Inspectieonderzoek van de Raad voor de Rechtshandhaving naar de veiligheid op het gebied van cyber security, terrorisme en grensbewaking.

Colofon

Uitgever	: Raad voor de rechtshandhaving
Jaar	: 2020
Maand	: September
Plaats	: Willemstad, Curaçao
Vindplaats Internet	: www://raadrechtshandhaving.com

Inhoudsopgave

Lijst met gebruikte afkortingen

AIVD	Algemene Inlichtingen en Veiligheidsdienst
CARICERT	Caribbean Cyber Emergency Response Team
CARICOM	Caribbean Community
CSIRT	Cyber Security Incident Response Team
DRR	Directie Risicobeheersing en Rampenbestrijding
FTF-ers	Foreign Terrorist Fighters
ICC	Intelligence Center Curaçao
ICT	Informatie en Communicatie Technologie
IDB	Inter Development
KPC	Korps Politie Curaçao
Kmar	Koninklijke Marechaussee
KW	Kustwacht
MvJ	Ministerie van Justitie
NCSC	Nationaal Cyber Security Coördinator
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
OAS	Organization of American States
OM	Openbaar Ministerie
RST	Recherche Samenwerkingsteam
SBIR	Stichting Beheer ICT Rechtshandhaving
TIRP	Terroristisch Incident Response Plan
VDC	Veiligheidsdienst Curaçao

Voorwoord

De Raad voor de rechtshandhaving verrichtte het inspectieonderzoek naar de integrale veiligheid en infrastructuur op de terreinen cyber security, terrorisme en grensbewaking vanuit het besef dat het één niet los kan worden gezien van het ander en het daardoor steeds noodzakelijker wordt om veiligheidsonderwerpen integraal aan te pakken.

De zorg voor de veiligheid op deze terreinen is van cruciaal belang. Naast het onveiligheidsgevoel dat criminele handelingen voortvloeiende uit cyber crime, terrorisme en grensoverschrijdende criminaliteit teweegbrengen, kunnen deze activiteiten aanzienlijke fysieke en materiele schade veroorzaken. Curaçao dient met name vanwege zijn geografische ligging en infrastructuur deze ontwikkelingen en de daarmee inherente risico's serieus te nemen.

Het doel van dit inspectierapport is om inzicht te geven in de huidige situatie en daarmee een bijdrage te leveren aan de veiligheid van het land.

De Raad voor de rechtshandhaving,

mr. L.M. Virginia, voorzitter
mr. T. P.L. Bot,
mr. M.R. Clarinda.

SAMENVATTING

Dit inspectierapport beschrijft en toetst de veiligheid op de terreinen cyber security, terrorisme en grensbewaking. Het zorgdragen voor de veiligheid van een gemeenschap is een punt van voortdurende zorg voor een regering. In het regeerakkoord van Curaçao wordt erkend dat het veiligheidsniveau in Curaçao niet goed genoeg is. De regering spreekt de voornemens uit om gerichte acties te ondernemen tegen de criminelen, onder andere op het gebied van cyber crime.

Cyber en terroristische aanvallen zijn niet meer territoriaal gebonden en kunnen overal plaatsvinden. Vooral bij terrorisme speelt grensbewaking een belangrijke rol. Immers terroristen komen via de fysieke grenzen een land binnen of zijn er al woonachtig dan wel keren terug na een buitenlandse terroristische activiteit te hebben gepleegd. Informatievergaring en -deling is in dit verband cruciaal.

Het doel van dit inspectierapport is om inzicht te verkrijgen in de integraliteit van de aanpak van het veiligheidsbeleid in Curaçao voor wat betreft terrorisme, cybersecurity en grensbewaking en vast te stellen in hoeverre de justitiële kolom in staat is om uitvoering te geven aan het beleid.

Om de hoofdvraag te kunnen beantwoorden, werden naast open bronnen, ontvangen documenten bestudeerd en interviews gehouden met respondenten van de geïnspecteerde diensten.

Centrale vraag

De centrale vraag luidde als volgt:

In hoeverre zijn de organisaties binnen de justitiële kolom in staat om uitvoering te geven aan het integraal veiligheidsbeleid voor wat betreft de terreinen grensbewaking, cyber security en terrorismebestrijding?

Om antwoord te geven op de centrale vraag komen de volgende deelvragen aan de orde:

1. *Hoe is het integraal veiligheidsbeleid voor wat betreft bovengenoemde terreinen vormgegeven?*
2. *Welke zijn de veiligheidsrisico's en -incidenten en hoe worden die aangepakt door de organisaties binnen de justitiële kolom?*
3. *Wat is de stand van zaken omtrent de fysieke infrastructuur, capaciteit, kennis en middelen om op adequate wijze het veiligheidsbeleid uit te voeren?*
4. *Welke zijn de verbeterpunten?*

Integraal veiligheidsbeleid
Voor wat betreft het veiligheidsbeleid werd in 2016 enkele documenten opgesteld om op integrale wijze de vijf prioritaire thema's die door het Driehoeksoverleg werden goedgekeurd aan te pakken. Deze vijf prioritaire thema's zijn de volgende:

- atrako (straatroof in het publieke domein en overval in het besloten domein, woning en bedrijf);
- geweld (relationeel geweld en vuurwapenbezit en -gebruik);
- inbraken en diefstal (woning- en bedrijfsinbraak en autodiefstal);
- verkeer; en
- criminele samenwerkingsverbanden.

Cyber security, terrorisme en grensbewaking komen niet voor in de bovenstaande lijst. Wel zijn criminele samenwerkingsverbanden mogelijkerwijs actief binnen al deze drie gebieden.

Cyber security
Bij cyber security is er, met uitzondering van de beveiliging van de data in de rechtshandhavingsketen, nog geen sprake van een integrale noch conventionele aanpak. Gebleken is dat cyber security voor geen van de geïnspecteerde organisaties hoog op de prioriteitenlijst voor komt. Uit de interviews is gebleken dat de organisaties nog weinig oog hebben voor de gevaren en mogelijke consequenties van cyber crime. Van een partnerschap voor dit thema tussen de justitiële organisaties met andere overheidsdiensten, het bedrijfsleven en de burgerij is niet gebleken.

Gezien de mogelijk uiterst schadelijke gevolgen van een succesvolle cyberaanval, zoals bijvoorbeeld het lamleggen van de overheid, (vitale) bedrijven of de samenleving als geheel, komt de Raad tot de conclusie dat cyber security verheven dient te worden tot het niveau van nationale veiligheid. Dit houdt onder andere in het verhogen van het niveau van prioriteit van cyber security, het investeren in cyber security, het uitbreiden van de cyberwetgeving, het verhogen van het niveau van de interne en externe samenwerking en van de informatievergaring en -deling.

Terrorisme
In het Regeerakkoord 2017 – 2021 heeft de regering het voornemen geuit om, voor wat betreft de grensoverschrijdende criminaliteit, verder te investeren in de samenwerkingsbanden binnen het Koninkrijk en met andere landen in de regio. Het is onduidelijk of en in welke mate dit voornemen is gekristalliseerd. In september 2005 werd de werkgroep Terroristisch Incident Response Plan (TIRP) opgericht, bestaande uit hoofden of vertegenwoordigers van verschillende organisaties, en met als doel de preventie en repressie van terroristische aanslagen op Curaçao. In 2006 is hieruit een plan voortgekomen, welke later in het jaar 2015 door de Directie Risicobeheersing en Rampenbestrijding (DRR) geüpdatet werd. Het feit dat het plan uitgaat van verschillende entiteiten die samen de bestrijding van het terrorisme ter hand nemen

duidt op een integraal plan, maar hoe het gesteld is met de samenwerking met het bedrijfsleven, de onderlinge ter beschikkingstelling van expertise, capaciteit, en bevoegdheden is niet duidelijk. Om te voorkomen dat terroristische aanslagen worden gepleegd, wordt door de VDC, Korps Politie Curaçao (KPC) en Kustwacht (KW) informatie verzameld en gedeeld. Dreigings- en risicoanalyses zijn door het Openbaar Ministerie (OM) en de veiligheidsdiensten in het Caraïbisch gebied opgesteld, maar de resultaten zijn niet gepubliceerd. Wel worden vanuit een centraal punt verschillende scenario's gezamenlijk geoefend ter voorbereiding op een ramp.

Alhoewel er geen indicaties van terroristische aanslagen zijn waarbij Curaçao op de ene of andere manier betrokken is, dient rekening te worden gehouden met mogelijke dreigingen, waaronder ook vanuit het Caraïbisch gebied zelf. Ter illustratie van deze mogelijke dreigingen moge dienen de terugkerende Foreign Terrorist Fighters (FTF-ers), de Amerikaanse aanwezigheid, de olieraffinaderij en mogelijke soft targets. De Raad is van mening dat het dreigingsniveau, evenals in Nederland, onderzocht, vastgesteld en bekend gemaakt dient te worden. Ook in de ketensamenwerking tussen de verschillende partners is transparantie geboden.

Bij de bestrijding van rampen of andere crises veroorzaakt door (dreiging van) terroristische acties complementeren de ministeries van Algemene Zaken (crisisbeheersing) en Justitie (handhaving openbare orde) elkaar, (onder andere) in de zin dat na een gepleegde terroristische aanslag de bestrijding van de ramp en het voorkomen van maatschappelijke onrust voor rekening komt van Algemene Zaken en de benodigde acties bij het handhaven van de rechtsorde en bij vervolgdreigingen voor rekening komen van Justitie. Ook kan het zijn dat de opschaling niet gelijktijdig geschiedt bij beide ministeries en dat de prioriteiten verschillen.[1]

Grensbewaking

Bij de grensbewaking wordt onderscheid gemaakt tussen de lucht- en maritieme grenzen. De KW is betrokken bij de bewaking van de maritieme grenzen en de Marechaussee bij de luchtgrenzen. Zowel bij de organisaties van de lucht- en maritieme grenzen is sprake van een bestaande samenwerking tussen de verschillende partners, zoals het KPC, Koninklijke Marechaussee, de KW, het OM en Curaçao Airport Partners. De burgers en het bedrijfsleven ervaren de onveiligheid het meest en kunnen vanuit hun optiek informatie verstrekken over onder andere de vorm, aard en gevolgen van de criminaliteit. Ze kunnen ook aanbevelingen doen. Hierbij zijn het bedrijfsleven en de burgerij niet voldoende betrokken. Anders dan bij cyber security en terrorisme zijn de betrokken partners wel actief bezig met het versterken van de grensbewaking.

Een goede grensbewaking is nodig om ervoor te zorgen dat illegale goederen en personen het land niet binnenkomen en dat legale personen en goederen op een vooropgezette manier het land binnenkomen of verlaten. Het feit dat Curaçao een

[1] Provincie Noord-Holland, Bestuurlijke aandachtspunten bij rampen veroorzaakt door terroristische aanslagen, januari 2006, pag. 7 e.v.

eiland is, maakt het moeilijk om illegale personen en goederen buiten te houden. In de praktijk vinden dan ook geregeld aanlandingen plaats waarbij illegale personen en goederen het land binnen komen. Vaak worden ook drugs en vuurwapens in beslag genomen, hetgeen erop duidt dat ook deze goederen op illegale wijze het land binnen komen.

Om de grenzen goed te kunnen bewaken is het, evenals bij cyber security en terrorisme, van belang om tijdig te beschikken over goede informatie en deze op de correcte wijze te analyseren en te delen. Ook hierbij is een intensieve samenwerking met de regio van groot belang.

De regering heeft een werkgroep Taskforce Ongedocumenteerden in het leven geroepen ten einde regelgeving vast te stellen over de wijze waarop met het fenomeen ongedocumenteerde vreemdelingen zal worden omgegaan.

In oktober 2019 werd de Advanced Passenger Information System (APIS) geïntroduceerd, waardoor autoriteiten van tevoren weten welke personen een ticket geboekt hebben om het land binnen te komen of om via dit land door te vliegen naar een andere bestemming.

Aangezien de grensbewaking van de landen binnen het Caraïbisch deel verschillend is ingericht, is de werkgroep “Grip op de grenzen” opgericht met als doel te komen tot een gezamenlijke standaard om grip te krijgen op de grenzen. Hiertoe is een werkgroep in het leven geroepen voor de luchtgrenzen en een andere werkgroep voor de maritieme grenzen. Voor beide grenzen heeft het JVO in 2019 de door deze werkgroepen aangeboden verbetervoorstellen vastgesteld en als mede een implementatieteam ingesteld om in het jaar 2020 te komen met aanbevelingen tot implementatie van deze baselines.

Veiligheidsrisico’s en incidenten

Om inzicht te verkrijgen in de mogelijke belemmeringen om tijdig de gestelde doelen te halen en hierop in te spelen, worden normaliter risicoanalyses gemaakt. Behoudens enige uitzonderingen zijn er geen risico- en dreigingsanalyses opgemaakt, waardoor het niet mogelijk is om inzicht te verkrijgen in de relevante feiten en omstandigheden. Uitzonderingen hierop vormen enige dreigings- en risicoanalyses die door het OM en VDC in samenwerking met de andere veiligheidsdiensten in het Caraïbisch gebied zijn uitgevoerd. De resultaten van deze analyses zijn echter niet bekendgemaakt. De veiligheidsrisico’s waarmee Curaçao kampt, zijn dus onbekend. Ook is niet bekend of en welke veiligheidsincidenten zich hebben voorgedaan. Er is immers bijvoorbeeld geen wettelijke registratieplicht voor eenieder die een cyberincident heeft meegemaakt.

Fysieke infrastructuur, capaciteit, kennis en middelen

Zoals hierboven aangegeven is er nog geen sprake van een (volledige) integrale aanpak van criminaliteit op de genoemde terreinen. Belangrijke partners, zoals de semioverheid, het bedrijfsleven en de burgerij, zijn niet of niet volledig betrokken bij deze aanpak. Of er voldoende capaciteit, kennis en middelen aanwezig zijn in de hele keten om op adequate wijze het (vastgestelde) veiligheidsbeleid uit te voeren, is niet duidelijk. Voor wat betreft de justitiële diensten verkeren de gebouwen in goede staat van onderhoud om andere fysieke infrastructuur zoals computers en andere digitale media te beheren. In deze gebouwen is beveiliging aanwezig, zodat niet iedereen rechtstreeks toegang heeft tot de ICT-infrastructuur. Een aandachtspunt blijft de bereikbaarheid van deze gebouwen. Met uitzondering van het onderkomen van de KW kan het publiek en dus ook een eventuele terrorist gemakkelijk bij de buitenmuren van het gebouw komen. Geen enkele organisatie heeft aangegeven over speciale software te beschikken om een cyberaanval tegen te gaan. Hierop vormen de beveiligde data middels de Stichting Beheer ICT Rechtshandhaving (SBIR) een uitzondering. Voor het “interne” internetverkeer zijn geen speciale maatregelen, zoals specifieke software, veiligheidsbewustzijn trainingen ingevoerd.

Conclusies

Cybersecurity

Naar aanleiding van de bevindingen en de analyse in de voorgaande hoofdstukken, komt de Raad tot de conclusie dat voor wat betreft cyber security er geen specifieke wet- en regelgeving en beleid bestaan. Er worden geen dreigings- en risicoanalyses uitgevoerd en er is geen centraal meldpunt aangewezen voor het melden van cyberincidenten, waardoor het veiligheidsniveau op het gebied van cyber security in Curaçao dan ook niet bepaald kan worden. Het risico van succesvolle cyberaanvallen is dan ook niet uit te sluiten. Het verhogen van de cyberveiligheid is noodzakelijk, gezien de desastreuze gevolgen die cyberaanvallen teweeg kunnen brengen voor de burgers, het bedrijfsleven, de overheid en de vitale infrastructuur. Met andere woorden, cyber security dient als prioriteit voor de veiligheid in het algemeen en voor de economie van het land in het bijzonder gezien te worden. Een ander risico voor een hoge graad van cyberveiligheid wordt gevormd door het gebrek aan integraal management met betrokkenheid van alle stakeholders. De infrastructuur hiertoe dient alsnog geschapen te worden.

Terrorisme

Ook voor wat betreft het terrorisme concludeert de Raad dat er geen sprake is van specifieke wet- en regelgeving en beleid. De veiligheidsdiensten en het OM verrichtten enige analyses, maar doordat de resultaten hiervan onbekend zijn, kan het veiligheidsniveau niet bepaald worden. De aanwezigheid van de verschillende Amerikaanse objecten en subjecten in Curaçao en de internationale vermenging van criminaliteit en terrorisme, maken dat Curaçao een mogelijk doelwit is voor terroristen.

Rekening dient te worden gehouden met het feit dat Curaçao ook als onderdeel van het Koninkrijk, waarvan Nederland met een substantieel dreigingsniveau deel uitmaakt, een aantrekkelijk doelwit vormt. De Raad kan tot geen andere conclusie komen dan dat het noodzakelijk is om de terrorismebestrijding naar een hoger prioriteitsniveau te tillen, waarbij de verhoging van de veiligheid begint bij de totstandkoming van wet- en regelgeving. Belangrijk is dat ook hier het wiel niet uitgevonden hoeft te worden. Er dient daarnaast geïnvesteerd te worden in de internationale samenwerking, aangezien terrorisme, evenals de cybercriminaliteit, geen grenzen kent.

Grensbewaking

Op het gebied van de grensbewaking is er een begin gemaakt om de samenwerking tussen de justitiële en niet-justitiële diensten te verbeteren. Naast de justitiële diensten zijn ook de Douane, de KW en de Koninklijke Marechaussee betrokken bij de grensbewaking. Er is ook een begin gemaakt met de integrale aanpak van de grensbewaking en het wachten is op de concretisering en vaststelling van het nieuwe beleid. De Raad juicht toe dat het JVO in 2019 een Baseline grensbewaking heeft vastgesteld en dat dit jaar nog voorstellen tot implementatie hiervan door het implementatieteam aan het JVO aangeboden zullen worden. Voor wat betreft het veiligheidsniveau zelf kan ook dat niet vastgesteld worden, aangezien geen dreigings- en risicoanalyses zijn gemaakt. Vaststaat dat met regelmaat vreemdelingen op zowel legale als illegale wijze het land binnenkomen en hier langer blijven dan hen toegestaan is. Ook na het opleggen van vreemdelingenbewaring of een meldplicht levert dit de nodige problemen op.

Conclusie

De conclusie van de Raad is dat het (externe) veiligheidsniveau voor wat betreft de dreigingen van cyber security en van terrorisme op Curaçao niet bepaald kan worden en dat de impact als gevolg van een succesvolle cyberaanval of een terroristische daad derhalve niet overzien kan worden. De vitale infrastructuur en daarmee ook de economie van het eiland kan hierdoor lamgelegd worden, zodat ook in de eerste levensbehoeften als water en elektriciteit niet kan worden voorzien.

Aanbevelingen

Aan de minister

- Draag op korte termijn zorg voor de totstandkoming van specifieke wet- en regelgeving en beleid op de terreinen cyber security, terrorisme en grensbewaking;

- Draag er zorg voor dat cyber security, terrorisme en grensbewaking officieel tot prioriteiten op niveau van nationale veiligheid worden verheven;
- Draag er zorg voor dat cyber security opgenomen wordt in het takenpakket van het Ministerie van Justitie en belast dit ministerie met de coördinatie van de terrorismebestrijding;
- Breng de CARICERT onder bij het Ministerie van Justitie en wijs deze aan als de CSIRT voor Curaçao en als het centraal meldpunt voor cyberincidenten;
- Draag er zorg voor dat periodiek dreigings- en risicoanalyses worden uitgevoerd op de terreinen van cyber security, terrorisme en grensbewaking;
- Draag zorg voor een centraal justitieel opleidingsplan in het kader van het integraal management omtrent cyber security, terrorisme en grensbewaking;
- Draag zorg voor integraal management omtrent cyber security, terrorisme en grensbewaking.

1. Inleiding

1.1 Aanleiding

Mensheid en criminaliteit gaan hand in hand of zoals Kamini Dashora het uitdrukt: "*Crime is a social and economic phenomenon and is as old as the human society. … Crime and criminality have been associated with man since his fall. Crime remains elusive and ever strives to hide itself in the face of development. … One thing is certain; it is that a nation with high incidence of crime cannot grow or develop*."[2]

Criminaliteit heeft altijd bestaan. Evenals de technologie ontwikkelt de criminaliteit zich ook gestaag en tegenwoordig zelfs mede dankzij de technologie. Wat voor de meeste mensen een kans op vooruitgang in leven en werken betekende, werd door een kleine groep omgezet in een dreiging voor de mensheid. Cyber crime, terrorisme en grensoverschrijdende criminaliteit zijn sprekende voorbeelden hiervan.

Voor een integrale aanpak van deze criminaliteit is het van belang dat de aard en omvang ervan inzichtelijk wordt gemaakt. Het is een feit van algemene bekendheid dat de criminaliteit steeds complexer wordt, aangezien criminelen zich steeds meer ontwikkelen en gebruik gaan maken van de techniek, ICT en het internet, waardoor de grenzen vervagen. Dat betekent dat ook medewerkers van de overheidsdiensten en private ondernemingen zich moeten mee ontwikkelen om ten minste gelijke pas te houden.

1.2 Doel

Het doel van dit inspectierapport is inzicht te verkrijgen in de integraliteit van de aanpak alsmede het veiligheidsbeleid in Curaçao voor wat betreft terrorisme, cybersecurity en grensbewaking en vast te stellen in hoeverre de justitiële kolom in staat is geweest uitvoering te geven aan het vastgestelde beleid.

1.3 Centrale vraag

De centrale vraag in dit inspectierapport luidt als volgt:

[2] Kamini Dashora, Cyber Crime in the Society: Problems and Preventions, in Journal of Alternative Perspectives in the Social Sciences (2011) Vol 3, No 1, pag. 240-242.

In hoeverre zijn de organisaties binnen de justitiële kolom in staat om uitvoering te geven aan het integraal veiligheidsbeleid voor wat betreft de terreinen grensbewaking, cybersecurity en terrorismebestrijding?

Deelvragen:

1. *Hoe is het integraal veiligheidsbeleid voor wat betreft bovengenoemde terreinen vormgegeven?*
2. *Welke zijn de veiligheidsrisico's en -incidenten en hoe worden die aangepakt door de organisaties binnen de justitiële kolom?*
3. *Wat is de stand van zaken omtrent de fysieke infrastructuur, capaciteit, kennis en middelen om op adequate wijze het veiligheidsbeleid op die terreinen uit te* voeren*?*

1.4 Toetsingskader

Het toetsingskader bestaat uit wet- en regelgeving en internationale normen.

1.5 Afbakening

Dit inspectierapport beperkt zich tot een onderzoek naar de integrale aanpak van de veiligheid op het gebied van cyber security, terrorisme en grensbewaking door de justitiële diensten gedurende de periode 2016 tot 2019.

1.6 Definitiebepaling

In het regeerakkoord van Curaçao over de periode 2017 – 2021 is aangegeven dat het nodig is om te investeren in de samenwerkingsbanden binnen het Koninkrijk en met andere landen in de regio. De Raad zal in dit rapport uitgaan van de door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) gehanteerde definitie voor terrorisme en cybersecurity.

"Terrorisme is het uit ideologische motieven plegen van op mensenlevens gericht geweld, dan wel het aanrichten van maatschappij-ontwrichtende zaakschade, met als

doel maatschappelijke ondermijning en destabilisatie te bewerkstelligen, de bevolking ernstige vrees aan te jagen of politieke besluitvorming te beïnvloeden."[3]

De NCTV definieert cybersecurity als volgt: "Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan."[4]

De Raad verstaat onder grensbewaking het bewaken van de grenzen met als doel slechts personen toe te laten die van rechtswege of middels een vergunning toegang tot het land Curaçao hebben gekregen.[5]

1.7 Fasering onderzoek

Ter oriëntatie op dit onderwerp werden literatuur, beleidsstukken en van de diensten ontvangen documentatie doorgenomen.

In de daaropvolgende fase werden interviews afgenomen van respondenten van het Openbaar Ministerie (OM), het Korps Politie Curaçao (KPC), het Ministerie van Justitie (MvJ), de Kustwacht (KW) en de Veiligheidsdienst Curaçao (VDC).

In de derde fase werd aan de hand van de verzamelde gegevens een concept-inspectierapport opgesteld. Dit rapport werd aan de betrokken diensten aangeboden ter becommentariëring. Na verwerking van de commentaren werd het rapport aan de Minister van Justitie aangeboden, die ook in de gelegenheid gesteld werd om het rapport van commentaar te voorzien. Hierna werd het rapport vastgesteld en aangeboden aan de minister.

1.8 Leeswijzer

In dit inleidende hoofdstuk komen de aanleiding, doelstelling, centrale vraag, de onderzoeksvragen en de afbakening aan bod. In hoofdstuk 2 worden de bevindingen van dit onderzoek gepresenteerd, gevolgd door een analyse van de bevindingen en gevolgd door enige aanbevelingen in hoofdstuk 4.

[3] Nationaal Coördinator Terrorismebestrijding en Veiligheid, Nationale Contraterrorisme strategie 2016 – 2020, pag. 6.
[4] Nationaal Coördinator Terrorismebestrijding en Veiligheid, De Nederlandse Veiligheidsagenda, Nederland digitaal veilig, pag.9.
[5] Artikel 1 en 2 Landsverordening Toelating en uitzetting.

2. Bevindingen

2.1 Aanleiding

Vooral de laatste jaren is het duidelijk geworden dat niet alleen de overheid voor de veiligheid in een land zorg kan dragen. Hiervoor dienen ook de burgers en bedrijven vanuit hun eigen optiek middels deelname aan door de overheid opgerichte werkgroepen een bijdrage aan het veiligheidsdenken te leveren. Dit is dan ook het doel van integrale veiligheid, namelijk dat de verschillende actoren samenwerken om tot een zo optimaal mogelijke veiligheid van allen te geraken.
In dit hoofdstuk wordt nagegaan in hoeverre de integrale aanpak van de veiligheid binnen de justitiële kolom ten aanzien van cybersecurity, grensbewaking en terrorisme is ingevoerd. Daar waar mogelijk wordt in het kort verwezen naar enige citaten teneinde te illustreren dat het wiel al uitgevonden is. Hierna wordt nagegaan in hoeverre wetgeving en beleid geïmplementeerd zijn voor wat betreft cybersecurity, terrorisme en grensbewaking.

2.1.1 Integrale aanpak

Het OM heeft besloten het voortouw te nemen in de opzet van een integrale aanpak van de criminaliteit, aangezien het besef gegroeid is dat een strafrechtelijke aanpak alleen niet toereikend is. Deze opzet gaat uit van de gedachte dat de aanpak van criminaliteit onderdeel moet zijn van een gezamenlijk gedragen strategie door verschillende partners binnen en buiten justitie. De regering is uiteindelijk verantwoordelijk voor de hierna te behandelen veiligheidsagenda en kan hierop ook aangesproken worden.[6]

Bij de integrale aanpak gaat het om publieke, semipublieke, private organisaties en de bevolking die, gebruikmakend van elkaars expertise, capaciteit, bevoegdheden en informatie, gemeenschappelijke doelen en ambities stellen en samenwerken om dezen te verwezenlijken. Het voordeel van de integrale aanpak is dat er veel meer mogelijkheden ontstaan om crimineel gedrag te voorkomen of te beperken door preventie, resocialisatie, nazorg en het bij betrekken van sociaal-maatschappelijke partners. In het geval het crimineel gedrag al heeft plaatsgevonden dient hierop een

[6] Ministerie van Justitie, Openbaar Ministerie en Korps Politie Curaçao, Veiligheidsagenda Curaçao 2016 - 2018, pag. 2

passende reactie te volgen, zoals het afpakken van crimineel vermogen, bestuurlijke handhaving en het opwerpen van bestuursrechtelijke barrières, de inzet van multidisciplinaire teams en alternatieve afdoeningsmodaliteiten.[7] Deze aanpak vergt een constante monitoring en betrokkenheid en het elkaar aanspreken op elkaars taken en verantwoordelijkheden. Bij de informatie-uitwisseling in het kader van de integrale aanpak komt niet naar voren of en in welke mate in Curaçao de uitwisseling van persoonsgegevens wettelijk een belemmering vormt.[8] Duidelijk moet worden welke persoonsgegevens wel gedeeld kunnen worden en onder welke voorwaarden. Aangezien de uitwisseling van informatie een belangrijk onderdeel is van de integrale aanpak bij de criminaliteitsbestrijding, dient het niet kunnen uitwisselen van persoonsgegevens geen reden te zijn tot het niet optreden.[9]

2.1.2 Veiligheidsagenda

Om het hoofd te bieden aan de stijgende zware en ondermijnende vormen van criminaliteit en teneinde deze fors te verlagen middels een integrale aanpak heeft de regering een veiligheidsagenda doen opstellen. De “Veiligheidsagenda Curaçao 2016 – 2020” (hierna: Veiligheidsagenda) beoogt een antwoord te geven op de vraag hoe het onveiligheidsgevoel binnen de gemeenschap zoveel mogelijk weggenomen kan worden.

In de Veiligheidsagenda wordt geconstateerd dat bij de bestrijding van criminaliteit te veel de nadruk ligt op de strafrechtelijke aanpak en te weinig op een integrale aanpak. De pakkans voor de criminelen is klein en zelfs bij eventuele aanhoudingen en bestraffingen, zijn criminelen korte tijd daarna weer actief in de misdaad, onder andere als gevolg van de heersende werkloosheid.

Volgens het OM zijn de landen qua infrastructuur en instituties op dit moment nog onvoldoende in staat om op afdoende wijze aan de criminaliteit het hoofd te bieden.[10] Het OM, het Ministerie van Justitie (MvJ) en het KPC hebben in het jaar 2016 besloten een op een integrale aanpak gebaseerde veiligheidsstrategie op te stellen, waarbij door een gerichte integrale samenwerking en informatiedeling tussen de overheid, de

[7] Openbaar Ministerie, Parket Procureur-Generaal Curaçao, Sint Maarten, Bonaire, Sint Eustatius & Saba, Perspectief op de criminaliteitsbestrijding 2016 – 2021, pagina 3 e.v.
[8] Zie ook De rol van gemeenten in de bestuurlijke en integrale aanpak van ondermijning, Voorlichting van de Afdeling advisering van de Raad van State van 20 maart 2019, pag. 30.
[9] Idem, pag. 57.
[10] Openbaar Ministerie, Parket Procureur-Generaal Curaçao, Sint Maarten, Bonaire, Sint Eustatius & Saba, Perspectief op de criminaliteitsbestrijding 2016 – 2021, pagina 2.

burger en het bedrijfsleven meer en betere resultaten bereikt kunnen worden. Binnen de strafrechtsketen berust de regie bij het MvJ.

Het doel van de veiligheidsagenda is het verbeteren van de veiligheidssituatie in Curaçao middels het uitwerken en in onderlinge samenhang realiseren van een groot aantal beleidsinitiatieven en maatregelen rondom vijf prioritaire thema's die door de gezagsdriehoek in Curaçao vastgesteld zijn.[11] Per maatregel of set aan maatregelen wordt een ministerie aangewezen, dat in overleg met andere relevante ministeries verantwoordelijk is voor de integrale uitwerking van de maatregelen.

Om na te gaan welke de grootste oorzaken zijn van de onveiligheid in de gemeenschap, hebben de betrokken diensten een analyse gemaakt die het volgende resultaat heeft opgeleverd:

- geringe effectiviteit in het optreden van de betrokken instanties als gevolg van een onwenselijke versnippering van mensen en middelen;
- ambtenaren krijgen in hun taakuitoefening te maken met agressie, afpersing, represaille en geweld, terwijl aan de andere kant in sommige gevallen de integriteit te wensen overlaat;
- weinig zichtbare aanwezigheid van bij veiligheid direct betrokken instanties en andere betrokkenen in de publieke ruimte, en
- de rechtshandhavingsketen heeft een kwalitatieve impuls nodig terwijl ook de ketensamenwerking beter moet.

2.2 Cyber security

2.2.1 Inleiding

Informatie en Communicatie Technologie (ICT) is tegenwoordig niet meer weg te denken. Bijna alle objecten zijn verbonden met het Internet en kunnen vaak op de een of andere manier met elkaar communiceren. ICT wordt in alle kringen gebruikt en speelt aldus een belangrijke positieve rol binnen de overheid en in het private domein. Dezelfde ICT kan door oneigenlijk gebruik grote schade teweegbrengen bij personen,

[11] Zie ook Strategiedocument OM-KPC 2016, pag. 1.

bedrijven en overheden. Met oneigenlijk gebruik wordt bedoeld, gebruik door hackers, terroristen en criminelen met het oogmerk om grote schade aan de economie, het dagelijks leven en het functioneren van de overheid toe te brengen.

Over de hele wereld neemt de cyberdreiging toe. Het is bekend dat terroristische netwerken gretig gebruik maken van ICT om nieuwe leden te werven en geld in te zamelen voor hun acties. De praktijk heeft geleerd dat verschillende landen in de laatste decennia slachtoffer zijn geworden van hackers die netwerken in die landen hebben lamgelegd. In oktober 2019 is het hackers gelukt het netwerk van de overheid binnen te dringen en heeft de geplaatste ransomware de bestanden van enkele afdelingen – ongeveer 100 gebruikers - van het ministerie van Bestuur, Planning en Dienstverlening door encryptie ontoegankelijk gemaakt. De overheid van Curaçao heeft geweigerd het losgeld te betalen en heeft ervoor gekozen zelf de bestanden weer op te bouwen. In bijvoorbeeld het jaar 2018 werd het netwerk van de overheid van Sint Maarten gedurende enkele dagen volledig lamgelegd. Het is zaak voor de nodige veiligheid zorg te dragen, zodat onbevoegden de netwerken van de overheid, personen en organisaties niet ongemerkt kunnen binnendringen.

2.2.2 Wet- en regelgeving

Omtrent het belang van specifieke wet- en regelgeving op het terrein van cyber security in de justitiële kolom, wordt op pagina 19 van het “2016 Cybersecurity Report, Cybersecurity, Are we ready in Latin America and the Caribbean?” het volgende gesteld:

“Effective criminal justice is an essential part of a cybersecurity strategy. This involves the investigation, prosecution and adjudication of offences against and by means of computer systems and data, as well as the securing of electronic evidence in relation to any crime for the purposes of criminal proceedings. The transnational nature of cybercrime and, in particular, of volatile electronic evidence means that criminal justice cannot be effective without efficient international cooperation.

Comprehensive legislation covering both substantive law (conduct to be defined as a criminal offence) and procedural law (investigative powers for law enforcement) is the foundation of a criminal justice response".[12]

Adequate wet- en regelgeving is van immens belang voor de bestrijding van criminaliteit.

Een van de overwegingen in de Preambule bij het Verdrag van Boedapest van 23 november 2011 (Budapest Convention) geeft aan dat de samenleving beschermd dient te worden tegen strafbare feiten verbonden met elektronische netwerken onder andere door het invoeren van passende wetgeving en het bevorderen van internationale samenwerking. Dit verdrag is door het Koninkrijk getekend op 23 november 2001, geratificeerd op 16 november 2006 en in werking getreden op 01 maart 2007.[13]

In de Budapest Convention is een basis gelegd voor wet- en regelgeving die door alle aangesloten landen gebruikt kunnen worden.[14] Deze basis is door de meeste landen ter wereld gebruikt om hun cybersecurity wet- en regelgeving op orde te stellen.[15]

Nederland beschikt over specifieke cybersecurity wet- en regelgeving, onder andere de "Wet beveiliging netwerk- en informatiesystemen" die op 01 januari 2019 in werking is getreden, met als doel de vergroting van de cyberweerbaarheid van Nederland, de introductie van een meldplicht voor essentiële internetaanbieders en hun verplichting om alle veiligheidsmaatregelen te nemen ten einde de kans en gevolgen op en van een succesvolle cyberaanval te beperken.

Bepalingen omtrent cybersecurity zijn in verschillende regelingen opgenomen, onder andere het Wetboek van Strafrecht, de landsverordening Auteursrecht en de Landsverordening bescherming persoonsgegevens.

Respondenten van de verschillende organisaties in de justitieketen alsmede de Caribbean Cyber Emergency Response Team (CARICERT) hebben aangegeven niet op de hoogte te zijn van specifieke wet- en regelgeving betreffende de cyber security

[12] Alexander Seger (CoE | Council of Europe), The State of Cybercrime Legislation in Latin America and the Caribbean – A Few Observations, pag. 19 in Cyber security, Are we ready in Latin America and the Caribbean, 2016 Cybersecurity Report.
[13] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.
[14] Convention on Cybercrime, Budapest, 23 November 2001.
[15] European Commission, COM (2015) 185, The European Agenda on Security, Pag. 20.

in Curaçao. Het Bureau Telecommunicatie concipieert cybersecuritywetgeving voor de telecommunicatiesector. Alhoewel Bureau Telecommunicatie en Post sinds de oprichting van de CARICERT in 2012 optreedt als de sponsor van de CARICERT, is deze organisatie toch niet zo bekend bij de justitiële overheidsdiensten.

2.2.3 Beleid

Middels beleid wordt de richting waar een organisatie naar toe wil en welke de middelen zijn die de organisatie nodig heeft om de gestelde organisatiedoelen te bereiken, weergegeven. Voor cyber security betekent dit dat beleid uitgestippeld dient te worden om Curaçao weerbaarder te maken tegen risico's en dreigingen. In dit beleid dient minimaal vastgelegd te worden welke maatregelen moeten worden getroffen om cyberincidenten te voorkomen en tegen te gaan.

In het regeerakkoord van Curaçao over de periode 2017 – 2021 wordt gesteld dat de kwetsbaarheid van organisaties in onze gemeenschap ten aanzien van cybercrime een punt van zorg is. "Wij bevinden ons in een toestand waarbij de veiligheid in onze gemeenschap niet op het gewenste niveau is."[16] Het beleid zal er een zijn van zerotolerantie, waarbij gerichte acties ondernomen zullen worden tegen o.a. cyber crime. Ook heeft de regering het voornemen geuit om te investeren in de samenwerkingsbanden binnen het Koninkrijk en met andere landen in de regio. De overheid behoort ten minste een coördinerende rol te spelen bij de bescherming van de bevolking tegen inbreuken op het gebied van cybersecurity. In zijn brief aan de Tweede Kamer onderschrijft de Nederlandse Minister van Veiligheid en Justitie de belangrijke rol die de overheid speelt, waarbij de overheid voorzorgsmaatregelen moet nemen indien er bijvoorbeeld risico's bestaan dat de nationale veiligheid in het gedrang komt.[17]

Curaçao beschikt over een eigen CARICERT, maar deze organisatie is niet bij alle justitiële diensten bekend. De Directie Risicobeheersing & Rampenbeleid (DRR) heeft een risicoprofiel laten opstellen door het Lectoraat Crisisbeheersing van het Instituut Fysieke Veiligheid uit Nederland. Hiertoe werden de risico's ingedeeld in zes

[16] Regeerakkoord 2017 – 2021, pag. 37
[17] Minister van Justitie en Veiligheid, Brief aan de voorzitter van de Tweede Kamer van 16 juli 2019 met referentienummer 2019Z05647/2019D15161.

deelgebieden. Deze inventarisatie werd afgesloten met een risicoduiding ter voorbereiding op de risicoanalyse.

De VDC beschikt niet over een eigen eenheid die specifiek belast is met cyber security en maakt ook geen deel uit van een samenwerkingsverband dat zich bezighoudt met dit onderwerp. Wel is de VDC op de hoogte van het bestaan van de CARICERT.

Volgens een respondent komt het OM pas aan zet, indien er sprake is van cyber criminaliteit, dus pas in de fase van opsporing en vervolging. Indien nodig kan het OM aan de voorkant adviseren. Bedrijven en overheidsinstanties moeten volgens het OM het voortouw nemen ter voorkoming van cyber criminaliteit. Het vervolgen van mensen heeft geen enkele zin als het systeem zo lek is als een mandje. Wat het OM betreft is vervolging niet de prioriteit aangezien de oplossing van cyber security in de security zit en niet in de repressie.

Volgens de respondent van het MvJ heeft de regering nog geen visie ontwikkeld op het gebied van cyber security. Volgens deze respondent is het Ministerie van Bestuur, Planning en Dienstverlening (BPD) van mening dat dit ministerie belast moet zijn met de taak van beveiliging van het overheidsnetwerk terwijl het Ministerie van Justitie de mening toegedaan is dat deze taak aan dit ministerie toebedeeld is.

De KW is ingebed in een militaire omgeving en leunt op het defensiesysteem MULAN aangaande cybersecurity. De KW maakt gebruik van ACTPOL, een borgingssysteem dat gebruikt wordt voor het invoeren van mutaties. De KW heeft geen samenwerkingsverbanden ten aanzien van cyber security. De KW onderhoudt evenmin contacten met de CARICERT.

Alle computers die bij de KW in gebruik zijn, worden beveiligd door MULAN. Het gevolg is dat de leden van de KW niet zomaar op internet kunnen, maar het voordeel is dat het systeem beveiligd is waardoor het risico op oneigenlijk gebruik drastisch afneemt. De KW is onderdeel van het cyber domein van Defensie. Als er sprake is van een cyberaanval of bijvoorbeeld phishing, dan wordt de KW gewaarschuwd.

Er zijn ruimtes waar telefoons, digitale horloges en andere gegevensdragers niet toegestaan zijn. Er is geen controlemechanisme, maar het is een standaardprocedure, dat iedereen die een briefing meemaakt, geen gegevensdragers bij zich mag hebben.

Het uitgangspunt is dat alle personen die voor een briefing worden uitgenodigd, bekenden en professionals zijn, die zich ook hieraan houden.

Voor het KPC komt cyber security niet hoog voor op de prioriteitenlijst. De prioriteiten liggen meer op de terreinen die van invloed zijn op de leefbaarheid van de gemeenschap. Deze prioriteiten zijn gericht op de vijf punten die al eerder genoemd zijn, atrako's, inbraken en diefstal, verkeersveiligheid, geweldsmisdrijven en criminele samenwerkingsverbanden.

Volgens de respondenten van het KPC maakt het KPC geen deel uit van werkgroepen of andere samenwerkingsvormen die aandacht besteden aan cyber security. Het KPC heeft wel regelmatig contact en overlegt met bankverenigingen die aandacht besteden aan cyber security.

Voor het KPC is cyber security vooralsnog een niet ontgonnen gebied. Samen met het RST kijkt het KPC uit naar bepaalde vormen van cyber crimes, bijvoorbeeld kinderporno, maar de bestrijding van cybercrime wordt niet als prioriteit beschouwd.

In het kader van de beveiliging van de eigen systemen, heeft het KPC voorzorgsmaatregelen getroffen, zoals bijvoorbeeld firewalls, voor het geval bijvoorbeeld hackers in zijn systemen proberen binnen te dringen. Het KPC onderhoudt weinig contacten met andere netwerken ter voorkoming dat via deze netwerken de eigen systemen binnengedrongen kunnen worden.

Voor de justitiële keten biedt de Stichting Beheer ICT Rechtshandhaving (SBIR) bescherming tegen inbreuken op de cyberveiligheid van de informatievoorziening binnen de rechtshandhavingsdiensten.

Deze stichting is verantwoordelijk voor de veiligheid en die wordt jaarlijks geauditeerd door FOX IT[18]. De Stichting SBIR zorgt voor het nodige digitale onderhoud en voor de voortgang van bepaalde trajecten. Hierdoor wordt voorkomen dat door budgettekorten noodzakelijke investeringen achterwege blijven. Daarom hebben de landen binnen het Koninkrijk in het Caraïbisch gebied de handen ineengeslagen en deze stichting belast met de beveiliging van de informatie-uitwisseling tussen de organisaties binnen deze landen. Deze landen dienen allemaal bij te dragen in de kosten.

[18] SBIR werd op 26 maart 2015 opgericht onder de naam Stichting Beheer ICT Rechtshandhaving.

2.3 Terrorisme

2.3.1 Inleiding

Het beschermen van de bevolking tegen daden van terreur is onder meer een overheidstaak. Daarnaast moeten personen en bedrijven zorgdragen voor de eigen veiligheid en de veiligheid van hun bedrijven. Vanaf het begin van het jaar 2018 zijn meer dan 200 personen afkomstig uit het Caraïbisch gebied afgereisd naar Syrië en Irak en deze personen vormen na hun terugkeer door middel van de door hen in het buitenland opgedane ervaring als terrorist voor het thuisfront en andere landen een bedreiging.[19] [20]

Elk land dient zich voor zover mogelijk in te spannen om terroristische daden tegen de mensheid en kritieke infrastructuur te voorkomen (preventie), zich daarop voor te bereiden (voorbereiding), voor zover nodig daarop te reageren (bescherming) en de daders op te pakken en voor het gerecht te brengen (vervolgen). Hiertoe dient de wet- en regelgeving en beleid periodiek aangepast en vastgesteld te worden en de implementatie dient goed te verlopen. Ook dienen de risico's in kaart te worden gebracht.

2.3.2 Wetgeving

Op internationaal gebied legt de "2005 Warsaw Convention on the Prevention of terrorism" de landen de verplichting op om maatregelen te treffen ter voorkoming van terrorisme en het nodige te doen om de negatieve effecten van terroristische aanslagen zoveel mogelijk te beperken. Wet- en regelgeving spelen hierbij een belangrijke rol, zoals ook blijkt uit de "Additional Protocol to the Convention on the prevention of terrorism" die de aangesloten landen verplichten om bijvoorbeeld bepaalde aspecten van het terrorisme strafbaar te stellen.
In Curaçao stelt het Wetboek van Strafrecht terrorisme en terrorismefinanciering strafbaar. De respondenten hebben aangegeven niet op de hoogte te zijn van het bestaan van specifieke wet- en regelgeving op het terrein van het terrorisme.

[19] CARICOM counter-terrorism strategy, pag 5, 6
[20] Gov.UK, https://www.gov.uk/foreign-travel-advice/trinidad-and-tobago/terrorism, laatstelijk gedownload op 27 augustus 2020, pag 1.

2.3.3 Beleid

Om terrorisme effectief te kunnen bestrijden, dient de overheid beleid uit te stippelen. Eerst dient een dreigings- en risicoanalyse te worden uitgevoerd. Verschillende landen onderhouden een eigen beleidssysteem. In de Verenigde Staten zijn onder anderen de “prevention, preparedness en strong partnerships” belangrijke onderdelen van het beleid.[21] In Europa wordt sinds 2018 een driedeling gebruikt, bestaande uit “prevention, prosecution en protection”.[22]

In het jaar 2001 hebben de landen van het Koninkrijk de wens tot “intensivering van samenwerking tussen de landen ter bestrijding van het internationale terrorisme, in het belang van de internationale rechtsorde en de veiligheid van hun bevolkingen” al eens uitgesproken.[23] Als instrument hiertoe werd door het Eilandgebied Curaçao op 05 februari 2007 de oprichting van de werkgroep Terroristisch Incident Respons Plan (TIRP) vastgesteld. Deze werkgroep bestaat uit hoofden of vertegenwoordigers van 15 verschillende instanties. Deze werkgroep werd in september 2005 opgericht en heeft tot doel de preventie en repressie van eventuele terroristische aanslagen. Het multidisciplinair plan zelf dateert van 29 mei 2006.

In het Regeerakkoord 2017 – 2021 wordt terrorisme één keer vermeld. Het voornemen van de overheid is om in het kader van de bestrijding van de grensoverschrijdende criminaliteit, waaronder witwassen, mensenhandel, drugstransport en terrorisme, in deze regeerperiode verder te investeren in de samenwerkingsbanden binnen het Koninkrijk en met andere landen in de regio. De regering heeft nog niet bekend gemaakt op welke wijze dit beleidsvoornemen geconcretiseerd zal worden.

Uit gesprekken met respondenten zijn verder van overheidswege geen plannen of maatregelen ter voorkoming, repressie en nazorg van terrorisme gebleken. In ieder geval is bij hen niet bekend dat er een contra-terrorisme strategie bestaat, waarin bijvoorbeeld aangegeven wordt wat onder vitale infrastructuur valt en wat er gedaan wordt aan de bescherming van deze vitale infrastructuur en de bevolking.

[21] National Strategy for Counterterrorism of the United States of America, October 2018, pag. Ii.
[22] Committee of Ministers, Council of Europe Counter-Terrorism Strategy, CM (2018)86-addfinal, 4 July 2018.
[23] Zie Eilandsbesluit van 5 februari 2007.

2.3.4 Preventie

Bij het voorkomen van aanslagen spelen de informatievergaring, informatieverzameling en informatiedeling een grote rol. Uitermate belangrijk is om te weten welke terroristen zich in de regio bevinden en of aanslagen in voorbereiding zijn en welke objecten doelwit vormen. “Information and intelligence sharing concerning the identity of FTF’s, returnees, relocators and known terrorist supporters, will remain fundamental.”[24]

Op Curaçao zijn officieel de VDC en de politiekorpsen met de informatievergaring belast. De rol van de VDC bij terrorismebestrijding is het vergaren van inlichtingen en deze via de TCI-officier ter beschikking van de ketenpartners te stellen. De VDC beschikt vaak over vertrouwelijke informatie die niet kan worden onthuld. Volgens de respondent van de VDC maakt de VDC geen deel uit van een internationaal samenwerkingsverband, maar maakt de VDC wel deel uit van het niet geformaliseerde Team Caraïbisch gebied, een samenwerkingsverband tussen de Algemene Inlichtingen en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen en Veiligheidsdienst (MIVD).

Terrorismebestrijding is een prioriteit voor de KW.[25] De rol van de KW hierbij is gelegen in het opbouwen van een informatiepositie met als doel zoveel mogelijk informatie te delen binnen de justitiële keten. Hierbij gaat het om uit internationale kringen verkregen informatie over bepaalde individuen en organisaties omtrent een mogelijke terroristische dreiging of een terroristische actie. Deze informatie wordt gedeeld met de andere partners.

De KW speelt ook een rol bij de voorkoming van aanslagen op of via de zee. Indien er in het maritieme domein sprake is van een terroristische dreiging en bij de dreiging een schip betrokken is, dan wordt het schip gedetecteerd en geïntercepteerd. Ook beschikt de KW over een Joint Rescue Coordination Centre als onderdeel van de communicatieketen. Dit centrum coördineert de inzet van de diensten.

Informatiedeling vindt vaak bilateraal plaats tussen de diensten, maar de informatiedeling tussen alle betrokken organisaties vindt plaats in het Intelligence

[24] CARICOM, CARICOM Counter-Terrorism Strategy, pag. 15, punt 42.
[25] Kustwacht voor het Koninkrijk der Nederlanden in het Caribisch Gebied, Jaarverslag 2018, pagina 6.

Center Curaçao (ICC). Hierin hebben het RST, de KMAR, de KW, de Douane, de Belastingdienst, de VDC en het KPC zitting. De KW investeert in zichzelf, maar ook in de samenwerking met de ketenpartners. Als er sprake is van een volledig informatiebeeld, is de kans groter dat er ingegrepen kan worden voordat er een terroristische daad plaatsvindt.

Het KPC participeert in het ICC. De verkregen informatie wordt geanalyseerd en omgezet in projectvoorstellen. Dit gebeurt niet alleen in het kader van de opsporing, maar ook in het kader van de handhaving alsmede op het bestuurlijke vlak.

2.3.5 Voorbereiding

De justitiële diensten die deel uitmaken van de TIRP zijn de VDC, de KW, het KPC, het OM, de KMAR, de Toelatingsorganisatie en het Interpol. Doorgaans neemt ook een vertegenwoordiger van het Amerikaans Consulaat deel aan de vergaderingen. Dit samenwerkingsverband komt op afroep samen en heeft een plan opgesteld dat uitgevoerd moet worden in het geval zich op Curaçao een terroristische actie voordoet. De laatste versie van dit plan dateert uit het jaar 2015. Deze in het gelijknamige eilandsbesluit genoemde organisaties hebben zich over het fenomeen terrorisme gebogen en hieruit is het Terrorisme Incident Respons Plan voortgekomen. In dit plan is opgenomen hoe de coördinatie en communicatie plaats dient te vinden in het geval terroristen hier te lande een terroristische daad zouden plegen en welke acties de betrokken diensten dan moeten ondernemen. Tevens beschrijft het plan een aantal rampenscenario's die zich kunnen voordoen. In de praktijk worden onverwachts oefeningen gehouden, waarbij een bepaalde situatie die verband houdt met terrorisme gesimuleerd wordt. Laatstelijk werd bijvoorbeeld onder leiding van de directeur van de D.R.R. een desktopoefening gehouden. Er zijn 34 verschillende scenario's en het is de bedoeling dat de diensten voor elk scenario hun plannen opstellen, zodat in het geval van een terroristische daad de plannen gereed zijn en reeds eerder beoefend werden. De TIRP zal worden geactiveerd zodra er informatie voorhanden is dat een terroristische dreiging eminent is of wanneer een daad van terrorisme heeft plaatsgevonden. Thans komt deze groep niet zo vaak samen, omdat er geen indicaties zijn van een terroristische dreiging, aldus een respondent.

2.3.6 Bescherming

Indien een terroristische daad op zee plaatsvindt, dan verricht de KW een onderzoek om de toedracht vast te stellen. De bedoeling is om de veiligheid na het incident te borgen door onder andere het veiligstellen van het plaats delict. Via het College van Korpschefs onderhoudt het KPC een goede band met de Dienst Speciale Interventie (DSI) uit Nederland. Recentelijk is begonnen met het verzorgen van trainingen in het kader van de Staf Grootschalig en Bijzonder Optreden (SGBO). Deze trainingen komen ook van pas in gevallen van terrorisme. Zodanig beschikt het KPC over een staf, getraind op verschillende gebieden, die in geval van terrorisme in samenwerking met andere partners, voor respons kan zorgdragen. Ook is het KPC in samenwerking met DSI en de Commandant der Zeemacht in het Caraïbisch gebied bezig met de vorming van een Quick Response Team. Dit team bestaat in eerste instantie uit het Arrestatieteam van het KPC, maar gezien de mogelijke vergaande gevolgen is het nodig om ook ervoor te zorgen dat er een voorziening bestaat, waaraan naast het KPC ook de Marine en andere organisaties deelnemen.

2.3.7 Vervolging

Als er activiteiten door personen of groeperingen plaatsvinden die terrorisme faciliteren of veroorzaken of indien financiële instellingen gebruikt worden om in Europa of Amerika terrorisme te financieren, is dit strafrechtelijk relevant voor het OM. Het voorgaande zou aanleiding kunnen zijn om vervolging in te stellen.

Bij de vervolging van terroristen beoordeelt het OM de juridische aspecten op basis van de wetgeving. Hiertoe beschikt het OM over een officier die zich gespecialiseerd heeft in terrorisme en terrorismebestrijding.

2.4 Grensbewaking

2.4.1 Inleiding

Een van de middelen om onder andere terrorisme te bestrijden, is het bewaken van de grenzen in de landen tegen ongeautoriseerde toegang door ongewenste personen. Bij grensbewaking wordt onderscheid gemaakt tussen lucht- en maritieme grenzen. Een land dat niet investeert in een goede grensbewaking, maakt zichzelf kwetsbaar voor ongewenste gevolgen voor de bevolking en de economie van het land. “*Today*

extremist organisations utilise modern information and communication technologies (ICTs) as well as globalised trade and travel to extend their reach far beyond their points of origin. As a result, no part of the world is immune from this scourge. Even if not an actual target for terrorist attacks, a country may be the source of terrorists and or terrorist sympathisers who prepare for, provide assistance to, or travel to another country for the purpose of committing a terrorist act."[26] Ook om deze redenen is het van belang om over een goede grensbewaking te beschikken om onder andere illegale goederen, terroristen en illegale personen tijdig te detecteren, hen de toegang te weigeren en of te verwijderen om te voorkomen dat strafbare feiten gepleegd worden die nadelige gevolgen kunnen hebben voor de bevolking en de economie.

Ook voor de invoer en uitvoer van legale goederen is een goede grensbewaking onontbeerlijk. "Improved port control techniques in the region will not only serve to interdict illicit drug trafficking and other contraband, but also act to facilitate licit traffic and so enhance the region's economies." [27] Hoe moeilijk het is om de grenzen van een eiland goed af te sluiten, blijkt wel uit de stroom buitenlanders, drugs en vuurwapens die via snelle boten de kusten bereiken. Vele illegalen worden (later) opgepakt, maar anderen lukt het wel om ongezien hier aan land te komen, te verblijven en te werken.

De grensbewaking wordt uitgevoerd door het KPC en de Koninklijke Marechaussee voor wat betreft de luchtgrenzen en door de KW voor wat betreft de maritieme grenzen, beiden in samenwerking met de Douane.

CARICOM-landen erkennen dat hun grensbewaking niet op het vereiste peil is om de grensoverschrijdende criminaliteit tegen te gaan.[28] Door de Caribbean Basin Security Initiative worden de CARICOM-landen vanuit geopolitiek standpunt gezien als de "derde grens" van de Verenigde Staten, na de landgrenzen van de VS met Canada en Mexico. In de regio wordt het belang van een goede grensbewaking ingezien en zijn de versterking van de grensbewaking en de hiermee verband houdende informatievergaring en –deling zelfs tot strategische doelen verheven.

[26] CARICOM, Counter Terrorism Strategy, pag. 1.
[27] UNODC Regional Programme (2014 – 2016), In support of the CARICOM Crime and Security Strategy | Preventing and Countering Illicit Trafficking and Organized Crime for Improved Governance, Justice and Security, Pag. 29
[28] CARICOM Counter terrorism Strategy, pag. 5 e.v.

2.4.2 Wet- en regelgeving

De Landsverordening Toelating en Uitzetting en het Toelatingsbesluit regelen de toelating van personen tot Curaçao. Het Wetboek van Strafrecht regelt de strafbaarstelling van feiten die verband houden met grensoverschrijdende criminaliteit. De respondenten geven aan dat de justitiële diensten thans bezig zijn met het uitwerken van een nieuwe integrale werkwijze op het gebied van grensbewaking. De bedoeling is dat na afronding hiervan eventueel relevante wet- en regelgeving, beleid en procedures opgesteld en/of geüpdatet zullen worden. Nadat in 2019 de verbetervoorstellen door het JVO werden vastgesteld, kreeg een implementatieteam de opdracht om een implementatieplan op te stellen en het plan in 2020 aan het JVO aan te bieden.

2.4.3 Beleid

Twee werkgroepen, de Taskforce Ongedocumenteerden en de Taskforce Grip op de Grenzen, waren ten tijde van het onderzoek bezig met het uitwerken van plannen om grip te krijgen op de grenzen. Na het aanbieden van de resultaten aan het JVO, is het de bedoeling dat de verdere instructies van de ministers van justitie van de vier landen zullen worden uitgewerkt en uitgevoerd. Ook de kostenverdeling tussen de landen maakt deel uit van het implementatieplan. In het jaar 2017 kreeg de samenwerking met de Douane en de KW een extra dimensie met de instelling van een taskforce door de Minister van Justitie met als doel alle middelen in te zetten in de strijd tegen de wapen- en drugshandel en de grote stroom ongedocumenteerde vreemdelingen. Bezien vanuit zijn taken en prioriteiten heeft de KW een belangrijk aandeel in de grensbewaking.

2.4.4 Taskforce Ongedocumenteerden

De Taskforce ongedocumenteerden (TFO), is een ministeriële werkgroep die zich bezighoudt met regelgeving voor wat betreft ongedocumenteerden. De leden van deze werkgroep zijn de DRR, KPC, Douane, Interpol, DBB, KMAR, KW, de Secretaris Generaal van het ministerie van Algemene Zaken en de Secretaris Generaal van het MvJ, MEO en GMN. De TFO vergadert vaak in kleine groepjes, waarvan de samenstelling afhankelijk is van het onderwerp van bespreking.

Om te weten welke personen het land binnenkomen, heeft de Minister van Justitie een protocol getekend met de CARICOM om gebruik te maken van de Advanced Passenger Information System (APIS). Via dit systeem kunnen ongewenste vreemdelingen, zoals onder andere FTF-ers, de toegang worden geweigerd op het moment dat zij nog in het vertrekland verkeren.[29]

2.4.5 Grip op de Grenzen

Conform het jaarverslag 2018 van de KW voor het Koninkrijk der Nederlanden is de KW vanuit haar taakstelling betrokken bij het verstevigen van grip op de maritieme grenzen. Het Justitieel Beleidsplan speelt hierop in. In het Justitieel Beleidsplan 2018-2021 zijn vier beleidsspeerpunten benoemd als basis voor de taakstellingen van de KW. Deze vier beleidsspeerpunten zijn een uitvloeisel van het Poortwachtproject oftewel 'grip op grenzen', waarbij de betrokken diensten, zowel op regionaal als internationaal gebied, samenwerken om de Koninkrijksgrenzen te versterken.
De vier beleidsspeerpunten als basis voor de taakstelling van de Kustwacht zijn de bestrijding van:

1. Transport van verdovende middelen en strategische goederen;
2. Mensensmokkel en mensenhandel;
3. Vervoer van en handel in illegale vuurwapens;
4. Terrorisme[30]

Op initiatief van het Justitieel Vierlanden Overleg is de werkgroep "Grip op de grenzen" opgericht. De aanleiding hiertoe was dat binnen de landen van het Koninkrijk verschillende standaarden van grensbewaking aangehouden werden. De wens was om tot een gezamenlijke standaard van grensbewaking voor het Caraïbisch deel van het Koninkrijk te komen, met als resultaat een baseline van minimale processen om grip op de grenzen te kunnen hebben. Deze opdracht werd gegeven aan het College van korpschefs. Op Curaçao zijn twee werkgroepen opgericht, namelijk een voor de lucht en een voor de maritieme grens. De KW, de Douane, het KPC, de Immigratie,

[29] CARICOM, Counter-terrorism Strategy, pag.13.
[30] Kustwacht voor het Koninkrijk der Nederlanden in het Caribisch Gebied, Jaarverslag 2018, pagina 5,6.

de VDC en de KMAR maken deel uit van de werkgroep maritiem. De werkgroep voor de luchtgrens bestaat uit het KPC, de KMAR, de CAP, het OM en de Airport Authority. Uitgangspunt was om na te gaan welke processen minimaal nodig zijn om grip te hebben op de grenzen. Nadat deze processen geïdentificeerd waren, is onderzocht wat er op dat moment al aanwezig was en wat nog verbeterd moest worden. De verbetervoorstellen werden in 2019 aan het JVO aangeboden, die het concept vaststelde en tevens een implementatieteam instelde die de taak kreeg om in het jaar 2020 met aanbevelingen te komen voor de implementatie van de baselines.[31]

2.4.6 Maritieme grenzen

De Taskforce Grip op de grenzen begon met een inventarisatie van de activiteiten van de diensten omtrent grensbewaking, waarna de processen op elkaar zijn afgestemd. Volgens de KW werd toen duidelijk dat de organisaties KW, Immigratie en Douane in feite eigenlijk aan elkaar gekoppeld zijn in het proces. De KW functioneert op het water, maar zodra een boot een haven binnenvaart zijn het de Douane en de Immigratie die de controle voor wat betreft de lading en personen moeten uitvoeren. Daarom hebben deze drie organisaties de processen geïdentificeerd en beschreven en waar nodig, verbetervoorstellen aangedragen. In de verbetervoorstellen wordt uitgegaan van multidisciplinaire teams en het inrichten van checkpoints waar met multidisciplinaire teams kan worden opgetreden. Hierdoor kunnen de expertises, middelen, bevoegdheden en personen van alle betrokken organisaties optimaal ingezet worden.

Helaas verloopt dit proces langzaam en moeizaam, omdat de diensten overbelast zijn, aldus de respondent van de KW.[32] De verbetervoorstellen zijn aan het JVO aangeboden ter besluitvorming. De verwachting is dat na consensus binnen het JVO, de organisaties weer bij elkaar komen om een plan van aanpak te maken om de verbetervoorstellen te implementeren.

[31] Kustwacht voor het Koninkrijk der Nederlanden in het Caribisch gebied, Jaarplan 2020, pag. 2.
[32] Zie ook Kustwacht voor het Koninkrijk der Nederlanden in het Caribisch gebied, Jaarverslag 2018, pag. 8.

Voor wat betreft de natuurlijke grenzen rondom het eiland werkt het KPC samen met de Douane en de KW. Er worden dagelijks patrouilles uitgevoerd langs de kust en vooral bij de plaatsen waar in het verleden aanlandingen hebben plaatsgevonden.

2.4.7 Luchtgrenzen

Het KPC heeft een specifieke taak voor wat betreft de grensbewaking. Het betreffende onderdeel van het KPC is gehuisvest op de luchthaven. Met een schietpartij op Hato in het achterhoofd, werd in het jaar 2016 in samenwerking met de KMAR een project opgestart, waarbij het KPC gekozen heeft voor de aanwezigheid van politiefunctionarissen op Hato, omdat bekend is dat criminele processen op vliegvelden bij elkaar komen. Samen met de KMAR heeft het KPC een gemengd team gevormd dat tijdens drukte op het vliegveld een oog in het zeil houdt.

Samen met andere stakeholders, zoals de KMAR, het OM, CAP, Airport Authority, is het KPC betrokken bij het project Poortwachter. Een resultaat van dit project was dat de sterke en zwakke schakels van de grensbewaking in kaart zijn gebracht en mogelijke oplossingen aangedragen.

2.5 Veiligheidsrisico's en -incidenten

Ook het OM geeft aan dat alle veiligheidsdiensten binnen *het Caribisch deel van het Koninkrijk*, samen met de AIVD, een risico- en veiligheidsanalyses hebben gemaakt. Het OM heeft in het jaar 2016 een presentatie op basis van een open bronnenonderzoek gehouden voor het JVO. De conclusie was dat voor een terroristische inschatting een aantal factoren relevant zijn, namelijk dat er sprake moet zijn van een reële dreiging, het doel moet aantrekkelijk zijn en er moet sprake zijn van een zekere waarschijnlijkheid. Uit deze inschatting is gebleken dat Curaçao aantrekkelijk is voor een terroristische daad, alleen al vanwege de aanwezigheid van een Amerikaanse militaire basis. Verder blijkt uit het onderzoek van het OM de radicalisering in Trinidad en mogelijk ook in Suriname een dreiging vormt. Tijdens het JVO op Bonaire in het jaar 2017 werd aan alle ministers van Justitie een inzicht in de dreigingsinschatting voor wat betreft terrorisme gegeven.

Uit interviews met de respondenten is, behoudens bij de VDC, niet gebleken, dat door andere diensten dreigings- en risicoanalyses zijn opgemaakt, waarbij de resultaten gedeeld werden met andere ketenpartners.

Volgens de respondenten heeft geen van de diensten dreigings- en risicoanalyses gemaakt op het gebied van de cyber security en de grensbewaking.

Er werden geen incidenten gemeld en er was geen centraal meldpunt aangewezen voor incident waar de publieke en private sector cyberincidenten die zich in hun omgeving hebben voorgedaan zouden kunnen doorgeven. Als potentiële dreigingen voor Curaçao ziet de VDC de onvoldoende gecontroleerde in- en uitvoer van reizigers en de vitale infrastructuur.

2.6 Capaciteit

2.6.1 Cyber security

Om het complexe fenomeen cyber crime adequaat te kunnen bestrijden, zijn specialisten nodig. Over hoeveel specialisten het gaat dient door analyses bepaald te worden. Dit geldt evenzeer voor de verdeling van de specialismen over de hierbij betrokken organisaties.

De vraag of justitie over voldoende capaciteit beschikt om het hoofd te kunnen bieden aan cyber crime, wordt door de diensten verschillend beantwoord. Volgens de respondent van het KPC, vormt cyber security op dit moment geen prioriteit voor het KPC en beschikt het niet over voldoende personeel voor het uitvoeren van al hun taken. Onder andere, beschikt het KPC over een financieel team, maar er kan niet gezegd worden dat er voldoende personeel aanwezig is. Het KPC kan meer analisten, cyber rechercheurs en bedrijfshulpverleners gebruiken. Het KPC is echter van mening dat in het geval cyber security in de toekomst een prioriteit wordt, dat het KPC dan samen met het RST, waarschijnlijk wel over voldoende digitale en financieel rechercheurs en kennis zal kunnen beschikken. Verder stelt de respondent van het KPC dat het KPC qua mankracht over een onderbemand financieel team beschikt, en dat dit blijkt uit het feit dat er voldoende zaken zijn die door het KPC niet opgepakt kunnen worden. Aan de opbouw van de financiële recherche wordt door het KPC de nodige prioriteit toegekend.[33] Het OM beschikt over een dieptespecialist cyber

[33] Strategiedocument OM-KPC 2016, pag. 6.

security op Sint Maarten voor de hele Caraïbische regio. Hij organiseert conferenties om mensen bij elkaar te brengen en om kennis te vergroten bij de officieren. In het geval er onderzoeken gepleegd moeten worden, moet het OM een beroep doen op onderzoekers van het KPC en RST.

Voor de interne ICT-aangelegenheden beschikt de VDC over een hbo-er die onder andere zorgt voor de ICT-veiligheid binnen de VDC.

Volgens de respondent van het MvJ is cyber security een nieuw traject binnen justitie. Het is een vrij ingewikkeld onderwerp en hiervoor zijn er goed opgeleide experts nodig. Op dit moment wordt vaak gebruik gemaakt van de experts van het RST die de expertise in huis hebben. Dit moet verder ontwikkeld worden. Bij het KPC is er een Infodesk die zich ook bezig moet gaan houden met cyber crime. Het KPC beschikt al over enige opgeleide analisten, die de analyses uitvoeren. Volgens de respondent gaat het erom dat vroegtijdig wordt gedetecteerd dat en wanneer iemand in de toekomst een klacht indient, bijvoorbeeld wanneer de persoonlijke informatie, is gestolen en als gevolg hiervan de persoon al zijn geld kwijt is, dit ook onderzocht moet kunnen worden . Indien nu een melding wordt gedaan, dan zal gebruik moeten worden gemaakt van Nederlandse experts, maar Curaçao moet ook de eigen experts in huis hebben en in deze zal in de toekomst dan ook geïnvesteerd worden. Aangezien er nog geen eigen cybersecurityspecialisten ter beschikking zijn, wordt voorlopig gebruik gemaakt van een op Curaçao gevestigd particulier bedrijf. Dit betekent dat de overheid voor deze service moet betalen.

2.6.2 Terrorisme

Om terrorisme te bestrijden dient Curaçao over voldoende en gespecialiseerd personeel te beschikken. Volgens het MvJ is er voldoende capaciteit en kwaliteit ter beschikking voor de bestrijding van het terrorisme.

Of Curaçao over voldoende capaciteit, kennis en infrastructuur beschikt is volgens het OM afhankelijk van verschillende factoren, waaronder de informatiepositie, oftewel is Curaçao afhankelijk van informatie van de lokale veiligheidsdienst en relevante andere veiligheidsdiensten. Ook stelt de respondent dat het OM pas om de hoek komt kijken bij de opsporing en vervolging. Het OM heeft een terrorismeofficier binnen haar gelederen die in Nederland hiertoe een speciale training gevolgd heeft.

Het KPC heeft aangegeven niet over voldoende personeel te beschikken en zeker niet over voldoende opgeleide bedrijfshulpverleners (bhv-ers). De KW beschikt niet over voldoende personeel om 24/7 interceptie-eenheden inzetbaar te hebben. De KW wordt tijdelijk door Defensie ondersteund om zoveel mogelijk wel hun deel van de taken in het geval van een terroristische aanslag uit te voeren. De KW beschikt wel over voldoende bhv-ers. Het personeel is opgeleid, getraind en er worden oefeningen gehouden.

2.6.3. Grensbewaking

Volgens de respondent van de KW vormt het ontbreken van voldoende analyse capaciteit een groot probleem. De KW zelf beschikt over één analist en bij het KPC ontbreekt het ook aan voldoende analisten. Om over een zodanig informatiebeeld te beschikken dat er gezegd kan worden dat er grip is op de grenzen, is, volgens de respondent van de KW, het beschikken over voldoende analysecapaciteit onontbeerlijk en is het ook noodzakelijk dat de diensten beschikken over een informatieknooppunt waarin alle diensten actuele informatie in kunnen brengen en uit kunnen halen. Het KPC heeft aangegeven niet over voldoende personeel te beschikken om alle werkzaamheden uit te voeren.

2.7 Fysieke infrastructuur

De gebouwen van de betrokken diensten verkeren qua uiterlijk in een redelijke staat van onderhoud. De diensten maken gebruik van zeker één vorm van beveiliging, bestaande vooral uit elektronische beveiliging. Het gaat hierbij vooral om de toegangscontrole en camerabeveiliging. Enkele organisaties hebben naast de elektronische toegangscontrole ook beveiligingsbeambten tot hun beschikking. De gebouwen worden in principe adequaat beschouwd voor de uitvoering van de werkzaamheden gerelateerd aan cyber security, terrorisme en grensbewaking. Qua beveiliging dient voor wat betreft cyber security ook aandacht besteed te worden aan de Internet of Things (IoT), aangezien deze apparaten meestal met het Internet verbonden zijn. Deze apparaten kunnen in de macht van hackers komen, die dan het personeel en bezoekers het effectief gebruik van het gebouw kunnen ontzeggen.

Voor wat betreft het terrorisme, dienen beveiliging barrières geïnstalleerd te worden ten einde te voorkomen dat voertuigen (bijvoorbeeld autobommen) tot dicht bij het gebouw geparkeerd kunnen worden. Voor wat betreft de locatie van hun gebouw, is de respondent van de VDC de mening toegedaan dat de locatie van het gebouw de dienst kwetsbaar maakt bij bijvoorbeeld een staking.

2.8 Technische hulpmiddelen

In de context van terrorisme op zee, beschikt de KW over ruim voldoende technische hulpmiddelen. Of het in alle gevallen over voldoende middelen beschikt, is afhankelijk van wat er zich zal afspelen. Voor bijvoorbeeld een passagiersschip dat zich hier bevindt met een groot aantal passagiers aan boord, beschikt de KW in geval van een terroristische daad op zee niet over voldoende middelen. In zo'n geval wordt dit dan als een ramp aangemerkt en is de KW aangewezen op hulp vanuit de regio en van binnen en buiten het Koninkrijk.

Door het College van Korpschefs worden thans de minimale voorzieningen waarover elk korps moet beschikken in kaart gebracht. Tevens worden in kaart gebracht de gespecialiseerde voorzieningen die op basis van samenwerkingsvormen beschikbaar moeten zijn. Voor wat betreft cyber security beschikken de diensten over eigen apparatuur, maar op het gebied van de beveiliging van data is een particulier bedrijf in de arm genomen die hiervoor zorgdraagt. Het KPC beschikt over digitale en financiële basisvoorzieningen, maar in complexe gevallen gaat het KPC de samenwerking aan met bijvoorbeeld het RST. Ook is er een overeenkomst met de Nationale Politie in Nederland voor ondersteuning bij zeer complexe gevallen.

Over het algemeen maakt de VDC geen gebruik van technische hulpmiddelen van andere diensten. De VDC heeft zijn eigen hulpmiddelen, maar vindt het wel nodig dat geïnvesteerd wordt in nieuwe hulpmiddelen. Ook het onderhoud van de bestaande hulpmiddelen is een punt van zorg.

2.9 Veiligheidsbewustzijn

Bij de KW bestaat er over het algemeen aandacht voor veiligheid. De KW leunt hierbij op de organisatie van de Commandant der Zeemacht in het Caribisch Gebied (CZMCARIB), die over een beveiligingsfunctionaris beschikt die regelmatig de

gebouwen, locaties en faciliteiten controleert. Ook maakt hij mensen door middel van informatie en educatie bewust van bepaalde veiligheidsrisico's. De leden van de KW zijn zich bewust van het feit dat zij als individu te maken hebben met de veiligheid van de hele KW.

Volgens de respondent van het KPC is de laatste tijd hard gewerkt aan het algemene veiligheidsbewustzijn van het personeel. Dit proces is geïntensiveerd door een gebeurtenis uit oktober 2018 waarbij een behoorlijk aantal kilo's drugs vanuit het recherchebureau verdween. In dit geval ging het om in beslaggenomen drugs die op een andere plaats bewaard werd dan normaal. Voor de opslag van deze hoeveelheid drugs werden geen extra beveiligingsmaatregelen genomen, noch fysiek noch elektronisch. Deze zaak was tijdens dit onderzoek van de Raad nog niet afgerond.

Voorheen was iedereen bij het MvJ zich bewust van het feit dat het niveau van de beveiliging van het Ministerie verhoogd moest worden. De implementatie van de verhoging van het niveau van de beveiliging heeft zijn voordelen en nadelen waarmee het personeel rekening moet houden. Het personeel moet zelf haar steentje bijdragen om afdoende beveiligd te blijven. Met het veiligheidsbewustzijn is het goed gesteld, aldus de respondent van het MvJ.

3. Analyse

3.1 Inleiding

Uit interviews met de verschillende respondenten van de verschillende diensten, blijkt dat met uitzondering van de grensoverschrijdende criminaliteit als drugs-, wapen- en mensenhandel, in tegenstelling tot de regio en Europa, in Curaçao niet veel aandacht besteed wordt aan overige vormen van grensoverschrijdende criminaliteit zoals terrorisme en cyber security. In dit verband is de Raad van oordeel dat terrorisme een gemene deler is voor wat betreft de cyber security en grensbewaking. Terroristen maken gebruik van de cyber space om propaganda te verspreiden en financiering te verkrijgen en zijn actieve deelnemers aan grensoverschrijdende criminaliteit, zoals drugs- en wapenhandel.

3.2 Prioritaire thema's

De Veiligheidsagenda benoemt vijf prioritaire thema's. Deze thema's zijn in feite intern van aard. De in dit rapport onderzochte thema's hebben allemaal een voor Curaçao extern aspect en maken geen deel uit van de Veiligheidsagenda. De Raad is van oordeel dat gezien het risico op aanzienlijke schade aan onder andere de economie, de overheid en de veiligheid in het algemeen cyber security, terrorisme en grensbewaking als prioritaire thema's aan de Veiligheidsagenda toegevoegd dienen te worden. Immers de nationale veiligheid is hierbij in het geding.

3.3 Wet- en regelgeving en beleid

De Raad constateert dat er geen sprake is van specifieke wet- en regelgeving en beleid op de geïnspecteerde terreinen en is van mening dat de benodigde informatie in hoofdlijnen in specifieke wet- en regelgeving en beleidsplannen vastgelegd dient te worden. Het te voeren beleid en de te volgen procedures dienen gebaseerd te zijn op bestaande wet- en regelgeving. Gezien het grensoverschrijdende karakter van grensbewaking, cybercrime en terrorisme is het ook aanbevelenswaardig om intensievere internationale en regionale samenwerking, zeker met de CARICOM, na te streven.

3.4 Integraal management

De Raad is van oordeel dat de benodigde informatie, kennis en vaardigheden met betrekking tot ICT versnipperd is over de verschillende instanties en dat er geen sprake is van voldoende samenwerking. De overheid moet het initiatief nemen en alle ministeries, het bedrijfsleven en particuliere organisaties bij elkaar brengen om integraal cybermanagement te realiseren.

Voor wat betreft een integrale aanpak heeft de Raad geconstateerd dat op het gebied van cyber security hier geen sprake van is terwijl dit niet door alle diensten als een prioriteit wordt ervaren.

Bij het terrorisme is er wel sprake van enige betrokkenheid van de semioverheid en de private sector, maar een integraal plan ontbreekt.

Voor wat betreft de grensbewaking is sprake van betrokkenheid van de semioverheid, maar de private sector is nog te weinig bij betrokken. Er zijn twee commissies gevormd voor de lucht- en maritieme grens.

3.5 Cyber security

3.5.1 Aanwijzing ministerie

De Raad constateert dat het op ambtelijk niveau niet duidelijk is welke het eerstverantwoordelijke ministerie is voor cybersecurity. Er moet naar het oordeel van de Raad een ministerie worden aangewezen dat eindverantwoordelijk is voor cyber security op Curaçao.

3.5.2 Cyberdreiging

De Raad is van mening dat het moeilijk is om de cyberdreiging voor Curaçao in te schatten aangezien meetinstrumenten ontbreken. De Raad acht het in ieder geval noodzakelijk om een centraal meldpunt voor cyberincidenten in te stellen.

3.6 Terrorisme

3.6.1 Coördinatie terrorismebestrijding

De Raad is van mening dat een ministerie belast dient te zijn met de algehele coördinatie van de terrorismebestrijding. De Raad is van mening dat het MvJ met deze rol belast kan worden, aangezien de regierol voor wat betreft de veiligheid van het land bij de Minister van Justitie ligt. Aangezien na een terroristische actie meestal sprake is van een ramp en het bestrijden van rampen onder de verantwoordelijkheid van de Minister van Algemene Zaken valt, is de Raad voorts van mening dat vanaf de fase van de bescherming van de bevolking en vitale infrastructuur, er sprake dient te zijn van een gedeelde verantwoordelijkheid tussen de Minister van Justitie en de Minister van Algemene zaken.

De APIS speelt een belangrijke rol in het voorkomen dat ongewenste personen zoals bijvoorbeeld FTF-ers zich naar Curaçao begeven. Dit betekent dat de identiteit van deze personen bekend moet zijn, reden waarom de Raad van oordeel is dat een samenwerking met de veiligheidsdiensten van de CARICOM-landen van grote waarde is.

3.7 Grensbewaking

De Raad juicht het toe dat voor wat betreft grensbewaking er een aanvang is gemaakt met een integrale aanpak dat moet leiden tot meer grip op de grenzen. Deze samenwerking tussen justitiële en niet-justitiële diensten heeft tot resultaat gehad dat spoedig beleid op dit terrein verwacht kan worden. Wel is de Raad van mening dat jaarlijks risico- en dreigingsanalyses opgesteld dienen te worden, zodat het veiligheidsbeeld voor wat betreft de grensbewaking vastgesteld en gemonitord kan worden.

3.8 Veiligheidsrisico’s

De Raad constateert dat behalve bij terrorisme waarbij, volgens de respondenten, dreigings- en risicoanalyses worden gemaakt, op de terreinen van cyber security en grensbewaking geen dreigings- en risicoanalyses worden opgesteld. Uit preventief

oogpunt acht de Raad het noodzakelijk dat met de nodige regelmaat dreigings- en risicoanalyses uitgevoerd worden. Alhoewel het terrorisme en onvoldoende grensbewaking blijkbaar geen aanzienlijke risico's opleveren, is de Raad van mening dat wel degelijk rekening dient te worden gehouden met de groeiende aantrekkingskracht tussen terroristische- en overige criminele netwerken, de aanwezigheid van Amerikaanse objecten en subjecten hier te lande, de radicalisering in het Caraïbisch gebied tezamen met de terugkeer van regionale FTF-ers.

3.9 Capaciteit

De Raad is van mening dat elke justitiële organisatie, conform het eigen formatieplan, over een minimumaantal eigen specialisten moet beschikken om hun eigen taken te kunnen uitvoeren. Hiervoor acht de Raad noodzakelijk dat cursussen en trainingen worden verzorgd zodat het personeel ook het benodigde niveau bereikt. Ten einde kosten te besparen en het een en ander te coördineren, dient hiertoe een opleidingsplan opgesteld te worden door het MvJ. Het is ook mogelijk dat het Ministerie de opleidingsplannen van de diensten op de totale behoefte afstemt, rekening houdende met de taken van de diensten.

3.10 Infrastructuur

De gebouwen van de geïnspecteerde diensten zijn allemaal beveiligd. De realiteit is echter dat deze gebouwen niet voldoende beveiligd zijn tegen terroristische aanslagen. Behoudens het gebouw van de KW zijn de overige gebouwen op vrij eenvoudige wijze bereikbaar voor het publiek. Het is noodzakelijk aandacht te besteden aan de bereikbaarheid van de muren van de gebouwen in verband met autobommen.

De Raad is hierbij van mening dat voor wat betreft cyber security aandacht dient te worden besteed aan de Internet of Things (IoT), aangezien door deze apparaten die met het Internet verbonden zijn, hackers het gebruik van het gebouw negatief kunnen beïnvloeden en geld eisen om het probleem op te heffen.

4. Aanbevelingen

Aanbevelingen aan de Minister

- Draag op korte termijn zorg voor de totstandkoming van specifieke wet- en regelgeving en beleid op de terreinen cyber security, terrorisme en grensbewaking;
- Draag er zorg voor dat cyber security, terrorisme en grensbewaking officieel tot prioriteiten op niveau van nationale veiligheid worden verheven;
- Draag er zorg voor dat cyber security opgenomen wordt in het takenpakket van het Ministerie van Justitie en belast dit ministerie met de coördinatie van de terrorismebestrijding;
- Breng de CARICERT onder bij het Ministerie van Justitie en wijs deze aan als de CSIRT voor Curaçao en als het centraal meldpunt voor cyberincidenten;
- Draag er zorg voor dat periodiek dreigings- en risicoanalyses worden uitgevoerd op de terreinen van cyber security, terrorisme en grensbewaking;
- Draag zorg voor een centraal justitieel opleidingsplan in het kader van het integraal management omtrent cyber security, terrorisme en grensbewaking;
- Draag zorg voor integraal management omtrent cyber security, terrorisme en grensbewaking.