Advies 'Naar structurele inzet van innovatieve toepassingen van nieuwe technologieën voor de cyberweerbaarheid van Nederland'

CSR
Cyber Security Council
Cyber Security Raad

Advies 'Naar structurele inzet van innovatieve toepassingen van nieuwe technologieën voor de cyberweerbaarheid van Nederland'

Gericht aan:

De minister van Justitie en Veiligheid
De staatssecretaris van Economische Zaken en Klimaat

Cyber Security Council
Cyber Security Raad

18 september 2020

CSR-advies 2020, nr. 5

Excellentie,

Hierbij ontvangt u van de Cyber Security Raad (hierna de raad) het advies *'Naar structurele inzet van innovatieve toepassingen van nieuwe technologieën voor de cyberweerbaarheid van Nederland'.*

Bescherming digitale infrastructuur belangrijker dan ooit

Het beschermen van onze digitale infrastructuur ligt ten grondslag aan het beschermen van onze open, vrije en welvarende maatschappij en dit vraagt onze continue aandacht. De huidige coronacrisis onderstreept de urgentie; het virus heeft de transitie naar de digitale samenleving versneld. Een groot deel van de Nederlandse bevolking werkt nu op afstand, studeert op afstand en onderhoudt sociale contacten op afstand. Ook in de zorgsector zijn de digitale mogelijkheden versneld omarmd. De enorme toename van het gebruik van digitale toepassingen is relatief soepel verlopen en Nederland kan er gepast trots op zijn dat onze digitale infrastructuur is opgewassen tegen de gevolgen van een crisis van deze omvang. Het heeft Nederland in staat gesteld om te schakelen naar een nieuwe realiteit en organisaties en gebruikers in hoog tempo geleerd om te gaan met (nieuwe) digitale toepassingen. We hebben daarmee een grote sprong voorwaarts weten te maken.

Groeiende afhankelijkheden en kwetsbaarheden

De huidige ontwikkelingen hebben echter ook tot gevolg dat onze digitale afhankelijkheid en daarmee ook onze kwetsbaarheid aanzienlijk toenemen. De raad constateert twee belangrijke ontwikkelingen als gevolg van de coronacrisis:

- Digitale toepassingen zijn in Nederland in hoog tempo op grote schaal geïntroduceerd. De digitale veiligheid en privacy van deze toepassingen zijn echter niet in alle gevallen afdoende op orde[1].
- Cybercriminaliteit neemt sterk toe, ook onafhankelijk van corona[2]. Criminelen richten zich daarbij op de meest kwetsbare plekken waarbij bovendien crises als corona als gelegenheid worden misbruikt, bijvoorbeeld via gerichte *phishing,* een toename van *WhatsApp*-fraude en specifieke kwetsbaarheden doordat werknemers ineens op grote schaal thuiswerken via een (thuis)computer. Zowel bedrijven als individuen zijn hier het slachtoffer van.

Inzet nieuwe technologieën om cyberweerbaarheid te versterken

Nieuwe technologische ontwikkelingen scheppen nieuwe kansen, maar introduceren ook telkens weer nieuwe kwetsbaarheden, hetgeen ons dwingt om opnieuw te doordenken hoe Nederland met deze kwetsbaarheden moet omgaan. Bij het versterken van onze cyberweerbaarheid spelen nieuwe technologieën een steeds crucialere rol, evenals bestaande technologieën met nieuwe toepassingsmogelijkheden[3]. Zonder de inzet van nieuwe technologieën zal het niet lukken om ons voldoende te beschermen. Cyberaanvallen zullen bijvoorbeeld geautomatiseerd moeten worden bestreden door het gebruik van geautomatiseerd kwetsbaarheden-management dat detectie en mitigerende maatregelen grotendeels autonoom door systemen uit laat voeren[4].

De raad heeft het Rathenau Instituut (RI) opdracht verleend onderzoek te doen naar de wijze waarop nieuwe technologieën kunnen bijdragen aan het verhogen van de cyberweerbaarheid in Nederland en wat de randvoorwaarden zijn voor het creëren en benutten van deze technologische kansen.

[1] Het datalek in de Infectieradar app bij het Rijksinstituut voor Volksgezondheid en Milieu (https://www.rivm.nl/nieuws/geen-misbruik-datalek-infectieradar) en het gebruik van videoconference platforms zijn hier twee voorbeelden van.
[2] 'Beyond the pandemic how COVID-19 will shape the serious and organised crime landscape in the EU', Europol, 30 april 2020
[3] Vanaf hier worden, wanneer gesproken wordt over 'nieuwe technologieën', ook reeds bestaande technologieën met nieuwe toepassingsmogelijkheden bedoeld.
[4] Kennis- en innovatieagenda Veiligheid, Ministerie van Economische Zaken & Klimaat, 2019

Het RI-onderzoek[5] toont aan dat de inzet van nieuwe technologieën, zoals kunstmatige intelligentie (*artificial intelligence* – AI), post-kwantumcryptografie, LiFi, 5G netwerken of gedistribueerde systemen, inderdaad kansen biedt om de cyberweerbaarheid te verhogen. Zo vergemakkelijkt AI het automatisch traceren en herstellen van bestaande kwetsbaarheden in software. Met post-kwantumcryptografie moeten we uiteindelijk dataversleuteling mogelijk maken, die bestand is tegen aanvallen waarbij gebruik wordt gemaakt van de rekenkracht van een kwantumcomputer. Hoewel de kwantumcomputer de komende jaren onvoldoende ver ontwikkeld zal zijn om in de praktijk te kunnen worden gebruikt, zullen we toch de komende jaren al maatregelen moeten nemen om IT-systemen te beschermen tegen het risico van een aanval met een kwantumcomputer. Het *Internet of Things* (IoT) is op zich geen nieuwe technologische ontwikkeling, maar zal een grote vlucht nemen de komende jaren.
Het gebruik van al deze (nieuwe) technieken zal uiteindelijk een noodzaak blijken. Immers, zodra de kwantumcomputer het mogelijk maakt om bestaande vormen van encryptie te breken, is post-kwantumcryptografie een noodzakelijke voorwaarde om de veiligheid van data te borgen.

Een extra zorgpunt van de raad in dit verband is de groeiende afhankelijkheid van Nederland als het gaat om de inzet van nieuwe technologische toepassingen of diensten die afkomstig zijn van buitenlandse technologiebedrijven. Ook voor de (verdere) ontwikkeling en implementatie van genoemde nieuwe technologieën, zoals AI, kwantumcomputing, satelliet- en 5G-netwerken, geldt dat grote buitenlandse bedrijven op veel gebieden vooroplopen. Hoewel Nederland zelf (zeer) sterk is op gebieden als kwantumcomputing, encryptie, photonics en lithografie, ontstaan op andere gebieden potentieel nieuwe afhankelijkheden aangaande beveiliging, detectie van cyberdreigingen, continuïteit, potentiële *vendor lock-in* en in uitzonderlijke gevallen mogelijke toegang tot data door buitenlandse mogendheden.

Deze afhankelijkheid gaat verder dan de specifieke technologische toepassingen zelf. Om op grote schaal gebruik te kunnen maken van data-analyse door middel van AI, is bijvoorbeeld enorme rekenkracht vereist. De verwachting is dat de Cloud-infrastructuur die hiervoor benodigd is het fundament wordt voor de Nederlandse en Europese innovatie- en kennisinfrastructuur. Daarover, en over andere sleuteltechnologieën, zeggenschap houden, is een wezenlijk deel van de Nederlandse strategische autonomie[6]. Van essentieel belang is dat leveranciers van data- en clouddiensten die actief zijn binnen de Europese Digital Single market - ongeacht waar hun hoofdkantoor is gevestigd - zich dienen te houden aan de Europese regelgeving, normen en waarden, inclusief de vereiste waarborgen voor security en privacy. Daarnaast moet goed gedefinieerd worden welke data geopolitieke bescherming vragen. De overheid wordt uitgenodigd hierover duidelijkheid te verschaffen. We moeten ervoor waken dat we niet terechtkomen op een onomkeerbaar pad van geleidelijke erosie van onze strategische autonomie.

Niet verassend is dat voornoemde afhankelijkheden van buitenlandse partijen en de impact daarvan op de digitale autonomie en concurrentiepositie van Europa hebben geleid tot een reeks van Europese beleidsvoorstellen[7]. Het belangrijkste doel van deze voorstellen is te komen tot een gezamenlijke Europese digitale innovatiestrategie en agenda. De raad is van mening dat ons land hierin een stevige positie moet innemen en zal in een later stadium een separaat advies hierover uitbrengen.

[5] Van Boheemen, G. Munnichs, L. Kool, G. Diercks, J. Hamer & A. Vos (2019). Cyberweerbaar met nieuwe technologie – Kans en noodzaak van digitale innovatie. Den Haag: Rathenau Instituut

[6] Timmers, P. There will be no global 6G unless we resolve sovereignty concerns in 5G governance. Nat Electron 3, 10–12 (2020). Zie ter vergelijking ook de Duitse 'Industrial Strategy 2030. Guidelines for a German and European industrial policy', waarin men erkent dat onvoldoende grip op nieuwe technologieën een direct risico betekent voor het behoud van de technologische soevereiniteit van de Duitse economie.

[7] Zie met name: Europese Commissie, 'Een Europese datastrategie', COM(2020)66, 19 februari 2020; Europese Commissie, White Paper 'On Artificial Intelligence - A European approach to excellence and trust', 19 februari 2020; 'A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem', het door Duitse en Franse regering geïnitieerde GAIA-X project, oktober 2019, dat gebaseerd is op basis van beginselen van *sovereignty-by-design.*

Voorwaarden benutten technologische kansen

Om de kansen van nieuwe technologieën voor optimaal te kunnen benutten, is het belangrijk om een integraal en actueel beeld te hebben van alle relevante nieuwe technologieën met kansen of risico's voor onze cyberweerbaarheid en digitale autonomie. Op dit moment is deze informatie in Nederland niet voorhanden. Dit blijkt ook uit de visie die brancheorganisatie Cyberveilig Nederland in 2020 heeft opgesteld[8]. Onderzoek toont aan dat in Nederland onvoldoende kennisontwikkeling en -uitwisseling plaatsvindt binnen en tussen bedrijven en kennisinstellingen[9]. Er is ook een duidelijker beeld nodig van het functioneren van de kennis- en innovatieketen voor cybersecurity in Nederland en er ligt een uitdaging om te komen tot meer samenhang tussen enerzijds fundamenteel en toegepast onderzoek en anderzijds valorisatie[10]. Door hier niet op te acteren, lopen we het risico kansen te missen en risico's te laat te onderkennen[11]. Tot slot ontbreekt een inventarisatie van welke kennis, technologie en industriële capaciteiten Nederland - en Europa - op het gebied van deze technologieën zelf in huis dient te hebben, hoe dit met actief Nederlands industriebeleid kan worden geborgd en hoe de Nederlandse inbreng op dit gebied bij Europese initiatieven kan worden versterkt. Europese samenwerking in dit opzicht is gewenst, zoals ook beschreven staat in de Nederlandse Digitaliseringsstrategie 2020.

Initiatieven en ontwikkelingen

Ons land zit niet stil op het gebied van cybersecurity en innovatie. In 2019 verscheen de Kennis- en Innovatie Agenda (KIA) Veiligheid[12] als onderdeel van de KIA Sleuteltechnologieën 2020-2023[13]. De KIA Veiligheid richt zich in een meerjarig missiegedreven innovatieprogramma cyberveiligheid onder andere op (toegepaste) cybersecurity-innovaties binnen de Nederlandse topsectoren. De raad ziet dit als een positieve ontwikkeling en ziet graag een afspiegeling hiervan buiten de topsectoren zodat de cyberweerbaarheid ook buiten de topsectoren kan worden vergroot. Het ministerie van Economische Zaken en Klimaat (EZK) kondigde begin 2020 in een brief aan de Kamer[14] een aanpak aan die zal bestaan uit een nieuw samenwerkings-platform dat de krachten op het terrein van cybersecurity onderzoek, innovatie en onderwijs moet bundelen. Binnen dit *Samenwerkingsplatform Cybersecurity en Innovatie* worden alle relevante partijen, expertise, instrumenten en middelen uit het cybersecuritydomein bij elkaar gebracht. *De raad juicht de komst van het platform toe, mits het ook de vereiste slagkracht, mandaat en benodigde middelen krijgt. Het benutten en creëren van kansen en adresseren van risico's vergt een integrale aanpak met weloverwogen keuzes en meer middelen[15] dan tot op heden voorzien[16]. Dit vereist regie over departementen en beleidsterreinen heen op basis van een gezamenlijke strategie en gevolgd door nauwe coördinatie bij de uitvoering.*

Grip op nieuwe technologische ontwikkelingen

Nieuwe technologieën moeten standaard cyberveilig zijn en blijven. Om daar grip op te krijgen en te houden is het noodzakelijk om zicht te hebben op het landschap waarin technologieën worden ontwikkeld en vermarkt. Bovendien is inzicht nodig in de dynamiek die bestaat tussen de verschillende spelers, belangen en afwegingen in dat landschap. Om hierin te voorzien en kansen tijdig te kunnen benutten, dient er enerzijds een beeld te komen dat dit inzichtelijk maakt en anderzijds beleid om dit te faciliteren en grip uit te oefenen. Innovaties moeten ruim baan krijgen, maar wel voldoen aan gestelde eisen aangaande cyberveiligheid. Tevens moeten we onnodige kostbare correcties in grootschalige digitale infrastructuren voorkomen. We moeten dus vooraf goed in kunnen schatten welke mogelijke problemen met nieuwe

[8] Digitale Veiligheid als voorwaarde voor digitale transformatie, Cyberveilig Nederland, 2020
[9] Onderzoek naar versterken van de innovatieketen op het terrein van cybersecurity, TNO in opdracht van het Ministerie van Economische Zaken en Klimaat, 2020
[10] Kamerbrief over resultaten verkenningen en vervolgaanpak cybersecurity kennisontwikkeling en innovatie, Ministerie van Economische Zaken en Klimaat, d.d. 9 april 2020
[11] Zie ook 'Krachtiger kiezen voor sleuteltechnologieën', Adviesraad voor wetenschap, technologie en innovatie, 2020
[12] Kennis- en innovatieagenda Veiligheid, Ministerie van Economische Zaken en Klimaat, 2019
[13] Kennis- en innovatieagenda Sleuteltechnologieën 2020-2023, Ministerie van Economische Zaken en Klimaat, 2019
[14] Kamerbrief over resultaten verkenningen en vervolgaanpak cybersecurity kennisontwikkeling en innovatie, Ministerie van Economische Zaken en Klimaat, d.d. 9 april 2020
[15] Krachtiger kiezen voor sleuteltechnologieën, Adviesraad voor Wetenschap, Technologie en Innovatie, 2020
[16] Kennis- en Innovatieconvenant 2020-2023, Den Haag (2019): Hierin is € 5,5 miljoen gereserveerd over een periode van vijf jaar ten behoeve van cyberveiligheid.

technologieën en leveranciers zich kunnen aandienen. Zaken als (Europese) normering, toezicht en certificering van belang, evenals standaardisatie moeten hierop aansluiten. Hoewel op deze gebieden reeds een en ander is ondernomen[17], valt er nog veel te winnen. Een periodieke rapportage over de verwachte impact (zowel positief als negatief) van nieuwe technologie op onze cyberweerbaarheid en digitale autonomie kan daaraan een nuttige bijdrage leveren.

Gericht en daadkrachtig innovatie- en industriebeleid

De raad acht van belang dat er gericht wordt geïnnoveerd en geïnvesteerd in de inzet van nieuwe technologieën die noodzakelijk zijn voor het vooruitbrengen en het beschermen van onze digitale samenleving. Gezien de grote belangen die op het spel staan, zullen we bewust positie moeten innemen. Zowel op nationaal als Europees niveau. Het gaat dan over het maken van keuzes omtrent de inzet van nieuwe technologie om enerzijds op wereldschaal mee te kunnen doen en de kansen die deze technologieën bieden te kunnen pakken en anderzijds voor het behoud van onze digitale weerbaarheid, digitale autonomie en de normen en waarden in onze democratie. Daarbij is het van belang dat bedrijven in Nederland in een florerend ecosysteem acteren; een ecosysteem waarin zij de mogelijkheid hebben om te groeien door voldoende toegang tot onder andere talent, data en financiering. Er dient bovendien bewust geïnventariseerd te worden welke start-ups, 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.

Een goed voorbeeld van een proactieve technologie strategie is de Defensie Industrie Strategie[18]. Hierin is vanuit nationaal veiligheidsbelang (hetgeen uitdrukkelijk ook cyberdreigingen omvat) beoordeeld welke kennis, technologie en industriële capaciteiten Nederland zelf in huis dient te hebben en hoe dit met actief Nederlands industrieel participatiebeleid kan worden geborgd, waarbij Defensie vaker optreedt als *launching customer*. Hierdoor kan ook de Nederlandse inbreng bij de Europese digitale agenda en initiatieven worden versterkt. Hoewel de *Defensie Industrie Strategie* een goed voorbeeld is, *acht de raad een nog fundamentelere bundeling van (financiële) krachten noodzakelijk om onze cyberveiligheid en digitale autonomie ook in de toekomst te borgen. Publieke en private organisaties en ook wetenschappelijke instituten die zich bezighouden met initiatieven op het terrein van cyberweerbaarheid zullen moeten samenwerken om een eenduidige innovatieagenda voor cyberweerbaarheid en digitale autonomie uit te voeren. Alleen dan kunnen we als Nederland een relevante bijdrage leveren, ook aan de Europese digitale strategische agenda.*

[17] Denk aan de Wbni uit 2018, die stelt dat aanbieders ‘passende en evenredige technische en organisatorische maatregelen’ moeten treffen om opgeslagen of verwerkte gegevens te beveiligen. Daarnaast is in 2018 de Europese Cybersecurity Act aangenomen, die voorziet in een Cybersecurity Certificates Framework voor digitale producten en diensten.

[18] Defensie Industrie Strategie, Ministerie van Defensie en het Ministerie van Economische Zaken en Klimaat, 2018

ADVIEZEN

Naar het oordeel van de raad geeft het rapport van het Rathenau Instituut (RI) een goed inzicht in de wijze waarop nieuwe technologieën kunnen bijdragen aan het verhogen van de cyberweerbaarheid in Nederland en wat de randvoorwaarden zijn voor het benutten van deze technologische kansen, dit conform de opdracht van de raad. De raad acht echter de nieuwe technologieën dermate onderling verweven, dat bij een eenzijdige focus op cyberweerbaarheid, de grotere implicaties voor de digitale autonomie van Nederland worden gemist. De raad beveelt dan ook aan over te gaan tot het opstellen van een jaarlijkse rapportage waar de technische ontwikkelingen in kaart worden gebracht die relevant zijn voor het benutten en creëren van kansen, het borgen van cyberweerbaarheid en de bredere digitale autonomie van Nederland.

Het is de overtuiging van de raad dat zonder inzage in de snel veranderende technologie om ons heen en de daaruit voortvloeiende afhankelijkheden, ons land terecht zal komen op een onomkeerbaar pad van geleidelijke erosie van onze nationale technologische en industriële capaciteiten. Dit vereist een transparante gezamenlijke investering over departementen en beleidsterreinen heen, gevolgd door nauwe coördinatie bij de uitvoering op basis van een actief industriebeleid voor cybersecurity.

1. **De overheid ontwikkelt integraal beleid rondom nieuwe technologieën met impact op cyberweerbaarheid.**
2. **De overheid werkt aan het jaarlijks in kaart brengen van de technische ontwikkelingen die relevant zijn voor het benutten en creëren van kansen, het borgen van cyberweerbaarheid en de bredere digitale autonomie van Nederland.**
3. **De overheid voert een actief industriebeleid voor cybersecurity.**
4. **De overheid stimuleert (inter)nationale samenwerking bij relevante technologieën voor cybersecurity.**

Ad 1. De overheid ontwikkelt integraal beleid rondom nieuwe technologieën met impact op cyberweerbaarheid.

Nieuwe technologieën bieden kansen en risico's voor de cyberweerbaarheid van Nederland. De raad is bezorgd dat de snelheid waarmee beleid wordt ontwikkeld en geïmplementeerd, achterblijft op de snelle ontwikkeling van nieuwe technologieën. De realisatie van het Samenwerkingsplatform Cybersecurity en Innovatie binnen het Ministerie van Economische Zaken en Klimaat is volgens de raad een grote stap in de goede richting voor het realiseren van regie op samenwerking, de uitvoering van een meerjaren-programmering, zoals beschreven in de KIA Veiligheid, en het voorzien in de dekkende middelen die hiervoor nodig zijn.

Het tijdig benutten van kansen die nieuwe technologieën bieden, vereist nauwe interdepartementale samenwerking tussen de relevante stakeholders waaronder de ministeries van Defensie, Justitie en Veiligheid, Economische Zaken en Klimaat en Onderwijs, Cultuur en Wetenschap (OCW) [19].

Ad 2. De overheid werkt aan het jaarlijks in kaart brengen van de technische ontwikkelingen die relevant zijn voor het benutten en creëren van kansen, het borgen van cyberweerbaarheid en de bredere digitale autonomie van Nederland.

Voor het opstellen en uitvoeren van een integraal beleid rondom nieuwe technologieën met impact op cyberweerbaarheid is vereist dat er een periodiek geactualiseerd overzicht is van relevante nieuwe technologieën en bestaande technologieën met nieuwe toepassingsmogelijkheden bezien vanuit kansen en risico's voor de cyberweerbaarheid van Nederland. Ook dient de rapportage afhankelijkheden in kaart te brengen van buitenlandse of monopolistische leveranciers die gevolgen (kunnen) hebben voor onze digitale autonomie. Het beschermen van onze vitale processen in de vitale infrastructuur en het beschermen van intellectueel eigendom binnen onze topsectoren behoeven hierbij specifieke aandacht. De rapportage zal verder goed moeten aansluiten bij ontwikkelingen geschetst in het Cybersecuritybeeld Nederland (CSBN) en andere initiatieven op het gebied van technologische ontwikkelingen.

Ad 3. De overheid voert een actief industriebeleid voor cybersecurity.

De overheid heeft een leidende rol bij het voeren een actief industriebeleid. Organisaties in de wetenschap, publieke en private sector bouwen voortdurend aan technologische en industriële capaciteiten die uniek zijn in de wereld. In navolging van het industriebeleid in de Defensie Industrie Strategie, dienen ook de andere departementen daarin hun traditionele subsidiërende rol uit te breiden met een rol als launching customers. De overheid heeft direct baat bij de inzet van nieuwe technologieën en biedt tegelijkertijd een aantrekkelijk perspectief aan organisaties die zich daarvoor inzetten.

De uitvoering van dit industriebeleid vereist een nog fundamentelere bundeling van (financiële) krachten binnen de overheid. Dit omvat het gereserveerde budget van 5,5 miljoen voor het samenwerkingsplatform Cybersecurity en Innovatie, vermeerderd met de budgetten die zijn gereserveerd binnen de andere (sleutel)technologieën in de Kennis & Innovatieagenda voor onderzoek en ontwikkeling ten behoeve van cyberweerbaarheid. Deze bundeling van (financiële) krachten maakt ook gerichte investeringen vanuit het bedrijfsleven mogelijk. De raad adviseert om deze bundeling ook door te voeren in een tussentijdse update van de KIA Veiligheid (de KIA Veiligheid 2021) in aansluiting op de digitaliseringsstrategie 2020. De totale investeringen kunnen dan, in navolging van de huidige KIA Veiligheid, worden opgenomen in het Convenant KIA Veiligheid 2021. De doelgroep van deze KIA Veiligheid 2021 dient daarbij breder te zijn dan alleen de topsectoren en zich ook te richten op de vitale infrastructuur, nationale veiligheid en grootschalige collectieve bulkoplossingen voor het midden- en kleinbedrijf. Lokale overheden kunnen ook interessante investerings- en innovatiepartners zijn, denk daarbij aan smart cities.

Ad 4. De overheid stimuleert (inter)nationale samenwerking bij relevante technologieën voor cybersecurity.

Publieke en private organisaties en ook wetenschappelijke instituten, die zich bezighouden met initiatieven op het terrein van cyberweerbaarheid, zullen nauw moeten samenwerken om een eenduidige

[19] Kamerbrief over resultaten verkenningen en vervolgaanpak cybersecurity kennisontwikkeling en innovatie, Ministerie van Economische Zaken en Klimaat, d.d. 9 april 2020

innovatieagenda voor cyberweerbaarheid en digitale autonomie uit te voeren. Een periodiek beeld van technologieën biedt de mogelijkheid om relevante technologieën vroegtijdig te identificeren zodat er eventueel coalities kunnen worden gesloten waarbinnen kennis over cybersecurity kan worden opgebouwd en informatie gedeeld. Nederland heeft reeds enkele succesvolle coalities voor nieuwe technologieën als blockchain en Artificiële Intelligentie. De raad vraagt bestaande coalities hier ook voldoende aandacht aan te besteden.

Veel van de betrokken organisaties werken ook op Europees niveau samen. Door het vormen van gerichte internationale coalities van gelijkgestemde Europese landen rondom specifieke nieuwe technologieën kan Nederland haar technologische en industriële capaciteiten breder stimuleren. Instrumenten die deze ontwikkeling kunnen bevorderen (zoals normering, standaardisering en certificering), moeten hiertoe worden ingezet.

GERICHTE ADVIEZEN

De adviezen van de raad zijn gericht op de overheid en via de overheid ook op het bedrijfsleven. Alleen als er beter wordt samengewerkt tussen de publieke sector, de private sector en kennisinstellingen kan de cyberweerbaarheid ook in de toekomst worden gegarandeerd en kan de Nederlandse samenleving ook in de toekomst vertrouwen op de veiligheid en continuïteit van onze digitale maatschappij.

De raad adviseert de minister van Justitie en Veiligheid en de staatssecretaris van Economische Zaken en Klimaat gezamenlijk om, in samenwerking met de belangrijkste stakeholders (publiek, privaat en wetenschap)[20], de volgende acties in gang te zetten:

1. Maak begin 2021 een aanvang met het ontwikkelen van krachtdadig technologiebeleid voor cyberweerbaarheid gebaseerd op het jaarlijks te actualiseren overzicht van technische ontwikkelingen die relevant zijn voor cyberweerbaarheid. Het creëren en benutten van kansen, het borgen van cyberweerbaarheid en de bredere digitale autonomie van Nederland staan in deze rapportage centraal.

De raad adviseert de staatssecretaris van Economische Zaken en Klimaat om in samenwerking met de belangrijkste stakeholders de volgende acties in gang te zetten:

2. Lanceer uiterlijk 1 oktober 2020 het Samenwerkingsplatform Cybersecurity en Innovatie en draag ervoor zorg dat dit platform over voldoende slagkracht, mandaat en (financiële) middelen beschikt. Het samenwerkingsplatform brengt vraag, aanbod en financiering voor cybersecurity in het onderwijs, onderzoek, innovatie en collectieve toepassingen bij elkaar.
3. Stimuleer een actief industriebeleid voor cybersecurity door het subsidiëren van onderzoek te combineren met een interdepartementale rol als launching customer.
4. Draag zorg voor het sluiten van nationale en internationale coalities en de inzet van bevorderende instrumenten (zoals normering, standaardisering en certificering). Interdepartementale samenwerking en samenwerking met lokale overheden dient hierbij te worden versterkt.

’s-Gravenhage,
Namens de Cyber Security Raad,

Hans de Jong
Covoorzitter CSR

Pieter-Jaap Aalbersberg
Covoorzitter CSR

[20] Zoals ook benoemd in de brief van staatssecretaris Keijzer van het ministerie van Economische Zaken en Klimaat, gericht aan de voorzitter van de Tweede Kamer der Staten-Generaal inzake 'Resultaten verkenningen en vervolgaanpak cybersecurity kennisontwikkeling en innovatie', dd. 9 april 2020.