Digitale Opsporing in Caribisch Nederland: een Cybercrime Casestudy

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

8 juli 2022

Caribische Politiestrategie voor Digitale Opsporing

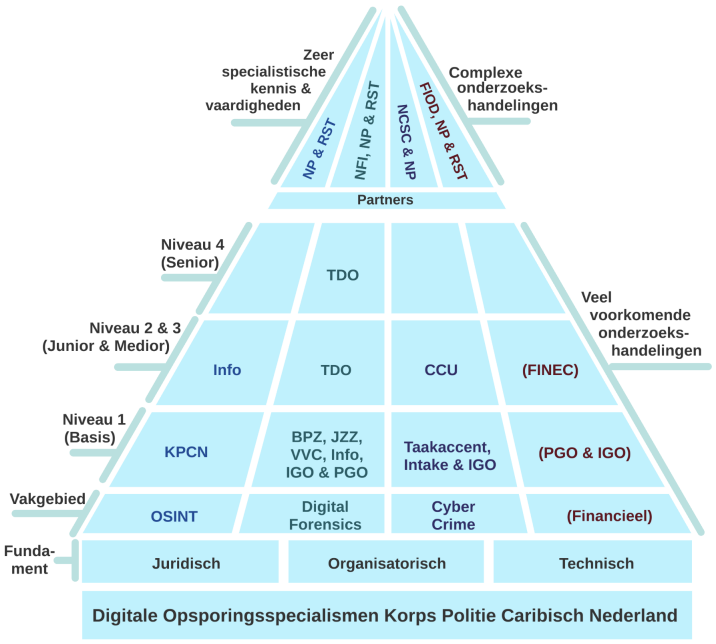
Er is nauwelijks nog politiewerk te vinden zonder digitale component. Digitale opsporing is het containerbegrip voor digitaal-forensisch onderzoek aan gegevensdragers, onderzoek naar cybercrime en onderzoek middels open en gesloten internetbronnen (OSINT). Deze vorm van opsporing heeft vaste grond onder de voeten bij de nationale politie in Europees Nederland. Heel anders is de situatie op de Caribische eilanden binnen het Koninkrijk der Nederlanden. Daar moeten digitale opsporingsspecialismen feitelijk nog een aanvang nemen. Zo had Korps Politie Caribisch Nederland van 2016 tot 2021 geen cybercrime-, digitaal-forensische (TDO) of OSINT-afdelingen. Er was slechts één digitaal rechercheur, die alleen eenvoudige digitaal-forensische handelingen kon uitvoeren, en daardoor zeer afhankelijk was van het Recherche Samenwerkingsteam (RST) te Curaçao. Het gevolg van deze situatie is dat het KPCN ontbrak aan de benodigde juridische, organisatorische en technische middelen om digitale opsporingsspecialismen uit te kunnen voeren.

*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. Operationeel contact: cybercrime [at] politiekpcn.com. De auteurs bedanken Garry Clementina, Sharon Heymans, Gino van Hoogstraten, Ian Steba en Ronald Zwarter voor hun waardevolle aanvullingen op het artikel.

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. 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].

Vanaf 2021 hebben KPCN, het Ministerie van Justitie en Veiligheid en de nationale politie flink geïnvesteerd in de ontwikkeling van de digitale opsporingsspecialismen binnen het korps, onder andere door de oprichting van een TDO en Cyber Crime Unit (CCU). Afbeelding 1 visualiseert de strategie van KPCN waarbij het korps groeit 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 1: In de strategie van KPCN groeit het korps naar een sterk fundament, specialistische afdelingen en duurzame contacten met meerdere sleutelpartners om zo de meest voorkomende digitale onderzoekshandelingen zelf uit te kunnen voeren. 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.

Cybercrime: 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 zo draagvlak en besluitvorming op middenmanagementniveau te stimuleren. De matrix van de Cyber Crime Unit heeft drie aan elkaar verbonden doelen, zie Afbeelding 2. 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, bruikbaar en regionaal intelligencebeeld. Dit beeld wordt ingezet voor het derde doel: de bestrijding van cybercriminaliteit.

Focus op kwetsbare groepen en slachtoffers Het regionale intelligencebeeld van de CCU laat zien dat de kennis over cybercrime en cybersecurity op de eilanden zeer laag is. Om deze reden is de aanpak van cybercrime primair gericht op het verhogen van de bewustwording en het bieden van een handelingsperspectief aan de inwoners, het midden- en kleinbedrijf (MKB) en - wanneer

het werkniveau het toelaat - de vitale infrastructuur van de BES. De interventies zijn gericht op hen die nog geen slachtoffer zijn maar wel kwetsbaar, en zij die daadwerkelijk slachtoffer zijn geworden.

Focus op daders en infrastructuur Omdat daders en aanvalsinfrastructuur zich doorgaans in het buitenland zullen bevinden richt de CCU zich op samenwerking en harmonisatie met een vijftal internationale politieknooppunten: i) nationale politie voor Europees Nederland, ii) Europol voor de Europese Unie, iii) de Amerikaanse *National Cyber-Forensics and Training Alliance* (NCFTA) voor de Verenigde Staten, iv) de multilaterale organisatie CARICOM IMPACS voor de Caribische regio, en v) INTERPOL voor de overige werelddelen (via de bestaande sub-NCB van KPCN). Omdat deze knooppunten grotendeels gericht zijn op Russisch- en Engelstalige cybercriminelen en 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.

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; cybersecu-ritybedrijven	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 2: In deze versie van de Tactische Cybermatrix staan enkele voorbeelden van slachtoffergerichte interventies. De verschillende werkniveau's uit de strategische pyramide (zie Afbeelding 1) zijn gekoppeld aan de matrix, namelijk de complexiteit van de cyberdreigingen waar de bevolking, MKB en vitale infrastructuur mee te maken hebben. Zo zijn de werkniveau's 1 en 2 (Basis en Junior) gekoppeld aan de aanpak van lokale, relatief eenvoudige vormen van gedigitaliseerde criminaliteit ('cybercrime in ruime zin') 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 criminaliteitsvormen hebben simpele, *low-tech* MO's waarbij lokale context van belang is, zoals het gebruik van lokale financiële instellingen of de Nederlandse, Papiamentse of Pidgin Engelse taal.

Cybercrime: Operationele Focus op Vaardigheden, Intelligencebeeld & Uitvoering

De strategische pyramide en de tactische matrix geven invulling aan de samenstelling, samenwerking en werkzaamheden van de CCU.

Samenstelling van & -werking met de Cyber Crime Unit De drie fulltime CCU-medewerkers zijn geworven uit de afdelingen Opsporing, Info en Intake. Ook zijn er twee taakaccenthouders, waarvan er één op Sint Eustatius is gestationeerd. Vanwege de niet-technische achtergrond van de medewerkers en geringe grootte van de CCU is interne samenwerking met andere afdelingen binnen KPCN cruciaal. Bij opsporingsonderzoeken van CCU naar 'echte' cybercrime (IT als doel) doet TDO al het digitaal-forensisch werk, zoals het uitlezen van gegevensdragers. Samenwerking met de afdeling Communicatie is belangrijk vanwege de nadruk op preventie. FINEC assisteert bij financieel-economisch aspecten van cybercrime. Daarnaast ondersteunt de CCU ook weer andere afdelingen, zoals JZZ en IGO, bij gedigitaliseerde criminaliteit (IT als middel). Denk respectievelijk aan het onderzoeken van de browsergeschiedenis op in beslag genomen gegevensdragers van zedenverdachten of het analyseren van IP-tap data van een verdachte.

Werkzaamheden van de Cyber Crime Unit De eerste vaardigheid is het begrijpen van cybercrime in het algemeen en het herkennen van specifieke *modi operandi* (MO), zoals ransomware. Overige vaardigheden zijn een reactie op cybercriminaliteit, namelijk verschillende bestrijdings- en onderzoeksmethoden en technieken, zoals het gebruik van technische *tooling*, het opnemen van aangiftes of geven van inhoudelijke adviezen aan partners. De CCU houdt hiervoor diverse 'levende' documenten bij wat en hoe men bepaalde vaardigheden heeft geleerd. De vaardigheden worden ingezet om een intelligencebeeld te creëren. 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. Deze inzichten worden ingezet om interventies te bedenken. Deze ideeën worden bijgehouden via een *scrum board* zodat duidelijk is welke collega wat doet en wat de status is van een bepaalde interventie. De uitvoering van interventies helpt ook weer te inventariseren welke verbeteringen het juridisch, technisch en organisatorisch fundament van KPCN nodig heeft.

Vaardigheden, intelligence & uitvoering in de praktijk
Een opsporingsonderzoek van de CCU liet zien dat inwoners van Bonaire worden geworven als geldezel. Tijdens de kennisvergaring over dit fenomeen leerde de CCU dat tien procent van de Nederlandse geldezels van Antilliaanse afkomst is [3].[a] Daarnaast reizen er elk jaar jongeren vanuit de BES voor het eerst naar Nederland voor studie en werk. De bevolking van de eilanden moet dus weerbaarder worden tegen ronselaars van geldezels in Caribisch en Europees Nederland. Om deze reden geeft de CCU nu voorlichting over geldezels aan Bonairiaanse jongeren die voor het eerst naar Europees Nederland reizen.

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

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 [4]. 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. Het *evidence-based* plan van KPCN heeft al geleid tot tal van successen op het gebied van onder andere - maar niet uitsluitend - de bestrijding van cybercrime op de BES. Tegelijkertijd zit het korps nog in de beginfase van het groeiplan en is verdere samenwerking tussen Caribisch en Europees Nederland een blijvende noodzakelijkheid. Daarbij kunnen de nationale politie en het Ministerie van Justitie en Veiligheid een sleutelrol vervullen door bij te dragen aan drie speerpunten:

Balanceer tussen informele samenwerking & formele beleidsdoelen
De successen van KPCN zijn voor een groot deel het gevolg van informele samenwerkingsverbanden tussen enthousiaste collega's uit Caribisch en Europees Nederland. Deze contacten 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 Harmonisatie begint met (h)erkenning van gedeelde strategische belangen [5]. De BES is niet in de huidige cybersecurity- en cybercrimeprogramma's van het Ministerie van

Justitie en Veiligheid en de nationale politie opgenomen.[1] 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 investeren in wetgeving om cybercrime en gedigitaliseerde criminaliteit effectief te bestrijden op de eilanden. Het ontbreekt 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 hun collega's in Caribisch Nederland. Het is belangrijk dat dit ter plaatse gebeurt, zodat het opdoen van vaardigheden, het creëren van intelligence 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.

[1] 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.

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

[4] 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

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