Digitale Opsporing in Caribisch Nederland: een Cybercrime Casestudy

Erik van de Sandt, Elston Martis, Alwyn Braaf, Steven Senior & Melvin Sint Jago*

25 juli 2022

1 Digitale Ambities in Caribisch Nederland

Er is nauwelijks nog politiewerk te vinden zonder digitale component. Digitale opsporing is het containerbegrip voor digitaal-forensisch onderzoek aan gegevensdragers, onderzoek naar cybercrime en onderzoek middels open en gesloten internetbronnen (OSINT). Deze vorm van opsporing heeft vaste grond onder de voeten bij de nationale politie in Europees Nederland. De lijst die betrekking heeft op de institutionalisering van het thema is eindeloos. Zo zijn er landelijke voorzieningen, overleggen en vakgroepen, landelijke en regionale Teams Digitale Opsporing (TDO) en cybercrimeteams, expertisecentra en kwaliteitskaders, portefeuillehouders en programma's, en onderwijsmogelijkheden via Politieacademie en universiteiten.

Heel anders is de situatie op de Caribische eilanden binnen het Koninkrijk der Nederlanden. Hoewel wettelijk is vastgesteld dat digitaal onderzoek een taakgebied is van de korpsen op de Caribische eilanden,[1] moeten de digitale opsporingsspecialismen feitelijk nog een aanvang nemen. Sinds 2021 is Korps Politie Caribisch Nederland geleidelijk de digitale opsporing aan het invoeren, onder andere door de oprichting van een TDO en Cyber Crime Unit (CCU). Omdat digitale opsporing een transitie is die het korps en sleutelpartners raakt op politiek-bestuurlijk-, management- en werkvloerniveau, heeft KPCN een strategisch, tactisch en operationeel plan opgesteld om het specialisme vorm te geven en te borgen op lange, middellange en korte termijn. Dit artikel beschrijft deze plannen en de uitvoering daarvan met als casestudy de aanpak van cybercrime op de BES.

*Allen werkzaam bij Korps Politie Caribisch Nederland. Respectievelijk kwartiermaker Cyber, coördinator Team Digitale Opsporing, hoofd Opsporing, chef Opsporing en hoofd Informatie. Corresponderend auteur: erik.van.de.sandt [at] politie.nl. De auteurs bedanken Garry Clementina, Sharon Heymans, Gino van Hoogstraten, Ian Steba en Ronald Zwarter voor hun waardevolle aanvullingen op het artikel.

[1] Zie artikel 7 lid 2 sub a van de Rijkswet politie van Curaçao, van Sint Maarten en van Bonaire, Sint Eustatius en Saba.

De inzichten van dit artikel dragen bij aan de concrete beleidsinvulling op meerdere bestuurslagen, waaronder i) het huidige regeerakkoord met hernieuwde aandacht voor het Caribisch gebied én de bestrijding van cybercrime, ii) intensievere samenwerking tussen de nationale politie, RST en de Caribische korpsen waaronder KPCN, en iii) verdere ontwikkeling van digitale opsporingsspecialismen in het Caribisch gebied binnen het Koninkrijk der Nederlanden.

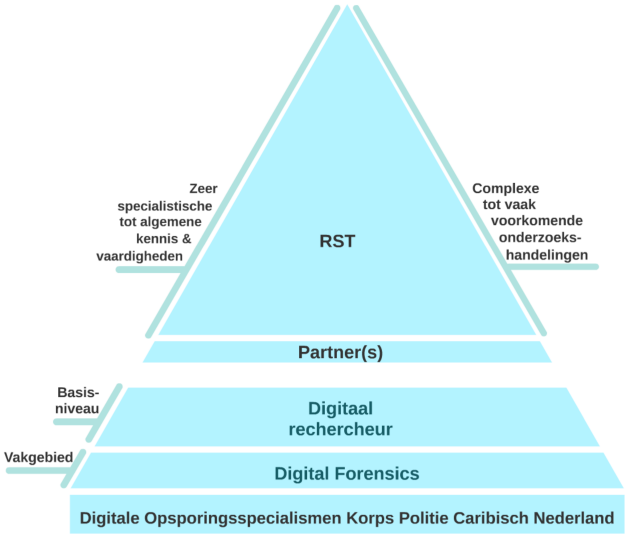
Politie in Caribisch Nederland
Sinds 10 oktober 2010 vormen de BES-eilanden - Bonaire, Sint Eustatius en Saba - samen Caribisch Nederland (CN), en zijn de eilanden aangemerkt als bijzondere gemeenten binnen Europees Nederland. Ondanks deze status hebben de BES-eilanden wel een eigen korps - het Korps Politie Caribisch Nederland (KPCN) - met als korpsbeheerder het Nederlandse Ministerie van Justitie en Veiligheid. De BES kent eigen wet- en regelgeving, waaronder een Wetboek van Strafrecht en Strafvordering BES en Wet Politiegegevens BES, die worden opgesteld en uitgevaardigd door het Nederlandse Ministerie van Justitie en Veiligheid. De autonome landen binnen het Koninkrijk - Aruba, Curaçao en Sint Maarten, ook wel CAS of 'de landen' genoemd - hebben ook hun eigen korpsen, respectievelijk KPA, KPC en KPSM, maar stellen wel hun eigen wet- en regelgeving op. De landen Curaçao, Sint Maarten en Nederland voor wat betreft Bonaire, Sint Eustatius en Saba hebben elk een eigen OM. Aan het hoofd van de OM's staat één gezamenlijke procureur-generaal (PG). Voor de inrichting en organisatie van KPCN, zie [1]. Voor de geschiedenis van de korpsen in het Caribisch gebied binnen het Koninkrijk der Nederlanden, zie [2].

2 Situatie bij KPCN vóór 2021

Deze sectie beschrijft de historische achtergrond van digitale opsporing binnen KPCN. De situatie voor het jaar 2021 kan worden getypeerd als grote afhankelijkheid van het Recherche Samenwerkingsteam (RST) die verschillende gevolgen had voor KPCN.

Afhankelijkheid RST Van 2016 tot 2021 had KPCN één digitaal rechercheur en geen cybercrime-, digitaal-forensische (TDO) of OSINT-afdelingen, zie Afbeelding 1. In de samenwerking tussen RST en de vier Caribische politiekorpsen is RST verantwoordelijk voor de portefeuille interceptie, digitale ondersteuning en technische/specialistische ondersteuning, inclusief het verzorgen van digitaal-forensische trainingen en opleidingen [3]. Het betreft hier dus louter digitaal-forensische ondersteuning aangezien RST geen cybercrimeteam heeft en OSINT niet valt onder de bovengenoemde ondersteuningsportefeuille. In de praktijk betekent dit dat de enige digitaal rechercheur van KPCN volledig afhankelijk van RST was en niet in contact stond met zijn vakgenoten in Europees Nederland of de Politieacademie. In de jaren 2016-2021 is er één leermoment door RST verzorgd voor de digitaal rechercheur van KPCN. Dit lage aantal is ook verklaarbaar. RST bestaat grotendeels uit tijdelijk uitgezonden Nederlandse politieambtenaren en is primair een opsporingsteam. Verder was en is RST verantwoordelijk voor het uitvoeren van digitaal-forensisch onderzoek aan gegevensdragers die KPCN zelf niet kan uitvoeren. In de jaren 2016-2021 werd er jaarlijks slechts enkele keren beroep gedaan op RST om gegevensdragers uit te lezen, juist omdat er weinig kennis was wat het RST kon betekenen. In

de praktijk betekende dit dat in beslag genomen gegevensdragers vanuit de BES naar Curaçao werden overgevlogen omdat op laatstgenoemde eiland de benodigde mensen, kennis en apparatuur aanwezig waren. Het betreft hier louter digitaal-forensische ondersteuning aangezien RST geen cybercrimeteam heeft en OSINT niet valt onder de portefeuille interceptie, digitale ondersteuning en technische/specialistische ondersteuning.



Figuur 1: Tussen 2016 en 2021 had KPCN geen afdelingen voor digitale opsporing, weinig (inter)nationale sleutelpartners en kon het korps niet vaak voorkomende digitaal-forensische onderzoekshandelingen uitvoeren omdat het niet de daarvoor benodigde algemene kennis en vaardigheden in huis had.

Juridische, organisatorische en technische gevolgen De digitaal-forensische handelingen van de enige digitaal rechercheur in Caribisch Nederland waren eenvoudig van aard, zoals het veiligstellen van camerabeelden op locatie of het maken partiële (lees: niet-volledige) extractie van een mobiele telefoon. Algemene kennis en vaardigheden ontbraken grotendeels waardoor hij niet alleen complexe, maar ook vaak voorkomende onderzoekshandelingen niet kon uitvoeren. Voor de meeste digitaal-forensische onderzoekshandelingen was KPCN dus afhankelijk van de centrale locatie van RST te Curaçao.

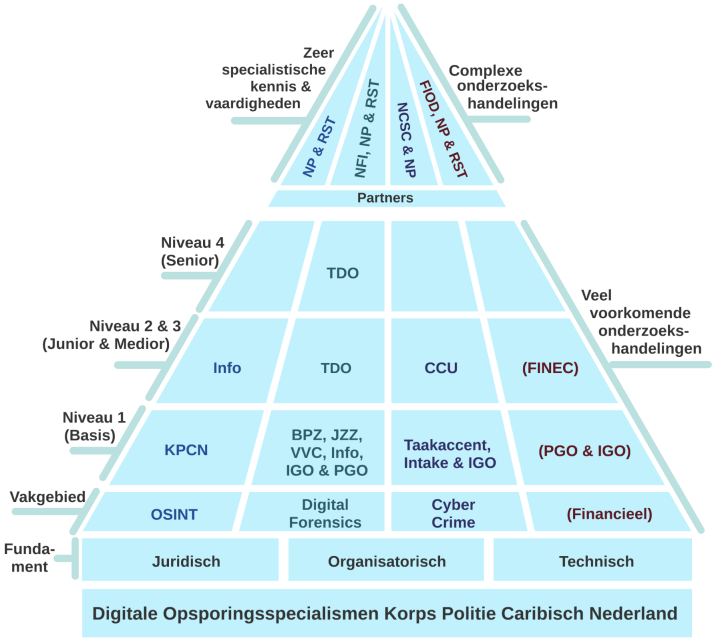
Deze situatie creëerde meerdere, aan elkaar gerelateerde, juridische, organisatorische en technische gevolgen voor KPCN. Noodzakelijke digitaal-forensische apparatuur en werkomgevingen ontbraken op de BES. De wél aanwezige apparatuur was vaak niet geüpdatet. Wanneer gegevensdragers naar RST te Curaçao werden verzonden om te worden uitgelezen 'concurreerden' de gegevensdragers uit de BES met de gegevensdragers van RST die afkomstig zijn van veel zwaar-

dere en meer georganiseerde criminaliteit. Het kon maanden duren voordat in beslag genomen gegevensdragers werden uitgelezen en teruggestuurd naar de BES. Zulke vertragingen hadden zijn weerslag op de generieke opsporing. Als een zaak met alleen tactische methoden en technieken tot een einde konden worden gebracht werden gegevensdragers niet meer naar Curaçao gestuurd. Uit gesprekken met rechercheurs en leidinggevenden van KPCN komt het beeld naar voren dat het voor hen niet helder was wat het digitaal-forensische vakgebied omvat waardoor mogelijk belangrijke opsporingskansen werden gemist. Zo werd de digitaal rechercheur ingezet voor Internetonderzoek van sociale media (wat onder het basisniveau van OSINT valt). Het gebrek aan kennis en ervaring uitte zich ook in juridisch zin. In de gesprekken met de wetgevers in Den Haag was het lastig voor KPCN om te formuleren welke wet- en regelgeving op het gebied van digitale opsporing noodzakelijk werden geacht voor een goede uitvoering van zijn politietaak.

3 Strategische Focus op Fundament, Bulkzaken & Harmonisatie

Vanaf 2021 hebben KPCN, het Ministerie van Justitie en Veiligheid en de nationale politie flink geïnvesteerd in de ontwikkeling van de digitale opsporingspecialismen binnen het korps, en dan met name op cybercrime en *digital forensics*. KPCN heeft een strategie ontwikkeld waar het korps naar toe wilt groeien in de komende jaren, zie Afbeelding 2. De kern van deze strategie is groeien naar:

1. een sterk juridisch, organisatorisch en technisch fundament om digitale opsporingsspecialismen effectief uit te kunnen voeren;
2. een werkniveau waarbij KPCN zelf de meest voorkomende digitale onderzoekshandelingen kan verrichten; en
3. harmonisatie met sleutelpartners die specialistische kennis hebben voor weinig voorkomende onderzoekshandelingen.



Figuur 2: In de visie van KPCN groeit het korps naar een sterk fundament, verschillende afdelingen voor digitale opsporing en duurzame contacten met meerdere sleutelpartners om zo veel mogelijk zelf de bulk van de zaken af te kunnen handelen. BPZ, IGO en PGO, JZZ en VVC staan respectievelijk voor de afdelingen basis politiezorg, incident-gerichte opsporing en probleem-gerichte opsporing, jeugd- en zedenzaken en veel voorkomende criminaliteit.

Robuust juridisch, organisatorisch en technisch fundament Allereerst werken KPCN en het Ministerie van Justitie en Veiligheid aan een robuust juridisch, organisatorisch en technisch fundament voor de opsporing. Wet- en regelgeving dient mee te gaan met wereldwijde ontwikkelingen, of het nu gaat om strafbaarstellingen, opsporingsbevoegdheden of instrumentarium om (inter)nationaal samen te werken. De unieke kenmerken en omstandigheden in Caribisch Nederland helpen in prioritering van nieuwe wet- en regelgeving. De afwezigheid van datacenters betekent dat de opsporingsbevoegdheid van een netwerkzoeking KPCN extra slagkracht zal geven en onderstreept ook het belang dat het Verdrag van Boedapest van de Raad van Europa (ook bekend als het Cybercrimeverdrag) van toepassing is op de BES. Het organisatorische fundament betekent het opzetten en borgen van specialismen binnen de politie. Welke functies, rollen en taken zijn noodzakelijk, welke medewerkers zijn bevoegd en startbekwaam, waar worden nieuwe specialismen organisatorisch en fysiek in het gebouw ondergebracht, of hoe ziet de samenwerking eruit met andere afdelingen binnen KPCN, met publieke en private partijen op de BES en met buitenlandse politiediensten? Het technische fundament bestaat uit de benodigde hardware, software en online & offline (informatie)systemen die nodig zijn om de specia-

lismen uit te kunnen voeren.

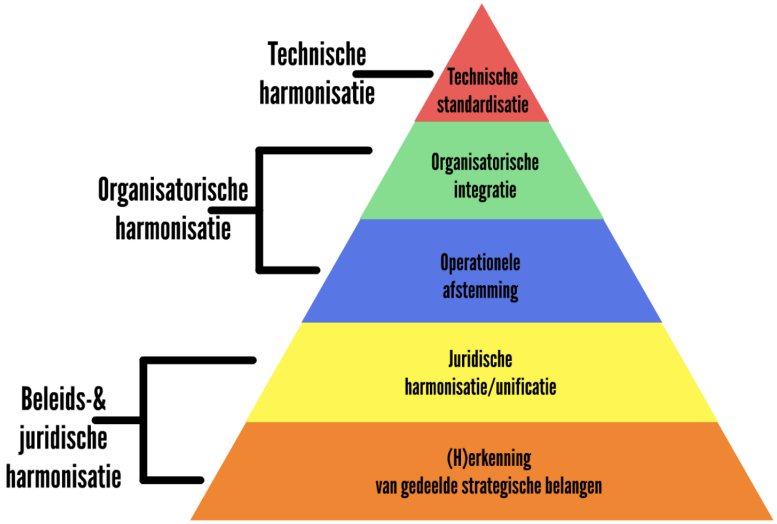
Juridisch fundament voor de bestrijding van cybercrime niet op orde
De digitale dreiging voor de nationale veiligheid is in het Caribische deel van het Koninkrijk, net als in Europees Nederland, permanent. In 2019, 2021 en 2022 waren er succesvolle ransomwareaanvallen op respectievelijk het ziekenhuis in Aruba, de Centrale Bank van Curaçao en Sint Maarten en het water- en elektriciteitsbedrijf van Sint Maarten. Stel dat een ransomwareaanval wordt uitgevoerd op de vitale infrastructuur in Caribisch Nederland, hebben lokale en Europees-Nederlandse overheidsinstanties dan voldoende juridische middelen tot hun beschikking? Omdat de Algemene verordening gegevensbescherming (AVG) en Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) niet van toepassing zijn op Caribisch Nederland heeft het Europees-Nederlandse Nationaal Cybersecurity Centrum van het Ministerie van Justitie en Veiligheid geen mandaat om respectievelijk *cyber threat intelligence* te delen en *incident response* aan te bieden. Het Wetboek van Strafvordering BES kent geen afdelingen binnen de titel bijzondere opsporingsbevoegdheden die onderzoek binnen geautomatiseerde werken en het vorderen van gegevens toestaan (zoals de Europees Nederlandse artikelen 126na, 126nd en 126ng WvSv). Hierdoor is het Cybercrimeverdrag niet van toepassing op Caribisch Nederland. Het versturen van internationale informatieverzoeken (die bijvoorbeeld betrekking hebben tot aanvalsservers) zijn dus zeer moeizaam voor het lokale OM. Wanneer uit een dergelijke vordering een dynamisch IP-adres naar voren komt van een lokaal mobiel telefoonnummer zal een nieuwe vordering naar de plaatselijke telecomaanbieder vruchteloos zijn: Caribisch Nederland kent geen Telecommunicatiewet met verplichtingen voor de telecomaanbieder om dergelijke gegevens te verstrekken. Als laatste biedt de Wet bescherming persoonsgegevens BES weinig bescherming voor burgers wanneer hun persoonlijke gegevens zijn gestolen tijdens de ransomwareaanval. De wet kent namelijk geen meldplicht bij de Commissie toezicht bescherming persoonsgegevens BES.

Specialismen voor bulkzaken De vorm van de pyramide geeft weer dat de specialismen worden ingezet om de bulk van de zaken op de BES aan te kunnen pakken. Met andere woorden, het korps wil de kennis en expertise in huis hebben om zelf de meest voorkomende onderzoekshandelingen uit te kunnen voeren. Hierbij is het belangrijk om meetbare en gestandaardiseerde kennisniveau's aan te brengen, zoals het DO-5 model voor digitaal opsporen van de nationale politie [4]. Vervolgens geeft de pyramide aan welke afdelingen naar welke niveau van specialismen moeten groeien om vakbekwaam of specialist te worden. Zo is het van belang dat de diverse afdelingen binnen KPCN de basis kennen - lees: digivaardig worden - op cybercrime, digital-forensics en OSINT. Een praktisch voorbeeld is dat er nu in elke surveillanceauto een zak van Faraday ligt. De collega's van de BPZ hebben uitleg gekregen van TDO hoe zij op digitaal-forensisch verantwoorde wijze een veiliggestelde gegevensdrager in de zak kunnen doen en overdragen aan TDO.

Casus: KP-verdachte op Darkweb
Via de afdeling JJZ kwam en melding binnen dat een persoon op Bonaire zich mogelijk via het Darkweb (Tor) toegang verschafte tot kinderpornografie. JJZ nam mobiele telefoons en een laptop van deze verdachte in beslag. Door *state-of-art* digitaal-forensische hardware en software en de benodigde kennis en ervaring kon TDO de data op deze gegevensdragers veiligstellen en inzichtelijk maken. Omdat TDO aan JZZ had geleerd om de digitaal-forensische software te gebruiken konden de digivaardige zedenrechercheurs zelf vaststellen dat er kindermisbruikmateriaal stond op bijna alle gegevensdragers. De CCU keek naar het Internetgedrag op de gegevensdragers en stelde vast dat de verdachte niet alleen buitengewoon geïnteresseerd was in geavanceerde vormen van informatiebeveiliging, maar zich middels Tor (het '*Darkweb*') ook toegang had verschaft tot besloten kinderpornografische omgevingen. Vanwege de zeer specialistische aard om online toegang te krijgen tot deze omgevingen werd de hulp ingeroepen van Team Bestrijding Kinderpornografie en Kindersekstoerisme (TBKK) van de nationale politie. Dit team stelde vast dat de verdachte sinds 2015 accounts heeft (gehad) in meer dan zes kinderpornografische omgevingen op het Darkweb. JZZ nam deze bevindingen weer mee in het verhoor van de verdachte en op in het strafdossier. Het Gemeenschappelijk Hof van Justitie van Aruba, Curaçao, Sint Maarten en van Bonaire, Sint Eustatius en Saba heeft de verdachte veroordeeld tot een gevangenisstraf en maatregelen opgelegd.

Harmonisatie met partners Een relatief klein korps als KPCN kan geen zeer specialistische kennis in huis hebben voor weinig voorkomende onderzoekshandelingen. Voor de top van de strategische pyramide uit Afbeelding 2 zal het korps voor digitale opsporing - cybercrime, digital-forensics en OSINT - de samenwerking moeten zoeken met meer partners dan alleen RST. Voor die samenwerking is harmonisatie het sleutelwoord. Harmonisatie impliceert afstemming en samenwerking met respect voor de eigen cultuur van organisaties. De term impliceert ook een mate van flexibiliteit en wendbaarheid die nodig is in snel veranderende omgevingen waar wetgevers tegelijkertijd invloed moeten kunnen uitoefenen met betrekking tot regulering en toezicht. Uiteindelijk kan harmonisatie leiden tot standaardisatie – lees: bindende afspraken - maar dat hoeft niet [5]. Wil KPCN verbonden zijn met de rest van de wereld dan zullen de komende jaren de beleidsmatige/juridische, organisatorische en technische fundamenten van KPCN steeds meer moeten gaan aansluiten op de fundamenten van sleutelpartners. Beleidsmatige en juridische harmonisatie betekent respectievelijk de (h)erkenning van gedeelde strategische belangen en beleidsdoelen met sleutelpartners en noodzakelijke internationale verdragen en afspraken voor samenwerking op orde zijn. Organisatorische harmonisatie betekent dat KPCN aansluiting vindt bij (inter)nationale politieknooppunten en kenniscentra. Voor de relatie tussen Europees Nederland en Caribisch Nederland betekent dit bijvoorbeeld fysieke deelname van TDO aan de DEX-XL vakdagen in Nederland, online deelname aan de TDO-vakgroepen van de nationale politie en het volgen van opleidingen aan de Politieacademie. Bij technische harmonisatie ligt de nadruk op overeenkomstige systemen, software en dataschema's. Een voorbeeld van deze vorm van harmonisatie is het politiesysteem ACTPOL dat door alle Caribische korpsen - KPA, KPC, KPSM - wordt gebruikt en in gezamenlijkheid wordt doorontwikkeld. Ook kan men denken aan aansluiting op de besloten onderzoeksomgeving 'Digitaal Transferium' van de nationale politie waar grote

hoeveelheden beslag op kan worden opgeslagen en een veelvoud aan analysetools op is geïnstalleerd.



Figuur 3: Harmonisatie op verschillende niveau's - zowel binnen KPCN als met partners - is noodzakelijk waarbij de onderliggende laag doorgaans randvoorwaardelijk is voor een volgende stap. Zo is eerst juridische inbedding en afstemming van een onderwerp nodig - in casu cybercrime - voordat het organisatorisch ingebed kan worden. Pas hierna is technische harmonisatie van gedeelde data, dataschema's en software mogelijk.

4 Tactische Focus op Slachtoffers, Daders & Infrastructuur

De specialismen zijn uitgewerkt in een tactische matrix die op een meer gedetailleerd niveau de middellange termijnfocus weergeeft om draagvlak en besluitvorming op middenmanagementniveau te stimuleren. De matrix van de Cyber Crime Unit is weergegeven in Tabel 4, en heeft drie aan elkaar verbonden doelen. Het eerste doel is het ontwikkelen van politievaardigheden op het gebied van cybercrimebestrijding. Deze vaardigheden worden ingezet om het tweede doel te bereiken namelijk het creëren van een tijdig, relevant, nauwkeurig en bruikbaar intelligencebeeld. Dit beeld wordt ingezet voor het derde doel dat in deze sectie verder wordt uitgelegd: de bestrijding van cybercriminaliteit. Vanwege de specifieke lokale context van de BES is de aanpak van cybercrime primair gericht op slachtoffers en secundair op daders en misbruikte technische infrastructuur.

Cybercriminelen misbruiken infrastructuur om slachtoffers te maken
Cybercrime bestaat uit drie componenten: 1. daders maken gebruik van 2. technische infrastructuur (lees: servers) om 3. slachtoffers te maken. Wanneer één van deze drie componenten op een grondgebied aanwezig is heeft het OM rechtsmacht om een opsporingsonderzoek te starten. Doorgaans bevinden deze drie componenten zich niet in dezelfde jurisdictie. Cybercrime is immers per uitstek een transnationaal misdrijf. Daarom stemmen veel cybercrimeteams hun aanpak af op de lokale situatie. Europees Nederland heeft veel datacentra waar servers staan die worden misbruikt door de Russischtalige georganiseerde cybercriminaliteit om wereldwijd slachtoffers te maken. Om deze reden heeft Team High Tech Crime van de Landelijke Eenheid primair een infrastructuurgerichte aanpak. Het cybercrimeteam van de politieregio Oost-Nederland is verantwoordelijk voor het thema VIN-fraude. Deze vorm van fraude wordt hoofdzakelijk gepleegd door Nederlandssprekende daders, middels WhatsApp, met Nederlandse slachtoffers. Om deze reden hanteert dit team een dadergerichte aanpak met aandacht voor slachtoffers.

Slachtoffergerichte aanpak op de BES Het algemene intelligencebeeld van de CCU laat zien dat de kennis over cybercrime en cybersecurity op de eilanden zeer laag is. Om deze reden is de focus van de unit om de bewustwording te verhogen en een handelingsperspectief aan te bieden aan de inwoners, het midden- en kleinbedrijf (MKB) en de vitale infrastructuur van de BES. Met andere woorden: KPCN heeft primair een slachtoffergerichte aanpak waarbij CCU adviezen geeft hoe slachtofferschap kan worden voorkomen en persoonlijke hulp aan hen die hulp behoeven. Dit is een logische keuze, aangezien de BES nauwelijks grootschalige technische infrastructuur heeft (denk aan datacenters waarin servers staan) en ook geen - zo lijkt het - grote lokale daderpopulatie. Verder zijn aangiftes vanuit de bevolking en het bedrijfsleven ('brengzaken') een belangrijke bron voor het intelligencebeeld op het gebied van cybercrime. Maar wanneer burgers en ondernemers slachtofferschap van cybercrime niet herkennen, kunnen zij ook geen aangifte doen. Omdat uit recent onderzoek blijkt dat slachtoffers van cybercrime geen aangifte doen omdat ze het idee hebben dat de politie niets zal doen [6], probeert de CCU veel aandacht te geven aan slachtoffers. Deze persoonlijke benadering past bij KPCN dat diep geworteld is in de hechte gemeenschappen van Caribisch Nederland.

Casus: ransomwareaanval op bedrijf
Gijzelsoftware (ook wel bekend als ransomware) is een wereldwijd probleem waarbij verdachten zelden worden vervolgd. In 2021 deed een bedrijf op de BES aangifte van een succesvolle ransomwareaanval. Het bedrijf had geen losgeld betaald, maar wel meer dan $80.000 aan financiële schade. Inmiddels waren de bedrijfsprocessen weer opgestart. Aan de hand van screenshots die de aangever had gemaakt, een verklaring van de systeembeheerder en open en gesloten Internetbronnen (OSINT) kon de CCU achterhalen welke ransomwarefamilie het betrof, hoe deze *ransomware-as-a-service* doorgaans opereert en hoe de aanvallers vermoedelijk bij dit bedrijf waren binnengekomen. Eén aangetroffen kwetsbaarheid was bij het bedrijf nog niet bekend waardoor hervictimisatie mogelijk was. Door de rapportage van de CCU nam het bedrijf extra maatregelen om een nieuwe aanval te voorkomen.

Wat de matrix verder laat zien is dat de niveau's van de medewerkers van de CCU gekoppeld zijn aan de mate van complexiteit van cyberdreigingen waarmee de bevolking, MKB en vitale infrastructuur te maken hebben. Op niveau's

1 en 2 (Basis en Junior) leert de CCU lokale, relatief eenvoudige vormen van gedigitaliseerde criminaliteit ('cybercrime in ruime zin') aan te pakken waar voornamelijk burgers mee te maken hebben. Denk aan verschillende vormen van fraude en oplichting, zoals Vriend-in-Noodfraude (VIN-fraude), phishing en identiteitsfraude. Dergelijke vormen van fraude hebben simpele, *low-tech* MO's waarbij lokale context van belang is. Bij VIN-fraude gaat het, bijvoorbeeld, om chatberichten die in het Nederlands, Papiaments of pidgin Engels zijn geschreven, of gebruikmaken van lokale financiële instellingen bij phishing. Niveau's 2 en 3 (Junior & Medior) richten zich op de regionale cyberdreigingen met *medium-tech* MO's waar het MKB last van heeft zoals factuurfraude, ransomware en BEC ('*business email compromise*'). De regionale component komt niet alleen tot uiting doordat aanvallers een groter bereik kunnen hebben door de *lingua francae* van Caribisch Zuid-Amerika te gebruiken (namelijk Engels en Spaans), maar ook in een mogelijke aanpak. Informatiedeling over dergelijke aanvallen zouden in regionaal - lees: Caribisch Zuid-Amerikaans - verband moeten plaatsvinden. Hoewel de CCU op de middellange termijn *niet* voorziet in de groei van medewerkers naar het hoogste Niveau 4 (Senior), richt dit niveau zich op de aanpak van globale cyberdreigingen tegen de vitale infrastructuur op de BES. Deze aanvallen hebben *high-tech* MO's ('*advanced persistent threats*') en de aanpak hiervan vereist nauwe samenwerking met wereldwijd opererende publiek en private organisaties.

Samenwerking met cyberknooppunten voor daders en infrastructuur
Wat is dan de aanpak van die andere twee componenten van cybercrime, namelijk daders en technische infrastructuur? Allereerst is het zo dat wanneer verdachten zich ophouden op de BES, de CCU onder leiding van het Openbaar Ministerie BES een opsporingsonderzoek zal starten met als doel vervolging. Wanneer inhoud of metadata van aanvalsservers nodig zijn voor de waarheidsvinding, is de CCU afhankelijk van de medewerking van andere landen, en dat is ook het geval wanneer daders zich in het buitenland bevinden. Voor het intelligencebeeld en in die gevallen dat sporen naar het buitenland leiden zijn goede contacten met het buitenland van belang. KPCN heeft niet de capaciteit om relaties te onderhouden met veel politiediensten. Daarom richt de CCU zich op een vijftal cyberknooppunten binnen internationale politienetwerken: i) nationale politie voor Nederland, ii) Europol voor de Europese Unie, iii) de Amerikaanse *National Cyber-Forensics and Training Alliance* (NCFTA) voor de Verenigde Staten, iv) het *Regional Intelligence Fusion Centre* van de multilaterale organisatie CARICOM IMPACS voor de Caribische regio, en v) INTERPOL voor de overige werelddelen (via de bestaande sub-NCB van KPCN).

Veel publiek-private cybersecuritynetwerken draaien om het delen van informatie die betrekking heeft op Russisch- en Engelstalige cybercriminelen. Om te voorkomen dat KPCN binnen deze netwerken alleen haalt en niets brengt, heeft de CCU drie verdiepende niches: Papiaments sprekende, Caribische en Latijns-Amerikaanse cybercriminele netwerken. In de praktijk betekent dit dat opgedane OSINT-vaardigheden ook worden ingezet om dreigingsanalyses ('*cyber*

threat intelligence reports') te schrijven over deze relatief onbekende cybercriminele gemeenschappen. In 2022 is de eerste dreigingsanalyse van KPCN over de Latijns-Amerikaanse ondergrondse cybereconomie gedeeld binnen één van de eerdergenoemde internationale cyberhubs. De opgedane kennis en ervaring over deze specifieke ondergrondse gemeenschap komt weer het algemene intelligencebeeld ten goede, en dus ook de lokale bevolking, het MKB en de vitale infrastructuur van de BES.

TACTISCHE CYBER-MATRIX	**Wat?**		**(Door & met) wie?**			**Hoe?**
	Doelstelling	***Type dreigingen***	***Werkniveau CCU***	***Publieke partners***	***Private partners***	***Gremium/ interventies***
Cyber-vaardigheden KPCN	Ontwikkelen van politievaardigheden op het gebied van cybercrimebestrijding	Alle cybercrime-dreigingen in de ruime zin van het woord	Niveau's 1 t/m 4	KPCN & partners	Cyber threat intelligence & cybersecuritybedrijven	Uitleren basis dmv 'presenteren/doceren', 'zien', 'doen', 'praten', 'lezen', 'cursus' en 'luisteren' ohgv 'fenomeen', 'OSINT', 'technisch', 'juridisch', 'financieel', 'interventies' en 'tools'
Vaardigheden inzetten voor ⇓						
Intelligencebeeld voor 'Cyber BES'	Het verzamelen, opslaan & analyseren van relevante gegevens over cybercrime	Alle lokale & regionale cyberdreigingen	Niveau's 1, 2 & 3 (Basis, Junior & Medior)	Politiediensten Caribische regio, Nederland en daarbuiten	Inwoners, MKB & vitale infra BES; banken; cybersecuritybedrijven	Bovenstaande basisvaardigheden worden ingezet om een intelligencebeeld te maken. Het intelligencebeeld vormt de input voor onderstaande interventies
Intelligence inzetten voor ⇓						
Inwoners Caribisch Nederland (BES)	Bewustwording *lokale* cyberdreigingen & aanbieden van handelingsperspectief	WhatsApp- & identiteitsfraude; phishing	Niveau 1 en 2 (Basis & Junior)	RijksdienstCN; BZK/RvIG; KPCN	Inwoners; banken	Publiekscampagnes 'Voorkom identiteitsfraude' en 'Veiligheidstip van de maand'; voorlichting aan studenten over geldezels; interactieve cybergame 'Framed' voor middelbare scholieren
Midden- en kleinbedrijf (MKB)	Bewustwording *regionale* cyberdreigingen & aanbieden van handelingsperspectief	Ransomware; CEO-, BEC- & factuurfraude; online bankfraude; phishing	Niveau 2 & 3 (Junior & Medior)	KvK; CBP BES; KPCN	MKB; cybersecurity-bedrijven; banken	Voorlichtingscampagne 'Incident responseplan voor het MKB'; seminars; supporting partner van Europol's NoMoreRansom-initiatief
Vitale infrastructuur	Bewustwording *globale* cyberdreigingen & aanbieden van handelingsperspectief	Advanced persistent threats; ransomware	Niveau 3 & 4 (Medior & Senior)	RijksdienstCN; NCSC; KPCN; OLB;	WEB; luchthaven; ziekenhuis; internetproviders; havenbedrijf	Periodiek overleg met lokale financiële instellingen; Crisisoefening digitaal incident met grootschalige impact;
KPCN & partners	Bewustwording *alle* cyberdreigingen, belang samenwerking & kansen regionale bestrijding	Nadruk op *bestaande* lokale, regionale en globale cyberaanvallen	Niveau's 1 t/m 4	Slachtoffers: alle bovenstaande partners; daders/infra: internationale cyberhubs	Alle bovenstaande partners	Presentaties binnen KPCN en bij partners over werkzaamheden Cyber Crime Unit

Figuur 4: In deze Tactische Cybermatrix staan alleen voorbeelden en suggesties. *) Voor de periode 2021-2024 voorziet KPCN niet in het opleiden van Seniors op Niveau 4.

5 Operationele Focus op Vaardigheden, Intelligencebeeld & Uitvoering

De strategische pyramide en de tactische matrix geven invulling aan de dagelijkse werkzaamheden. Hiervoor houden TDO, CCU en OSINT diverse 'levende' documenten bij die telkens worden aangevuld naar gelang er nieuwe inzichten zijn. Deze documenten samen vormen het operationeel plan. Zoals in de vorige sectie staat beschreven bestaat dit plan voor de CCU uit drie aan elkaar gerelateerde componenten: i) het uitleren van cybervaardigheden, ii) het opstellen van het cyberintelligencebeeld BES en iii) het uitvoeren van diverse interventies.

Vaardigheden teams & sleutelpartners Het eerste jaar waren de CCU-medewerkers taakaccenthouders. Dit betekent dat medewerkers op andere afdelingen zaten maar twee dagen per week werkten binnen de CCU om cybervaardigheden te ontwikkelen. Door de successen en het werkaanbod heeft de leiding van KPCN besloten om van de CCU een volwaardig team te maken met 3FTE. De nadruk op slachtoffers, (inter)nationale samenwerking en harmonisatie vormen belangrijke uitgangspunten voor de samenstelling van de Cyber Crime Unit. De CCU-medewerkers zijn geworven uit de afdelingen Opsporing, Info en Intake. Vanwege de niet-technische achtergrond van de medewerkers en geringe grootte van de CCU is interne samenwerking met andere afdelingen binnen KPCN cruciaal. TDO doet alle digitaal-forensische zaken voor CCU, zoals het uitlezen van gegevensdragers. De afdeling Communicatie is belangrijk vanwege de nadruk op preventie. FINEC ondersteunt bij alle financieel-economisch aspecten van cybercrime. Daarnaast ondersteunt de CCU ook weer andere afdelingen, zoals JZZ en IGO, met name op het analyseren van Internetgedrag van verdachten. Denk respectievelijk aan het onderzoeken van de browsergeschiedenis op in beslag genomen gegevensdragers van zedenverdachten of de data van een IP-tap op de mobiele telefoon van een verdachte van drugshandel. De lokale kenmerken van Caribisch Nederland - denk aan de ligging, de status van bijzondere gemeente, en de afwezigheid van datacenters - heeft ook gevolgen voor de samenstelling en vaardigheden van de teams. Zo hoeft TDO niet te leren hoe servers moeten worden veiliggesteld bij een eventuele cyberaanval. Wel zouden de CCU en TDO in de toekomst specifieke vaardigheden kunnen ontwikkelen voor een cyberaanval op vitale infrastructuur, zoals *emergency response* voor de periode dat er nog geen specialistisch team van een sleutelpartner op de eilanden is gearriveerd. De focus en het groeiplan van de CCU roept ook de vraag op welke vaardigheden sleutelpartners moeten hebben om cybercrime mede te bestrijden. Lokaal bestuur en de vitale infrastructuur hebben geen kennis en ervaring in risicobeheersing van een cyberincident met significante impact. De CCU heeft daarom samen met NCSC het initiatief genomen om een kleinschalige cyberoefening voor de BES te houden zodat sleutelpartners deze vaardigheden kunnen ontwikkelen.

Uitleren van vaardigheden De eerste vaardigheid is het begrijpen van cybercrime in het algemeen en het herkennen van specifieke modi operandi. Overige vaardigheden zijn een reactie op cybercriminaliteit namelijk verschillende bestrijdings- en onderzoeksmethoden en technieken, meer specifiek:

- OSINT die specifiek toepasbaar is voor cybercrime en -security, zoals het verzamelen en interpreteren van gegevens uit open en gesloten Internetbronnen;
- Internettechnologie, zoals kennis van IP-adressen, domeinnamen, Internet Service Providers en servers;

- Rechtsgeleerdheid, zoals het juridisch kwalificeren van delictsomschrijving, opnemen van aangiftes, schrijven van bevindingen en vorderingen;
- Financiële aspecten van cybercrime, zoals basisbegrip van digitale valuta, cryptocurrencies en online betaalsystemen;
- Praktische tools, zoals Cellebrite Reader voor het analyseren van mobiele telefoons, Maltego voor het bevragen en visualiseren van domeinen en IP's en Hunchly voor het vastleggen van OSINT-bevindingen; en tools voor kritisch denken en samenwerken, zoals het opstellen en toetsen van hypotheses en werken met de projectmanagementmethode Scrum.
- Interventies die verder gaan dan alleen het uitvoeren van opsporingsonderzoek voor vervolging van verdachten, zoals het opzetten van publiekscampagnes, schrijven en distribueren van dreigingsanalyses en geven van algemene presentaties en specifieke adviezen aan partners.

Deze vaardigheden worden klassikaal uitgeleerd door:

- Klassikale en online cursussen;
- Aanpak van cybercrime 'te doen';
- Te netwerken en gesprekken te voeren met, inclusief presentaties te bekijken van, publieke en private partners.

Ook leren de medewerkers van de CCU vaardigheden door zelfstandig films te kijken, podcasts te luisteren of blogs te lezen. Eén van de belangrijkste manier van leren is door opgedane kennis zelf weer uit te leren (doceren) aan anderen. In de praktijk betekent dit dat de CCU andere afdelingen binnen KPCN opleidt naar Niveau 1 (Basis) en presentaties geeft op conferenties en aan publieke en private partners.

OPERATIONEEL 'LEVEND' DOCUMENT CURRICULUM CYBERVAARDIGHEDEN KORPS POLITIE CARIBISCH NEDERLAND							
CYBERCRIME ALGEMEEN	**Presenteren & Doceren**	**Cursus**	**Doen**	**Netwerken & Gesprekken met partners**	**Zien**	**Lezen**	**Luisteren**
	Presentatie MBO-4 IT	Europol - E-First;	Threat analysis opstellen		Zero Days (EN)	Krebs on Security (EN)	Darknet Diaries (EN)
	Presentatie MBO-4 KPCN	THTC - Introduction to Cybercrime;	MO's herkennen		Spying on the Scammers (EN)	Security.nl (NL)	Cyberhelden (NL)
	Presentatie Aspiranten	Certified Secure;	Zaken bijhouden/muteren		HackerHunterSeries (EN)	Tweakers (NL)	
	Presentatie Framed SGB						
Fenomeen	Presentaties afdelingen KPCN					Info Security (EN)	
OSINT		RST OSINT-cursus; Certified Threat Intelligence Analyst (commercieel);		Cyber threat intellbedrijven			
		UCD Network Investigations (TDO);		Anti-virusbedrijven (ESET)			
Technisch				Internet access providers (Telbo, Flamingo, Digicel)			
Juridisch		Minicursus Rechtshulp (NP/LIRC)	WvSr/WvSv: aangifte, bevindingen, vorderingen	Openbaar Ministerie; MinJenV; CBP BES;		Cybercrimeverdrag	
Financieel				Banken (MCB)			
Tools		UFED-training (TDO) Axiom-training (TDO) Online Maltegocursus (commercieel) Online Hunchlycursus Certified Threat Intelligence Analyst (commercieel);	DomainTools Chrome Extensions Cygnus Maltego INTERPOL/NCB Hunchly TraceLab VM				
		Certified Threat Intelligence Analyst (commercieel);		VS: FBI, USSS, DEA	CyberDEX		
				DEX XL			
				NCSC One			
Interventies				Slam Spam			

Figuur 5: In dit voorbeeld staan de verschillende leervormen hoe de medewerkers van de CCU begrip krijgen van de verschillende aspecten van het thema 'cybercrime algemeen'.

Opstellen cyberintelligencebeeld BES Vaardigheden worden ingezet om uit verschillende bronnen informatie te halen over cybercrime en cybersecurity. Wanneer afzonderlijke informatiepunten met elkaar worden verbonden tot een verhaal over cybercrime en cybersecurity ontstaat het intelligencebeeld. Dit beeld is niet een uitgeschreven of gevisualiseerd product. Eerder zijn het vele gesprekken onder teamleden van de CCU waarbij op een hoger abstractieniveau nieuwe inzichten worden gedeeld. Op basis van deze inzichten worden interventies bepaald (zie volgende paragraaf). Het beeld verandert dus voortdurend en is nooit af. Doordat verschillende bronnen, methoden en technieken worden gebruikt om informatie te verzamelen worden blind vlekken beperkt. Zo waren er in 2021 geen aangiftes van burgers met betrekking tot phishing. Wel waarschuwen regionale banken via websites, chatgroepen en webinars over deze vorm van cybercrime. Op een hoger abstractieniveau zou dit kunnen betekenen dat er mogelijk Papiaments sprekende dadergroepen zijn die slachtoffers maken onder de lokale bevolking, maar dat banken en bevolking geen stimulans hebben om aangifte te doen. Een ander voorbeeld is dat er meerdere aangiftes waren door het midden- en kleinbedrijf (MKB) van ransomware. Literatuuronderzoek en opsporingsonderzoeken van CCU tonen aan dat het MKB in het algemeen, en het MKB op de BES in het bijzonder, niet altijd voorbereid zijn op dergelijke incidenten. Met andere woorden, er is behoefte aan meer kennis wat bedrijven zelf kunnen doen en duidelijkheid wanneer de politie een rol heeft. Als laatste voorbeeld, onderzoek van een Nederlandse recherchekundige toont aan dat 10% van de Nederlandse geldezels van Antilliaanse afkomst is [7],[2] terwijl een opsporingsonderzoek van de CCU laat zien dat Bonairiaanse inwoners worden geworven als geldezel. Daarnaast reizen er elk jaar jongeren vanuit de BES

[2]De politieonderzoekster heeft op aanvraag van KPCN een specifieke zoekslag gemaakt binnen haar onderzoek naar het aantal geldezels in Nederland die geboren zijn in de Nederlandse Antillen.

voor het eerst naar Nederland. Deze kennis roept de vraag op wat KPCN kan doen om de lokale bevolking weerbaar te maken tegen ronselaars van geldezels in Caribisch en Europees Nederland.

Uitvoeren aanpak cybercrime Het zijn bovenstaande intelligencebeelden die de input vormen voor een integrale aanpak van cybercrime: reactief ('brengzaken') en proactief ('haalzaken'), publiek en privaat, lokaal, nationaal en internationaal, preventief en repressief, op slachtoffers en daders. Hoe ziet deze integrale aanpak er dan uit in de praktijk? Neem de ransomwareproblematiek waar het MKB mee te maken krijgt op de eilanden. Om het lokale MKB weerbaarder te maken tegen cyberaanvallen heeft de CCU een *incident response*-plan geschreven. In dit plan staat wat bedrijven kunnen doen om aanvallen te voorkomen, hoe een *incident response*-plan en -proces eruit zien, en wat de rol van KPCN en andere overheidspartijen op de BES is tijdens een cyberaanval. In de repressieve aanpak van dergelijke aanvallen zijn afspraken gemaakt met de Nederlandse Ransomware Taskforce over hoe bevindingen van de CCU over dadergroepen, misbruikte infrastructuur en aanvallen kunnen worden gedeeld, zodat internationale opsporingsonderzoeken kunnen worden gestart. Ook is KPCN *supporting partner* van het *No More Ransom*-platform van Europol. Tijdens de uitvoer van interventies worden op verschillende manieren vaardigheden uitgeleerd, zoals het het begrijpen van een specifieke MO, inzetten van OSINT, opnemen van een aangifte, het juridisch kwalificeren van handelingen en gedragingen naar een delictsomschrijving en het schrijven van een rapportage ten behoeve van het slachtoffer. Verder gaf de regionale eenheid Oost-Brabant een verdiepende presentatie over ransomware, terwijl THTC ter lering een geanonimiseerd opsporingsdossier deelde met de CCU. De uitvoering van interventies helpt ook weer te inventariseren welke verbeteringen het juridisch, technisch en organisatorisch fundament van KPCN nodig heeft.

6 Hoe nu verder?

In het nieuwe regeerakkoord 'Omzien naar elkaar, vooruitkijken naar de toekomst' belooft de coalitie voor de kabinetsperiode 2021-2025 meer structurele aandacht te hebben voor Caribisch Nederland en het Caribisch gebied binnen het Koninkrijk [8]. Ook wordt er geschreven over versterking van de aanpak van cybercriminaliteit. Wat de ambities van het kabinet zijn is dus duidelijk, maar hoe deze ambities in de praktijk worden gebracht zal nog moeten blijken. Onderhavig artikel is een beschrijving van een *evidence-based* plan hoe de eilanden en Europees-Nederland in gezamenlijkheid het Caribisch deel van het Koninkrijk weerbaarder kunnen maken tegen cybercrime. De focus heeft al geleid tot tal van successen op het gebied van onder andere - maar niet uitsluitend - de bestrijding van cybercrime op de BES: van preventiecampagnes voor kwetsbare groepen tot vervolging van verdachten, van lokale tot internationale samenwerkingen, en van groeien naar een volwaardige Cyber Crime Unit tot het doceren van basisvaardigheden aan andere politiecollega's binnen KPCN. Tegelijkertijd

zit het korps nog in de beginfase van het groeiplan en is verdere samenwerking tussen Caribisch en Europees Nederland een blijvende noodzakelijkheid. Daarbij vervullen de nationale politie en het Ministerie van Justitie en Veiligheid een sleutelrol door bij te dragen aan drie speerpunten:

1. balanceer tussen spontane samenwerking & formele beleidsdoelen;
2. maak van harmonisatie een formeel beleidsspeerpunt;
3. stel een strategisch aanjager aan in Europees Nederland om de eerste twee punten vorm te geven en uit te voeren, en plaats operationeel specialisten in Caribisch Nederland om de startende teams verder te begeleiden.

Balanceer tussen informele samenwerking & formele beleidsdoelen De successen van KPCN zijn voor een groot deel het gevolg van informele contacten en spontane samenwerkingen tussen individuele ambtenaren in Caribisch en Europees Nederland. Er zijn talloze enthousiaste collega's vanuit Europees Nederlandse ministeries en de nationale politie die zich belangeloos inspannen om de BES-eilanden weerbaarder te maken tegen cybercrime. Deze samenwerkingsverbanden blijken een kracht. Kennis- en productuitwissing gaan vanzelf wanneer mensen wíllen samenwerken en er een duidelijke behoefte is aan kennis en initiatieven in Caribisch Nederland. Kortom, veel projecten, processen en onderzoeken zijn vermoedelijk gelukt, juist omdat niet alles van te voren in beton is gegoten. De vrijblijvendheid van deze samenwerkingsvormen is tegelijkertijd een zwakte. Ambtenaren in Caribisch Nederland kennen niet altijd de relevante ambtenaren in Europees Nederland. Ook wordt soms duidelijk dat de kennis- of productoverdracht te veel inspanning gaat kosten van individuele ambtenaren in Europees Nederland. Het is daarom belangrijk dat ten minste één beleidsdoel wel geformaliseerd wordt zodat daar ook de nodige resources voor worden vrijgemaakt: harmonisatie, met name op juridisch vlak.

Maak van harmonisatie een formeel beleidsspeerpunt Afbeelding 3 laat zien dat harmonisatie begint met (h)erkenning van gedeelde strategische belangen [9]. De BES is niet in de huidige cybersecurity- en cybercrimeprogramma's van het Ministerie van Justitie en Veiligheid en de nationale politie opgenomen.[3] Naast verplichtingen ten opzichte van Caribisch Nederland zijn er wel degelijk strategische belangen voor Europees Nederland: goed functionerende cybercrime teams in het Caribisch gebied kunnen niet alleen de oren en ogen zijn voor de nationale politie met betrekking tot de cyberontwikkelingen in de Caribische en Zuid-Amerikaanse regio, maar ook ondersteuning bieden wanneer er cyberzaken zijn in Europees Nederland met Papiaments sprekende verdachten, getuigen en slachtoffers. Een volgende noodzakelijke stap is zo snel mogelijk

[3] Binnen dergelijke programma's wordt doorgaans een onderscheid gemaakt tussen initiatieven binnen Nederland (lees: regionaal en nationaal niveau) en tussen initiatieven van Nederland met andere landen en internationale organisaties (internationaal niveau). Uit gesprekken met betrokken ambtenaren komt naar voren dat de BES regelmatig onder geen van beide indelingen wordt opgenomen.

investeren in wetgeving om cybercrime en gedigitaliseerde criminaliteit effectief te bestrijden op de eilanden. Zoals eerder beschreven in dit artikel ontbreekt het in CN aan meerdere essentiële wet- en regelgevingen om cyberincidenten te voorkomen en effectief te bestrijden. Los van deze noodzakelijke juridische inspanningen kunnen ook al enkele stappen richting organisatorische en technische harmonisatie worden genomen, zoals aansluiting op Nederlandse ontwikkelingen op het gebied van bijvoorbeeld kennisuitwisseling en *tooling*.

Stel een strategisch aanjager aan in Europees Nederland & plaats operationeel specialisten in Caribisch Nederland Om de juridische, organisatorische en technische harmonisatiedoelstellingen uit te voeren en informele samenwerkingsverbanden te stimuleren, zou de nationale politie een strategische aanjager kunnen aanstellen. Deze aanjager adviseert KPCN en - wanneer wenselijk - de andere Caribische korpsen wat noodzakelijk is om het plan voor digitale opsporing verder vorm te geven. Ook maakt de aanjager verbinding met de Europees Nederlandse organisaties waar CN behoefte aan heeft. Tegelijkertijd kan een strategisch aanjager Europees Nederlandse overheidsinstanties aanzetten om te zien of hun project van toepassing kan zijn op CN of wijzen op eventuele verplichtingen ten opzichte van CN. Daarnaast is een operationele bijdrage vanuit de nationale politie wenselijk waarbij digitale opsporingsspecialisten van de nationale politie hun kennis en ervaring delen met lokale collega's in Caribisch Nederland. Het is belangrijk dat dit ter plaatse gebeurt, zodat het opdoen van nieuwe vaardigheden, het opzetten van intelligencebeeld en de uitvoering van interventies verder kunnen worden ontwikkeld in lijn met de visie van KPCN.

References

[1] O. Nauta and P. van Egmond, "Inrichting en organisatie Brandweerkorps en Korps Politie Caribisch Nederland," DSP-groep, Tech. Rep., 2015. [Online]. Available: https://repository.wodc.nl/handle/20.500.12832/2150

[2] A. G. Broek, *De geschiedenis van de politie op de Nederlands-Caribische eilanden (1839-2010); Geboeid door macht en onmacht.* Amsterdam: Uitgeverij Boom, 2011.

[3] Openbaar Ministerie, "Beleidsplan recherchesamenwerking in het Caribisch deel van het Koninkrijk 2020-2023," Tech. Rep., 2019. [Online]. Available: https://www.openbaarministerie.org/

[4] Portefeuilleteam Landelijk Expertisecentrum Digitaal Opsporen, "Vakontwikkeling Digitaal Opsporen 2022," Nationale politie, Tech. Rep., 2021.

[5] E. Van de Sandt, M. Den Hengst, P. De Bruine, R. Westerhof, and S. Van der Maden, "Het datagedreven bestrijden. Nieuwe loot aan de stam in de bescherming van de rechtsstaat," *Politie Cahiers*, vol. 1, no. 62, pp. 117–130, 2022.

[6] S. van de Weijer, R. Leukfeldt, and S. Van der Zee, "Reporting cybercrime victimization: determinants, motives, and previous experiences," *Policing*, vol. 43, no. 1, 2020. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/PIJPSM-07-2019-0122/full/html

[7] R. Wajon, *Vissen naar geldezels. Een onderzoek naar de rekrutering en opsporingsonderzoek van money mules.* Apeldoorn: Politieacademie, 2021.

[8] VVD, D66, CDA, and ChristenUnie, "Omzien naar elkaar, vooruitkijken naar de toekomst," 2021. [Online]. Available: https://www.rijksoverheid.nl/documenten/publicaties/2022/01/10/coalitieakkoord-omzien-naar-elkaar-vooruitkijken-naar-de-toekomst

[9] E. Van De Sandt, *The Deviant Security Practices of Cyber Crime*. Leiden: Brill | Nijhoff, 2021. [Online]. Available: https://brill.com/view/title/60184