwerken en snel kunnen reageren op nieuwe fenomenen. Specifieke aandacht moet gaan naar internationale samenwerking die vereist vanwege het internationale karakter van cybercrime, en naar alternatieve wijzen om cybercrime aan te pakken (bijvoorbeeld met het afpakken van criminele winsten om cybercrime minder aantrekkelijk te maken). Ook zijn structurele investeringen in mensen en middelen vereist om het data-gedreven werken van de politie en de KMar verder te ontwikkelen. Het gebruik van nieuwe technologieën en een intensievere inzet van data is noodzakelijk voor het effectief kunnen opsporen van cybercrime.

Daarnaast dienen de investeringen in initiatieven die voorkomen dat mensen participeren in de criminaliteit en (potentiële) cybercriminelen helpen uit de criminaliteit te ontsnappen te worden verdubbeld. Zo moet er meer onderzoek gedaan worden naar de drijfveren voor mensen om te participeren in criminaliteit zodat hierop gehandeld kan worden, onder andere door het opzetten en verstevigen van onderzoeks-partnerschappen en -platforms. Daarnaast moeten jeugdige (potentiële) daders meer kansen geboden worden om uit de cybercriminaliteit te ontsnappen, onder andere door ze samen met het bedrijfsleven meer perspectief te bieden (bijvoorbeeld Hack_Right).

Ook is het van belang een aanvalsprogramma ‘bad content’ op te zetten en te operationaliseren, waarbij de focus moet liggen op inzet van publiek-private samenwerking om hier verdere stappen in te nemen. Mocht die samenwerking niet tot de gewenste resultaten leiden, dan kan op termijn overwogen worden om ook wettelijke middelen in te zetten. Zowel de overheid als de hostingsector spelen hier een belangrijke rol. Binnen de telecomsector lopen al verschillende waardevolle initiatieven die ‘bad content’ weren, maar deze focussen zich nu vaak op een specifiek fenomeen zoals kinderporno. Van de gehanteerde aanpak kan veel geleerd worden over hoe deze aanpak ook voor andere fenomenen ingezet kan worden, zoals het Anti-Abuse Netwerk momenteel al doet. Om de handhavingsketen te bevorderen moet er een beter beeld zijn van welke partijen in de internetsector een belangrijke rol kunnen spelen bij het weren van ‘bad content’; kijk hierbij naast webhosters bijvoorbeeld ook naar grotere platformen die onrechtmatige content hosten. Daarbij moet er in kaart worden gebracht hoe hostingbedrijven beter ondersteund kunnen worden om hosting van ‘bad content’ actief tegen te gaan, en moet het duidelijk worden gemaakt welke (wettelijke) handvatten zij hiervoor hebben[106]. Hier moet wel rekening worden gehouden met het principe van netneutraliteit. Er zijn nu losstaande initiatieven vanuit de sector, maar een overkoepelende en gecoördineerde aanpak over de gehele handhavingsketen heen ontbreekt. Zo kan er, wanneer publiek-private samenwerking niet de gewenste resultaten oplevert, verkend worden hoe verschillende rechtsgebieden kunnen dienen voor ontmoedigen, voorkomen en straffen van misdaad. Naast het strafrecht kan daarnaast verkend worden hoe bijvoorbeeld ook het bestuurs- en civielrecht beter benut kunnen worden om partijen die een faciliterende rol spelen, zoals bad hosters, harder aan te pakken, zonder direct terug te vallen op het strafrecht. Zo heeft minister Grapperhaus recentelijk de wet ‘bestuursrechtelijke aanpak online kinderpornografisch materiaal’[107] voorgesteld; ICT-bedrijven die niet binnen 24 dit soort materiaal verwijderen riskeren een bestuurlijke boete van maximaal 4 procent van de bedrijfsomzet. Om dit af te dwingen wordt een Autoriteit aanpak online kinderpornografisch materiaal in het leven geroepen[108]. Door het spectrum van interventies te vergroten kan ook effectiever en in een eerder stadium worden opgetreden.

105 De adviezen in deze alinea zijn in lijn met de position paper van de politie: de politie van morgen en overmorgen (2020). Let hierbij wel op dat de politie ook structurele investeringen vraagt voor het beveiligen van eigen infrastructuur en interceptie. Wegens de scope van deze business case zijn deze gevraagde investeringen hier niet in opgenomen. Bron: https://www.om.nl/documenten/publicaties/om-onderdelen/pag-om/map/position-paper-de-politie-van-morgen-en-overmorgen

106 Neem hierin ook de Digital Services Act package van de Europese Commissie mee in overweging.

107 https://www.internetconsultatie.nl/autoriteitkp

108 https://www.rijksoverheid.nl/actueel/nieuws/2021/02/16/ict-bedrijven-verplicht-online-kinderporno-te-verwijderen-van-servers

109 Het structureel benodigde bedrag voor data-gedreven werken is niet de genoemde € 33,7 miljoen van 2024 maar € 42,4 miljoen omdat de investering na aankomende kabinetsperiode nog blijft stijgen.

Baten van de aanvullende adviezen

Inzichtelijker maken van cybercrime

Het inzichtelijker maken van cybercrime maakt het mogelijk om te bepalen waar ingegrepen moeten en welke middelen hiervoor het meest gerechtvaardigd zijn. Hierdoor wordt het mogelijk om de handhavingsketen effectiever in te richten en het gat tussen de criminele flexibiliteit tegenover de handhavingseffectiviteit te verkleinen. Door daarnaast te investeren in de kennis en het bewustzijn van de samenleving wordt ook de kwetsbaarheid gereduceerd. Deze maatregelen dragen beide bij aan het reduceren van cybercriminaliteit en verhoogd de kosteneffectiviteit van handhaving.

Structureel investeren in de aanpak van cybercrime

Door structureel te investeren in preventie, opsporing en vervolging op zowel publiek als privaat vlak, wordt het absorptievermogen en daarmee de pakkans van criminelen vergroot. Dit maakt criminaliteit onaantrekkelijker, zal de impact hiervan op de Nederlandse samenleving reduceren, en kan het vertrouwen van burgers in technologie en rechtstaat laten toenemen.

Kosten van de aanvullende adviezen

De geschatte investeringen voor de periode 2021-2024 voor de aanvullende adviezen om cybercrime tegen te gaan door OM, Politie en KMar zijn opgenomen in de volgende tabel. De onderbouwing van de inschatting wordt daaronder verder uiteengezet.

Advies	2021	2022	2023	2024 (structureel)	Eenmalige investering (2021-2024)	Totaal (2021-2024)
Zet monitor met publieke en private informatie op die een volledig beeld van cybercrime biedt	€ 1.000.000	€ 1.500.000	€ 2.000.000	€ 2.000.000	-	€ 6.500.000
Stimuleer bedrijven en particulieren om melding en aangifte te doen van cybercrime	-	-	-	-	€ 5.000.000	€ 5.000.000
Breng bestaande initiatieven samen in een entiteit die burger en samenleving handelings-perspectieven biedt	€ 400.000	€ 600.000	€ 750.000	€ 750.000	-	€ 2.500.000
Investeer in de slagkracht van het Openbaar Ministerie	€ 3.050.000	€ 6.500.000	€ 10.650.000	€ 14.400.000	-	€ 34.600.000
Investeer in instrumentatie en digitale vaardigheden van de politie	€ 4.100.000	€ 27.200.000	€ 36.100.000	€ 40.900.000	-	€ 108.300.000
Investeer in data-gedreven werken van de politie	€ 4.200.000	€ 25.500.000	€ 31.700.000	€ 33.700.000 [109]	-	€ 95.100.000
Investeer in instrumentatie en digitale vaardigheden van de KMar	€ 3.760.000	€ 7.026.000	€ 7.246.000	€ 10.240.000		€ 28.272.000
Investeer in data-gedreven werken van de KMar	€ 5.250.000	€6.000.000	€ 6.000.000	€ 6.000.000	€ 5.000.000	€ 28.250.000
Verdubbel de investering in initiatieven die (potentiële) cybercriminelen helpen te ontsnappen uit criminaliteit	-	-	-	-	€ 20.000.000	€ 20.000.000
Herzie en herformuleer de wettelijke rol van hostingbedrijven met betrekking tot onrechtmatige en strafbare content	€ 450.000	€ 450.000	-	-	-	€ 900.000
Structurele, eenmalige en totale investeringen komende kabinetsperiode (2021-2024)				**€ 107.990.000**	**€ 30.000.000**	**€ 329.422.000**

Zet monitor met publieke en private informatie op die een volledig beeld van cybercrime biedt

Als voorbeeld van een dergelijk monitor kan worden gekeken naar EOKM voor kindermisbruik. Hiervoor wordt momenteel € 800.000 per jaar voor uitgetrokken. Om een dergelijke monitor voor een breder scala aan cybercrime gerelateerde onderwerpen te gebruiken, zal grofweg een investering nodig zijn die tussen 2-3 keer groter is. Uitgaande van een schaalvergroting van 2,5 is er structureel € 2 miljoen euro per jaar nodig.

Stimuleer bedrijven en particulieren om melding en aangifte te doen van cybercrime

Een manier om dit te stimuleren is met een informatiecampagne om mensen en bedrijven te wijzen op het belang en het gemak van melding en aangifte doen en hoe het proces verloopt en wordt afgehandeld. Volgens de Jaarevaluatie Campagnes Rijksoverheid 2019 kost een gemiddelde campagne ongeveer € 1 miljoen. Er wordt ervan uitgegaan dat dit een continue activiteit is en dat er ook coördinerende ondersteuning nodig is.

Breng bestaande initiatieven samen in een entiteit die burger en samenleving handelingsperspectief biedt

Voor het samenbrengen van bestaande initiatieven om bedrijven en burgers handelingsperspectief te geven is met name uitvoerende capaciteit nodig om ideeën en instantie samen te brengen en de uitvoering procesmatige te ondersteunen. Aangenomen dat hier een minimaal team van 5 fte voor nodig is.

Investeer in de slagkracht van het Openbaar Ministerie

Het Openbaar Ministerie vraagt voor deze vergroting van de capaciteit € 34,6 miljoen voor de aankomende vier jaar. Dit bedrag wordt stapsgewijs opgebouwd, van € 3,05 miljoen in het eerste jaar naar € 14,4 miljoen in het vierde jaar. Dit wordt gedaan om te borgen dat de organisatie mee kan groeien met de investeringen, en de investeringen goed benut worden. Vanaf 2025 is de structurele vraag € 14,4 miljoen per jaar.

Investeer in instrumentatie en digitale vaardigheden van de politie

De politie vraagt € 108,3 miljoen voor de aankomende vier jaar voor het instrumenteren en digitaal vaardig maken van de organisatie voor de aanpak van cybercrime. Dit bedrag wordt stapsgewijs opgebouwd, van € 4,1 miljoen in het eerste jaar naar € 40,9 miljoen in 2024. Vanaf 2025 wordt structureel € 40,9 miljoen gevraagd. Dit wordt gedaan om te borgen dat de organisatie mee kan groeien met de investeringen en dat de investeringen goed benut worden.

Investeren in data-gedreven werken van de politie

De politie vraagt € 95,1 miljoen voor de aankomende vier jaar voor de investering in data-gedreven werken van de organisatie voor de aanpak van cybercrime. Dit bedrag wordt stapsgewijs opgebouwd, van € 4,2 miljoen in het eerste jaar naar € 33,7 miljoen in het vierde jaar. Dit wordt gedaan om te borgen dat de organisatie mee kan groeien met de investeringen en dat de investeringen goed benut worden. Vanaf 2025 zijn de benodigde investeringen structureel € 42,2 miljoen per jaar. Dit valt echter buiten de scope van dit adviesrapport. De gemiddelde investering ligt de aankomende kabinetsperiode daarom lager dan de structurele investering na de aankomende kabinetsperiode.

Investeer in instrumentatie en digitale vaardigheden van de KMar

De KMar vraagt € 28,27 miljoen voor de aankomende vier jaar voor het instrumenteren en digitaal vaardig maken van de organisatie voor de aanpak van cybercrime. Dit bedrag wordt stapsgewijs opgebouwd, van € 3,76 miljoen in het eerste jaar naar € 10,24 miljoen in 2024. Vanaf 2025 wordt structureel € 10,24 miljoen gevraagd. Dit wordt gedaan om te borgen dat de organisatie mee kan groeien met de investeringen en dat de investeringen goed benut worden.

Investeren in data-gedreven werken van de KMar

De KMar vraagt € 28,25 miljoen voor de aankomende vier jaar voor de investering in data-gedreven werken van de organisatie voor de aanpak van cybercrime. Dit bedrag wordt stapsgewijs opgebouwd, van € 5,25 miljoen in het eerste jaar naar € 6 miljoen in het vierde jaar. Tevens is er een eenmalige investering van € 5,0 miljoen hiervoor begroot. Er is gekozen voor een stapsgewijze opbouw om te borgen dat de organisatie mee kan groeien met de investeringen, en de investeringen goed benut worden. Vanaf 2025 zijn de benodigde investeringen structureel € 6 miljoen per jaar. Dit valt echter buiten de scope van dit adviesrapport. De gemiddelde investering ligt de aankomende kabinetsperiode daarom lager dan de structurele investering na de aankomende kabinetsperiode.

Uitbreiden van investeringen in initiatieven die (potentiële) cybercriminelen helpen te ontsnappen uit criminaliteit

De raad schat in dat voor een kabinetsperiode van vier jaar een eenmalige investering van € 20 miljoen is vereist om een kenniscentrum te kunnen opzetten en uitbouwen. Er wordt geschat dat hiervan € 5 miljoen benut kan worden voor een jaarlijkse voorlichtingscampagne om de aantrekkingskracht van cybercrime tegen te gaan, en € 5 miljoen als fonds voor onderzoek naar preventie van cybercrime. Daarnaast wordt € 10 miljoen geschat voor ongeveer 16 fte die onderzoeks-partnerschappen op gaan zetten en uit gaan breiden, en praktische initiatieven als Hack_Right opzetten om (potentiële) cybercriminelen te helpen te ontsnappen uit criminaliteit.

Herzie en herformuleer de wettelijke rol van hostingbedrijven met betrekking tot onrechtmatige en strafbare content

Voor het herzien en herformuleren van de wettelijke rol van hostingbedrijven wordt aangenomen dat 3 fte nodig zijn voor een periode van twee jaar.

Foto: Jeroen de Bakker

SPEERPUNT 5

ZORGPLICHT VAN LEVERANCIERS VOOR VEILIGE PRODUCTEN EN DIENSTEN VOOR BURGERS, BEDRIJFSLEVEN EN OVERHEID

Introductie en huidige staat

Bij het gebruik van digitale producten en diensten worden burgers en het mkb vaak (zonder hun weten) aan cyberonveiligheid blootgesteld; digitale producten en diensten zijn namelijk vaak onvoldoende beveiligd[110]. Veiligheid van afgenomen digitale producten en diensten moet vaak nog door oplettende gebruikers zelf afgedwongen worden, ofwel door eigen onderzoek naar veilige producten, ofwel door het actief integreren van cyberveiligheid in inkoop- en contractenmanagement. De cyberveiligheid van digitale producten en diensten zou echter een gegeven zijn, en om dit te realiseren moeten er meer handvatten zijn om leveranciers te dwingen minimale cybersecurity te borgen in hun producten en diensten. Op dit moment is dat niet het geval. Door het invoeren van een wettelijke zorgplicht worden leveranciers aansprakelijk voor de gevolgen van onveilige digitale producten en diensten. In samenwerking met effectief toezicht op naleving en burgers en het mkb beter in staat stellen veilige producten te selecteren, is dit een belangrijke stap om Nederland 'by design' cyberveiliger te maken en om onveilige producten en diensten van de markt te halen. Deze maatregelen zullen zorgen voor de vergroting van handelingsbekwaamheid wat op den duur weer resulteert in meer veiligheid en veiligheidsgevoel bij zowel burger als het mkb. Ook haalt het veel druk van overheidsactoren af en zal met het gebruik van veilige digitale producten en diensten de zelfredzaamheid en weerbaarheid van de gehele Nederlandse economie worden versterkt. De twee onderstaande paragrafen lichten toe welke initiatieven er momenteel binnen dit domein lopen.

110 Roadmap Digitaal Veilige Hard- en Software, Ministerie van Economische Zaken en Klimaat & Ministerie van Justitie en Veiligheid (2018)

Zorgplicht voor cybersecurity van hard- en software

Nederland maakt zich in de Europese Unie sterk voor het stellen van wettelijke minimum digitale veiligheidseisen aan IoT-apparaten via de Europese richtlijn voor radioapparatuur (de Radio Equipment Directive, RED)[111]. Op termijn gaan die gelden voor alle IoT-apparaten in de Europese markt. Producten die niet aan de minimumeisen voldoen, kunnen dan van de markt geweerd en gehaald worden. Op dit gebied is in 2019 ook de Europese Cyber Security Act in werking getreden[112]. Dit vormt een raamwerk voor certificering van ICT-producten, waarvan certificering van clouddiensten nu uitgewerkt wordt. Het moet nog duidelijk worden hoe effectief dit zal zijn. Daarnaast is een onderdeel van de cybersecuritystrategie van de Europese Commissie het beter beveiligen van alle IoT-producten op de Europese markt, o.a. met de zorgplicht[113].

Voor de bescherming van al gekochte digitale producten en diensten is in 2020 een Europese richtlijn aangenomen waarin een verplicht updateregime voor digitale inhoud en tastbare goederen is ondergebracht[114]. Er wordt onderzocht met de Autoriteit Consument en Markt (ACM), Autoriteit Persoonsgegevens (AP), en Nederlandse Voedsel- en Warenautoriteit (NVWA) in welke mate zij voldoende geëquipeerd zijn om toezicht te houden op dit beleid. Daarnaast ontwikkelt de overheid in samenwerking met diverse private partijen een lijst met cybersecurity-eisen die bedrijven kunnen stellen aan dienstverleners, de ICO-Wizard. Deze is voor een groot deel afgerond en online beschikbaar gesteld[115].

Hoewel dit belangrijke initiatieven zijn, hebben ze nog niet geleid tot een sluitend mechanisme van verantwoordelijkheid voor veilige hard- en software in zowel de Europese Unie[116] als Nederland; momenteel hanteren verschillende Europese Unie lidstaten hun eigen wetgeving rondom de voorgenoemde zorgplicht. Er zijn daarom nog verbeterpunten mogelijk.

Daarbij moet rekening gehouden worden dat zorgplicht in toenemende mate van landsbelang wordt daar waar er een enorme toename is van maatschappelijke en economische afhankelijkheid van digitale producten, zoals Internet of Things verbonden met kritische clouddiensten in de productie, levering en gebruik van vaccins en medische apparatuur. Bijvoorbeeld in het kader van coherent Cloud-beleid zal voor bepaalde sectoren een zorgplicht of op z'n minst een zorgverantwoordelijkheid verwacht worden, zoals voor logistiek en gezondheid. Het politieke belang maakt duidelijk dat Nederland dit onder eigen beheer moet houden.

Ondersteuning van burgers en het mkb bij cyberveilig gedrag

Er zijn meerdere campagnes opgezet om burgers en het mkb beter bewust te maken van cybersecurityrisico's. Specifieke aandacht gaat hierbij naar het bieden van handelingsperspectieven. Zo zijn er in 2019 in een samenwerking van meerdere ministeries onder andere een publiekscampagne uitgevoerd op het vlak van phishing, een campagne over veiligheid van IoT-apparaten, en bewustzijn van online risico's[117]. In 2020 is de campagne 'Doe je updates' gestart die burgers op het risico van onveilige IoT-apparatuur wijst[118].

Sinds 2019 wordt gewerkt aan de monitor waar besmette IoT-apparaten gedeeld kunnen worden[119]. Langs twee sporen wordt opvolging gegeven aan de resultaten. Het DTC gaat in gesprek met fabrikanten en andere stakeholders over kortetermijnmaatregelen die zij kunnen nemen om besmette apparaten veilig te maken. Door besmettingsinformatie over apparaten te delen met Abuse Information Exchange kunnen internetaanbieders klanten ondersteunen bij het opruimen van besmette IoT-apparaten.

111 Kamerbrief Voortgang integrale aanpak van cybercrime, Ministerie van Justitie en Veiligheid (2020)
112 Kamerbrief Voortgang Digitaal Veilige Hard- en Software, Ministerie van Economische Zaken en Klimaat (2019)
113 Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade, European Commission, 2020
114 Kamerbrief Voortgang Roadmap Digitaal Veilige Hard- en Software, Ministerie van Economische Zaken en Klimaat (2019).
115 Kamerbrief Voortgang Digitaal Veilige Hard- en Software, Ministerie van Economische Zaken en Klimaat (2019)
116 Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, ENISA (2017).
117 Kamerbrief Voortgang Digitaal Veilige Hard- en Software, Ministerie van Economische Zaken en Klimaat (2019)
118 Nederlander laat digitale voordeur wagenwijd openstaan, Website Rijksoverheid (https://www.rijksoverheid.nl/actueel/nieuws/2020/02/04/nederlander-laat-digitale-voordeur-wagenwijd-openstaan), 2020
119 Nederlander laat digitale voordeur wagenwijd openstaan, Website Rijksoverheid (https://www.rijksoverheid.nl/actueel/nieuws/2020/02/04/nederlander-laat-digitale-voordeur-wagenwijd-openstaan), 2020

Tot slot heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties de eerste stap gezet richting de coördinatie en facilitering met betrekking tot de ontwikkeling van een universeel digitale authenticatievorm in Nederland; in 2020 is een onafhankelijke strategisch-juridisch adviesbureau ingeschakeld om een strategische visie Plan van Aanpak voor een geïntegreerd eID-stelsel uit te brengen[120].

Hoewel er goede stappen worden gezet om burgers en het mkb handvatten te bieden voor cyberveilig gedrag is dit een ambitieus doel dat doorlopende investeringen vereist, om het grote publiek te bereiken en gedragsverandering te realiseren.

Standpunten en eerdere adviezen van de raad

Voor veel gebruikers is het lastig om veilige van onveilige producten te onderscheiden. Vanuit de markt lijkt er onvoldoende druk te zijn om veilige producten en diensten te leveren. Daarom vindt de raad dat leveranciers verantwoordelijk gehouden moeten worden voor de veiligheid van hun producten, en dat hier effectief op gehandhaafd moet kunnen worden. Vandaar dat de raad in het verleden al heeft geadviseerd om onder andere de zorgplicht van leveranciers voor de cybersecurity van hun hard- en software verder uit te werken. Echter, gezien het feit dat de meeste hard- en softwareleveranciers niet in Nederland zijn gevestigd, is het van groot belang om deze zorgplicht op EU-niveau te agenderen en harmoniseren. Daarbij moet op EU-niveau ook gekeken worden naar wetgeving om veiligheid van hard- en software beter in te passen in het (bestaande) regime van productaansprakelijkheid (inclusief bestaande zorgplichten), waardoor fabrikanten wettelijk aansprakelijk gehouden kunnen worden voor economische schade als gevolg van kwetsbaarheden in het product[121]. In het verlengde hiervan moet geïdentificeerd worden welke bestaande Nederlandse en Europese toezichthouders fabrikanten kunnen aanspreken op basale veiligheidsproblemen in hun producten.

Daarnaast is een compleet effectieve en sluitende wettelijke zorgplicht voor leveranciers complex en waarschijnlijk niet compleet realiseerbaar op korte termijn. Om die reden vindt de raad dat de gebruiker simultaan moet worden ondersteund bij het maken van keuzes tussen veilige en onveilige producten, en bij het verwijderen van eerder aangeschafte producten die onveilig blijken te zijn. De raad heeft in het verleden dan ook geadviseerd om door middel van voorlichtingscampagnes gebruikers bij het inkopen van veilige middelen te stimuleren (zoals veilige authenticatie-oplossingen)[122].

Aanvullende adviezen van de raad

Zorgplicht voor cybersecurity van hard- en software

Een EU-brede aanpak is noodzakelijk om de zorgplicht effectief door te voeren en ervoor te zorgen dat de plicht op zoveel mogelijk leveranciers van toepassing is. Er moeten dan ook vanuit de Europese Unie richtlijnen ingevoerd worden die leveranciers van digitale producten en diensten aan burgers (B2C) en bedrijven (B2B) in Nederland (en andere Europese lidstaten) meer verantwoordelijk houdt voor economische schade als gevolg van het verzaken van zorgplicht op het vlak van cybersecurity. Hierbij is het noodzakelijk om de zorgplicht goed te omschrijven en de aansprakelijkheid van leveranciers duidelijk te formuleren, bijvoorbeeld door deze bij contracten te verbinden aan een bewijs van cybersecurityvolwassenheid. Zowel tijdens het formuleren als bij het invoeren van de zorgplicht zal moeten worden gekeken naar de handhaafbaarheid hiervan en zal actief moeten worden gezocht naar internationale samenwerking (met onder andere leveranciers van buiten de Europese Unie).

Het invoeren van wetgeving met betrekking tot de zorgplicht is belangrijk voor B2C omdat burgers weinig invloed hebben op de beveiliging van een product en de beveiliging niet zelf kunnen laten aanpassen. De fabrikant is hier vaak de ‘cheapest cost avoider’, degene die tegen de laagste kosten schade ten gevolge van cyberonveiligheid kan voorkomen.

120 Strategische visie Plan van Aanpak geïntegreerd eID-stelsel – Definitied rapport, Hooghiemstra & Partners (2020)

121 Zie bijlage 2 voor buitenlandse voorbeelden cybersecuritywetgeving en toezicht.

122 Dit kan onder andere door middel van het invoeren van een labeling-systeem van producten (waarbij per product een aantal indicatoren wordt genoemd over de cybersecurity van het product), of met een monitor van gehackte en kwetsbare IoT-apparaten (zo kan publieke informatie gedeeld worden over welke fabrikanten en leveranciers hun apparaten onvoldoende beveiligen)

Daarnaast resulteert cybercrime (dat door onveilige hard- en software wordt gefaciliteerd) ook vaak in substantiële economische schade voor het mkb. Voor het borgen van de zorgplicht in B2B-relaties in de huidige aansprakelijkheidspraktijk[123], is het van belang om te kijken naar een oplossing die goed bestand is tegen de snel veranderende dynamiek in cybersecurity. Europese wetgeving is niet zinvol omdat het snel verouderd zal zijn, en de contractvrijheid te veel inperkt. De oplossing kan een set aan Europese cybersecurityrichtlijnen zijn die in goed overleg door branches zelf via co-regulering een *default* zorgplicht van hard- en softwareleveranciers wordt.

Dit werkt op de volgende manier: branches (bijvoorbeeld de branche voor cybersecurityleveranciers, maar ook een branche die gebruikers vertegenwoordigd) en wetenschappelijke experts stellen cybersecurityrichtlijnen op die gelden als een standaard zorgplicht in een B2B-contract. Deze richtlijnen bevatten regels over preventie, detectie en response bij incidenten die gelden als een cybersecuritydienstverlener een product of dienst verkoopt[124]. Deze kunnen dan bijvoorbeeld in een contract tussen een administratiekantoor en een cybersecuritydienstverlener over de IT-beveiliging worden benut. Het is van groot belang dat de richtlijnen enerzijds door experts in partnerschap worden ontwikkeld en *state of the art* zijn, en dat ze tegelijk ook dynamisch zijn en de laatste nieuwe ontwikkelingen steeds volgen. Dit systeem van co-regulering sluit aan bij de huidige ontwikkelingen om via publiek-private samenwerking best practices/handreikingen te ontwikkelen om leverancier en afnemer te ondersteunen bij het opstellen van afspraken. Deze best practices en handreikingen kunnen namelijk input zijn voor het opstellen van de standaarden waaraan bedrijven zich in de nieuwe dynamische standaard zorgplicht moeten voldoen mits ze niet iets anders afspreken.

Aansluitend op dit (contractuele en zelfregulerings-) systeem en de harde wetgeving op het gebied van B2C moet er een goed werkend verzekeringssysteem gestimuleerd worden voor zowel gebruiker (in het kader van B2B) als leverancier (B2C en B2B). Hierbij is de aanname dat de voorgenoemde Europese wetgeving zal leiden tot verhoging van de aansprakelijkheid van leveranciers met betrekking tot het leveren van veilige digitale producten en diensten – dit zou kunnen resulteren in een toename in leveranciers die zich willen verzekeren in het geval zij mogelijk de zorgplicht schenden. Voorwaarde daarvoor is wel dat er behoorlijk wat spelers op de markt zijn die ook bereid zijn het product aan te bieden en dat er ook een redelijk concurrerende verzekeringsmarkt zou dienen te zijn. Ook is van belang dat verzekeraars over diepgaande cybersecurity kennis moeten beschikken om de verplichtingen van leveranciers te kunnen toetsen. Dat betekent in het ideale geval:

- De verzekeraar legt ten aanzien van zowel gebruikers als leveranciers die hij verzekert (verzekeringnemer) bepaalde plichten op met het oog op preventie, detectie en respons van cybersecurity. Dit zal bijdragen aan het leveren van veilige digitale producten en diensten en het daadwerkelijk benutten van de richtlijnen voor de zorgplicht in de praktijk.
- Vervult de verzekeraar zijn rol goed, dan kan verzekering dus aan toenemende bewustwording bijdragen en een optimale preventie, detectie en response bevorderen.

Dit zal ertoe leiden dat meer veilige hard- en software op de markt wordt geïntroduceerd, waardoor de kans dat burgers met onveilige hard- en software in aanraking komen en slachtoffer worden van cybercrime-en aanvallen wordt gereduceerd.

Het moet internationale aanbieders daarnaast onmogelijk gemaakt worden onveilige apparaten in de Europese Unie (en daarmee Nederland) te verkopen of te leveren. Internationale wetgeving die dit aanpakt moet gestimuleerd worden, zoals investeren in de uitbreiding van het Radio Equipment Directive naar IoT-apparaten.

Op nationale en internationale wetgeving op het vlak van veilige hard- en software moet toezicht gehouden worden door een nationale toezichthouder. Voor een onderdeel daarvan, een verplicht updateregime, wordt al onderzocht of dit bij AP, ACM of NVWA kan. Er moet uitgezocht worden waar het mogelijk is om in brede zin het toezicht op wetgeving op het vlak van veilige hard- en software belegd kan worden, en er moet geïnvesteerd worden in deze toezichthouder om te borgen dat dit op effectieve wijze ingevuld kan worden. De investering in de toezichthouder moet periodiek geëvalueerd worden op basis van aanpassingen in nationale en internationale wetgeving (die om een toename van capaciteit kunnen vragen).

123 Aansprakelijkheid voor digitale onveiligheid in b2b-relaties, Centre for the Law and Economics of Cyber Security (2020)

124 Men kan ook denken aan subsets van regels voor verschillende type contracten, om fijnmaziger te werk te gaan.

Ondersteuning van burgers en het mkb bij cyberveilig gedrag

Ten eerste moet meer geïnvesteerd worden in bewustwordingscampagnes om burgers en het MKB te overtuigen van het belang van het kopen van veilige producten. Denk hierbij aan het op Europees niveau invoeren van het labeling-systeem waarbij van elk digitaal product, of product dat aangesloten kan worden op het internet, op het label is aangegeven hoe veilig het is.

Ten tweede moet een collectief arrangement worden gerealiseerd waarbij gebruikers van onveilige producten en diensten in staat worden gesteld om collectief actie te ondernemen tegen leveranciers die de zorgplicht hebben geschonden. Hier kan bijvoorbeeld gebruik worden gemaakt van bestaande wetten en organisaties die opkomen voor de belangen van Nederlandse consumenten[125]. Het is sinds 1 januari 2020 met de Wet afwikkeling massaschade in collectieve actie (WAMCA) namelijk mogelijk om collectief naar de rechter te stappen voor schadevergoeding bij massaschade[126]. Er moet onderzocht worden in welke mate de WAMCA geschikt is om massaschade volgend uit onveilige hard- en software aan te pakken.

Baten van de aanvullende adviezen

Instellen van een zorgplicht voor cybersecurity van hard- en software

Het op EU-niveau verplicht stellen van leveranciers om veilige producten en diensten te leveren leidt ertoe dat onveilige producten en diensten de toegang tot de Nederlandse markt wordt geweigerd. Hierdoor worden gebruikers vanaf het moment van aankoop minder blootgesteld aan kwetsbaarheden die uitgebuit kunnen worden door cybercriminelen, wat resulteert in een hoger veiligheidsgevoel onder gebruikers en verlaging van de druk op de bestrijding van cybercrime, wat bijdraagt aan de cyberweerbaarheid van Nederland. Ook kan de zorgplicht innovatie van veilige hard- en software in de EU in de hand werken, wat ons minder afhankelijk maakt van (onveilige) hard- en software van buiten de EU, en zo bij kan dragen aan de digitale autonomie van de EU.

Ondersteunen van burgers en het mkb bij cyberveilig gedrag

Het ondersteunen van burgers en het mkb bij het uitvoeren van cyberveilig gedrag zal zowel het bewustzijn als handelingsbekwaamheid van de Nederlandse samenleving op het gebied van onveilige digitale producten en diensten laten toenemen, wat leidt tot de verlaging van kwetsbaarheid voor cybercrime. Ook dit zal bijdragen aan het veiligheidsgevoel van gebruikers en de nationale cyberweerbaarheid.

Kosten van de aanvullende adviezen

De geschatte investeringen voor de periode 2021-2024 om de aanvullende adviezen te realiseren zijn opgenomen in de volgende tabel. De onderbouwing van de inschatting wordt daaronder verder uiteengezet.

125 Denk bijvoorbeeld aan de Consumentenbond.

126 https://www.rijksoverheid.nl/actueel/nieuws/2019/12/12/collectief-naar-rechter-voor-schadevergoeding-bij-massaschade

Advies	2021	2022	2023	2024 (structureel)	Eenmalige investering (2021-2024)	Totaal (2021-2024)
Voer op EU-niveau richtlijnen in die leveranciers verantwoordelijk houden voor economische schade als gevolg van onveilige producten	€ 380.000	€ 560.000	€ 750.000	€ 750.000	-	**€ 2.400.000**
Beleg toezicht op wetgeving bij een bestaande toezichthouder	€ 1.500.000	€ 2.250.000	€ 3.000.000	€ 3.000.000	€ 1.000.000	**€ 10.750.000**
Stimuleer het cyberverzekerings-systeem om aan te sluiten op innovatieve co-regulering	€ 1.900.000	€ 2.800.000	€ 3.750.000	€ 3.750.000	-	**€ 12.200.000**
Investeer in jaarlijkse grote bewustwordingscampagnes die burgers overtuigen van het belang van veilige producten	-	-	-	-	€ 5.000.000	**€ 5.000.000**
Voer het labeling-systeem in waarbij van elk digitaal product, of product dat aangesloten kan worden op het internet, op een label aangegeven is hoe veilig het is	€ 150.000	€ 300.000	€ 300.000	€ 300.000	-	**€ 1.050.000**
Realiseer een collectief arrangement dat het mogelijk maakt om naar de rechter te stappen voor schade-vergoeding bij massaschade door onveilige producten en diensten	€ 450.000	€ 450.000	-	-	-	**€ 900.000**
Structurele, eenmalige en totale investeringen komende kabinetsperiode (2021-2024)				**€ 7.800.000**	**€ 6.000.000**	**€ 32.340.000**

Voer op EU-niveau richtlijnen in die leveranciers verantwoordelijk houdt voor economische schade als gevolg van onveilige producten

Hier zal op EU-niveau samengewerkt moeten worden om effectieve invloed op grote producenten en leveranciers te hebben, en om zorgplicht toezicht op EU-niveau te beleggen. Nederland zal zich hiervoor moeten inzetten, waarvoor eenmalige voor vier jaar een team van minimaal 5 fte.

Beleg toezicht op wetgeving bij een bestaande toezichthouder

Voor het beleggen van toezicht op wetgeving op het vlak van veilige hard- en software wordt aangenomen dat de belasting voor de toezichthouder vergelijkbaar is met de investeringen in toezichthouders in het kader van de Wbni. Dit betekent een structurele jaarlijkse investering van € 3 miljoen voor de toezichthouder, en een eenmalige investering van € 1 miljoen om de toezichtsfunctie op te starten.

Stimuleer het cyberverzekeringssysteem om aan te sluiten op innovatieve co-regulering

Voor het realiseren van adviezen 3 en 4 kan een actie- en kenniscentrum[127] worden opgericht dat branches (zoals de cybersecuritybranche en verzekeringsbranche) en experts verenigt voor het stimuleren van het co-reguleringssysteem; hier ontwikkelen zij in samenspraak dynamische zorgplicht-richtlijnen. Daarnaast kan dit centrum met deze richtlijnen ook de cyberverzekeringsmarkt verder helpen ontwikkelen, door bijvoorbeeld verzekeraars te stimuleren om bij toetreding van nieuwe verzekerden hen verplicht te stellen om deze richtlijnen op te volgen. De schatting is dat dit team uit minimaal 25 fte moet bestaan.

127 Dit zou bijvoorbeeld bij het Ministerie van Economische Zaken en Klimaat kunnen worden ondergebracht.

Investeer in jaarlijkse grote bewustwordingscampagnes die burgers overtuigen van het belang van veilige producten

Een manier om dit te stimuleren is met een informatiecampagne om mensen en bedrijven te wijzen op het belang en de mogelijkheden. Volgens de Jaarevaluatie Campagnes Rijksoverheid 2019 kost een gemiddelde campagne ongeveer € 1 miljoen. Ervan uit gaande dat dit een continue activiteit is en er ook coördinerende ondersteuning nodig is, wordt uitgegaan van € 5 miljoen voor een periode van vier jaar.

Voer een labeling-systeem in waarbij elk digitaal product, of product dat aangesloten kan worden op het internet, op een label aangeeft hoe veilig het is

Dit vereist voornamelijk inzet op Europees niveau om te zorgen dat ook grote producenten gebonden worden aan dit systeem. Hiervoor zijn voornamelijk eigenaarschap en daadkracht nodig om dit te realiseren. Daarnaast zal naar de praktische implementatie gekeken moeten worden over de criteria voor de labels en de controle daarop, maar deze kosten worden pas relevant na de invoeren van dergelijke wetgeving, wat meerdere jaren in beslag zal nemen. Nederland zal zich hiervoor moeten inzetten, met een team van minimaal 2 fte gedurende vier jaar.

Realiseer een collectief arrangement dat het mogelijk maakt om naar de rechter te stappen voor schadevergoeding bij massaschade door onveilige producten en diensten

Het collectief arrangement kan mogelijk worden gerealiseerd door gebruik te maken van bestaande wetgeving als de WAMCA. Aangenomen dat hier met name een investering nodig is in de uitvoerende capaciteit met een minimaal team van 3 fte's voor een periode van twee jaar.

Foto: Jeroen de Bakker

BIJLAGE 1

OVERZICHT CYBERWEERBAARHEID STAKEHOLDERVELD

In onderstaand overzicht zijn partijen opgenomen die een bijdrage leveren aan de cyberweerbaarheid van Nederland. De partijen in de landschapskaart zijn geïdentificeerd op basis van bestaande overzichten, aangevuld met de kennis en ervaring van het Deloitte projectteam. Naast het identificeren van belangrijke Nederlandse spelers op het gebied van cyberweerbaarheid, maakt deze kaart ook inzichtelijk dat dit landschap versnipperd is en de structurele regie op samenwerking ontbreekt. Dit overzicht is geen uitputtende lijst maar geeft hoog-over een overzicht van de belangrijkste stakeholders.

	Rijksoverheid	Bedrijfsleven	Wetenschap
Regie op samenwerking en informatie-deling	• Ministerie van Justitie en Veiligheid (incl. Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)/Nationaal Cyber Security Centrum (NCSC)) • Ministerie van Defensie (incl. Militaire Inlichtingen- en Veiligheidsdienst (MIVD)) • Ministerie van Economische Zaken en Klimaat (incl. Digital Trust Center (DTC)) • Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (incl. Algemene Inlichtingen- en Veiligheidsdienst (AIVD)) • Ministerie van Infrastructuur en Waterstaat • Nationale Politie • Koninklijke Marechaussee	• Cyberveilig Nederland • VNO-NCW	• Erasmus Universiteit Rotterdam: Centre for the Law and Economics of Cyber Security • Tilburg University: Tilburg Institute for Law, Technology, and Society • Universiteit van Amsterdam: Instituut voor Informatierecht (IViR) • Universiteit Leiden: Cybersecurity Governance
Weerbare vitale processen	• Ministerie van Justitie en Veiligheid (incl. Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)/Nationaal Cyber Security Centrum (NCSC) • Ministerie van Infrastructuur en Waterstaat • Ministerie van Economische Zaken en Klimaat • Ministerie van Financiën • ICT Response Board • Ministerie van Defensie (Militaire Inlichtingen- en Veiligheidsdienst (MIVD))/Algemene Inlichtingen- en Veiligheidsdienst (AIVD) • Stichting Digitale Infrastructuur Nederland (DINL)	• Cyberveilig Nederland • Organisatie CERT's	• Eindhoven University of Technology: security and embedded networked systems groep

	Rijksoverheid	Bedrijfsleven	Wetenschap
Versterken van onderzoek en onderwijs	• Politie • Openbaar Ministerie • Ministerie van Defensie • Ministerie van Onderwijs, Cultuur en Wetenschap (OCW) • Ministerie van Economische Zaken en Klimaat • Koninklijke Marechaussee	• Cyberveilig Nederland • TNO • Nederlandse Vereniging van Banken (NVB) • FME • NLdigital	• The Hague Centre for Strategic Studies (HCSS) • Vrije Universiteit Amsterdam: Center for law and internet & Systems Security • Maastricht University: European Centre on Privacy and Cybersecurity • Eindhoven University of Technology: coding theory and cryptography groep • Rijksuniversiteit Groningen: Information Systems Group • Radboud Universiteit: Digital Cyber Security Group
Realiseren van cybercrime handhavings-keten	• Politie • Koninklijke Marechaussee • Openbaar Ministerie • De Rechtspraak • Inspectie Leefomgeving en Transport (ILT) • De Nederlandsche Bank (DNB) • Agentschap Telecom • Autoriteit Persoonsgegevenso	• ISPConnect • ECTF Electronic Crimes Taskforce • Nederlandse Vereniging van Banken (NVB)	• Centrum Wiskunde & Informatica (CWI): Cryptologie • Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR): Cluster Cybercrime • Open Universiteit: Onderzoeksgroep security and privacy • Technische Universiteit Delft: Techniek, Bestuur en Management & faculteit elektrotechniek, wiskunde en informatica • Universiteit Twente: Design and Analysis of Communication Systems Group & Services and Cybersecurity (SCS) • Universiteit van Amsterdam: System and Networking Laboratory • Vrije Universiteit Amsterdam: Systems security
Zorgplicht veilige producten en diensten	• Ministerie van Economische Zaken en Klimaat (incl. Digital Trust Center (DTC))	• FME • Verenigde Maakindustrie Oost (VMO) • Nederlandse Vereniging van Banken (NVB) • VNO-NCW • Cyberveilig Nederland	• Erasmus Universiteit Rotterdam: Centre for the Law and Economics of Cyber Security

BIJLAGE 2

BENCHMARKONDERZOEK INTEGRALE AANPAK CYBERWEERBAARHEID

Management samenvatting

- De Nederlandse overheid investeert gemiddeld significant minder in cyberweerbaarheid dan andere landen waarmee de Nederlandse uitgaven vergelijken zijn in dit onderzoek. Zo hebben Denemarken, het Verenigd Koninkrijk en België de ambitie om respectievelijk 9%, 56%, en 1457% meer in cyberweerbaarheid te investeren dan Nederland.
- Voor Singapore is geen ambitie vastgesteld. Echter, uitgaven van de Cyber Security Agency tussen 2014 en 2018 worden 737% hoger geschat dan de Nederlandse investeringsambitie tussen 2018 en 2022. Als aangenomen wordt dat de investeringen in Singapore minimaal gelijk zijn gebleven wijst dit op een significant verschil in investeringen tussen Singapore en Nederland, voor de periode 2018-2022.
- Voor dit benchmarkonderzoek zijn specifieke cyberweerbaarheidsdomeinen onderzocht: (1) nationale cyberstrategie, (2) cybercrime & handhaving, (3) informatiedeling, (4) onderzoek & wetenschap, (5) diplomatie & handel, en (6) defensie en crisisrespons. Met uitzondering van diplomatiediplomatie en handel kan Nederland voor de overige domeinen een voorbeeld nemen aan de vergelijkingslanden en de manier waarop zij hier invulling aan geven om de nationale cyberweerbaarheid te verhogen.

1. Achtergrond benchmarkonderzoek

Om richting te geven aan de benodigde omvang van cyberweerbaarheidsinvesteringen in Nederland is onderzoek gedaan naar de omvang van de cyberweerbaarheid investeringsambitie in vergelijkbare landen (zie figuur 1 voor een overzicht van de vergelijkingslanden). Een investeringsambitie is een bedrag wat een land zich voorneemt toe te kennen aan cyberweerbaarheid, door deze bijvoorbeeld op te nemen in een nationale cyberweerbaarheidsstrategie. Dit onderzoek richt zich dus op additionele investeringen die door overheden in cyberstrategieën of regeerakkoorden zijn vastgelegd en bestemd zijn voor de verdere ontwikkeling van cyberweerbaarheid, bovenop de reguliere investeringen in cyberweerbaarheid (zie 'verantwoording scope' voor een nadere toelichting op dit besluit). In deze benchmark wordt daarnaast onderzocht waarin specifiek geïnvesteerd wordt door deze vergelijkbare landen. De benchmark is gestructureerd op basis van de categorieën uit de Cyber Readiness Index uit 2015 ('CRI'): (1) nationale cyberstrategie, (2) cybercrime & handhaving, (3) informatiedeling, (4) onderzoek & wetenschap, (5) diplomatie & handel, en (6) defensie en crisisrespons. Daarnaast is specifiek gekeken naar uitgaven binnen de verschillende CRI-categorieën. Waar data beschikbaar was, is voor vergelijkingslanden gebruikgemaakt van de bedragen die geïnvesteerd worden in een specifieke CRI-categorie. Wanneer er geen (betrouwbare) cijfers voor handen zijn, is gebruik gemaakt van kwalitatieve inzichten die zijn opgehaald tijdens het uitvoeren van deze benchmarkanalyse, inclusief bestaande benchmarks[128].

128 The Global Cybersecurity Index, EU Cybersecurity Dashboard, Cyber Readiness Index 2.0 en de Cyber Power Index.

Verantwoording scope
In deze benchmark-analyse is de totale omvang van investeringen in cyberweerbaarheid gedefinieerd als additionele ambities voor investeringen. Met andere woorden: overheidsinvesteringen die zijn uitgesproken of in cyberweerbaarheidstrategieën of regeerakkoorden zijn vastgelegd, maar nog niet daadwerkelijk zijn gedaan. Ook zijn additionele investeringen bestemd voor de verdere *ontwikkeling van cyberweerbaarheid bovenop de reguliere overheidsuitgaven aan cyberweerbaarheid. Deze keuze komt voort uit de observatie dat reguliere cyberweerbaarheidsinvesteringen voor zowel Nederland als de vergelijkingslanden slechts gedeeltelijk of vaak niet te achterhalen zijn; sommige regeringen zijn pas recentelijk begonnen met het publiceren van hun (cyberweerbaarheids-)budgetten, maken hun budget slechts deels bekend, of specificeren niet precies hoe en waarin deze bedragen geïnvesteerd worden. Om vervolgens de Nederlandse investeringen in cyberweerbaarheid op een eerlijke manier met de vergelijkingslanden te kunnen vergelijken, worden daarom enkel de ambities van investeringen met elkaar vergeleken; immers, deze bedragen zijn in cyberstrategieën en regeerakkoorden vastgelegd. Tevens onthullen ambities van investeringen ook hoe Nederland en de vergelijkingslanden cyberweerbaarheid prioriteren. In de analyse wordt niet gekeken naar investeringen in cyberweerbaarheidsmaatregelen op ICT-systemen van overheidsorganisaties zelf, zoals maatregelen als het inrichten van patch-management.*

De additionele ambities voor investeringen van Nederland zijn gemiddeld significant lager dan die van vergelijkingslanden (zie figuur 2). Daarom is onderzocht of de lagere investeringen in 2016 door Nederland verklaard kunnen worden door al gedane en hogere investeringen in eerdere jaren ten opzichte van de vergelijkingslanden. Voor dit onderzoek zijn twee bronnen geraadpleegd: de Global Cybersecurity Index (CGI) (2018) en Dutch Investments in ICT and Cybersecurity: Putting it in Perspective van The Hague Centre for Strategic Studies (2016). De CGI kent ieder land een score toe op basis van de bestaande cyberinvesteringen en -initiatieven. De CGI-scores van de vergelijkingslanden zijn relatief gelijk aan die van Nederland (zie figuur 2), wat impliceert dat de vergelijkingslanden geen cyberweerbaarheidsachterstand op Nederland hebben. Deze implicatie wordt onderschreven door het onderzoek van The Hague Centre for Strategic Studies waarin beschreven wordt dat Nederland over de periode 2014-2020 minder in cyberweerbaarheid heeft geïnvesteerd dan landen zoals Frankrijk, Denemarken en het Verenigd Koninkrijk.

2. Aanpak en beperkingen

Aanpak

Zoals eerder beschreven wordt bij het uitvoeren van de benchmarkanalyse onderzocht op welke wijze overheden investeren in zes cyberweerbaarheidscategorieën van de Cyber Readiness Index (2015). Als startpunt van de benchmarkanalyse zijn de variabelen, wegingscriteria, en selectiecriteria voor de potentiele vergelijkingslanden vastgelegd. Vervolgens heeft de raad de shortlist van vergelijkingslanden gevalideerd. Om tot een shortlist te komen van vergelijkingslanden waarop de benchmark is uitgevoerd heeft het onderzoeksteam de onderstaande stappen genomen:

1. Van de top-12 Europese landen uit de Digital Economy and Society Index[129] (DESI), toevoeging van Frankrijk op verzoek van de subcommissievergadering op 12 oktober en toevoeging van Singapore om de mogelijkheid te geven een perspectief van buiten de EU mee te nemen.
2. Eerste selectie van landen op basis van BBP per capita en/of bevolkingsomvang waardoor Malta, Estland, Luxemburg en Spanje afvallen.
3. Opstellen van een shortlist van vergelijkingslanden waarbij in aanvulling op de DESI-positie ook de samenstellingen van de economie, overheidsstructuur en BBP per capita positie zijn vermeld ter illustratie van de bredere overeenkomsten met deze landen.

129 Index van de Europese Commissie (2020) waarin connectiviteit, menselijk kapitaal, gebruik van internetdiensten, integratie van digitale technologie en digitale publieke diensten wordt gemeten

Let hierbij wel op dat uiteindelijk enkel 4 van de 9 shortlisted vergelijkingslanden met elkaar zijn vergeleken in het kader van totale investeringen in cyberweerbaarheid (zie figuur 2). De overige vergelijkingslanden zijn afgevallen vanwege een gebrek aan data.

Overzicht shortlist vergelijkingslanden.

Vergelijkings-criteria		Neder-land	Finland	Zweden	Dene-marken	Ierland	VK	België	Duitsland	Frankrijk	Singa-pore
DESI 2020 plaats		4	1	2	3	6	8	9	12	15	1[130]
Samen-stelling economie[131]	Industrie	18%	28%	33%	23%	39%	20%	22%	31%	20%	24%
	Services	70%	69%	65%	76%	60%	79%	77%	69%	79%	76%
Overheidsstructuur		Centraal	Centraal	Centraal	Centraal	Centraal	Centraal	Federaal	Federaal	Centraal	Centraal
BBP per capita positie[132]		13	21	16	12	4	24	17	15	26	2

Vervolgens zijn de variabelen deels verzameld uit vier bestaande benchmarks: *The Global Cybersecurity Index, EU Cybersecurity Dashboard, Cyber Readiness Index 2.0* en de *Cyber Power Index*. Naast deze bestaande benchmarks is ook hulp ingeschakeld van collega's van het onderzoeksteam die werkzaam zijn in de voor de benchmark geselecteerde landen – het onderzoeksteam heeft met deze lokale security- en publieke sector experts gesprekken gevoerd en de vraag gesteld of zij voor (zo ver dat mogelijk is) informatie kunnen aanleveren dat publiek beschikbaar is. Er is informatie opgevraagd met betrekking tot de partijen waarin de overheid investeert, het aantal fte dat bij deze partijen betrokken is, en de totale nationale uitgaven per categorie.

Beperkingen

Het benchmarkonderzoek kent een aantal algemene beperkingen. Ten eerste is de aangeleverde data gebaseerd op ambitie investeringen in cyberweerbaarheid, en niet de werkelijke uitgaven in cyberweerbaarheid. Ten tweede verschaffen bestaande benchmarks alleen kwalitatieve interpretaties van cyberinvesteringen, en geen financiële data. Ten derde is een deel van de opgenomen data verouderd (bijvoorbeeld de investeringen in cyberweerbaarheid die door Singapore in 2014 gedaan zijn) of onvolledig en is een deel ook simpelweg niet publiekelijk beschikbaar.

130 World Bank Digital Adoption Index (2016)

131 Central Intelligence Agency, The World Factbook, GDP – composition, by sector of origin (2017)

132 World Bank (2019)

3. Uitkomsten

Verhouding totale investeringen cyberweerbaarheid

Figuur 2. Overzicht totale investeringen in cyberweerbaarheid over een 4-jarige periode.

	Nederland(1)	Denemarken (2)	VK (3)	Singapore (4)	België (5)
Totale investeringen in cyberweerbaarheid	€ 380 miljoen (2018 tot 2022)	€ 161 miljoen (2018 tot 2022)	€ 2.06 miljard (2016 tot 2020)	€ 941.6 miljoen (2014 tot 2018)	€ 3.6 miljard (2019 tot 2023)
Bruto Binnenlands Product	€ 774,7 miljard (2018)	€ 302,5 miljard (2018)	€ 2481,0 miljard (2016)	€ 229,1 miljard (2014)	€ 476,1 miljard (2019)
Totale investeringen in cyberweerbaarheid t.o.v. BBP[133]	0,049 %	0,053 %	0,083 %	0,410 %	0,764 %
Verschil in totale investeringen cyberweerbaarheid t.o.v. BBP vergeleken met Nederland		+9 %	+56 %	+737%	+1457 %
The Global Cybersecurity Index (CGI)[134]	0.885	0.852	0.931	0.898	0.814

Nederland heeft een lagere investeringsambitie in nationale cyberweerbaarheid dan Denemarken, het Verenigd Koninkrijk, België, en Singapore: zij investeren respectievelijk 9%, 56%, 1265% en 737% meer in cyberweerbaarheid (genormaliseerd op basis van het BBP van elk land – zie Figuur 2). Het onderzoeksteam heeft voor deze vier landen betrouwbare data kunnen ophalen. Voor de andere vergelijkingslanden[135] is onvoldoende data beschikbaar om een volledig beeld te schetsen. Om tussen de vergelijkingslanden een eerlijke vergelijking uit te voeren, worden de totale investeringen in cyberweerbaarheid met elkaar vergeleken over een periode van 4 jaar.

Verantwoording gegevens Figuur 2

(1) Nederland heeft in het regeerakkoord van 2017 de ambitie voor een structurele investering van 95 miljoen euro in cybersecurity vastgelegd[136]; dit bedrag wordt vanaf het jaar 2018 in cybersecurity geïnvesteerd. Door de 95 miljoen over een periode van vier jaar bij elkaar op te tellen, kan gesteld worden dat Nederland de ambitie heeft om over de periode 2018 tot 2022 380 miljoen euro in de Nederlandse cyberweerbaarheid te investeren. Dit is 0,049 % van het Nederlandse BBP in 2018 (774,65 miljard euro[137]). Hierbij dient te worden vermeld dat in de periode 2018 tot 2021 de ambitie om jaarlijks € 95 miljoen in de Nederlandse cyberweerbaarheid te investeren niet daadwerkelijk is gerealiseerd; in de toelichting van het regeerakkoord staat vastgelegd dat deze jaren enkel respectievelijk € 3 miljoen, € 35 miljoen, en € 42 miljoen zal worden geïnvesteerd[138].

133 BBP data gebaseerd op World Bank Open Data (https://data.worldbank.org/). De bedragen (oorspronkelijk in Amerikaanse Dollars) zijn omgerekend naar euro's, waarbij gebruik is gemaakt van de gemiddelde dollar/euro wisselkoers van het éérste jaar van de gehanteerde tijdsduur per land (zie figuur 2).

134 The Global Cybersecurity Index 2018, International Telecommunication Union (ITU) Publications (2019).

135 Zie figuur 1 voor een overzicht van alle vergelijkingslanden

136 Regeerakkoord 2017: vertrouwen in de toekomst (2017). Let hierbij wel op dat dit de 95 miljoen euro een ambitie voor investering is. Dit betekent dat de daadwerkelijke uitgaven lager kunnen uitvallen (dit valt buiten scope – zie 'verantwoording scope').

137 In 2018 bedroeg het Nederlandse BBP 914.043 miljard dollar (https://data.worldbank.org/country/NL). Dit bedrag is vervolgens naar euro's omgerekend door de gemiddelde Dollar/Euro wisselkoers van 2018 te gebruiken (USD/EUR: 0,8475). Bron: https://www.exchangerates.org.uk/USD-EUR-spot-exchange-rates-history-2018.html#:~:text=This%20is%20the%20US%20Dollar,EUR%20on%2001%20Feb%202018.

138 Regeerakkoord 2017: vertrouwen in de toekomst (2017).

(2) In 2018 heeft de Deense regering een nationale cyberweerbaarheidsstrategie[139] gepubliceerd waarin wordt aangegeven dat zij de ambitie hebben om voor de periode 2018-2023[140] 1.5 miljard Deense Kronen in de Deense cyberweerbaarheid te investeren. Omdat in deze benchmarkanalyse de totale investeringen in cyberweerbaarheid over een periode van vier jaar met elkaar worden vergeleken, wordt de periode 2018 tot 2022 aangehouden voor het berekenen van de totale ambitie investeringen in de Deense cyberweerbaarheid. Dit bedrag wordt berekend door 80% van de 1.5 miljard Deense Kronen te nemen: 1.2 miljard Deense Kronen of 161 miljoen euro[141]. Dit bedrag is 0,053 % van het Deense BBP in 2018 (302,455 miljard euro[142]).

(3) De Britse regering heeft in 2016 een nationale cyberweerbaarheidsstrategie gepubliceerd waarin wordt aangegeven dat zij voor de periode 2016-2021 de ambitie hebben om 1,9 miljard Britse pond[143] in cybersecurity te investeren. Omdat in deze benchmark analyse de totale investeringen in cyberweerbaarheid over een periode van vier jaar met elkaar worden vergeleken, wordt de periode 2016 tot 2020 aangehouden voor het berekenen van de totale ambitie investeringen in de Britse cyberweerbaarheid. Vandaar dat voor deze periode enkel 80% van dit bedrag (1,52 miljard pond) voor dit onderzoek wordt gebruikt. Omgerekend naar euro's is dit een bedrag van circa 1,861 miljard euro[144]. Dit is 0,082% van het Britse BBP in 2016 (2,434 miljard euro[145]).

(4) Van Singapore is geen investeringsambitie vastgesteld. Omdat dit land zich op veel vlakken (economisch, afhankelijkheid van vitale infrastructuur) goed met Nederland laat vergelijken is toch vergelijking gemaakt. Deze vergelijking is gedaan op basis van het budget voor cybersecurity van Singapore in 2014 (408,6 miljoen Singaporese Dollars of 243,2 miljoen Euro)[146]. Voor Singapore is alleen data uit 2014 beschikbaar[147], waarbij het onderzoeksteam vervolgens de aanname heeft gemaakt dat de Singaporese overheid in de drie opvolgende jaren hetzelfde bedrag in cyberweerbaarheid heeft geïnvesteerd. Voor een periode van vier jaar wordt uitgegaan van vier keer dit bedrag (972,8 miljoen euro). Let hierbij op dat het om veronderstelde gedane investeringen gaat. Ondanks deze beperkingen bedraagt dit 0.411 % van het Singaporese BBP in 2014 (229.1 miljard euro[148]).

139 Danish Cyber and Information Security Strategy, The Danish Government (2018)

140 De periode van 2018-2023 wordt niet expliciet benoemd in de Deense cyberweerbaarheidsstrategie; deze periode is gebaseerd op een analyse van de Deense firma van het onderzoeksteam.

141 Op basis van de gemiddelde Deense Kronen/Euro wisselkoers van 2018 (0.13439). Bron: https://www.exchangerates.org.uk/DKK-EUR-exchange-rate-history.html

142 In 2018 bedroeg het Deense BBP 356,879 miljard dollar (https://data.worldbank.org/country/DK). Dit bedrag is vervolgens naar euro's omgerekend door de gemiddelde Dollar/Euro wisselkoers van 2018 te gebruiken (USD/EUR: 0,8475). Bron: https://www.exchangerates.org.uk/USD-EUR-spot-exchange-rates-history-2018.html#:~:text=This%20is%20the%20US%20Dollar,EUR%20on%2001%20Feb%202018.

143 National Cyber Security Strategy 2016-2021, HM Government (2016)

144 Voor de omrekening naar Euro's is gebruik gemaakt van de gemiddelde Britse Pond/Euro wisselkoers van 2016 (GBP/EUR: 1.2242). Bron: https://www.exchangerates.org.uk/GBP-EUR-spot-exchange-rates-history-2016.html

145 In 2016 bedroeg het Britse BBP 2.694 biljoen dollar (https://data.worldbank.org/country/GB). Dit bedrag is vervolgens naar euro's omgerekend door de gemiddelde Dollar/Euro wisselkoers van 2016 te gebruiken (USD/EUR: 0,9035). Bron: https://www.exchangerates.org.uk/EUR-USD-spot-exchange-rates-history-2016.html#:~:text=Best%20exchange%20rate%3A%201.1526%20USD,USD%20on%2020%20Dec%202016.

146 Bron: https://www.straitstimes.com/singapore/singapore-names-cyber-defence-chief. Dit bedrag is vervolgens naar euro's omgerekend door de gemiddelde SGD/EUR koers van 2014 te nemen (0,5952). Bron: https://www.exchangerates.org.uk/EUR-USD-spot-exchange-rates-history-2014.html#:~:text=Currency%20Menu&text=This%20is%20the%20Euro%20(EUR,USD%20on%2031%20Dec%202014.

147 Data gebaseerd op een analyse van de Singaporese firma van het onderzoeksteam.

148 In 2014 bedroeg het Singaporese BBP 314.851 miljard dollar (https://data.worldbank.org/). Dit bedrag is vervolgens naar euro's omgerekend door de gemiddelde Dollar/Euro wisselkoers van 2014 te gebruiken (USD/EUR: 0,7528). Bron: https://www.xe.com/currencytables/?from=USD&date=2014-01-01

(5) België heeft de ambitie om voor de periode 2019-2023 additioneel circa 3.6 miljard euro in nationale cyberweerbaarheid te investeren. Dit bedrag is gebaseerd op het *Nationaal Pact voor Strategische Investeringen* waarin het Strategisch Comité[149] aangeeft dat voor de periode 2019 tot 2030 dringend 15 miljard euro in cybersecurity zal moeten worden geïnvesteerd om de Belgische cyberweerbaarheid te verbeteren; van dit totaalbedrag zal 10 miljard euro moeten worden gefinancierd door de Belgische publieke sector. Deze 10 miljard euro is gedeeld door 11 (jaar) en vervolgens met 4 (jaar) vermenigvuldigd om een investeringsbudget (voor de overheid) voor de periode 2019-2023 af te leiden. De 3,636 miljard euro bedraagt 0,764% van het Belgische BBP in 2019 (461.4 miljard euro[150]). Hierbij dient te worden opgemerkt dat deze investeringen uit een ambitiebudget komen en (nog) niet geaccordeerd zijn door de in oktober 2020 gevormde regering[151]. Echter, de geadviseerde investeringen in cyberweerbaarheid (15 miljard euro) worden breed ondersteund aangezien 'politieke leiders uit het hele land, volksvertegenwoordigers, maatschappelijke spelers en middenveldorganisaties' hebben bijgedragen aan het schrijven van de adviezen[152]. De totale investeringen in de Belgische cyberweerbaarheid bestaan uit investeringen in de volgende 5 initiatieven: bouwstenen, kritieke infrastructuur, Cyber Greenhouse & veiligheid op het werk, de handhaving van cybermaatregelen, en onderzoek & ontwikkeling naar cyberveiligheid en talent.

Benchmarkonderzoek aan de hand van CRI-domeinen

1. Nationale cyberstrategie

Huidige Nederlandse situatie

De in 2018 opgerichte Nederlandse Cybersecurity Agenda (NCSA) is de kabinetsbrede agenda op het gebied van het verbeteren van de nationale cyberweerbaarheid. Naast de NCSA zijn meerdere cybersecurity (deel)strategieën opgesteld door de Rijksoverheid en decentrale overheden die decentraal worden uitgevoerd[153]. Er is nog onvoldoende duidelijkheid over de gemeenschappelijke visie en koers, welke onderling tussen de diverse stakeholders goed afgestemd is. Daarnaast missen meetbare doelstellingen en resultaten, worden taken en verantwoordelijkheden om maatregelen te realiseren onvoldoende belegd, en wordt in het NCSA bijvoorbeeld ook niet aangegeven hoe de investeringen moeten worden ingezet.

Algemene observaties vergelijkingslanden

1. Zes van de negen vergelijkingslanden hanteren een centrale cyberweerbaarheidsstrategie[154].
2. Ierland neemt in de nationale cyberweerbaarheidsstrategie concreet acties op die genomen moeten worden om de in de strategie opgenomen doelstellingen en maatregelen te realiseren.

Voorbeelden uitvoering vergelijkingslanden

- Denemarken stelt ministeries verplicht om cyberweerbaarheid sub-strategieën op te stellen voor kritieke sectoren die onder hun verantwoordelijkheid vallen (binnen de kaders van de Deense nationale cyberweerbaarheidsstrategie)[155].
- Zowel Singapore (CSA) als België (Het Centrum voor Cybersecurity België) beschikken over één nationale organisatie die de cyberweerbaarheidsstrategieën gecentraliseerd uitvoeren of coördineren; de organisaties zijn respectievelijk verantwoordelijk voor de cyberweerbaarheidsdomeinen binnen de Singaporese overheid en het overzicht houden op, coördineren en waken over de toepassing van de Belgische cyberweerbaarheidsstrategie[156].

149 "Een onafhankelijk Strategisch Comité, samengesteld uit zes leden van diverse horizonten van de Belgische economische wereld, werd in maart 2017 opgericht om tegen 2030 de investeringsprioriteiten in België te bepalen" https://www.npsi-pnis.be/nl/governance

150 In 2019 bedroeg het Belgische BBP 533.097 miljard dollar (https://data.worldbank.org/country/BE). Dit bedrag is vervolgens naar euro's omgerekend door de gemiddelde Dollar/Euro wisselkoers van 2019 te gebruiken (USD/EUR: 0.8931). Bron: https://www.exchangerates.org.uk/USD-EUR-spot-exchange-rates-history-2019.html#:~:text=This%20is%20the%20US%20Dollar,rate%20in%202019%3A%200.8931%20EUR.

151 https://www.belgium.be/nl/nieuws/2020/eedaflegging_van_de_nieuwe_federale_regering_0

152 Nationaal Pact voor Strategische Investeringen, Het Strategisch Comité (2018)

153 The Netherlands Cyber Readiness at a Glance, Potomac Institute for Policy Studies (2017).

154 België, Ierland, Denemarken, het Verenigd Koninkrijk, Singapore en Zweden. Frankrijk en Duitsland zijn niet in deze lijst opgenomen omdat de nationale cyberweerbaarheidsstrategieën die zij hanteren niet richtinggevend en gecentraliseerd genoeg zijn. Voor Finland is niet duidelijk of een centrale cyberweerbaarheidsstrategie gehanteerd wordt.

155 Danish Cyber and Information Security Strategy, The Danish Government (2018)

156 Over ons, Het Centrum voor Cybersecurity België (https://ccb.belgium.be/nl/organisatie)

- België beschikt over het Nationaal Pact voor Strategische Investeringen (2018) waarin wordt geadviseerd in welke onderdelen en acties de komende 11 jaar (2019-2030) zal moeten worden geïnvesteerd om de nationale cyberweerbaarheid te verhogen.
- De Ierse nationale cyberweerbaarheidsstrategie bevat een uitvoeringsagenda waarin duidelijk staat aangegeven welke concrete acties (en de daarbij behorende tijdslijnen, verantwoordelijke partijen en hoofdstakeholders) uitgevoerd moeten worden om de in de strategie benoemde maatregelen te realiseren[157].

2. Informatiedeling

Huidige Nederlandse situatie

Momenteel bestaan er initiatieven binnen de overheid, het bedrijfsleven en de wetenschap die als doel hebben om de informatiedeling binnen Nederland te bevorderen. Zo wisselt een groot aantal overheidspartijen en belangenorganisaties binnen de private sector onderling informatie uit, en wordt er geïnvesteerd in het voorlichten van burgers op het belang van digitale veiligheid. Daarentegen wordt dreigingsinformatie nog onvoldoende snel en gericht gedeeld waardoor organisaties binnen de overheid en het bedrijfsleven niet alle relevante informatie tot hun beschikking hebben om (geavanceerde) cyberdreigingen te weren.

Algemene observaties vergelijkingslanden

1. Met uitzondering van België is er voor de vergelijkingslanden geen kwantitatieve informatie beschikbaar over concrete investeringen in de nationale informatiedeling capability.
2. Informatiedeling-initiatieven in het Verenigd Koninkrijk zijn meer gecentraliseerd en gefocust dan in Nederland. Wat opvalt is dat in het Verenigd Koninkrijk tussen de publieke-en private sector systematischer, sneller en gerichter relevante (dreigings)informatie wordt gedeeld[158].

Voorbeelden uitvoering vergelijkingslanden

- Het Verenigd Koninkrijk heeft het Cybersecurity Information Sharing Partnership (CiSP) opgericht; dit is een gezamenlijk samenwerkingsverband tussen de publieke en private sector waar *realtime* (dreigings)informatie met leden wordt gedeeld (waaronder private organisaties, wethandhavingsinstanties en internationale partners). Het CiSP maakt ook gebruik van een online platform waardoor meer organisaties sneller toegang krijgen tot relevante informatie, en sneller informatie met elkaar en het Britse Nationale Cybersecurity Centrum kunnen delen. Tevens beschikt het Verenigd Koninkrijk over een 'Fusion Cell', een publiek-privaat samenwerkingsverband waarin een team een breed scala aan data met betrekking tot cyberdreigingen verzamelt en analyseert; vervolgens worden met regelmaat deze informatie, adviezen en notificaties met CiSP leden gedeeld[159].

1. Cybercrime en handhaving

Huidige Nederlandse situatie

In Nederland zijn veel partijen betrokken bij het opsporen en vervolgen van cybercrime op een (inter)nationaal niveau, zowel binnen de overheid, het bedrijfsleven en vanuit de wetenschap. Nederland heeft op het vlak van opsporing de afgelopen jaren grote stappen gezet en is met regelmaat betrokken bij het aanpakken van grote internationale cyber-criminele netwerken. Echter, in 2019 heeft het OM slechts 400 zaken kunnen behandelen, tegenover 13% slachtofferschap onder de Nederlandse bevolking. De opsporing kan daarmee gezien worden als een capability waarvan de richting en kwaliteit sterk zijn, maar de kwantiteit nog onvoldoende is.

Aanvullend op het bestrijden van cybercrime zien verschillende ministeries en overheidsinstanties toe op de handhaving van wetgeving ten behoeve van de cyberweerbaarheid. Zo zijn voor het toezicht op de Wbni verschillende instanties aangewezen (zoals het ILT en AT), verspreid over meerdere ministeries en sectoren. In de praktijk blijkt echter dat handhaving binnen bepaalde sectoren nog tot onvoldoende resultaten leidt. Daarnaast bestrijkt de handhaving maar een heel klein deel van het internetverkeer in Nederland en zijn er grote 'zwarte gaten' waar de overheid geen zicht en bij uitwassen geen effectieve mogelijkheid tot interventie heeft, anders dan opsporing (wat een kostbaar en complex middel is).

157 National Cyber Security Strategy 2019-2024, Government of Ireland (2019)
158 United Kingdom Cyber Readiness at a Glance, Institute for Policy Studies (2016).
159 United Kingdom Cyber Readiness at a Glance, Institute for Policy Studies (2016).

Algemene observaties vergelijkingslanden

1. Een aantal vergelijkingslanden hanteren wetgeving met betrekking tot cybersecurity – dit loopt uiteen van het verplicht stellen van minimale cybersecurity requirements tot het implementeren van toekomstbestendig beleid met betrekking tot opkomende technologieën[160].
2. Een kleine groep vergelijkingslanden zet in op het stimuleren van de ontwikkeling van innovatieve manieren om cybercrime op te sporen en bestrijden.

Voorbeelden uitvoering vergelijkingslanden

- De Belgische Cyber Security Coalition is een samenwerkingsverband tussen de overheid, de private sector en de academische wereld met als doel het tegengaan en terugbrengen van cybercriminaliteit. Activiteiten bestaan onder andere uit het verhogen van het bewustzijn van burgers en ondernemers met betrekking tot veilig internetten, het doen van beleidsaanbevelingen op het gebied van cybercrimebestrijding, het delen van (dreigings)informatie, en operationele samenwerking tussen leden voor een efficiëntere aanpak van cybercrime[161].
- België heeft de ambitie om het aantal beschikbare cyberexperts (binnen CERT.be, Defensie en de inlichtingen- en veiligheidsdiensten) te verhogen naar 1.500 fulltime medewerkers. Dit als doel om het zicht op het Belgische internetverkeer, mogelijkheid tot interventie te vergroten, en handhaving van cybermaatregelen te borgen. In het *Nationaal Pact voor Strategische Investeringen* (2018) wordt geadviseerd dat voor de periode 2019-2030 2.8 miljard euro wordt geïnvesteerd in de handhaving van cybermaatregelen. Dit bedrag zal grotendeels bestaan uit publieke financiering en is voornamelijk bestemd voor de werving van gespecialiseerde medewerkers[162].
- Voor de bestrijding van cybercrime op nationaal en lokaal niveau heeft het Verenigd Koninkrijk naast het National Cyber Crime Unit (NNCU) ook teams van toegewijde specialisten bij de Metropolitan Police Service, alle negen Regionale Organised Crime Units en bij elk lokaal politiekantoor in Engeland en Wales[163].
- Singapore heeft in 2019 de Cyberbeveiligingswet goedgekeurd waarbij wettelijk kaders zijn vastgesteld met betrekking tot het toezicht houden en onderhouden van de nationale cyberweerbaarheid[164]. België en het Verenigd Koninkrijk zijn respectievelijk van plan om wetgeving als instrument te gebruiken om minimumvereisten met betrekking tot cybersecurity af te dwingen en om zich voor te bereiden op opkomende en toekomstige technologieën en bedreigingen door beleidsimplementatie *future-proof* te maken[165].

2. Diplomatie en handel

Huidige Nederlandse situatie

Het ministerie van Buitenlandse Zaken investeert in cyberdiplomatie als onderdeel van de 'Geïntegreerde Buitenland- en Veiligheid Strategie'. Daarnaast wordt vanuit de Nederlandse Cybersecurity Agenda gewerkt aan internationale vrede en veiligheid in het internationale domein.

Algemene observaties vergelijkingslanden

1. Ten opzichte van vergelijkingslanden loopt het Verenigd Koninkrijk voor op het gebied van diplomatie en handel; het land is een pionier geweest op het gebied van ontwikkelen en bevorderen van internationale normen in cyberspace, en ook het inzetten van verschillende belanghebbenden bij internationale discussies over cybersecurity, cybercrime, economische ontwikkelingen en groei, en internetbeheer. Een voorbeeld hiervan is het door het Verenigd Koninkrijk opgerichte *London Conference on Cyberspace* (2011) waarbij verschillende landen bijeengekomen waren om normen van geaccepteerd gedrag in cyberspace te bespreken[166].

Voorbeelden uitvoering vergelijkingslanden

- De Ierse overheid werkt aan het versterken van de cyberdiplomatieke inzet van Ierland door 'cyber attachés' in belangrijk diplomatieke missies te plaatsen, en door bij te dragen aan het verhogen van cyberweerbaarheid van ontwikkelingslanden[167].

160 Dit laat onverlet dat er ook cybersecuritywetgeving is die de gehele EU beslaat, zoals de transposities van de NIS Directive in nationale wet- en regelgeving.
161 Over ons, Cyber Security Coalition (https://www.cybersecuritycoalition.be/nl/over-ons/)
162 Nationaal Pact voor Strategische Investeringen, Het Strategisch Comité (2018)
163 National Cyber Security Strategy 2016-2021 – Progress Report, Cabinet Office (2019)
164 Cybersecurity Act, CSA Singapore (https://www.csa.gov.sg/legislation/cybersecurity-act)
165 National Cyber Security Strategy 2016-2021 – Progress Report, Cabinet Office (2019)
166 United Kingdom Cyber Readiness at a Glance, Institute for Policy Studies (2016)
167 National Cyber Security Strategy 2019-2024, Government of Ireland (2019)

- Ter bevordering van handel heeft de Britse regering door de industrie geleide standaarden ontwikkeld om het Verenigd Koninkrijk te promoten als een veilige plek voor internethandel. Tegelijkertijd worden Britse bedrijven ook door de overheid geholpen om hun producten en diensten in het binnen-en buitenland te promoten, waarbij het Cyber Essentials programma deze bedrijven helpt om beter bestendigd te zijn tegen de meest voorkomende cyberdreigingen[168].
- De Belgische overheid is van plan om middels het *Centrum voor Cyber Security* een *Cyber Security Greenhouse* op te zetten om innovatieve cyberoplossingen en businessmodellen te ontwikkelen[169]. In het Nationaal Pact voor Strategische Investeringen (2018) wordt geadviseerd om in de periode 2019-2030 5.6 miljard euro (waarvan circa 3.5 miljard euro vanuit de overheid) te investeren in het opzetten van het Greenhouse en het veiliger maken van het bedrijfsleven. Het merendeel van dit bedrag is bedoeld om bedrijven te ondersteunen bij het invoeren van oplossingen voor cyberveiligheid. Tevens wil de overheid goed ondernemerschap en innovatie stimuleren door bedrijven te voorzien van fiscale voordelen (circa 1 miljard euro over de periode 2019-2030[170]).

3. Onderzoek en wetenschap

Huidige Nederlandse situatie

In Nederland bestaat een groot aantal opleidingen en wetenschappelijke onderzoeksinstituten die zich richten op (een domein binnen) cyberweerbaarheid. Op dit moment is er beperkt sprake van structurele samenwerking of prioriteitstelling op het gebied van onderzoek en wetenschap tussen deze opleidingen en instituten. Desondanks het feit dat Nederlandse universiteiten momenteel beperkt in staat zijn om (hoogwaardig) talent aan te trekken en vast te houden, werkt de Nederlandse overheid wel aan het structureel opnemen van cybersecurity in curricula van het basis en voortgezet onderwijs[171]. De Nederlandse overheid heeft in de periode 2012-2020 gemiddeld 7.5 miljoen euro per jaar in cybersecurity-onderzoek en innovatie geïnvesteerd[172]; dit is 0,0011 % van het Nederlandse BBP. Echter, deze investeringen worden ad-hoc gedaan en zijn daarmee onvoorspelbaar.

Algemene observaties vergelijkingslanden

1. In het Nationaal Pact voor Strategische Investeringen (2018) wordt geadviseerd dat de Belgische publieke sector jaarlijks circa 100 miljoen euro in cybersecurity gerelateerd onderzoek, onderwijs en wetenschap moet investeren[173]. Dit is 0,0217 % van het Belgische BBP en circa 1821,98 % meer dan wat de Nederlandse overheid jaarlijks in deze capability investeert (als er wordt gekeken naar de Belgische jaarlijkse ambitie investering ten opzichte van het Belgische BBP vergeleken met Nederland). Let op dat het hier om een ambitie bedrag gaat.
2. De Duitse overheid investeert jaarlijks 272.5 miljoen euro in dit domein[174]. Dit is 0,0082 % van het Duitse BBP (in 2019[175]) en circa 623,08 % meer dan wat Nederland jaarlijks in deze capability investeert (als er wordt gekeken naar de Duitse jaarlijkse investering ten opzichte van het Duitse BBP vergeleken met Nederland).
3. Alle vergelijkingslanden besteden veel aandacht aan cyber gerelateerd onderzoek, wetenschap en onderwijs in hun nationale cyberweerbaarheidsstrategieën door het opnemen van ambities en doelstellingen.

168 United Kingdom Cyber Readiness at a Glance, Institute for Policy Studies (2016).

169 Building a Cyber Resilient and Trusted Belgium – Cyber Security Themes for the Strategic Investment Pact 2030 (Centre for Cyber Security Belgium)

170 Nationaal Pact voor Strategische Investeringen, Het Strategisch Comité (2018)

171 Nederlandse Cybersecurity Agenda, Ministerie van Justitie en Veiligheid (2018).

172 Deze investeringen liepen middels het SBIR-instrument, TKI, NWO en doelfinancieringsprogramma's. Samenwerkingsplatform cybersecurity – Advies Kwartiermakers (2020).

173 Hier wordt geadviseerd dat de publieke sector in de periode 2019-2030 1.1 miljard euro vrijmaakt voor onderzoek & ontwikkeling naar cyberveiligheid en talent. Door dit bedrag door 11 te delen wordt een jaarlijks bedrag van 100 miljoen euro afgeleid. Bron: Nationaal Pact voor Strategische Investeringen, Het Strategisch Comité (2018)

174 Data gebaseerd op een analyse van de Duitse firma van het onderzoeksteam. Deze 272.5 miljoen euro is uitgesplitst in de volgende Duitse organisaties: Zentralstelle für Informationstechnologie im Sicherheitsbereich (ZITiS) (2.5 miljoen euro), Agency for Cyber Security Innovation (230 miljoen euro), en Ministry of the Interior, Building and Community (planned federal budget for disruptive innovations in cyber security and key technologies) (40 miljoen euro). Het onderzoeksteam heeft niet kunnen achterhalen aan welke specifieke activiteiten en initiatieven dit bedrag wordt uitgegeven.

175 Bron: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=DE

Voorbeelden uitvoering vergelijkingslanden

- Het Verenigd Koninkrijk is gastland van Europa's eerste cybersecurity startup accelerator, waarin bedrijven worden geholpen om cybersecurity-producten te ontwikkelen en het cyberinnovatie ecosysteem wordt bevorderd[176].
- Het Britse Kabinet, de Departement for Business, Energy and Industrial Reform, National Cyber Security Programme, en Government Communications Headquarters hebben een samenwerkingsverband om activiteiten te leiden en ondersteunen die als doel hebben een grotere poule aan hoogwaardige cybersecurity kennis in het Verenigd Koninkrijk op te bouwen. Zo worden in het 'CyberFirst'-programma geselecteerde individuen gesponsord om cyberrelevante bacheloropleidingen te volgen, cybervaardigheden op te doen tijdens zomerstages en na het afstuderen te gaan werken in de Britse cybersecurity-sector. Tevens wordt er gewerkt aan het opnemen van cybersecurity-theorie in curricula van het basis en voortgezet onderwijs[177].
- Het Singaporese CSA leidt het SG Cyber Talent initiatief waar cybersecurity enthousiastelingen vanaf een jonge leeftijd over cybersecurity worden onderwezen en de vaardigheden van cybersecurity professionals worden verdiept. CSA streeft om binnen drie jaar 20.000 mensen te bereiken en aan te moedigen om de Singaporese cybersecurity-industrie te betreden. Hier wordt samengewerkt met overheidsinstanties, de academische wereld, verenigingen, en de private sector en wordt gebruikt gemaakt van bestaande CSA-initiatieven[178].
- Het *National Pact voor Strategische Investeringen* (2018) adviseert de Belgische overheid en de private sector te investeren in een speciaal opgerichte 'cyber valley' om innovatie, onderzoek en de samenwerking tussen de publieke sector, academische wereld en private sector stimuleren[179].
- Zowel Duitsland als Singapore beschikken over en investeren in respectievelijk de Duitse Cyber Innovation Hub voor Defensie en Agency for Cyber Security Innovation, en Singaporese CASE Cybersecurity Co-Innovation and Development Fund. Dit laatste programma moedigt samenwerking aan tussen cybersecurity bedrijven en eindgebruikers door de winnaar te voorzien van twee jaar lange financieringssteun tot 1 miljoen Singaporese dollars[180].

4. Defensie en crisis response

Huidige Nederlandse situatie

Nederland signaleert actief aan andere landen dat zij de intentie heeft om op het gebied van defensie en crisis response een grotere cyberweerbaarheid op te willen bouwen en cyberverdedigingsmaatregeling na te streven[181]. Dit is terug te zien in het feit dat Nederland cyberspace heeft uitgeroepen tot het 5e werkgebied van de krijgsmacht[182], de publicatie van *Defensie Cyber Strategie 2018*[183], en het aantal onderdelen[184] binnen het ministerie van Defensie die zich met cybersecurity bezighouden. Echter, Nederland beschikt momenteel niet over het vermogen (onder andere vanwege onvoldoende financiering, middelen en capaciteit) om deze ambitie volledig te realiseren. Dit is terug te zien in de relatief lage score van Nederland in de Cyber Capability Index (CCI) ten opzichte van haar plaats in de Cyber Intent Index (CII) in het defensie domein[185].

176 Cyber Readiness Index 2.0, Potomac Institute for Policy Studies (2015)
177 United Kingdom Cyber Readiness at a Glance, Institute for Policy Studies (2016).
178 SG Cyber Talent, CSA Singapore (csa.gov.sg/programmes/sgcybertalent/about)
179 Building a Cyber Resilient and Trusted Belgium – Cyber Security Themes for the Strategic Investment Pact 2030, Centre for Cyber Security Belgium (2018)
180 CSA Cybersecurity Co-Innovation and Development Fund, CSA Singapore (https://www.csa.gov.sg/programmes/co-innovation-development-fund)
181 National Cyber Power Index 2020 – Methodology and Analytical Considerations, Belfer Center (Harvard Kennedy School) (2020).
182 https://www.defensie.nl/onderwerpen/cyber-security
183 Defensie Cyber Strategie 2018 – Investeren in digitale slagkracht voor Nederland, Ministerie van Defensie (2018)
184 Waaronder: Defensie Cyber Commando (DCC), de Joint Sigint Cyber Unit (JSCU), en het Defensie Computer Emergency Response Team.
185 De Cyber Intent Index (CII) geeft aan in welke mate een land een bepaald cybersecurity domein prioriteert, terwijl de Cyber Capability Index (CCI) het vermogen van een land om haar cybersecurity intentie te realiseren weergeeft (National Cyber Power Index 2020 – Methodology and Analytical Considerations, Belfer Center (Harvard Kennedy School (2020))). Voor het defensie cyberdomein staat Nederland in de CII op de tweede plek (in de top 10), terwijl zij in de CCI op de 6e plek staat (in de top 10).

Algemene observaties vergelijkingslanden

1. Ten opzichte van Nederland heeft het Verenigd Koninkrijk een hogere intentie om in het defensiedomein cyberverdedigingsmaatregelen na te streven en een grotere cyberweerbaarheid op te bouwen[186]. Een van de verklaringen voor deze hogere intentie is de uitspraak van de Britse overheid om van het Verenigd Koninkrijk het beste beschermde land in cyberspace te maken middels het inzetten van 'active cyber defense'[187]. Dit verschilt van de Nederlandse aanpak; Defensie heeft aangegeven uiterst terughoudend te zijn in het inzetten van offensieve cybercapaciteiten (tenzij daar een adequate basis voor is)[188]. Wat opvalt is dat het Verenigd Koninkrijk niet tot de top 10 behoort in de CCI – dit impliceert dat zij zich meer focussen op het uitvoeren van ontwrichtende acties in cyberspace, en zich relatief minder inzetten voor de versterking van cyber defensie capaciteiten[189].
2. In tegenstelling tot Nederland heeft Singapore een relatief lage intentie om aan andere landen te signaleren dat zij in het defensiedomein cyberverdedigingsmaatregelen zal na streven en een grotere cyberweerbaarheid zal opbouwen. Echter, Singapore focust zich wel op het versterken van de cyberdefensie capaciteiten[190].

Voorbeelden uitvoering vergelijkingslanden

- Het Singaporese ministerie van Defensie beschikt over een Defence Cyber Organisation dat uit 6 sub-sectoren bestaat[191]. Tevens heeft het ministerie van Defensie in 2019 twee Cyber Expert Schemes en een Training School opgericht ter bevordering van het cybersecurity ecosysteem[192].
- De Britse regering heeft in 2020 de oprichting van de National Cyber Force aangekondigd. Deze groep (bestaand uit deskundigen van het Government Communications Headquarters, het ministerie van Defensie, MI6 en het Defence Science and Technology Laboratory) houdt zich bezig met het uitvoeren van cyberoperaties tegen vijandige activiteiten van statelijk actoren, terroristen en criminelen[193].

186 Het Verenigd Koninkrijk staat op de eerste plek (in de top 10) in de Cyber Intent Index (CII) (National Cyber Power Index 2020 – Methodology and Analytical Considerations, Belfer Center (Harvard Kennedy School (2020)))
187 United Kingdom Cyber Readiness at a Glance, Potomac Institute for Policy Studies (2016).
188 The Netherlands Cyber Readiness at a Glance, Potomac Institute for Policy Studies (2017).
189 National Cyber Power Index 2020 – Methodology and Analytical Considerations, Belfer Center (Harvard Kennedy School (2020))
190 Singapore staat op de tweede plek (in de top 10) in de Cyber Capability Index (CCI), en komt niet voor in de top 10 van de Cyber Intent Index (CII) (National Cyber Power Index 2020 – Methodology and Analytical Considerations, Belfer Center (Harvard Kennedy School (2020))).
191 DSTA Networks, DSO Networks, Defence Industry Networks, SAF Military Networks, MINDEF Related Org Networks, Corporate IT and Internet-Facing Org Networks (https://www.mindef.gov.sg/web/portal/mindef/about-us/organisation/organisation-profile/defence-cyber-organisation)
192 https://www.mindef.gov.sg/web/portal/pioneer/article/regular-article-detail/technology/2019-Q1/20feb19_news
193 https://www.gov.uk/government/news/national-cyber-force-transforms-countrys-cyber-capabilities-to-protect-uk

Het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' is geschreven naar aanleiding van het verzoek dat de raad op 4 maart 2020 heeft ontvangen van de minister van Justitie en Veiligheid. In dit verzoek heeft de minister de raad gevraagd om advies uit te brengen over de benodigde investeringen in cybersecurity voor een volgende kabinetsperiode.

Over de CSR

De CSR is een nationaal en onafhankelijk strategisch adviesorgaan van het kabinet en via het kabinet ook het bedrijfsleven als het gaat om cybersecurity in Nederland en is samengesteld uit hooggeplaatste vertegenwoordigers uit de publieke, private en wetenschappelijke sector. Door deze unieke samenstelling bekijkt de raad de nationaal strategische cybersecurity-uitdagingen vanuit meerdere invalshoeken en worden gewogen strategische adviezen aan het kabinet en het bedrijfsleven gegeven. Daarbij houdt de raad oog voor de economische kansen die cybersecurity ons land kan bieden.

Samenstelling

Private sector:

- Dhr. H. (Hans) de Jong (covoorzitter), President Philips Nederland, lid van CSR namens VNO-NCW
- Mw. mr. I. (Ineke) Dezentjé Hamming-Bluemink, voorzitter FME (ondernemersorganisatie voor de technologische industrie), lid van CSR namens FME
- Dhr. W. (Wiebe) Draijer, voorzitter van de groepsdirectie van de Rabobank en bestuurslid van de Nederlandse Vereniging van Banken, lid van de CSR namens de financiële sector
- Dhr. mr. J. (Joost) Farwerck, CEO en voorzitter van de Raad van Bestuur bij KPN, lid van CSR namens NLdigital
- Mw. drs. C. (Claudia) de Andrade-de Wit, CIO, directeur Digital & IT Haven Rotterdam, lid van CSR namens het CIO Platform
- Dhr. drs. M. (Marc) van der Linden, CEO en voorzitter Raad van bestuur bij Stedin Holding N.V., lid van CSR namens de vitale sectoren
- Mw. T. (Tineke) Netelenbos, voorzitter ECP, lid van CSR namens ECP, Platform voor de Informatiesamenleving

Publieke sector

- Dhr. P.J. (Pieter-Jaap) Aalbersberg EMPM (covoorzitter), Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)
- Dhr. drs. E.S.M. (Erik) Akerboom MPM, Directeur-Generaal Algemene Inlichtingen en Veiligheidsdienst (AIVD)
- Dhr. vice-admiraal B.G.F.M. (Boudewijn) Boots, plaatsvervangend Commandant der Strijdkrachten bij het ministerie van Defensie
- Dhr. mr. G.W. (Gerrit) van der Burg, voorzitter van het College van procureurs-generaal
- Dhr. mr. H.P. (Henk) van Essen, Korpschef Politie
- Dhr. drs. F.W. (Focco) Vijselaar, Directeur-Generaal Bedrijfsleven en Innovatie bij het ministerie van Economische Zaken en Klimaat
- Mw. drs. M. (Marieke) van Wallenburg, Directeur-Generaal Overheidsorganisatie bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Wetenschappelijke sector

- Mw. prof. dr. B. (Bibi) van den Berg, hoogleraar Cybersecurity Governance verbonden aan het Institute of Security and Global Affairs van Universiteit Leiden
- Dhr. prof. dr. M.J.G. (Michel) van Eeten, hoogleraar Cybersecurity TU Delft
- Dhr. prof. dr. B.P.F. (Bart) Jacobs, hoogleraar Computerbeveiliging Radboud Universiteit Nijmegen
- Mw. prof. mr. E.M.L. (Lokke) Moerel, Senior Of Counsel Morrison & Foerster LLP, Hoogleraar Universiteit Tilburg

Secretaris

Mw. drs. E.C. (Elly) van den Heuvel-Davies


CSR
Cyber
Security
Raad