



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Bijlage 6 van het Bouwplan Cyberweerbaarheidsnetwerk (CWN)

Bouwplan CWN voor het Caribisch deel van het Koninkrijk

De aanpak van het NCSC om stappen te zetten in de samenwerking

Inleiding

In de periode september 2024 tot en met mei 2025 is er gewerkt aan een plan voor het Caribisch deel van het Koninkrijk der Nederlanden (CdvKNL). Het CdvKNL heeft andere behoeften op het gebied van het ontwikkelen van digitale weerbaarheid dan Nederland. Daarom is er een aparte aanpak opgesteld.

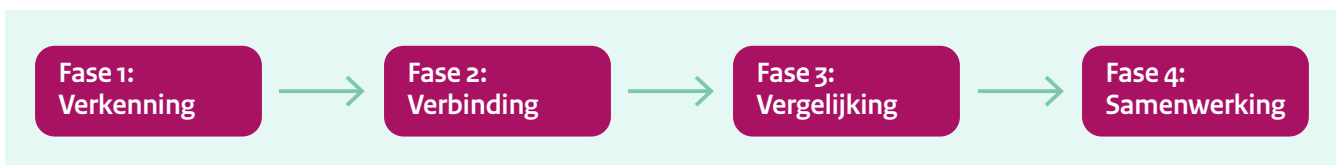
Dit plan is onderdeel van het bouwplan Cyberweerbaarheidsnetwerk (CWN) en is afgestemd met de verschillende betrokken beleidsdepartementen en uitvoeringsorganisaties. Het biedt een gestructureerd kader voor de aanpak van het opbouwen van een CWN in het CdvKNL dat recht doet aan de lokale context.

Van initiatieven naar netwerken

Er is een beleidskeuze gemaakt om het CWN te verbreden naar het volledige Koninkrijk der Nederlanden. Om het hele Koninkrijk te bereiken, moet actief worden gezocht naar een brede set met netwerkpartners die dit gezamenlijk mogelijk maken.¹ Daarom worden nieuwe netwerkpartners aangetrokken voor het CWN, zoals leveranciers van ICT- en securitydiensten die een belangrijke rol spelen in het weerbaar maken van organisaties.

In het Caribisch gebied komt steeds meer aandacht voor digitalisering en daarmee ook voor cybersecurity en digitale weerbaarheid. Omdat er daar (nog) geen vitale bedrijven zijn aangewezen, is er nog geen wettelijke plicht voor belangrijke bedrijven, zoals energie-, water- en telecombedrijven, om bepaalde maatregelen te treffen. Ook is er (nog) geen ondersteuning voor bedrijven en is er weinig samenwerking. Het project 'Versterken Cyberweerbaarheid Caribisch Nederland' van Matribu B.V. brengt daar verandering in, door laagdrempelige cybersecurity-scans aan te bieden en een ISAC-netwerk op te zetten. Hiermee wordt een begin gemaakt met het in kaart brengen en versterken van de weerbaarheid van bedrijven in dat deel van het Koninkrijk. In december 2024 kreeg het project de subsidie 'Versterking Cyberweerbaarheid' toegekend. Het DTC is de opdrachtgever van de subsidie en de uitvoering ligt bij de RVO.

Vanuit Nederland is er momenteel nog geen structureel overleg met het CdKNL. Het CWN kan binnen het hele Koninkrijk een faciliterende rol op zich nemen voor het verbinden van het netwerk om zo uiteindelijk in fases te werken aan een publiek-private-samenwerking. De fasering wijkt af van de bouw van het Cyberweerbaarheidsnetwerk binnen Nederland (zie hiervoor bijlage 1,2 en 3). Er wordt meer tijd uitgetrokken voor de bouw van het Cyberweerbaarheidsnetwerk met en binnen het CdKNL, waarbij de eerste focus zal liggen op de ontwikkeling in Caribisch Nederland². Wanneer daar de eerste stappen zijn gezet, zal er worden gekeken naar de opzet en samenwerking met de autonome landen. De aanloop daarnaartoe is uiteengezet in vier fases:



Figuur 1 – Vier fases opzetten netwerk

¹ Visie op het CWN pag. 41.

² Zie Bijlage A voor staatskundige verhoudingen, Caribisch Nederland is BES. Autonome landen zijn CAS.

Fase 1: Verkenning

Fase 1 staat in het teken van een brede verkenning met betrokken organisaties en stakeholders. Deze verkenning geeft inzicht in het huidige cyberdomein, bestaande samenwerkingen en initiatieven, wensen en behoeftes, risico's en afhankelijkheden, de cyberweerbaarheid in het CdKNL en de belangrijkste lokale netwerkpartners. Het uitgangspunt is dat het CWN voor CdKNL en voor de rest van het Koninkrijk dezelfde mogelijkheden biedt. Zowel de bijzondere gemeentes als de autonome landen, doen mee, waardoor er sprake is van een verschil in wet- en regelgeving³. Alle vormen van samenwerking en uitwisseling binnen het CWN moeten uiteraard in lijn zijn met de geldende wet- en regelgeving.

Momenteel bevinden we ons al in fase 1. Er is een begin gemaakt met het in kaart brengen van de netwerkpartners. Deze eerste verkenning vanuit het CWN is vooral gericht op Bonaire en is daarmee niet representatief voor het hele CdKNL. Het is raadzaam om deze verkenning eerst te verbreden naar de overige eilanden binnen Caribisch Nederland en daarna naar de autonome eilanden. In deze fase moet er aandacht voor en informatie over de lokale omstandigheden, sociaal-culturele context en huidige stand van zaken zijn. Zo moet er goed worden gekeken naar de verschillen in cultuur, handelen, expertise en beschikbare capaciteit en middelen in CdKNL ten opzichte van Nederland. Daarnaast is - zover deze er zijn - meer inzicht in bestaande samenwerkingen nodig, zodat deze op een passende manier bij het Cyberweerbaarheidsnetwerk betrokken kunnen worden en er gezamenlijk kan worden toegewerkt naar een reëel inzicht van de huidige cyberweerbaarheid in het CdKNL.

Fase 2: Verbinding

De uitkomsten van de verkenningsfase worden gebruikt in fase 2: verbinding. Van belang is om netwerkpartners met elkaar te verbinden en gezamenlijk de resultaten uit de verkenningsfase te analyseren. Zo kan een inventarisatie en prioritering worden gemaakt van de belangrijkste thema's op het gebied van cyberweerbaarheid. Deze thema's vormen de basis voor samenwerkingen binnen het CWN. Deze fase vindt plaats in een setting waar netwerkpartners in vertrouwen kunnen samenwerken, kennis kunnen delen en feedback kunnen geven.

Fase 3: Vergelijking

Fase 3 begint met de in fase 2 geprioriteerde thema's. Aan de hand daarvan wordt de gewenste situatie beschreven. Met een analyse van sterke en zwakke punten (gap-analyse) bekijken we vervolgens wat nog nodig is om bij deze gewenste situatie uit te komen. De uitkomsten vormen de beschrijvingen van de Cyberweerbaarheidsnetwerkfuncties en de basis waarop binnen het netwerk zal worden samengewerkt. Vanwege lokale omstandigheden kunnen de functies afwijken van die in Nederland. Wel is het van belang om uiteindelijk zoveel mogelijk de synergie op te zoeken tussen het CdKNL en Nederland, zo kan er efficiënt gebruik worden gemaakt van schaarse kennis, middelen en capaciteit binnen het CWN.

Fase 4: Samenwerking

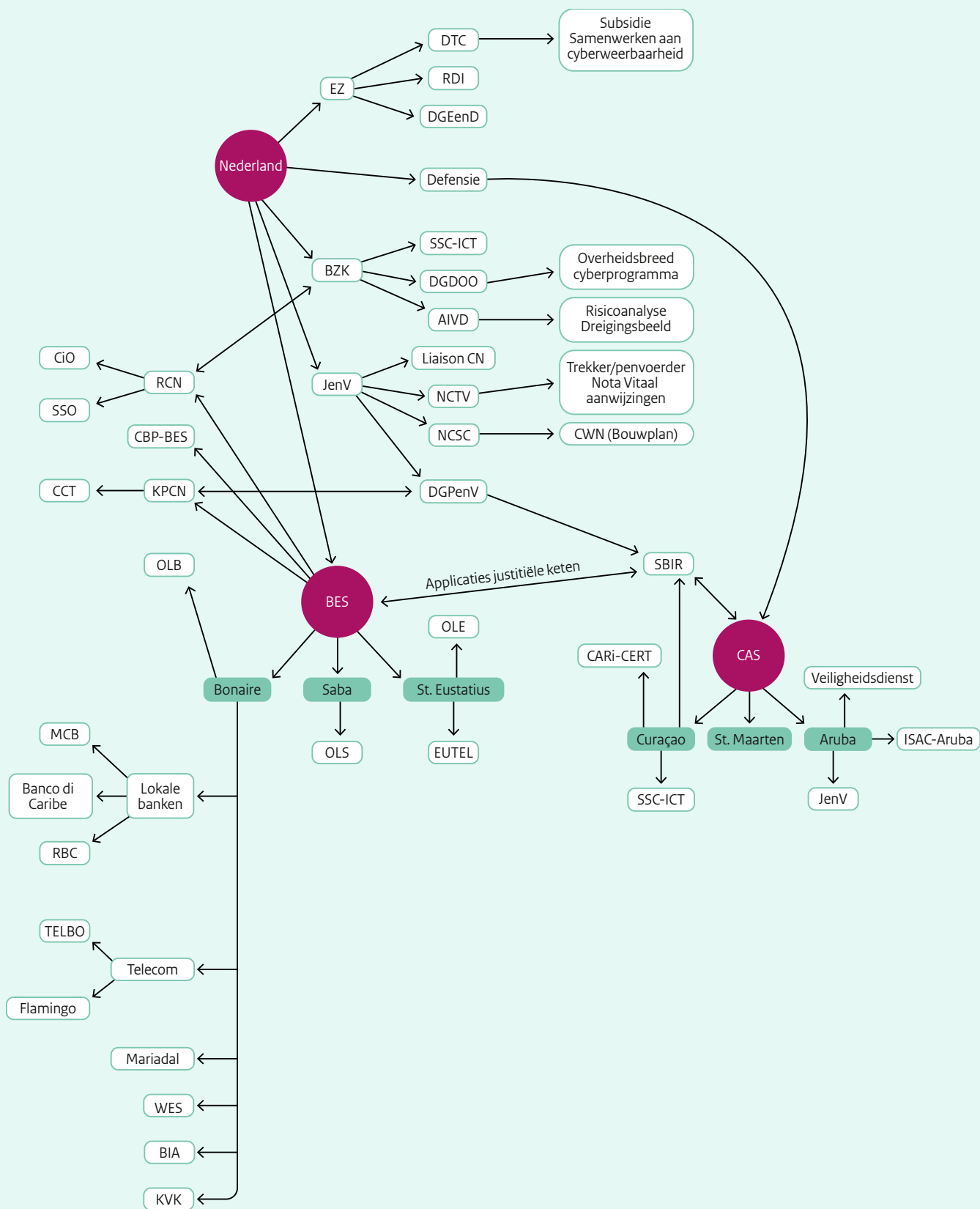
In fase 4 wordt er samen gewerkt aan de thema's en pijlers uit fase 2 en 3. Uitdagingen worden in vertrouwen met elkaar gedeeld en er wordt in het netwerk gezocht naar oplossingen. Er is een passend toekomstplan, opgezet door en voor de netwerkpartners, om de cyberweerbaarheid in het CdKNL te vergroten. De netwerkpartners zijn goed aangesloten bij de CWN's in het CdKNL en in Nederland. De netwerkpartners zijn in staat om zelfstandig de opgestelde Cyberweerbaarheidsnetwerkfuncties toe te passen en samen verder te ontwikkelen.

³ Voor de autonome landen geldt dat zij hun eigen wet- en regelgeving hebben, voor de Openbare Lichamen geldt dat oude Antilliaanse wetgeving al dan niet is gemoderniseerd en in gevallen Europees Nederlandse wetten ook voor CN van toepassing zijn zoals de Wet bevordering digitale weerbaarheid bedrijven.

Netwerkkkaart

De netwerkkkaart (Figuur 2) is ontstaan uit de eerste verkenning vanuit het Cyberweerbaarheidsnetwerk met de focus op Bonaire⁴. Het geeft een overzicht van (mogelijke) netwerkpartners en inzicht in onderlinge verhoudingen en afhankelijkheden. Er is niet met alle weergegeven organisaties contact geweest, wat voor een verdere verkenning wel gewenst is. Omdat we ons momenteel nog bevinden in fase 1, is de netwerkkkaart nog niet een complete weergave en zal deze nog worden aangevuld.

⁴ Deze netwerkkkaart geeft een eerste inzicht uit de verkenning vanuit het Cyberweerbaarheidsnetwerk. Derhalve bevat deze nog niet alle netwerkpartners, organisaties en/of initiatieven die betrekking hebben op het CdvNL (zowel voor het CdvNL als NL).



Figuur 2 – Netwerkkkaart verkenning

Activiteiten en Deliverables

Fase 1. Verkenning

Activiteiten	Deliverables	Timing en/of fase ⁵
In kaart brengen van netwerkpartners door NCSC vanuit CWN Zowel voor Caribisch Nederland (heeft de eerste focus) als voor de autonome landen. In samenwerking met BZK, EZ/DTC en JenV.	Publicatie van netwerkkaart met overzicht van netwerkpartners en samenhang.	Begin fase 1: • Caribisch Nederland: gereed Q1-2026; • Autonome landen: Q1-2027.
In kaart brengen van relevante initiatieven en overlap in gezamenlijkheid met NCSC, BZK, EZ/DTC en JenV Zowel voor Caribisch Nederland (heeft de eerste focus) als voor de autonome landen.	Publicatie-overzicht met initiatieven (zowel lokaal als departementaal).	Begin fase 1: • Caribisch Nederland: gereed Q1-2026; • Autonome landen: gereed Q1-2027.
Onderzoek naar wensen en behoeften door NCSC vanuit CWN met netwerkpartners • Werksessie voor het ophalen van wensen en behoeften met netwerkpartners. • Bijdragen en participeren in lokale initiatieven (zoals BQ-conferentie). • Zowel voor Caribisch Nederland (heeft de eerste focus) als voor de autonome landen.	Publicatie van de wensen en behoeften in het cyberdomein, inclusief mogelijke probleemanalyse.	Mid fase 1: • Caribisch Nederland: gereed Q2-2026; • Autonome landen: Q3-2027.
In samenwerking met BZK, EZ en JenV.		
Risicoanalyse door o.a. het NCSC (mogelijk ook andere betrokkenen) Uitvoeren van (aangepast) MASKeR-traject met lokale netwerkpartners.	Rapportage van risico's en ketenafhankelijkheden.	Mid fase 1: • Caribisch Nederland: gereed Q2-2026; • Autonome landen: Q3-2027.
Zowel voor Caribisch Nederland (heeft de eerste focus) als voor de autonome landen. Overkoepelende ketens (bijvoorbeeld SBIR ⁶ , SSO RCN).		
Ontwikkelen van rapportage 'stand van zaken cyberdomein in het CdKNL door het netwerk' • Verantwoording van de uitwerking van fase 1. • Vaststellen en bestendigen van activiteiten uitgevoerd in fase 1 die moeten worden vertaald naar jaarplannen/jaarkalender. • Uitwerking van de fases en concrete vervolgstappen	Rapportage van de bevindingen opgehaald in fase 1. Publicatie van jaarlijkse activiteiten.	Eind fase 1: Gereed Q4-2027.

⁵ Alle genoemde data zijn streefdata. Het realiseren van de deliverables binnen de gewenste termijn is afhankelijk van interne en externe factoren, waardoor de uiteindelijke opleverdatum kan afwijken van de streefdatum.

⁶ Stichting Beheer ICT-rechtshandhaving.

Fase 2. Verbinding

Activiteiten	Deliverables	Timing en/of fase
Organiseren/stimuleren samenwerkingsverband digitalisering en cyberweerbaarheid door het netwerk (ondersteuning o.a. NCSC) • Samenbrengen van de in kaart gebrachte netwerkpartners, zo veel mogelijk door lokale netwerkpartners. • Bestaande initiatieven waar mogelijk verenigen. • Netwerkpartners verenigen in samenwerkingsverband (mogelijk door convenant formaliseren) In samenwerking met BZK, EZ en JenV.	Formalisatie van netwerkpartners (mogelijk in samenwerkingsverband).	Begin fase 2: Gereed Q1-2028.
Samenwerkt thema's vaststellen en prioriteren door het netwerk (ondersteuning o.a. NCSC) Werksessies om gestructureerd thema's vast te stellen en te prioriteren in samenspraak met alle betrokken netwerkpartners.	Publicatie van eerste opzet van functies van het Cyberweerbaarheidsnetwerk.	Eind fase 2, begin fase 3: Gereed Q2-2028.

Fase 3. Vergelijking

Activiteiten	Deliverables	Timing en/of fase
Samenwerkt thema's vaststellen en prioriteren door het netwerk (ondersteuning o.a. NCSC) Werksessies om gestructureerd thema's vast te stellen en te prioriteren in samenspraak met alle betrokken netwerkpartners.	Publicatie van eerste opzet van functies van het Cyberweerbaarheidsnetwerk.	Eind fase 2, begin fase 3: Gereed Q2-2028.
Gap-analyse door het netwerk (ondersteuning o.a. NCSC) • Netwerkpartners maken individuele gap-analyse. • Werksessies om gap-analyse individuen te vergelijken Werkessie om gap-analyse te vergelijken met Nederlands Cyberweerbaarheidsnetwerk.	Publicatie-overzicht van plan uitvoering pijlers. Cyberweerbaarheidsnetwerk en aansluiting op het in Nederland opgezette Cyberweerbaarheidsnetwerk. Aansluiting CWN-Community.	Mid/eind Fase 3: Lange termijn Gereed Q4-2028.

Fase 4. Samenwerking

Activiteiten	Deliverables	Timing en/of fase
Toekomstplan Cyberweerbaarheidsnetwerk CdKNL door het netwerk • Uitwerking van het verloop en conclusies opgedaan door het doorlopen van de fases. • Successen en aandachtspunten. • Uitwerking van activiteiten die nog moeten worden ondernomen in het netwerk. In samenwerking met NCSC, BZK, EZ en JenV.	Publicatie toekomst. Cyberweerbaarheidsnetwerk en het CdKNL.	Fase 4: Gereed Q2-2029.

Randvoorwaarden

Er zijn enkele randvoorwaarden opgesteld om het CdKNL voorwaardig te betrekken in het opzetten en verder uitwerken van het Cyberweerbaarheidsnetwerk.

Wederzijdse verwachtingen

Bij de eerste verkenning vanuit het NCSC, is duidelijk geworden dat er zeer diverse stakeholders mee willen werken aan het vergroten van de cyberweerbaarheid in het CdKNL. Dat zorgt voor een breed scala aan ideeën, invalshoeken, behoeftes en wensen. Iedere stakeholder zal zijn eigen verwachtingen hebben over de thema's, pijlers en plannen die worden opgezet en uitgewerkt. Het is daarom belangrijk om in elke fase toe te zien op de verwachtingen en deze te bespreken met de betrokkenen en te besluiten wat wel en niet kan worden gerealiseerd. Enkel zo kan er vrijuit gezamenlijk worden gewerkt.

Ondersteuning

Het CWN is een netwerk voor en door de publieke en private netwerkpartners. Om het netwerk te doen slagen, wordt wederkerigheid verwacht in het netwerk. Daarmee wordt gezamenlijk geïnvesteerd om effectiviteit en kennis in het domein te verhogen. Dat neemt niet weg dat de aansluiting van het CdKNL een complexe puzzel is. Om dit in goede banen te leiden, is het van belang dat de juiste ondersteuning en handvatten worden geboden aan de stakeholders in het CdKNL, waaronder specifieke kennis en expertise van de bovenwindse eilanden. Vanuit de eerste verkenning wordt geadviseerd dat het NCSC een ondersteunende rol biedt in het doorlopen van de fases met de stakeholders en netwerkpartners. Bij deze ondersteuning hoort - naast het iteratief doorlopen van de fases - ook het borgen van de continuïteit. Om dit te bereiken, is structurele inzet voor het opzetten van het netwerk vanuit het NCSC noodzakelijk. Denk hierbij aan het opzetten en begeleiden van (werk)sessies. De ondersteuning van het NCSC bij het verder ontwikkelen van het Cyberweerbaarheidsnetwerk voor het CdKNL zal altijd in samenspraak moeten met andere betrokken ministeries en uitvoeringsorganisaties, zowel lokaal als in Nederland. Daarbij zal mogelijk ook structurele capaciteit van andere organisaties worden gevraagd. Dit zal later moeten worden uitgewerkt. Met betrekking tot voldoende financiering voor de opzet, invulling en beheer van CdKNL's CWN, is hoofdstuk 7.3.3 van het Bouwplan CWN van toepassing.

Planning

Elk (ei)land in het Koninkrijk der Nederlanden heeft zijn eigen historische invloeden, tradities en cultuur. Het samenwerken aan het CWN en de aansluiting met Nederlandse netwerkpartners zijn nieuw. Het is van belang om de tijd te nemen voor het krijgen van inzicht in het huidige cyberdomein, wensen en behoeftes, risico's en afhankelijkheden zoals beschreven in fase 1. Ook moet er ruimte geboden worden aan culturele verschillen en opbouw van een cyber community zodat kennis en ervaring kan worden gedeeld. Om dit op een gestructureerde manier op te zetten, wordt geadviseerd om de verkenning te beginnen met de bijzondere gemeenten en hun lessons learned mee te nemen in een latere verkenning met de autonome landen. Voor beide verkenningen wordt geadviseerd om een jaar de tijd te nemen.

Interdepartementale samenwerking

Om ervoor te zorgen dat de gewenste uitkomsten op digitale weerbaarheid worden behaald, is het van belang dat de departementen afstemmen over activiteiten die betrekking hebben op het CdKNL. Programma's en projecten kunnen overlap hebben of zelfs elkaar belemmeren. Goede communicatie, interdepartementale samenwerking en kennisdeling zijn daarom van belang. Op de eilanden is er beperkte capaciteit, expertise en kennis aanwezig om aan alle Nederlandse projecten en programma's invulling te kunnen geven. De departementen moeten waken voor overvraging van lokale organisaties voor dezelfde projecten en doelen. Coördinatie is dan ook noodzakelijk, bijvoorbeeld vanuit een zelfsturende coördinatiegroep die vertegenwoordiging heeft vanuit betrokken departementen.

Bijlage A

Definitie en Scope van Caribisch deel van het Koninkrijk

Op 10 oktober 2010 veranderden de staatkundige verhoudingen tussen de Caribische rijkdelen en Nederland. De Nederlandse Antillen zijn toen ontbonden. De eilanden Bonaire, Sint Eustatius en Saba (BES-eilanden) vormen sindsdien openbare lichamen binnen het land Nederland en worden samen aangeduid als Caribisch Nederland. Curaçao, Sint Maarten en Aruba zijn zelfstandige landen geworden binnen het Koninkrijk der Nederlanden. Na de staatkundige wijzigingen in 2010, is afgesproken om terughoudend te zijn bij het invoeren van nieuwe wetgeving. Dit had als voornaamste doel om de burgers en bestuurders een periode van rust en gewenning te gunnen. Het Kabinet Schoof zet in op heldere, goede prioritering op de te ondernemen activiteiten voor CdKNL, waarbij een duidelijk afwegingskader gewenst is. Het uitgangspunt van de voorgaande kabinetten ten aanzien van inspanning voor een gelijkwaardiger voorzieningenniveau in Caribisch Nederland is hiermee losgelaten.

De landen in het Caribisch gebied hebben de status van 'landen en gebieden overzee' (LGO). Deze status verwijst naar niet-Europese landen en gebieden die een bijzondere betrekking hebben met Nederland. Niet-Europees beschrijft hierin dat deze landen geen deel uitmaken van het grondgebied van de Europese Unie. Wet- en regelgeving die voor het Europese grondgebied geldt, is daarmee niet automatisch van kracht voor Caribisch Nederland, waaronder de NIS2. Nederland heeft er bij de NIS2 voor gekozen om deze niet te implementeren voor openbare lichamen. Daarmee is er geen cyberwetgeving in Caribisch Nederland. Ook binnen de autonome landen is geen wetgeving gericht op cyber. Ook de Algemene verordening gegevensbescherming (AVG) is niet van toepassing op Caribisch Nederland. De autonome landen hebben een eigen landverordening. Voor Curaçao en Sint Maarten is dit een landverordening bescherming persoonsgegevens. Voor Aruba betreft dit een landverordening persoonsregistratie. Bescherming van persoonsgegevens is voor de openbare lichamen geregeld in de Wet bescherming persoonsgegevens BES.

Mogelijk komt er verandering in de cyberwet- en regelgeving voor het CdKNL. De Veiligheidsstrategie voor het Koninkrijk der Nederlanden stelt bij 'Actielijn 7: Versterken van de digitale weerbaarheid' de volgende prioriteit voor de jaren 2023-2029: "Opbouwen van het cybersecuritybeleid voor het CdKNL. Wetgeving en beleidskaders zijn nodig ter bevordering van cybersecurity en tegengaan van cybercriminaliteit, waarbij ook versterkte kennisuitwisseling, samenwerking en technische bijstand tussen Nederland en het CdKNL van belang zijn. Daarnaast is meer inzet nodig voor het vergroten van het cyberbewustzijn, uitvoering van cybersecuritybeleid, en technische expertise; zowel onder burgers, overheid, als in het bedrijfsleven"⁷.

⁷ [Veiligheidsstrategie voor het Koninkrijk der Nederlanden | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid.](#)

Bijlage B

CWN en raakvlakken met andere initiatieven in het Caribisch deel van het Koninkrijk

Hoewel de meeste Nederlandse cyber wet- en regelgeving niet van toepassing is op het CdKNL, zijn er wel verschillende (beleids) initiatieven die ook dit deel van het Koninkrijk raken.

De Wet bevordering digitale weerbaarheid bedrijven (Wbdwb), die van kracht is sinds 1 oktober 2024, is wél van toepassing, zij het alleen in Caribisch Nederland. Deze wet legt de taken en bevoegdheden van de Minister van Economische Zaken (EZ) vast op het terrein van digitale weerbaarheid van niet-vitale bedrijven in Nederland, zoals het verspreiden van informatie over kwetsbaarheden, dreigingen, en incidenten en het bevorderen van samenwerking tussen bedrijven op het gebied van digitale weerbaarheid.

Op 4 november 2022 is de Werkagenda Waardengedreven Digitaliseren aan de Tweede Kamer aangeboden, die ook raakt aan de cyberweerbaarheid in het Caribisch gebied van het Koninkrijk. In december 2023 is de balans opgemaakt⁸. De Werkagenda is een uitwerking van elementen uit de brief Hoofdlijnen Beleid Digitalisering⁹ met concrete doelen en acties. Hij omvat vijf sporen: meedoen, vertrouwen en regie in de digitale samenleving, een goede digitale overheid en het versterken van de digitale samenleving in het CdKNL. Deze werkagenda wordt jaarlijks geactualiseerd.

Er wordt onder andere ingezet op het versterken van de digitale veiligheid en weerbaarheid. In een tijd waarin de wereld om ons heen onrustig is, is veiligheid van doorslaggevend belang. Met de cybersecuritystrategie van het Ministerie van Justitie en Veiligheid als leidend instrument, is er gewerkt aan het versterken van de digitale veiligheid en weerbaarheid. Zo is met de Herziening Europese Richtlijn Netwerk- en Informatiebeveiliging de basisnorm voor organisaties verhoogd. Tegelijkertijd is gewerkt aan passende ondersteuning. Bijvoorbeeld door instrumenten te realiseren die overheidsorganisaties helpen bij het veilig inkopen van ICT-producten en -diensten en door een overheidsbrede aanpak voor red teaming te ontwikkelen om zwakke plekken in de infrastructuur zo snel mogelijk te ontdekken.¹⁰

⁸ [De werkagenda: een jaar onderweg Werkagenda Waardengedreven Digitaliseren - Digitale Overheid.](#)

⁹ [Kamerbrief hoofdlijnen beleid voor digitalisering | Kamerstuk | Rijksoverheid.nl](#)

¹⁰ [De werkagenda: een jaar onderweg Werkagenda Waardengedreven Digitaliseren - Digitale Overheid.](#)

Kabinetsbeleid Digitalisering geeft in diens werkagenda aan dat het wil versterken op digitale samenleving in het CdKNL¹¹.

Het zet in op:

1. Digitaal volwaardig zijn zodat iedereen in Caribisch Nederland de beschikking heeft over voldoende kennis, dienstverlening en voorzieningen om te profiteren van kansen en risico's adequaat te mitigeren.
2. Samenwerken aan de digitale basis met de samenleving, het bedrijfsleven en de overheid van Aruba, Curaçao en Sint Maarten om te zorgen dat ook zij voldoende toegerust zijn.

Het Kabinetsbeleid Digitalisering ziet in het actieplan de uitdagingen die er zijn in de internationale connectiviteit, zowel in de Caribische regio als tussen die regio en Europa.¹²

Het Cyberweerbaarheidsnetwerk zal waar mogelijk inzetten op het aansluiten op, en verder versterken van, deze bestaande initiatieven op het gebied van cyberweerbaarheid in het CdKNL. In de volgende hoofdstukken zal dit verder worden toegelicht.

.....
¹¹ [5. Versterken digitale samenleving in het Caribisch deel van het Koninkrijk Versterken digitale samenleving op Caribisch deel koninkrijk - Digitale Overheid.](#)

¹² [5.2 Samenwerken aan de digitale samenleving binnen het Koninkrijk Versterken digitale samenleving op Caribisch deel koninkrijk - Digitale Overheid.](#)

Bijlage C

Huidige situatie

In het voorjaar van 2024 is begonnen met de invulling van de volgende doelstelling van de NLCS: “Er wordt gestart met een verkenning naar de benodigde stappen voor het verhogen van de digitale weerbaarheid van de vitale infrastructuur in Caribisch Nederland.” Deze verkenning is van start gegaan vanuit het NCSC en heeft geresulteerd in de eerste conclusies en de latere doelstelling(en). De huidige stand van zaken komt voort uit gesprekken met organisaties in het Caribisch gebied en door de samenwerking met de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Economische zaken en Justitie en Veiligheid.

1. Eerste verkenning en conclusies

Het streven om het CdKNL meer en beter te betrekken bij cyberontwikkelingen en cyberweerbaarheid is in lijn met de ontwikkelingen van het Cyberweerbaarheidsnetwerk. Uit de verkenning komt naar voren dat voortrekkers uit vitale organisaties op zoek zijn naar houvast en kaders om zich te verenigen en zo de cyberweerbaarheid te verhogen. Er zijn al voorzichtige stappen gezet voor samenwerkingsverbanden. Ook zijn er al sector overstijgende verkennende gesprekken over cyberweerbaarheid geweest, maar deze zijn (nog) niet structureel van aard. Daarbij maakt de culturele context het er niet gemakkelijk op om samen te werken met andere eilanden en Nederland. Verder is er een grote behoefte aan betere aansluiting op technische en operationele kennis, capaciteit in de vorm van medewerkers en (respons)bijstand vanuit Nederland, maar ook inzicht in de volwassenheid van het cyberdomein, oefeningen en opleidingen.

Concreet is er behoefte aan coördinatie en een (actie)plan om digitalisering en cyberweerbaarheid te verankeren. Een eerste stap hierbij is het verbeteren van de bekendheid en urgentie van het onderwerp bij vitale organisaties. Vervolgens kunnen vitale organisaties aansluiten op technische producten en diensten in Nederland. Vanuit daar kan er gefaseerd worden gewerkt in publiek-private samenwerking om het Cyberweerbaarheidsnetwerk te ontwikkelen. Echter, het is wel noodzakelijk dat organisaties het belang inzien en capaciteit beschikbaar stellen. Deze volgorde zorgt ervoor dat producten en diensten aansluiten bij het huidige beleid van vitale organisaties op de eilanden.

2. Verkenning Caribisch Gebied

Binnenlandse Zaken en Koninkrijkrelaties

Het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties werkt aan de basis en kernwaarde van de democratie voor zowel Nederland als het CdKNL. Daarnaast ondersteunt het ministerie de autonome landen Aruba, Curaçao en Sint Maarten bij een sterk fundament voor een goed leven en ondersteunt het de openbare lichamen met hun cyberweerbaarheid.

BZK heeft twee hoofdtaken op het gebied van informatiebeveiliging in Caribisch Nederland:

- Stelselverantwoordelijkheid: Zorgen voor de beveiliging van overheidsinformatie in alle delen van het Koninkrijk.
- Opdrachtgever voor projecten: De actieve rol van opdrachtgever voor digitaliseringsprojecten aannemen en daarbij een voorbeeld stellen op het gebied van veilige werkwijzen.

Momenteel wordt er gewerkt aan de planvorming voor de uitvoering van de hoofdtaken van BZK. Het ministerie voert gesprekken met openbare lichamen en andere relevante partners uit Caribisch Nederland. De primaire focus is om een goed beeld te krijgen van de cyberweerbaarheid en de uitdagingen hierbij. Vanuit BZK worden tevens projecten gestart die de openbare lichamen helpen bij hun cyberweerbaarheid. Hiervoor zal ook de aansluiting met het Cyberweerbaarheidsnetwerk worden gezocht. Daarnaast zal Caribisch Nederland betrokken worden bij de overheidsbrede cyberoefening die het ministerie jaarlijks organiseert.

Onderwerpen die op dit moment worden geadresseerd zijn in de planvorming van BZK:

- Coördinatie, baselines en inzicht;
- Werken aan relaties en vertrouwen;
- Awareness en technische opleidingen;
- Cybersecurity Community Building;
- Sectoraal CSIRT en Incident Response;
- Crisisbeheersing.

Economische Zaken

Het ministerie van Economische Zaken werkt aan een duurzaam en ondernemend Caribisch Nederland. Daarnaast draagt het ministerie bij aan duurzame economische groei met betrouwbare nutsvoorzieningen. Het ministerie helpt de eilanden om de prijs-kwaliteitverhouding van de telecom- en internetvoorzieningen te verbeteren door kaders te schetsen en subsidies te verlenen. In de Strategie Digitale Economie - Voortgangsrapportage 2024 is het volgende doel opgenomen: 'Het versterken van de digitale infrastructuur in Caribisch Nederland zodat de kwaliteit, betrouwbaarheid en betaalbaarheid worden verbeterd'¹³. In deze strategie wordt ook verwezen naar het Digital Trust Center (DTC) en de Subsidieregeling Cyberweerbaarheid. Het DTC is onderdeel van Economische Zaken. De missie van het DTC is om ruim twee miljoen Nederlandse bedrijven, van zzp'ers tot en met het grootbedrijf, te ondersteunen zich weerbaarder te maken tegen toenemende cyberdreigingen. Dit zijn alle bedrijven in Nederland die tot de niet-vitale sectoren behoren. Het DTC voert, onder de verantwoordelijkheid van de minister van EZ, de Wet bevordering digitale weerbaarheid bedrijven uit, die sinds 1 oktober 2024 van kracht is (zie ook Bijlage 1). Daarnaast is in de Staat van de Digitale Infrastructuur (SDI) een hoofdstuk opgenomen over de digitale infrastructuur in Caribisch Nederland, inclusief weerbaarheid en is met de SDI een rapport over de digitale infrastructuur in Caribisch Nederland aan de Tweede Kamer gestuurd.¹⁴

¹³ [Strategie Digitale Economie - Voortgangsrapportage 2024](#).

¹⁴ Staat van de Digitale Infrastructuur - [Tweede Kamer 2023-2024, 26643 nr 1119](#).

Justitie en Veiligheid

Het Ministerie van Justitie en Veiligheid zorgt voor het waarborgen van de rechtsstaat in Caribisch Nederland, zodat er in vrijheid kan worden samengeleefd ongeacht levensstijl of opvatting. De volgende departementen en diensten die onder het ministerie vallen zijn actief op Caribisch Nederland: Korps Politie Caribisch Nederland, Brandweer, Bureau Slachtofferhulp, Justitiële Inrichting Caribisch Nederland, Openbaar Ministerie, Reclassering, Kosteloze rechtskundige bijstand, de Immigratie- en Naturalisatiedienst Caribisch Nederland, Voogdijraad en Schadefonds Geweldsmisdrijven.

Om ook de veiligheid in Caribisch Gebied te waarborgen, is de Veiligheidsstrategie voor het Koninkrijk der Nederlanden opgesteld.¹⁵ Hierin wordt onder meer ingegaan op cyberdreigingen tegen het Koninkrijk. De strategie stelt: 'Ook het CdKNL kent voorbeelden van cyberaanvallen waarbij de gevolgen maatschappij ontwrichtend kunnen zijn. Een voorbeeld hiervan is de grote ransomware aanval in 2022 op het (enige) water- en elektriciteitsbedrijf van Sint Maarten. Door de aanval verloor het bedrijf de toegang tot de financiële data, terwijl er geen recente back-up beschikbaar was. Dit vormde een bedreiging voor de bedrijfsvoering en de continuïteit van twee vitale processen: water en elektriciteit.' In Actielijn 7: Versterken van digitale weerbaarheid, wordt ingegaan op het opbouwen van een cybersecuritybeleid voor het CdKNL en het versterken van de samenwerking tussen Nederland en het Caribisch deel. Daarbij moet er worden ingezet op het vergroten van het cyberbewustzijn, uitvoering van cybersecuritybeleid en technische expertise. Actielijn 12: Versterken van crisisbeheersing en vergroten paraatheid samenleving, richt zich verder op het verbeteren van informatiedeling en crisisplannen met nadrukkelijk meer oog voor lokale context en autonomie.

Momenteel komen organisaties niet in aanmerking voor een vitale status omdat de richtlijnen hiervoor zijn geënt op Nederlandse maatstaven. Momenteel onderzoekt de NCTV - in samenspraak met BZK, EZ en het NCSC - mogelijke oplossingsrichtingen. De verwachte tijdlijn is nog onbekend.

Het NCSC heeft de afgelopen jaren incidenteel contact gehad met organisaties in het CdKNL. Momenteel is het onduidelijk welke producten en diensten het NCSC aan CdKNL mag leveren. De huidige wetgeving geeft geen grondslag voor het bieden van structurele operationele ondersteuning en het delen van informatie met organisaties in het CdKNL. Dat neemt niet weg dat het NCSC de afgelopen jaren met organisaties uit het CdKNL heeft gekeken naar wat er wél mogelijk is. Met de verkenning vanuit het Cyberweerbaarheidsnetwerk, is er een begin gemaakt met het opzetten van een structurele basis en een relatie met vitale organisaties in het CdKNL.

¹⁵ [Veiligheidsstrategie voor het Koninkrijk der Nederlanden | Rapport | Rijksdienst Caribisch Nederland.](#)

Uitgave

Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie

www.ncsc.nl
info@ncsc.nl
[@ncsc_nl](https://twitter.com/ncsc_nl)

September 2025