Gooimeer 4-15
1411 DC Naarden

info@cyberveilignederland.nl
www.cyberveilignederland.nl

KvK 71802525

Ministerie van Justitie en Veiligheid
Aan:
Plv. NCTV en directeur Cybersecurity en Statelijke dreigingen
Hester Somsen

Naarden, 17 november 2022
Ref.: 202203

Betreft: Reactie Cyberveilig Nederland op Nederlandse Cybersecurity Strategie (NLCS)

Geachte mevrouw Somsen, beste Hester,

Recent heeft het kabinet de Nederlandse Cybersecurity Strategie (NLCS) naar de Tweede Kamer gestuurd. Cyberveilig Nederland, de belangenorganisatie van de cybersecuritysector in Nederland, is op verschillende momenten (inhoudelijk) betrokken geweest bij de totstandkoming van de NLCS.

Cyberveilig Nederland vindt het sterk dat Nederland nu een Cybersecurity Strategie heeft en dat niet, zoals in de voorliggende periode, is gekozen voor een agenda. Niet alleen geeft een strategie een duidelijke stip op de horizon, met prioriteiten, budget en keuzes, maar is deze ook minder vrijblijvend. Want actie op het onderwerp is noodzakelijk, zoals het Cybersecurity Beeld Nederland en diverse incidenten zoals die met Citrix en Log4j in de afgelopen jaren hebben laten zien.

In deze brief geven wij onze reactie op de NLCS én stellen wij voor hoe wij, als securitybranche, gaan bijdragen aan het slagen van de NLCS en daarmee aan het verhogen van de weerbaarheid van Nederland. In de bijlage geven wij aan waar Cyberveilig Nederland een rol voor zichzelf ziet weggelegd in de actiepunten, zoals deze zijn geformuleerd in de bijlage van de NLCS.

Het belang van een breed gedragen strategie

Het onderwerp cybersecurity is niet meer weg te denken. Discontinuïteit bij slachtoffers van cybercrime of hun ketenpartners is aan de orde van de dag. De huidige geopolitieke context zorgt voor een toenemende dreiging voor Nederland, waarbij niet alleen vitale sectoren doelwit zijn, maar ook het verwerven van hoogwaardige kennis een belangrijke doelstelling is van kwaadwillenden. Naast de IT-infrastructuur is ook de OT-infrastructuur (Operationele Technologie/Industrial Automation Control Systems) kwetsbaar voor aanvallen en verstoring. En ga zo maar door. Kortom: Cyberveilig Nederland is verheugd dat er voor de komende jaren een cybersecuritystrategie is vastgesteld die gaat bijdragen aan het verhogen van de cyberweerbaarheid van Nederland en het verminderen van de dreiging.

Graag willen we als cybersecuritysector een actieve bijdrage leveren aan deze strategie. In deze brief ga ik daarom in op zowel de sterke elementen van de strategie, als op de aandachtspunten die we zien. Verder hebben we op een rij gezet bij welke actielijnen we een rol voor onszelf en onze leden zien weggelegd om de overheid te helpen in het doen slagen van de strategie.

Het proces om te komen tot een breed gedragen strategie is een weerbarstige geweest. Cyberveilig Nederland ziet dat de NCTV, als coördinator van de NLCS, goed heeft geluisterd naar de input van Cyberveilig Nederland en haar leden en deze heeft verwerkt in de strategie.

Sterke elementen in de NLCS

Graag willen we de belangrijkste positieve elementen uit de strategie benoemen:

- **We herkennen ons in de vier gekozen pijlers van de NLCS**. Er is een duidelijke keuze in prioriteiten op hoofdlijnen voor wat de komende jaren voorrang heeft in het vergroten van de weerbaarheid en het tegengaan van dreigingen. Het is een goede zaak dat in de NLCS het uitgangspunt wordt gehanteerd dat de burger niet (meer) verantwoordelijk wordt geacht voor digitale veiligheid.
- De NLCS is een overheidsstrategie én tegelijkertijd wordt de **verbinding met private partners** gemaakt. Wij zijn van mening dat voor een effectieve cybersecurity-aanpak publiek en privaat intensief moeten samenwerken en juichen deze verbinding toe en dragen er graag aan bij. We vinden het bovendien sterk dat in deze strategie nadrukkelijk andere departementen, naast het ministerie van JenV, aan de lat staan om de cyberrisico's tegen te gaan en de weerbaarheid te vergroten.

- We zijn positief gestemd dat gekozen is voor een **strategietermijn van 6 jaar**. Door deze langere termijn aanpak wordt er voor continuïteit in de uitvoering gezorgd, ook wanneer een ander kabinet aan de lat staat om Nederland te regeren.

- De **integratie van het DTC, CSIRT-DSP en het NCSC zien we positief tegemoet** en we zijn van mening dat dit eigenlijk al veel eerder had moeten gebeuren. Wel vinden we het van belang dat er aandacht is voor het behouden van wendbaarheid en goede initiatieven van de kleinere organisaties die bij de integratie betrokken zijn. Verder hopen we dat de interne aandacht voor de integratie niet ten koste zal gaan van de belangrijke taak waar deze organisaties voor staan.

Aandachtspunten

Naast de positieve elementen in de strategie zien we ook enkele aandachtspunten die we willen meegeven:

- De overheid heeft met de NLCS een ambitieuze strategie neergezet. Hoewel er op hoofdlijnen in de pijlers focus is aangegeven, mist die **focus** wat ons betreft in de uitwerking van de meer dan 100 (!) actielijnen. We maken ons daarom zorgen over de prioriteiten en de uitvoerbaarheid en daarmee samenhangend de resultaatgerichtheid van de NLCS. Ook is de koppeling tussen de NLCS en de actielijnen niet altijd duidelijk. Waarom is voor deze acties gekozen en hoe dragen ze bij aan de doelen die zijn gesteld? Ook liggen veel acties bij dezelfde organisaties of zelfs soms personen. Het lijkt ons goed als in de uitwerking een heldere roadmap wordt vastgesteld met haalbare doelen en beschikbare middelen voor de kortere termijn.

- Op 17 plekken in de NLCS worden nadrukkelijk private organisaties genoemd om onderwerpen uit de NLCS (te helpen) op te pakken. De NLCS maakt echter onvoldoende duidelijk welke partijen hiermee worden bedoeld en wat de Nederlandse overheid gaat doen om te zorgen dat deze partijen ook daadwerkelijk uitvoering geven aan de gewenste acties. In de praktijk zien wij dat in de samenwerking met de overheid hooggespannen verwachtingen zijn van de **inzet van private organisaties**, bijvoorbeeld rondom het delen van (dreigings)informatie. Wij maken ons zorgen over de daadwerkelijke mogelijkheden die private organisaties hebben om de strategie te realiseren. Cyberveilig Nederland fungeert graag als gesprekspartner om namens de cybersecuritysector uit te werken hoe betrokkenheid vorm kan worden gegeven.

- Het is positief dat er zoveel overheidsorganisaties deelnemen aan de NLCS. Hierin missen we echter voldoende aandacht voor **Defensie en diens strategie**. Ook zien we kansen om de **samenwerking en afstemming tussen de ministeries** te verbeteren

zodat met één gezamenlijke stem wordt gesproken en duidelijk is wie welke onderwerpen onder zijn hoede heeft.

- De NLCS legt zowel de nadruk op weerbaarheid verhogen als op het verminderen van de dreiging. Echter het **tegengaan van dreigingen en het verhogen van weerbaarheid gaan hand in hand.** In de NLCS worden deze vanuit aparte entiteiten beschreven, terwijl deze volgens Cyberveilig Nederland nadrukkelijk in samenhang moeten worden opgepakt.
- **Operational Technology/IACS** is, wat Cyberveilig Nederland betreft, nog onderbelicht in de strategie. Dit terwijl niet alleen de vitale infrastructuur in Nederland afhankelijk is van een betrouwbaar, beschikbaar en integer IACS, maar heel Nederland 'draait' op IACS. Denk bijvoorbeeld aan bedrijven die betrokken zijn bij de productie, verwerking en distributie van levensmiddelen en aan bedrijven die betrokken zijn bij de productie, verwerking en distributie van chemische stoffen. We vragen daarom nadrukkelijke aandacht voor de opbouw van kennis en expertise in de uitvoering van deze strategie. Deze komt al wel aan bod in de NLCS, maar mist vanuit de mening van Cyberveilig Nederland aan urgentie en prioriteit.
- We missen de positieve framing en **kansen van cybersecurity** in de NLCS. Onderwerpen als Security by design of Security by default, die kansen bieden voor het (innovatieve) bedrijfsleven komen weinig aan de orde, terwijl deze juist voor het structureel verhogen van weerbaarheid essentieel zijn.
- Er zijn al diverse **private initiatieven** die ondersteunend kunnen zijn bij de implementatie van de NLCS. In plaats van het wiel opnieuw uit te vinden lijkt het ons goed als hiermee **samenwerking** wordt gezocht. Bijvoorbeeld rondom cybersecurity in het onderwijs. Het onderwijssysteem heeft tijd nodig om te bewegen. Tegelijkertijd zijn er al private initiatieven zoals HackShield die meermaals zijn gevalideerd, op impact en effect beoordeeld en breed worden gedragen bij publieke en private organisaties.
- Het **proces** rondom de totstandkoming van de NLCS is, wat ons betreft, voor verbetering vatbaar. Het is prettig als vooraf de tijdslijnen en mogelijkheden tot het geven van input worden gedeeld, waardoor wij en onze leden ons beter inhoudelijk kunnen voorbereiden op wat er nodig is. Ook vonden veel meetings plaats in de zomerperiode en was het soms onduidelijk waarom ons op bepaalde onderwerpen wel om input werd gevraagd en op andere niet. Graag worden we actief betrokken bij het voorbereidingsproces voor de implementatie van de NLCS zodat we de benodigde input vanuit de cybersecuritysector op goede wijze kunnen organiseren.

Prioritering acties vanuit Cyberveilig Nederland

In de bijlage bij deze brief hebben wij concreet uiteengezet waar wij als brancheverenigingmet onze leden verwachten van meerwaarde te kunnen zijn bij de uitvoering van de strategie. Aangezien de strategie en de bijbehorende actielijnen een langere periode betreffen, zijn wat ons betreft prioritair:

1. **Informatieuitwisseling**, met de focus op het Cyclotron-programma en het ontwikkelen van een register voor incidenten en kwetsbaarheden
2. Implementatie **NIB-richtlijn**, inclusief voorlichting en communicatie
3. **Certificering**, inclusief ontwikkelingen ABRO
4. **IACS**-coalitie

Tenslotte: met de nieuwe strategie zullen er vanuit de overheid in de komende jaren verschillende nieuwe initiatieven rondom de uitvoering van de NLCS worden ontplooid. We vragen nadrukkelijk aandacht voor het gegeven dat er al veel is bereikt in de afgelopen jaren en er daardoor al veel zaken in de basis al zijn gerealiseerd. Juist door deze initiatieven te consolideren en eenduidigheid na te streven (bijvoorbeeld over 'wat zijn de basismaatregelen') kunnen met weinig inspanning al snel de eerste positieve resultaten worden geboekt.

Over deze onderwerpen en onze betrokkenheid bij de implementatie van de NLCS gaan we met plezier verder in gesprek. Graag maken we de strategie gezamenlijk tot een succes!

Met vriendelijke groet,

Petra Oldengarm
Directeur Cyberveilig Nederland

Bijlage 1. Actiepunten NLCS

Pijler I Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties

Actie	Inbreng Cyberveilig Nederland (en leden)
Samen met het bedrijfsleven wordt een routekaart opgesteld voor de implementatie van een publiek-privaat platform voor wederkerige cybersecurity informatie- en kennisdeling. De basis voor dit traject is het opgeleverde Cyclotronrapport.	Als schakel (OKTT)-organisatie deelt CVNL momenteel al (dreigings)informatie met het NCSC en zijn we op andere vlakken begonnen met het uitwisselen vann informatie. Continuering van de huidige samenwerking en uitbouwen van verdere informatiedeling met (o.a.) het NCSC zal actief vanuit CVNL opgepakt worden.
Het NCSC verkent met partners de haalbaarheid van een centrale landelijke campus/locatie ter bevordering van samenwerking, informatiedeling, kennisontwikkeling en onderzoek tussen publieke en private partijen.	CVNL en de leden worden actief betrokken bij de verkenning vanuit het NCSC. Eerste reactie vanuit CVNL en de leden is dat zij hier graag aan meedenken/meehelpen.
In interdepartementaal verband worden eisen voor aansluiting op het LDS geformuleerd. Deze zullen verplichtend zijn voor overheidsschakelorganisaties en als richtinggevende leidraden gelden voor private schakelorganisaties. Private partners worden betrokken bij de uitwerking van deze leidraden	Als schakelorganisatie (OKTT) willen we vanuit CVNL actief meedenken aan de eisen aan en richtlijnen voor de (uitwerking van de) leidraden.
Het kabinet start in 2023 met uitgebreide voorlichtingscampagnes om organisaties die onder de nieuwe wet komen te vallen te informeren over voor hun geldende rechten en plichten, en hen actief te begeleiden bij de implementatie.	CVNL wil hierin gezamenlijk optrekken met de overheid om dezelfde boodschap te uitten. CVNL ziet voor zichzelf en haar leden een rol om de klanten van (leden van CVNL) te informeren over de voorlichtingscampagne rondom de implementatie van de NIB-richtlijn. Daarin is zicht op wie onder de NIB-richtlijn valt (op hoofdlijnen) noodzakelijk.
NCSC en DTC ontwikkelen nieuwe producten en diensten met onder andere aandacht voor inbedding van cybersecurity	CVNL (en haar leden) werkt (werken) op dit moment al met het NCSC en het DTC samen

in het risicomanagementproces; crisispreparatie; incidentrespons en thematische advisering. Deze gedifferentieerde en datagedreven informatie- en kennisproducten en -diensten worden gezamenlijk en laagdrempelig beschikbaar gesteld ten behoeve van organisaties op een manier die past bij het volwassenheidsniveau.	in de ontwikkeling van kennisproducten. Uiteraard gaan we hier graag mee door. Daarnaast nog twee kanttekeningen: 1. Kijk niet alleen naar nieuwe producten en diensten, maar kijk ook of bestaande (verouderde) producten en diensten in een 'nieuw jasje' kunnen worden gegoten 2. Betrek naast het DTC en NCSC ook andere overheidsorganisaties die kunnen bijdragen, zoals CIO Rijk, Agentschap Telecom, etc.
Realisatie van eerste versie van centrale registers voor cybersecurity gerelateerde informatie (i.e. type ransomware, kwetsbaarheden).	Vanuit de informatiedeling en de kennis over CVD zien wij een rol in het (vullen van) de centrale registers. CVNL zal op de zeer korte termijn een MISP-omgeving operationaliseren waar leden IOC's met elkaar kunnen delen. We betrekken het NCSC nauw bij deze ontwikkelingen en onze ervaring kan gebruikt worden voor de realisatie van een centraal register. Ook kan het CVNL-register gekoppeld worden aan het centrale register van het NCSC, vanuit de OKTT-status.
De aanpak om de beveiliging van Industrial Automation and Control Systems (IACS) te verhogen wordt versterkt door middel van een coalitie. Voorbeelden van acties binnen de coalitie zijn: • De ontwikkeling en implementatie van een (significante en realistische) IACS component in landelijke oefeningen, trainingen en opleidingen. • De versterking van kennisopbouw en de realisatie van instrumenten, bijvoorbeeld handreikingen en best practices om publieke en private organisaties te helpen om voor IACS de juiste maatregelen te implementeren en de juiste risico's te definiëren en aan te pakken. • Het delen van deze kennisproducten en instrumenten via een collectieve kennis hub IACS.	CVNL en onze leden willen graag participeren in deze coalitie. De cybersecuritysector heeft ervaring opgebouwd in cybersecurity van IACS, in zowel kennis, instrumentarium, best practices, etc.

Er wordt samen met het brede cybersecurityveld een monitoringssystematiek voor de digitale weerbaarheid van Nederland opgezet. Een eerste rapportage wordt 2024 verwacht.	CVNL en haar leden werken hier graag aan mee.
De nationale oefening ISIDOOR wordt georganiseerd. De deelnemers worden in aanloop hiernaartoe gestimuleerd dat organisaties eigen plannen en procedures hebben vastgelegd en hun medewerkers hiervoor zijn opgeleid en getraind.	CVNL neemt vanuit de OKTT-status al deel aan ISIDOOR. We willen nadrukkelijk in gesprek met het NCSC hoe de leden van CVNL (meer) betrokken kunnen worden bij ISIDOOR, aangezien veel klanten van onze leden al betrokken zijn bij ISIDOOR.
Ontwikkeling van kennisproducten/ diensten om organisaties te adviseren over hun incidentresponsprocessen (factsheets, whitepapers, runbooks etc.)	CVNL helpt al mee met verschillende kennisproducten van de overheid en gaat hier graag mee door.
Inlichtingengebaseerde incidentcoördinatie vanuit de AIVD en MIVD wordt verder uitgebouwd, onder andere via samenwerking in de CIIC.	CVNL ziet graag dat het CIIC wordt uitgebouwd met (specifieke) cybersecurity bedrijven. CVNL wil graag met het CIIC in gesprek over de voorwaarden voor de toetreding van private organisaties binnen het CIIC.

Pijler II Veilige en innovatieve digitale producten en diensten

Actie	Inbreng Cyberveilig Nederland (en leden)
Het kabinet maakt zich in de onderhandelingen voor de Europese Cyber Resilience Act (CRA) hard voor opname van een zorgplicht voor fabrikanten en leveranciers van alle ICT-producten, diensten en processen, inclusief bijbehorende standaarden en toezicht. Deze zorgplicht moet gedurende de hele levenscyclus blijven gelden.	CVNL wordt graag geïnformeerd over de stand van zaken. Hiertoe zijn al de contacten met EZK gelegd.
Het kabinet zet in op de ontwikkeling van Europese certificeringschema's voor veilige software en cybersecurity diensten.	CVNL pleit ervoor om in Nederland ontwikkelde certificeringsschema's ook binnen de EU in te zetten als keurmerk/certificeringsschema (normenkader) voor, bijvoorbeeld, NIS2. Voorbeelden zijn het al ontwikkelde keurmerk pentesten (beheerd door het

	CCV) en nieuw te ontwikkelen schema's voor bijvoorbeeld monitoringsdiensten, diensten rondom awareness en gedrag, incident respons diensten en risicoanalyses
Er wordt verkend hoe organisaties beter in staat kunnen worden gesteld om duidelijke afspraken te maken over cybersecurity met hun afnemers middels onderzoek naar de contractrechtpraktijk en best practices in business-to-business relaties tussen aanbieders van ICT-producten en -diensten en afnemers.	CVNL denkt hier graag over mee. Vanuit de Cybersecurity Alliantie heft CVNL al meegewerkt aan een 'praatplaat' hoe MKB-bedrijven beter het gesprek over cybersecurity kunnen aangaan met hun IT-partner.
Er worden Algemene Beveiligingseisen opgesteld voor de Rijksoverheid (ABRO), op basis van doorontwikkeling van het bestaande regime Algemene beveiligingseisen Defensieopdrachten (ABDO), waaraan bedrijven die gevoelige en/of gerubriceerde overheidsopdrachten vervullen moeten voldoen.	CVNL denkt graag mee in de opstelling van deze beveiligingseisen. Diverse leden van CVNL voldoen al aan de ABDO. Deze ervaring zetten wij graag in t.b.v. de ABRO.
De tool inkoopeisen cybersecurity overheid (ICO) wordt doorontwikkeld, verbreed en geïmplementeerd. Inclusief verdere ontwikkeling van overheidsbrede eisensets. Dit zal indirect de markt positief beïnvloeden om veilige producten en diensten te leveren.	CVNL is ruim vier jaar geleden opgericht om de kwaliteit en transparantie van de sector te vergroten. Inmiddels hebben we hier als vereniging diverse stappen in gezet. De ervaring die wij hebben opgebouwd willen wij graag delen om de tool van inkoop eisen cybersecurity overheid werkbaar en transparant te maken.
De productontwikkeling voor high assurance producten wordt gestimuleerd middels versterkt en eensgezind opdrachtgeverschap vanuit de Rijksoverheid, zodat Nederland de beschikking houdt over betrouwbare cryptografische oplossingen. Dat gebeurt in nauwe samenwerking met de Nederlandse cryptografische-industrie.	Via dcypher is CVNL aangehaakt op de productontwikkeling voor assurance producten. Dat continueren we graag. Wat CVNL betreft moet er wel sprake zijn van onderscheid tussen high assurance en low assurance. Voor het eerste geldt dan een trusted partnership met specifieke bedrijven omdat dit onderwerpen rondom nationale veiligheid betreft.
In samenwerking met bedrijven en wetenschappelijke instellingen wordt onderzoek uitgevoerd naar de ontwikkeling	CVNL onderhoudt nauwe contacten met dcypher en heeft ook zitting in het bestuur. Deze samenwerking continueren wij graag de komende tijd.

van moderne en hoogwaardige beveiligingsproducten.	
Het kabinet zet meerjarige thematische routekaarten op aan de hand waarvan onderzoek wordt uitgevoerd of uitgezet middels het platform dcypher. Dit is inclusief een routekaart op cryptocommunicatie en voor geautomatiseerd kwetsbaarhedenonderzoek.	CVNL onderhoudt nauwe contacten met dcypher en heeft ook zitting in het bestuur. Deze samenwerking continueren wij graag de komende tijd.
De cybersecurity kennis-en innovatiebehoefte van het bedrijfsleven en kennisinstellingen wordt onderdeel van het Nederlandse Topsectoren Programma	CVNL zit in de stuurgroep van CS4NL-BGP (Breed Gedragen Programma) en is op deze manier aangehaakt.

Pijler III Tegengaan van digitale dreigingen van staten en criminelen

Actie	Inbreng Cyberveilig Nederland (en leden)
Politie en OM zetten, naast strafrechtelijke interventies, met lokaal bestuur en private partners in op het ontwikkelen van niet-strafrechtelijke interventies ter bestrijding van cybercrime, waaronder ransomware.	CVNL werkt, samen met enkele incident respons leden, actief samen op dit onderwerp met het OM en de Politie. Graag continueren wij deze samenwerking.
Politie en OM zetten, naast strafrechtelijke interventies, met lokaal bestuur en private partners in op het ontwikkelen van niet-strafrechtelijke interventies ter bestrijding van cybercrime, waaronder ransomware.	CVNL werkt, samen met enkele incident respons leden, actief samen op dit onderwerp met het OM en de Politie. Graag continueren wij deze samenwerking.
De politie stelt jaarlijks een veiligheidsbeeld over cybercrime en gedigitaliseerde criminaliteit op, waarin de belangrijkste criminele fenomenen, werkwijzen en het risico hiervan voor de samenleving geschetst worden. De beelden geven richting aan de keuze van de politie en het OM voor de fenomenen waarop wordt ingezet en de onderzoeken die worden geprioriteerd.	CVNL draagt graag informatie aan die het veiligheidsbeeld kan aanvullen/versterken.

Pijler IV Cybersecurity-arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers

Actie	Inbreng Cyberveilig Nederland (en leden)
Onderwijsinstellingen werken aan bijen omscholingsprogramma's om de cybersecurity-expertise van werknemers te vergroten. Daartoe werken zij samen met het bedrijfsleven en andere relevante partijen. Hierbij worden o.a. knelpunten en beperkingen in die samenwerking voortvloeiend uit regelgeving geïnventariseerd en bezien welke oplossingen daarvoor nodig zijn.	CVNL en HackShield werken samen om met en via de CVNL leden, de politie, de gemeenten en alle andere HackShield partners gastlessen te verzorgen en kinderen mee te nemen in hun bijdrage aan een veilige digitale toekomst. Wij zetten ons graag in om samen met de overheid dit soort bestaande initiatieven breed te laten landen binnen het onderwijs.
Er wordt geïnvesteerd in hbo-opleidingen in de bètatechniek, waar cybersecurityopleidingen ook onderdeel van zijn. Middelen worden ingezet op (1) hogere instroom binnen de opleiding, (2) lagere uitval en switch, (3) hogere zijinstroom, (4) inductie/warme overgang van opleiding naar arbeidsmarkt. Het doel van deze maatregel is om de arbeidsmarkttekorten in te perken.	CVNL helpt opleidingen graag mee met het aanscherpen van het curriculum. Met verschillende hogescholen en MKB-opleidingen hebben we hier al positieve ervaringen mee.
De kwalitatieve en kwantitatieve tekorten op de cybersecurity arbeidsmarkt worden onderzocht, inclusief aanbevelingen hoe deze tekorten aan te pakken.	CVNL levert hier al op regelmatige basis input aan en zal dit continueren.
Het kabinet zet zich via de Human Capital Agenda ICT in om de instroom van cybersecurityspecialisten ICT-specialisten te vergroten en de kwaliteit van de instroom te beïnvloeden. Dit wordt in nauwe samenwerking met het bedrijfsleven, regionale en lokale overheidsinstellingen en onderwijsinstellingen opgepakt.	CVNL zet zich in voor een HCA voor cybersecurity. Immers cybersecurity is niet alleen een ICT-issue en door de HCA onder de HCA ICT te positioneren pak je het vraagstuk niet holistisch maar juist eendimensionaal op.
Via thematische routekaarten en communities worden gesprekken gefaciliteerd tussen kennisinstellingen en het bedrijfsleven met betrekking tot de	Via dcypher is CVNL hier al op aangesloten.

high-end kennisontwikkeling die nodig is om innovatieve productontwikkeling tot stand te brengen.	
JenV, EZK, BZK organiseren doelgroepspecifieke voorlichtingscampagneprogramma's cyberveiligheid gericht op de cybersecurity basismaatregelen. Er vindt een effectmeting plaats na elke campagne. De campagnes worden georganiseerd in samenwerking met gemeenten voor optimale inzet van de beschikbare gemeentelijke communicatiekanalen.	CVNL draagt al bij aan kennisproducten van de overheid en is ook bereid hier een (inhoudelijke) bijdragen aan te leveren.
De politie maakt vanaf 2023 voor meer cybercrime fenomenen het mogelijk om online melding of aangifte te doen.	CVNL helpt de politie graag mee om te zorgen dat het doen van aangiften wordt gestimuleerd.

Over Cyberveilig Nederland

Cyberveilig Nederland is dé belangenorganisatie voor cybersecurity bedrijven in Nederland. We brengen transparantie aan in de sector door de ontwikkeling van een gedragscode en keurmerk. We nemen actief deel aan het publieke debat en zien cybersecurity niet alleen als een risico, maar juist ook als een kans om Nederland te positioneren als een land dat veilige producten en diensten voortbrengt. We gaan het gesprek aan met de overheid en andere strategische partners om onze kennis en kunde van het cybersecurity werkveld voor het grotere belang in te zetten. We brengen verbindingen tot stand, tussen cybersecurity bedrijven onderling, maar ook brengen we vragers en aanbieders samen. We praten met de overheid en politiek om (toekomstige) knelpunten weg te nemen die de digitale weerbaarheid van Nederland in de weg staan. Maar vooral: we doen! We zijn initiatiefnemer en uitvoerder van het Cybersecurity Woordenboek en publiceren regelmatig documenten die de transparantie van de sector vergroten en vragers van cybersecurity diensten op weg helpen:

- https://cyberveilignederland.nl/woordenboek-cyberveilig-nederland/
- https://cyberveilignederland.nl/upload/userfiles/files/CVNLL_Buyersguide_Security_Testen_final2.pdf.