Anton de Kom Universiteit van Suriname
Bibliotheek

Universiteitscomplex, Leysweg 86, Paramaribo, Suriname, Postbus 9212
Telefoon (597)464547, Fax (597)434211, E-mail: adekbib@uvs.edu

APPROVAL

NAAM: Mullenhof Cenegery

verleent wel / ~~niet~~ aan de AdeKUS kosteloos de niet-exclusieve toestemming om haar / zijn Drs. / B.Sc. / M.Sc. afstudeerscriptie online beschikbaar te stellen aan gebruikers binnen en buiten de AdeKUS.

Plaats en datum, 13 oktober 2021

Handtekening C Mullenhof

ANTON DE KOM UNIVERSITEIT VAN SURINAME

Faculteit der Juridische Wetenschappen

BEWIJSVERGARING VAN CYBERCRIME DOOR DE POLITIE IN SURINAME

Thesis ter verkrijging van de graad van Bachelor of Laws (LLB)

Bacheloropleiding Rechten

Cenegay Mullenhof

Begeleider: mr. J. Headley

Paramaribo, oktober 2021

Inhoudsopgave

Voorwoord

Voor u ligt de thesis' Bewijsvergaring door de Surinaamse politie bij opsporing van Cybercrime'. Deze scriptie is geschreven in het kader van mijn afstuderen aan de Bacheloropleiding Rechten aan de Anton de Kom Universiteit van Suriname. Van november 2020 tot en met juni 2021 ben ik bezig geweest met het onderzoek en het schrijven van de thesis.

Ik had reeds een thema en onderzoeksvraag geformuleerd voor mijn thesis. Het uitgevoerde onderzoek was complex, mede vanwege Covid-19 en alle daardoor ontstane en verbandhoudende obstakels. Na (uitvoerig) kwantitatief onderzoek heb ik de onderzoeksvraag kunnen beantwoorden.

Ten eerste wil ik het cybercrimeteam onder leiding van de heer Melvin Pinas bedanken dat mee heeft gewerkt aan dit onderzoek. Zonder hun medewerking had ik dit onderzoek nooit kunnen voltooien. Vervolgens dank ik mijn begeleider mr. J. Headley voor haar begeleiding en screening.

Ook van mijn familie en vrienden heb ik wijze raad mogen ontvangen. Bovendien hebben ze mij in moeilijke tijden moreel ondersteund tijdens het schrijfproces om niet op te geven. Tot slot wil ik mijn vriend en oom bedanken die de collegegelden jaarlijks hebben betaald. Hun wijsheid en motiverende woorden hebben mij geholpen deze thesis tot een goed einde te brengen.

Paramaribo, september 2021

Cenegay Mullenhof

Inleiding

De politie in Suriname heeft de laatste jaren te maken met een veranderde omgeving en een dynamische samenleving, waarin nieuwe veiligheidsvragen zich aandienen. Hiermee wordt bedoeld dat met de digitalisering van de samenleving, nieuwe uitdagingen op het vlak van criminaliteit en veiligheid ontstaan, waaronder cybercrime. Dit vraagstuk staat niet op zichzelf en maakt deel uit van een serie mondiale ontwikkelingen waarmee de Surinaamse samenleving wordt geconfronteerd.

Bij gebruik van internet en mobiele communicatie wordt de betekenis van de fysieke locatie vanwaaruit de cybercrimineel handelt steeds geringer. Ten behoeve van de opsporing van cybercriminelen is het vinden van het elektronisch spoor tussen daad en dader onmisbaar. Dit spoor kan lopen over vele (internationale) schakels, waarbij voor het vergaren van bewijs veelal assistentie van buitenlandse opsporingsautoriteiten nodig zal zijn.. Internationale samenwerking ter vergaring van elektronisch bewijs is daarom onontbeerlijk. Het Cybercrime-Verdrag geeft vorm aan deze internationale samenwerking.[1] Dit verdrag is door de Raad van Europa in Boedapest op 23 november 2001 ondertekend om de wetgeving en de aanpak van computercriminaliteit mondiaal te benaderen en zo het opsporen en bestraffen van computercriminelen te vergemakkelijken. In dit verdrag zijn er vereisten voor bewijsvergaring opgenoemd die belangrijk zijn voor de opsporing van cybercrime door de politie. Het bovenstaande heeft mij aangespoord om te onderzoeken of de manier van bewijsvergaring door de Surinaamse politie voldoet aan de vereisten opgenoemd in het Cybercrime-Verdrag. Suriname heeft dit verdrag niet geratificeerd, maar gezien het feit dat Suriname bij het aanpassen van de strafbepalingen in het Wetboek van Strafrecht dacht aan het Cybercrime-Verdrag, geeft aan hoe belangrijk wij dit verdrag achten.

De probleemstelling in deze thesis luidt als volgt: ***Voldoet de manier van bewijsvergaring bij cybercrime door de politie in Suriname aan de vereisten die zijn opgenoemd in het Cybercrime-Verdrag?***

1. Wat is de aard en impact van cybercrime in Suriname?

[1] Kaspersen, 2004, p.12.

2. Op welke manieren vindt bewijsvergaring plaats door de Surinaamse politie bij de opsporing van cybercrime?
3. Welke zijn de vereisten die zijn opgenomen in het Cybercrime-Verdrag over bewijsvergaring om cybercrime aan te pakken?

Doel van het onderzoek

Het doel van deze verkennende studie is om inzicht te krijgen in de bewijsvergaring bij cybercrime door de Surinaamse politie en of deze voldoet aan de internationale vereisten opgenoemd in het Cybercrime-Verdrag. Daarbij is de focus gericht op de opsporing van cybercrime, met bijzondere aandacht voor het Cybercrime-Verdrag.

Methode van het onderzoek

Dit onderzoek is gebaseerd op theoretisch juridisch onderzoek (analyse van wetgeving, verdragen en jurisprudentie) en onderzoek in de praktijk om aan Surinaamse data te komen, namelijk vraaggesprekken en documentenonderzoek. Er is ervoor gekozen om vraaggesprekken te doen om zodoende inzicht te krijgen hoe de politie in de praktijk bewijs vergaart bij opsporing van cybercrime. Verder zijn recente relevante wetgeving, literatuur, jurisprudentie over het onderwerp goed bestudeerd om zodoende inzicht te krijgen in de materie om als toetsingskader te dienen voor de Surinaamse situatie.

Maatschappelijke relevantie

Dit onderzoek is bedoeld om inzicht te verschaffen over de bewijsvergaring bij de opsporing van cybercrime door de Surinaamse politie en of de aanpak voldoet aan de vereisten die opgenoemd zijn in het Cybercrime-Verdrag. Dit verdrag regelt een aantal belangrijke zaken die Suriname kan helpen om cybercrime te bestrijden. Het is daarom van belang om onze Surinaamse situatie aan dit verdrag te toetsen. Zodoende kan er in zekere mate inzicht worden verschaft over de huidige situatie en een bewustwording geschept worden over de gebreken in de aanpak van cybercrime in Suriname door de politie.

Wetenschappelijke relevantie

Met dit onderzoek wordt er meer theoretische inzicht en kennis verkregen over het vergaren van bewijs bij opsporing van cybercrime door de Surinaamse politie op grond van het Surinaams Wetboek van Strafvordering en of deze voldoet aan de internationale vereisten. De resultaten van dit onderzoek zullen de wetenschappelijke inzichten zeker ten goede komen,

omdat men daarmee zal ontdekken hoe we die gebreken kunnen aanvullen om zodoende de aanpak van cybercrime te verbeteren.

Juridische relevantie

Bewijsvergaring is essentieel in strafzaken, want het doel ervan is de waarheidsvinding. Zonder bewijs of zonder voldoende bewijs kan een strafzaak niet succesvol worden afgewikkeld tijdens de strafprocedure. Het niet kunnen vergaren van bewijs zorgt voor stagnaties tijdens het strafrechtelijk proces. Als doel van deze thesis is tevens gesteld om inzicht te verschaffen over de bewijsvergaring van de Surinaamse politie bij cybercrime-delicten en om aan te geven dat door interpretatie van verdragsartikelen (Cybercrime-Verdrag) de bewijsvergaring van cybercrime op veel adequatere manier kan geschieden. In de praktijk kan bewijs dat niet op de wijze zoals voorgeschreven door de wet is verkregen, door de rechter als onrechtmatig verkregen bewijs beoordeeld worden. Voor adequate en efficiënte bewijsvergaring door de politie wordt aanpassing van strafwetgeving aan het Cybercrime-Verdrag derhalve wenselijk geacht.

Opbouw van de thesis

In hoofdstuk 1 wordt er een algemene beschouwing van cybercrime gegeven. Daarnaast worden de aard en impact van cybercrime in Suriname besproken.

In hoofdstuk 2 wordt besproken hoe de bewijsvoering van cybercrime in de Surinaamse strafwetgeving is geregeld.

In hoofdstuk 3 worden de bepalingen in het Cybercrime-Verdrag nader uitgelegd die handelen over het vergaren van bewijs bij cybercrime en of de manier van bewijs vergaren door de Surinaamse politie voldoet aan deze bepalingen.

Deze thesis wordt tenslotte afgesloten met een conclusie waarbij een concreet antwoord op de gestelde centrale vraag zal worden gegeven.

1 Algemene beschouwing, aard en impact cybercrime in Suriname

Een goed onderbouwde aanpak van cybercrime is alleen mogelijk wanneer er een gedegen inzicht bestaat in de aard en impact van cybercrime zoals die zich in Suriname manifesteert.[2] Het doel van dit hoofdstuk is het bieden van dat inzicht. Dat inzicht wordt geboden door zoveel mogelijk die kennis te benutten die wordt opgedaan tijdens omvangrijke opsporingsonderzoeken. Dergelijke onderzoeken leveren unieke kennis op over de aanpak van cybercrime.[3]

Om een completer beeld te krijgen van de belangrijke thema's die binnen cybercrime spelen, zijn er ook bronnen buiten de politiesystemen geraadpleegd. Veel andere externe partijen zoals Compuact verzamelen gegevens of gebruiken andere bronnen die inzicht geven in de aard en omvang van cybercrime. Het beeld dat zij schetsen kan afwijken van wat er bij de politie wordt gemeld, waardoor er onbegrip ontstaat tussen deze partijen en de politie. Deze partijen constateerden dat cybercrime agressiever werd in Suriname. Ze trokken aan de bel en hebben de autoriteiten en openbare instellingen op de hoogte gesteld. Omdat er maatregelen uitbleven, kwamen zij tot de conclusie dat zij niet serieus werden genomen.

1.1 De aard van cybercrime in het algemeen

Bij de algemene beschrijving van de aard van cybercrime zullen de volgende aspecten aan de orde komen: de Modus Operandi bij cybercrime, het georganiseerde karakter van cybercrime en de verbanden van cybercrime met andere delicten. Tevens zal ook de impact van cybercrime besproken worden met de nadruk op de nadelige gevolgen ervan voor de samenleving.

1.1.1 Belang van Modus Operandi bij Cybercrime

Meriam Webster Dictionary heeft de term Modus Operandi gedefinieerd als een proceduremethode of het is verder uitgewerkt als een duidelijk patroon of een aparte werkwijze die het werk van een enkele crimineel in meer dan één misdaad aangeeft of suggereert. Het Oxford woordenboek benadrukte ook in zijn definitie dat het gaat om een bepaalde manier of methode om iets te doen. Deze methode is afhankelijk van verschillende variabelen, zoals de technologie die beschikbaar is, gewoonten en kennis van de persoon die een misdaad begaat en

[2] E. Leukfeldt, M. Domenie, W.Stol, 2009, p. 1.
[3] E.W. Kruisbergen, R.A Roks. E.R Kleemans, p. 9.

van het slachtoffer en processen, regels, voorschriften die de technologie en het gedrag van mensen regelen. De chef van het cybercrimeteam concludeerde dat traditioneel de technologie niet de dominante variabele is in het misdaadproces, maar met de opkomst van de informatie- en computertechnologie heeft het alle lagen van de wereld waaronder Suriname overspoeld. Hij constateerde dat cyberspace een nieuw instrument is om de oude misdaden op een nieuwe manier te plegen.[4]

In het arrest ECLI:NL:RBMNE:2020:3467 is te achterhalen hoe belangrijk de Modus Operandi is bij cybercrime. In casu werden slachtoffers via een link naar een phishingwebsite geleid, waar ze hun bankgegevens moesten invullen. Vervolgens werden (grote) bedragen van de rekeningen afgeschreven. De verdachte was vooral betrokken bij het technische deel. De aangevers die beide klanten zijn bij de ING bank hebben een identieke mail gehad, waarin hen werd verzocht de toegang tot de Mobiel Bankieren App te verlengen. Deze e-mail ontvingen zij in dezelfde periode, namelijk respectievelijk 23 en 24 mei 2018. In beide gevallen werd, nadat de aangevers hun gegevens hadden ingevuld op de website waar zij via de link in de e-mail naartoe werden geleid, de Mobiel Bankieren App geïnstalleerd op een telefoon die niet van de aangevers was, waarna de geldbedragen werden gepind of overgeboekt. Gelet op de identieke inhoud van de e-mails, de gelijke modus operandi en de periode waarin de phishing heeft plaatsgevonden, beoordeelt de rechtbank de bewijsmiddelen in onderlinge samenhang. Door zijn werkwijze kon de rechtbank wettig en overtuigend bewijzen dat hij betrokken is geweest bij de phishing van de gegevens.[5]

1.1.2 Het georganiseerde karakter als kenmerk van cybercrime

De definitie van georganiseerde misdaad van Europol luidt als volgt: Er is sprake van crimineel samenwerkingsverband wanneer minimaal twee personen gedurende een periode samenwerken met als doel geldelijk gewin of macht.[6] Cybercriminelen werken zelden alleen. Zelfs voor relatief eenvoudige delicten zijn vaak meerdere personen nodig. Hetzelfde geldt voor financieel gemotiveerde cybercrimes: er zijn niet alleen personen nodig met technische vaardigheden. Zo zijn er ook personen vereist die gespecialiseerd zijn in het versturen van grote hoeveelheden e-mails, het overtuigen van potentiële slachtoffers om mee te werken aan de scam, of personen

[4] Interview Melvin Pinas, Hoofd Digitale Recherche, 30 april 2021.
[5] Rb. Midden-Nederland, 26 augustus 2020, ECLI:NL: RBMNE:2020:3467.
[6] https://www.bjutijdschriften.nl/tijdschrift/justitieleverkenningen/2018/5/JV_0167-5850_2018_044_005_002/fullscreen [geraadpleegd op 1 april 2021]

die zich bezighouden met het cashen van crimineel verdiend geld of het verplaatsen of witwassen van het geld. Gezamenlijk vormen deze personen het crimineel netwerk.[7]

In Suriname is er nog geen sprake van zwaar georganiseerde criminaliteit bij cybercrime. Er is wel sprake van normaal georganiseerde criminaliteit. 'Een praktisch voorbeeld hiervan in Suriname is de vriend-in-noodfraude', zegt de Chef van het cybercrimeteam.[8] Door het coronavirus is cybercrime, zoals oplichting via Whatsapp toegenomen. Een oplichter doet zich op Whatsapp voor als vriend of bekende en benadert slachtoffers met de vraag om geld over te maken. Stemt het slachtoffer toe, wordt het geld overgemaakt naar een bankrekening van de persoon die zijn of haar bankrekening ter beschikking stelt van de oplichter. Het komt voor dat derden er niet bewust van zijn dat hun bankrekeningen worden gebruikt. Door de geldtransacties via derden te laten lopen, blijven de echte oplichters buiten schot. Deze mensen worden ook wel money mule of geldezels genoemd.

Het georganiseerde karakter van cybercrime in Suriname is ook grensoverschrijdend. Hetgeen binnen de ene nationale rechtsorde strafbaar of onrechtmatig is, behoeft dat niet binnen een andere rechtsorde te zijn. Als een hacker gestolen geld overmaakt naar een bankrekening in Suriname, is het moeilijker om het geld hier te innen, gezien alle wettelijke regelingen. Zij gaan een samenwerking aan met iemand in een land waar een bank makkelijk op te zetten is. Het geld wordt vervolgens overgemaakt naar die bank in het buitenland waar zij het makkelijker kunnen innen. Gezien er verschillen zijn tussen de betrokken nationale wetgevingen, moeten alle landen ter wereld naar mijn mening bij elkaar komen om tot meer gemeenschappelijke gedragsregels te komen. De regels die gelden in het ene land voor het opzetten van een bank, zouden in het andere land ook moeten gelden. De wereld zou nog hierover moeten beraadslagen.

1.1.3 De verbanden van cybercrime met andere delicten

Cybercriminaliteit in Suriname heeft ook verbanden met de traditionele delicten. In 2016 lag een aantal grote internetsites plat na een cyberaanval door de hackers groep Anonymous. Het ging om de belangrijke informatiewebsite van de overheid, die van de Nationale Democratische Partij, een informatiesite van NV Energie Bedrijven Suriname en de site van de Surinaamsche Bank. De hackers vroegen verder een bedrag van 10.000 Amerikaanse dollar om de sites weer vrij te geven. Het bedrag moest in bitcoins worden overgemaakt. Als dat niet gebeurde,

[7] https://dehaagsehogeschool.nl [geraadpleegd op 1 april 2021]
[8] Interview Melvin Pinas, Hoofd Digitale Recherche, 30 april 2021.

dreigden zij het bedrag elke dag te verhogen en gevoelige bankinformatie van klanten te publiceren.[9] Als aan dit politiedossier behalve art. 187b WvSr (hacken) ook art. 377 WvSr (afdreiging) is opgenomen, wijst dat aan op een verband tussen deze twee delicten. Naar mijn mening was de hack in dit geval de weg waarop de dader(s) de slachtoffers afdreigde(n).

1.1.4 Impact van cybercrime

Cybercrime is kostbaar voor de organisaties die ermee te maken krijgen. Deze organisaties hebben veel geld en andere schadekosten. Als een bedrijf aangevallen wordt, kunnen de gevolgen enorm groot zijn. Wanneer de klanten toegang hebben tot de geleverde diensten, zeggen ze op en vertrekken ze naar de concurrent. Er kan daarna nog lang sprake zijn van reputatieschade en het zorgt ervoor dat klanten zich minder aanmelden. De gevolgen van een digitale aanval kunnen moeilijk worden overschat. Een hack zorgt intern al voor chaos. Ook al zijn er geen directe nadelige gevolgen, zal geïnvesteerd moeten worden in het op peil brengen van de cybersecurity van de organisatie.

Behalve dat een digitale aanval veel onkosten oplevert, heeft cybercrime ook een impact voor de integriteit en reputatie van personen (natuurlijke personen en rechtspersonen). Hieronder wordt een aantal voorbeelden van mogelijke schades genoemd en nader uitgelegd:

- Reputatieschade

Klanten, businesspartners of de concurrent kunnen vraagtekens plaatsen bij de veiligheid van systemen of werkwijze wanneer een hack wereldkundig wordt gemaakt. Reputatieschade is meestal de reden waarom bedrijven een aanval stilhouden. Bedrijven zijn in Suriname niet huiverig om hulp te zoeken bij de politie, omdat zij bepaalde persoonlijke zaken niet vrij willen geven. Daarnaast proberen ze de privacy van hun cliënten te waarborgen.[10] Naar mijn mening is het van belang dat de bedrijven in Suriname aangifte doen van cybercrime bij de politie. Door de aangiften kan de politie informatie verzamelen en bestuderen, omdat ze veel inzicht geven in de wijze van handelen van de criminelen en hoe de criminele organisatie in elkaar zitten. De aangiften maken het ook mogelijk om nieuwe vormen van cybercrime te identificeren, waardoor de politie beveiligingssoftware, antivirusprogramma's en systemen erop kan

[9] https://www.google.com/s/amp/s/amp.nos.nl/artikel/2144890-belangrijke-surinaamse-websites-gehackt-door-anonymous.html [geraadpleegd op 1april 2021]
[10] www.kpn.com/zakelijk/blog/de-impact-van-cybercrime.html [geraadpleegd op 14 februari 2021]

aanpassen. Doen de bedrijven geen aangifte, is dit niet mogelijk en kan de politie geen ervaring opdoen.[11] In Suriname doen bedrijven bijna nooit aangifte bij de politie.

- Politieke reputatieschade

In sommige gevallen verkondigen cybercriminelen ideologische of politieke boodschappen via de gehackte website of social-mediakanalen van een bepaalde organisatie. Deze boodschappen staan vaak haaks op de boodschap en opvattingen van een bepaalde groep die zij menen te ondersteunen. Deze vorm van cybercriminaliteit komt veel voor in Suriname.[12] Toen in 2016 belangrijke informatiewebsites werden gehackt, gaven de hackers aan dat er geluisterd moest worden naar de actiegroep 'Wij zijn moe'. De oprichter van deze groep zei niets van de hack te weten. Dit zorgde natuurlijk voor de zogenaamde imagoschade.

- Verminderde bereikbaarheid

Een DDos aanval levert meestal geen permanente schade op, maar zorgt ervoor dat een website enige tijd niet bereikbaar is. In het geval van een grote webshop richt een tijdelijke slechte bereikbaarheid directe financiële schade aan. Wanneer de aanval in het nieuws wordt besproken, is reputatieschade een tweede gevolg van verminderde bereikbaarheid.[13] Klanten vertrouwen het bedrijf niet meer, waardoor zij zich niet meer aanmelden.

1.2 De aard van cybercrime in Suriname

De aard van cybercrime in Suriname zal hieronder aan de orde komen, zodat een beeld geschetst kan worden van de ernst van de cyberdelicten en de noodzaak voor tools om bewijs te kunnen vergaren om de daders te achterhalen. Over de aard en de organisatie van deze vorm van criminaliteit is nog niet veel informatie beschikbaar, terwijl kennis hierover essentieel is om dit fenomeen aan te kunnen pakken. De afdeling Digitale Recherche heeft de volgende verschijningsvormen van cybercrime in Suriname geconstateerd:

- Cyberbullying komt veel voor in Suriname op Facebook. Mensen worden dagelijks uitgelachen en beledigd. Volgens politieke gezagsdragers zou het verbannen van Facebook de oplossing kunnen zijn. Naar mijn mening ligt de oplossing niet in het verbannen van Facebook. In Suriname zijn er verschillende social media platforms

[11] www.kpn.com/zakelijk/blog/de-impact-van-cybercrime.html [geraadpleegd op 14 februari 2021]
[12] www.kpn.com/zakelijk/blog/de-impact-van-cybercrime.html [geraadpleegd op 14 februari 2021]
[13] www.kpn.com/zakelijk/blog/de-impact-van-cybercrime.html [geraadpleegd op 14 februari 2021]

waaronder Facebook, Twitter, TikTok en Instagram. Indien Facebook in Suriname wordt verbannen, zullen Surinamers gauw naar andere platforms opzoek gaan om verder te gaan met cyberbullying. Hetgeen we moeten aanpakken, is het gedrag van de Surinamers. Ondanks het beledigen van de president strafbaar gesteld is, wordt hij dagelijks vreselijk op social media beledigd. De wetten worden gemaakt om het gedrag van mensen aan te pakken, maar ze worden niet toegepast. Voordat we overgaan tot het verbannen van Facebook moeten we eerst het gedrag van deze Surinamers aanpakken. Ze moeten verplicht worden gestuurd naar psychologen om cursussen van gedragsbeïnvloeding te volgen. De plegers van deze uitingsdelicten moeten wel beseffen dat beledigen, lasteren en smaad van burgers absoluut onaanvaardbaar is in een geordende samenleving. In landen zoals Vietnam, Noord-Korea en Iran zijn er afspraken met Facebook gemaakt. Zodra de naam van de president of andere gezagsdragers in het bericht van een Facebookgebruiker is genoemd, wordt het bericht per direct van Facebook verwijderd. Dit zouden we ook in Suriname kunnen toepassen, maar niet zo extreem. De Surinaamse burgers moeten nog steeds hun mening kunnen uiten, maar binnen de grenzen van wet en recht.

- Het afgelopen jaar heeft die afdeling geconstateerd dat Suriname vatbaar is voor ransomware-aanvallen. AZP, het Academisch Ziekenhuis Paramaribo, is hierover in de publiciteit getreden.[14] Een ransomware aanval kan heel ingrijpend zijn. Alle servers, gegevens en zelfs back-ups hiervan kunnen ‘gegijzeld’ worden; alles wordt versleuteld, niemand kan er meer bij. Wat rest is een bericht waarin er "losgeld wordt gevraagd, meestal te betalen in bitcoin, een digitale vorm van betalen waarbij de ontvanger anoniem blijft. De daders blijven zo anoniem. Intussen ligt de betreffende organisatie stil, bedrijfsprocessen die afhankelijk zijn van computers stoppen onmiddellijk.[15]

- Het hacken van Facebook- en Whatsapp accounts. De hackers versturen een verificatiecode waarop de slachtoffers klikken, dan wordt het account overgenomen.

- Hackers gebruiken cyberdefacement om het uiterlijk van een website of webpagina te veranderen. Om dit te doen breken ze in op de webserver van het beoogde slachtoffer

[14] https://m.starnieuws.com/index.php/welcome/index/nieuwsitem/58626 [geraadpleegd op 28 februari 2021]
[15] https://ict-as.sr/ransomware-voorkom-dat-u-het-volgende-slachtoffer-wordt/ [geraadpleegd op 14 februari 2021]

en vervangen ze de gehoste website door hun eigen website. Staatsolie en Finabank zijn ooit slachtoffers geweest van deze vorm van cybercrime.

- De naam Huawei wordt in een mail als Huavvei verstuurd naar het slachtoffer. Wanneer hij daarop klikt, maakt hij een groot geldbedrag over naar de hackers.
- Er komt heel veel smaad en laster voor op Facebook, waarbij leden van politieke partijen en publieke figuren onophoudelijk worden beledigd. Er worden valse facebookaccounts van politieke functionarissen gemaakt die valse informatie verspreiden.
- Bij het hacken van de websites van bedrijven vragen de daders meestal naar een betaling in bitcoins, omdat cryptovaluta de anonimiteit bieden van cash en de snelheid van digitale betalingen.[16] Hierdoor kunnen criminelen in Suriname geld wegsluizen zonder een spoor achter te laten.

Om een completer beeld te krijgen van de situatie in Suriname heeft de Stichting Compuact Suriname een intuïtieve steekproef en een steekproef gebaseerd op ervaring volgens het systeem van Van der Pligt & Plankers, 2013, uitgevoerd. Deze twee steekproefmethoden zijn nauw verwant. Bij een intuïtieve steekproef selecteert de onderzoeker deelnemers op basis van zijn intuïtie: de onderzoeker schat zelf in of de persoon of groep representatief is. Bij een steekproef op basis van ervaring worden mensen of groepen geselecteerd op basis van bestaande informatie, bijvoorbeeld wanneer op grond van ervaring bekend is dat de resultaten van een specifieke groep zeer representatief zijn voor een populatie en deze groep jaarlijks wordt geënquêteerd bij een opiniepeiling.

Uit dit onderzoek bleek dat Surinaamse hackers, uit verveling of nieuwsgierigheid, - en wat nog ernstiger is - of in opdracht van bepaalde lokale (politieke) organisaties bezig geweest zijn om op een oneigenlijke manier informatie te verzamelen. Dat is aan te merken als cybercriminaliteit of cybercrime. Deze hackers zijn cybercriminelen die onder de noemer black hat hackers vallen. De privacy van burgers wordt geschaad en hun veiligheid kan in gedrang komen, omdat waardevolle gegevens voor eenieder zichtbaar of toegankelijk kunnen worden. Criminelen kunnen gebruik maken van de gelegenheid om schade aan te richten, waardoor de veiligheid van klanten in gedrang komt. Door dit fenomeen dreigt nu een sneeuwbaleffect te ontstaan. Burgers, financiële organisaties, bekende Surinaamse nieuwssites, Facebook pages, een

[16] https://economie.rabobank.com/publicaties/2018/oktober/cybercrimis-en-cryptoknaken/ [geraadpleegd op 28 februari 2021]

nummer om dataplan of internet te activeren. Regeringsfunctionarissen en anderen zijn slachtoffers van deze black hat hackers en hun opdrachtgevers.[17]

[17] https://www.starnieuws.com/index.php/welcome/index/nieuwsitem/56648 [geraadpleegd op 28 februari 2021]

2 Bewijsvergaring ingevolge de Surinaamse strafwetgeving betreffende cybercrime

In dit hoofdstuk worden de mogelijkheden van de Digitale Recherche bekeken om bewijsmateriaal te vergaren ten aanzien van cybercrime. Deze afdeling van de politie is belast met het opsporen van cybercrime. De focus wordt gelegd op de autonome bevoegdheden van politieambtenaren en vermelden voor welke onderzoeksdaden de tussenkomst van de leden van het Openbaar Ministerie verplicht is.[18]

Zo kan de vraag gesteld worden of een politieagent een telefoon mag doorzoeken die hij vindt tijdens een fouillering? Kan hij via een online chatbox contact opnemen met een verdachte om zodoende bewijs te verzamelen?[19] Is het mogelijk om informatie te verkrijgen van een telecommunicatiebedrijf in een onderzoek naar cybercrime? Al deze vragen gaan over bewijsvergaring door politieagenten. Digitaal bewijs is ongetwijfeld belangrijk om misdrijven zoals hacking, phishing of grooming bloot te leggen. Ook in een strafrechtelijk onderzoek naar traditionele misdrijven is digitaal bewijs eerder een regel dan een uitzondering. Inhoud van smartphones wordt in veel dossiers onderzocht. De chatberichten of zoekgeschiedenis kunnen op een oorzaak wijzen, locatiegegevens kunnen dan weer een alibi verschaffen, enz. Het doel van deze bijdrage is daarom vanuit een praktische invalshoek een beeld te geven van de manieren waarop digitaal bewijs wordt verzameld in de hedendaagse positie van de Surinaamse strafprocedure. Ze concentreert op de vraag of en onder welke voorwaarden politieambtenaren een onderzoekshandeling autonoom mogen stellen, dan wel of hiervoor tussenkomst van het Openbaar Ministerie nodig is.

Het belangrijkste instrument op internationaal vlak is het Cybercrime-Verdrag. Voor de taakvervulling van de politie zijn twee wetten van belang: het Surinaams Wetboek van Strafrecht en het Surinaams Wetboek van Strafvordering.

2.1 Het Wetboek van Strafrecht ten aanzien van cybercrime

Enkele grote wetswijzigingen geven het huidige regime van digitaal speurwerk vorm. Het Wetboek van Strafrecht is in het jaar 2020 gewijzigd, waarbij er nieuwe bepalingen ten aanzien

[18] C. de Poot, E. Lievens, W. Stol, 2020, p.21.
[19] C. de Poot, E. Lievens, W. Stol, 2020, p.21.

van cybercrime bij zijn komen kijken. Volgens het cybercrimeteam is ten aanzien van cybercrime het Surinaams Wetboek van Strafrecht in orde. Deze wetswijzigingen vindt de afdeling wel wenselijk. De echte uitdaging ligt niet zozeer op het vlak van materieel strafrecht, maar op het vlak van opsporing en onderzoek.

Bij de wijziging van het Surinaams Wetboek van Strafrecht is het volgende in bijna alle cybercrimebepalingen opgenomen:[20] Op vordering van de politie is eenieder tegen wie proces-verbaal is opgemaakt voor het begaan van cybercrime, in het belang van het onderzoek naar deze strafbare feiten verplicht tot overgave van het middel of de middelen waarvan het feit of de feiten is of zijn gepleegd. Indien geen medewerking wordt verleend, wordt hij gestraft met een gevangenisstraf van ten hoogste drie maanden en een geldboete van ten hoogste zeshonderd Surinaamse dollars. Dit zou in strijd zijn met het nemo tenutur beginsel, omdat een verdachte of dader niet mag worden verplicht om aan zijn eigen veroordeling te werken. Het cybercrimeteam verklaarde dat de wetgever hiermee rekening zou moeten houden gezien het feit dat hij de wetten maakt. De wetten worden gemaakt en houden zij zich aan hetgeen er in de wet staat. Deze verplichting is voor hen meer een voordeel, omdat de wet de verdachte zelf verplicht en het biedt toch enige zekerheid dat zij het bewijs zullen vinden.[21]

2.2 Bewijsvergaring cybercrime ingevolge het Wetboek van Strafvordering

De meeste relevante bepalingen die relevant zijn voor het digitaal speurwerk zijn in het Surinaams Wetboek van Strafvordering opgenomen. Volgens het cybercrimeteam is het Surinaams Wetboek van Strafvordering in tegenstelling tot het Surinaams Wetboek van Strafrecht niet voldoende om cybercrime aan te pakken, omdat de spelregels opgenomen moeten worden in een speciale wet waarbij opsporingsbevoegdheden van de politie bij cybercrime zijn vastgesteld. Het toepassen van de klassieke artikelen lukt wel, maar zij zouden meer successen boeken met een speciale wet, zodat de politie meer armslag heeft om de criminelen op te sporen en aan te houden. Zij kunnen hierdoor niet op een adequate manier bewijs vergaren, omdat zij rekening moeten houden met onrechtmatig verkregen bewijs. Er bestaat al een conceptwet waarin de regeling van bijzondere opsporingsbevoegdheden is opgenomen. De chef van de afdeling benadrukte dat het tijd is om deze conceptwet weer

[20] WET van 18 februari 2020 houdende nadere wijziging van het Wetboek van Strafrecht (G.B, 1911 no.1, zoals laatstelijk gewijzigd bij S.B. 2017 no.85)
[21] Interview Melvin Pinas, Hoofd Digitale Recherche, 30 april 2021.

bespreekbaar te maken.[22] Zij zouden als opsporingsambtenaren daardoor meer ruimte, mogelijkheden en bevoegdheden kunnen krijgen in die digitale omgeving dankzij deze wet.

Het Surinaams Wetboek van Strafvordering bepaalt dat alle voorwerpen die kunnen dienen om de waarheid aan het licht te brengen vatbaar zijn voor inbeslagneming.[23] Daarnaast stelt het wetboek dat politieambtenaren bij het vervullen van hun opdrachten van gerechtelijke politie als taak hebben voorwerpen in beslag te nemen en ter beschikking te stellen van de bevoegde overheden. Volgens het Surinaams Wetboek van Strafvordering kan iedere politieambtenaar goederen in beslag nemen.[24] Er is sprake van een ruime beslaggrond die geen onderscheid maakt tussen type voorwerpen en (gegevensdragers of niet). Er is dus in Suriname geen beperking op de inbeslagname van informaticasystemen. Dit is betwist omdat gegevensdragers heel wat privacygevoelige informatie kunnen bevatten.[25] Er is wel een beperking op de manier waarop zij aan de informatie komen. Bij een hacker moeten ze eerst op een rechtmatige manier aan de gegevensdragers van de verdachte komen om het te mogen doorzoeken voor bewijs. Zij mogen de telefoon of computer van de hacker of verdachte van een zedendelict niet op afstand hacken om aan bewijs te komen. Zij geven toe dat het hacken van de gegevensdragers veel makkelijker zou zijn, omdat ze niet fysiek op een bepaalde locatie hoeven te zijn om te doorzoeken om gegevens in beslag te nemen en op te slaan.[26] Informatie die op gegevensdragers staat moet zo snel mogelijk worden veiliggesteld, omdat die snel en makkelijk op afstand verwijderd kan worden door de verdachten. Het hacken van deze gegevensdragers zou ideaal zijn voor de politie en hen meer mogelijkheden tot bewijsvergaring bieden, want dan zouden ze als opsporingsinstantie de gegevens veel sneller kunnen opslaan. Het is momenteel wettelijk niet mogelijk voor de Digitale Recherche om te hacken in gegevensdragers, omdat de verdachte zich altijd kan beroepen op onrechtmatig verkregen bewijs.

2.2.1 Databeslag

Politieambtenaren hebben de bevoegdheid om de gegevens die ze tijdens een zoeking rechtmatig aantreffen, ook te kopiëren op dragers van de overheid, als de gegevens als bewijsmateriaal kunnen dienen. Dit noemt men databeslag. Als de informatie niet gekopieerd kan worden, dan worden ze verzegeld. Om problemen met onrechtmatig verkregen bewijs te

[22] Interview Melvin Pinas, Hoofd Digitale Recherche, 30 april 2021.
[23] Art. 82 lid 1 WvSv.
[24] Art. 83 lid 1 WvSv.
[25] C. de Poot, E. Lievens, W. Stol, 2020, p.28.
[26] Interview Melvin Pinas, Hoofd Digitale Recherche, 30 april 2021.

voorkomen, is het belangrijk dat men in Suriname overgaat tot de zogenaamde chain of custody. De chronologische documentatie van verschillende stappen worden in de digitale bewijsvergaring dan gerespecteerd. Dit houdt in dat authenticiteit en de integriteit van bewijsmaterialen moeten worden gerespecteerd. Het is daarom aan te bevelen dat politieambtenaren de verschillende stappen die ze bij de bewijsvergaring doorliepen zo gedetailleerd mogelijk in een proces-verbaal te verwoorden en van de belangrijkste momenten foto's of video's te maken. De dragers waarop de forensische kopieën worden genomen moeten ongebruikt zijn.[27]

Wanneer een verdachte van cybercrime op heterdaad is betrapt, kan op elke plaats waar het feit is begaan of sporen heeft achtergelaten een huiszoeking plaatsvinden.[28] Een politieambtenaar kan ter inbeslagneming huiszoeking doen op elke plaats waar het feit is begaan of sporen zijn achtergelaten.[29] Er worden dan voor inbeslagneming vatbare voorwerpen waaronder gegevensdragers, voor zover deze voor de hand liggen, in beslag genomen.[30] Tenzij het belang van het onderzoek dit vordert, wordt er niet overgegaan tot inbeslagneming pas nadat de bewoner of meerderjarige huisgenoten zijn gehoord en zonder succes zijn gevraagd het voorwerp vrijwillig af te geven voor inbeslagneming.[31] De politieambtenaar mag de bewoner of indien hij niet aanwezig is, een meerderjarige huisgenoot vragen een verklaring te geven omtrent de in beslag genomen voorwerpen, tenzij het belang van het onderzoek zich hiertegen verzet. Indien de verdachte zelf aanwezig is, geldt voor hem hetzelfde.[32] Bij de huiszoeking mag de verdachte voorzien zijn van een advocaat.[33]

Er worden telefoongesprekken, ten aanzien waarvan het vermoeden bestaat, dat de verdachte eraan deelneemt of zal deelnemen door een politieambtenaar afgeluisterd of opgenomen.[34] Eenieder die werkzaam is bij een instelling van telefonie ter zake van alle verkeer dat door tussenkomst van de instelling is geschied, ten aanzien waarvan het vermoeden bestaat dat de verdachte eraan heeft deelgenomen, verschaft de politieambtenaar in beginsel de gewenste inlichtingen.[35] Aangegeven is dat ze gebruik kunnen maken van hun verschoningsrecht. Er moet

[27] C. de Poot, E. Lievens, W. Stol, 2020, p.28
[28] Art. 84 WvSv .
[29] Art. 85.lid 1 sub 1 WvSv.
[30] Art. 85 lid 1 sub 2 WvSv.
[31] Art. 87 lid 1 WvSv.
[32] Art. 87 lid 2 WvSv.
[33] Art. 87 lid 3 WvSv.
[34] Art. 89 lid 1 sub a WvSv.
[35] Art. 89 lid 1 sub b WvSv.

binnen twee dagen een proces-verbaal worden opgemaakt van het beluisteren of opnemen.[36] Indien deze gegevens niet van belang zijn voor het onderzoek of mededelingen gedaan door een persoon die gebruik kan maken van zijn verschoningsrecht, worden ze door de rechter-commissaris vernietigd.[37]

2.2.2 Beroepsgeheimhouders

Beroepsgeheimhouders spelen een belangrijke rol bij het opsporen van cybercrime, omdat zij vaak privacygevoelige informatie van personen bezitten die van wezenlijk belang kan zijn bij de aanpak van cybercrime. Als het gaat om informaticasystemen van artsen en advocaten, telecommunicatiebedrijven et cetera, zijn de wettelijke voorwaarden in veel gevallen strikter. Voor het geven van getuigenissen of het beantwoorden van bepaalde vragen kunnen zich ook verschonen zij die uit hoofde van hun stand, hun ambt, hun beroep tot geheimhouding verplicht zijn, maar alleen omtrent hetgeen waarvan de wetenschap aan hen als zodanig is toevertrouwd.[38] Het beantwoorden van vragen of een huiszoeking kan alleen plaatsvinden als deze personen of instellingen zelf van deelname aan een strafbaar feit worden verdacht of als een derde gebruik heeft gemaakt van hun elektronische communicatiemiddelen.[39]

Het cybercrimeteam verklaarde dat de samenwerking met de telecommunicatiebedrijven in Suriname vaak niet goed verloopt, omdat zij te lang op belangrijke informatie moeten wachten. Het is van belang dat zij bepaalde informatie snel veiligstellen. Het registreren van simkaarten op namen van de klanten verloopt ook niet op de juiste manier bij de providers. De klanten kunnen de identiteitskaart van iemand anders gebruiken om een simkaart te kopen. Mocht de gebruiker van het telefoonnummer een strafbaar feit met de simkaart plegen, leidt het onderzoek naar de persoon die op zijn of haar naam de simkaart heeft gekocht. Dit bemoeilijkt onderzoekingen van het cybercrimeteam. De samenwerking met externe partijen laat vaak te wensen over.[40]

2.2.3 Toestemming bij bewijsvergaring cybercrime

De politieambtenaar oefent zijn bevoegdheid niet uit tot het binnendringen van een woning tegen de wil van de bewoner, tenzij hij voorzien is van een algemene of bijzondere schriftelijke last van een lid van het openbaar ministerie of een bijzondere schriftelijke last van de

[36] Art. 89 lid 3 WvSv.
[37] Art. 89 lid 4 WvSv.
[38] Art 198 WvSv.
[39] C. de Poot, E.Lievens, W, stol, 2020, p.28.
[40] Interview Melvin Pinas, Hoofd Digitale Recherche, 30 april 2021.

districtscommissaris.[41] De schriftelijke last wordt slechts gegeven en houdt in de verwezenlijking van een bepaald doel, om bij een algemene last alle woningen of bij een bijzondere last bepaald aangewezen woningen, binnen te treden.[42] De politieambtenaar mag tegen de wil van de bewoner een huis binnentreden als hij door een aan hem aangewezen bepaalde persoon wordt begeleidt. Er moet binnen twee dagen wel een proces-verbaal daarover worden opgemaakt.[43]

In de praktijk is er een lid van het Openbaar Ministerie, namelijk een speciale Officier van Justitie die specifiek belast is met cybercrimezaken. De samenwerking tussen het cybercrimeteam en het Openbaar Ministerie is heel goed. Ze zijn vaak met elkaar in contact om zaken te rapporteren. Er is wettelijk nog niet aangegeven bij welke cases zij toestemming nodig hebben van het Openbaar Ministerie, maar in de praktijk wordt er in de meeste gevallen wel afgestemd met het Openbaar Ministerie. De chef van het cybercrimeteam is een Hulpofficier van Justitie, waardoor hij zelf opdracht kan geven aan het team om bijvoorbeeld computergegevens veilig te stellen. Hij kan daarna rapporteren bij de Officier van justitie dat hij zo een besluit heeft genomen. Hij is niet verplicht eerst contact op te nemen met het Openbaar Ministerie, gezien het feit dat het ook niet in een wet is opgenomen.[44]

2.2.4 Bewaring van in beslag genomen gegevensdragers of computergegevens

In beslag genomen voorwerpen worden zoveel mogelijk afgesloten bewaard in een verzegelde omslag. Op de omslag dient te staan:

- De dag van de inbeslagneming
- Bij wie ze in beslag zijn genomen
- Een korte inhoudsopgave
- Handtekening van degene die de omslag heeft verzegeld

Indien het niet mogelijk is om de voorwerpen in een omslag te verzegelen, wordt er een strookje eraan gehecht, waarop dezelfde mededelingen staan. Kan aan het een of het ander niet worden voldaan, dan worden ze zoveel mogelijk gewaarmerkt. Er wordt aan de persoon bij wie ze in beslag zijn genomen een bewijs van ontvangst afgegeven.[45] De in beslag genomen voorwerpen

[41] Art. 113 lid 1 WvSv.
[42] Art. 114 WvSv.
[43] Art. 115 WvSv.
[44] Interview Melvin Pinas, Hoofd Digitale Recherche, 30 april 2021.
[45] Art. 102 lid 1 WvSv.

worden, zodra het belang van het onderzoek het toelaat, gesteld onder de hoede van een bij staatsbesluit aangewezen bewaarder.[46] De voorwerpen worden niet vervreemd, prijsgegeven of tot het ander doel dan het onderzoek gebruikt.[47] Indien de voorwerpen niet geschikt zijn voor opslag wordt een machtiging door het Openbaar Ministerie verleend aan de bewaarder of een ambtenaar die de voorwerpen in afwachting van hun vervoer, onder zicht heeft.[48]

2.2.5 Online infiltratie voor bewijsvergaring door de politie

Van online infiltratie bij cybercrime is er nog geen sprake, omdat er nog geen speciale wet bestaat. Het cybercrimeteam kan niet wachten totdat zij deze bevoegdheid kunnen uitoefenen, omdat zij van mening zijn dat undercoveroperaties interessante mogelijkheden kunnen bieden voor de Surinaamse politie, wegens de mogelijkheden tot het misleiden van verdachten en interacties met verdachten. Het Hansa Market arrest heeft wereldwijd laten blijken hoe belangrijk online infiltratie en de wettelijke basis voor bijzondere bevoegdheden zijn bij de opsporing van cybercrime[49] Die onderzoeksdaad houdt in dat bepaalde politiediensten onder een fictieve identiteit op het internet contact onderhouden met een of meerdere verdachten.[50] De Hansa Market was een illegale online marktplaats waar er verdovende middelen werden verhandeld. Op 20 juni 2017 werd een bevel van infiltratie afgegeven door de Officier van Justitie. Onder dit bevel is de infrastructuur van Hansa Market naar Nederlands grondgebied geëmigreerd en is de Hansa Market heimelijk en ongewijzigd door het onderzoeksteam overgenomen met als doel wachtwoorden, berichten, orderinformatie en bitcoins niet versleuteld af te vangen teneinde verdachten te identificeren en illegale goederen in beslag te nemen. Het onderzoeksteam fungeerde daarbij als beheerder van Hansa Market, reageerde op verzoeken van kopers, nam deel aan berichtenverkeer, onderhield contacten en verrichtte een aantal pseudokopen. Dit genereerde informatie met betrekking tot de verschillende online aanbieders en kopers van drugs wereldwijd. Op 20 juli 2017 werd de infiltratieactie stopgezet en werd de marktplaats offline gehaald. De actie viel onder de bijzondere bevoegdheden als bedoeld in het Nederlands Wetboek van Strafvordering. Het verweer van de raadsman dat een wettelijke basis ontbrak, werd daarom verworpen. Het was geen onrechtmatig verkregen bewijs, omdat er een wettelijke regeling bestaat waarop de handeling gebaseerd is. Zodra er zo een wet in Suriname is aangenomen, kunnen Surinaamse agenten infiltreren in een illegale

[46] Art. 102 lid 2 WvSv.
[47] Art. 103 lid 1 WvSv.
[48] Art. 103 lid 2 en 3 WvSv.
[49] Rb. Rotterdam,3 juli 2019, ECLI:NL:RBROT:2019:5339.
[50] C. de Poot, E. Lievens, 2020, p.31.

online marktplaats of een pedofiele chatgroep. Het is wel van belang dat wanneer deze wet in het leven wordt geroepen de uitvoering van de wet aan de volgende belangrijke voorwaarden voldoet:

- Voor deze handeling is de schriftelijke toestemming van de leden van het Openbaar Ministerie nodig
- De online infiltratie kan alleen plaatsvinden als er ernstige aanwijzingen zijn dat de personen strafbare feiten plegen of zouden plegen
- Het mag alleen toegestaan worden wanneer andere middelen niet voldoende zijn om de waarheid aan het licht te brengen
- De machtiging moet schriftelijk zijn, maar in spoedeisende gevallen is een mondelinge machtiging voldoende. Nadien kan de machtiging schriftelijk worden bevestigd
- Alle onderzoeksdaden moeten worden geregistreerd. Dit zorgt voor transparantie.
- De infiltrant mag wel noodzakelijke daden plegen, maar hij moet daarvoor wel een schriftelijke toestemming bij het Openbaar Ministerie aanvragen.

Hoofdstuk 3 Cybercrime-Verdrag en bewijsvergaring in Suriname

Het Cybercrime-Verdrag werd op 23 november 2001 in de schoot van de Raad van Europa ondertekend. Het is het eerste internationale verdrag dat criminaliteit en criminaliteitshandhaving in een elektronische omgeving in kaart brengt. Het Cybercrime-Verdrag is niet alleen ondertekend door de lidstaten van de Raad van Europa, het stond ook open voor niet leden. Cybercriminelen kunnen bijgevolg ook buiten Europa worden vervolgd.[51] Suriname heeft het Cybercrime-Verdrag nog niet ondertekend.

De drie belangrijkste doelen van het verdrag zijn:[52]

- Harmonisering van het materieel strafrecht beoogd met betrekking tot de specifieke informaticamisdrijven.
- Harmonisatie van de opsporingsbevoegdheden in relatie tot computersystemen en netwerken
- Internationale rechtshulp bevorderen ten behoeve van de opsporing van strafbare feiten te bevorderen

3.1 De vereisten in het Cybercrime-Verdrag ten aanzien van bewijsvergaring

Elke lidstaat moet wetgevende en andere maatregelen nemen om de politie de bevoegdheid te verlenen om op zijn grondgebied te doorzoeken of op vergelijkbare wijze toegang te verschaffen tot:[53]

- Computersysteem of onderdeel daarvan en de daarin opgeslagen gegevens
- Een opslagmedium voor computergegevens waarop computergegevens kunnen worden opgeslagen

[51] G. Vermeulen, 2007, p. 452.
[52] G. Vermeulen, 2007, p. 452.
[53] Art. 19 lid 1 Cybercrimeverdrag

Elke lidstaat neemt de wetgevende en andere maatregelen die nodig zijn om ervoor te zorgen dat wanneer de politie een specifiek computersysteem of een onderdeel daarvan onderzoekt of zich daartoe op vergelijkbare wijze toegang verschaft en redenen heeft te vermoeden dat de gezochte gegevens zijn opgeslagen in een ander computersysteem of een onderdeel daarvan op haar grondgebied en zij deze gegevens rechtmatig kunnen verkrijgen vanuit het initiële systeem, de politie in staat is het systeem terstond te doorzoeken.[54] Elke lidstaat maakt het wettelijk mogelijk voor de politie om deze computergegevens in beslag te nemen of op vergelijkbare wijze zeker te stellen. Deze maatregelen omvatten de bevoegdheid tot:[55]

- Het in beslag nemen of op vergelijkbare wijze zeker stellen van een computersysteem of onderdeel daarvan of een opslagmedium voor computergegevens
- Het maken en onder zich houden van een kopie van deze gegevens.
- Het handhaven van de integriteit van de desbetreffende computergegevens
- Het ontoegankelijk maken of verwijderen van die computergegevens uit het computersysteem waartoe toegang is verkregen

Elke lidstaat neemt de wetgevende en andere maatregelen die nodig zijn om de politie de bevoegdheid te geven een persoon die kennis heeft van het functioneren van het computersysteem of van maatregelen ter bescherming van de zich daarin bevindende computergegevens, te bevelen, voor zover in redelijkheid mogelijk, alle benodigde informatie te verstrekken om de bovengenoemde maatregelen mogelijk te maken.[56]

Elke lidstaat neemt de wetgevende en andere maatregelen die nodig zijn om aan de politie de bevoegdheid te geven:[57]

- In 'real-time' verkeersgegevens die betrekking hebben op specifieke communicatie die op het grondgebied van het land plaatsvindt door middel van een computersysteem, te vergaren of vast te leggen met gebruikmaking van de bestaande technische middelen op het grondgebied
- Een serviceprovider, binnen zijn bestaande technische mogelijkheden verplichten om in real-time verkeersgegevens die betrekking hebben op specifieke communicatie die op

[54] Art. 19 lid 2 Cybercrimeverdrag.
[55] Art. 19 lid 3 Cybercrimeverdrag.
[56] Art. 19 lid 4 Cybercrimeverdrag.
[57] Art. 20 lid 1 Cybercrimeverdrag.

het grondgebied van die partij plaatsvindt door middel van een computersysteem, te vergaren of vast te leggen door gebruik te maken van de bestaande technische middelen op het grondgebied of samen te werken met de politie bij het vergaren of vastleggen van de gegevens

Bij het onderscheppen van inhoudelijke gegevens gelden dezelfde maatregelen die eerder opgenoemd zijn. Wanneer een lidstaat de inhoudelijke gegevens niet kan vergaren, kan zij in plaats daarvan de nodige wettelijke en andere maatregelen treffen om de real-time vergaring of vastlegging van verkeersgegevens betreffende specifieke, op haar grondgebied verzonden communicatie te waarborgen door middel van de toepassing van de op dat grondgebied bestaande technische middelen. De wet moet de serviceprovider verplichten tot geheimhouding van de uitoefening van de bevoegdheid en iedere informatie daaromtrent.[58]

Elke lidstaat neemt de wetgevende en andere maatregelen die nodig zijn om zijn bevoegde autoriteiten de spoedbewaring te bevelen of op soortgelijke wijze de spoedbewaring te bewerkstelligen van de gespecificeerde computergegevens waaronder de verkeergegevens, die zijn opgeslagen door middel van een computersysteem, in het bijzonder wanneer er redenen zijn om te vermoeden dat de computergegevens bijzonder vatbaar zijn voor verlies of wijziging.[59] Wanneer een lidstaat hieraan uitvoering geeft door middel van een bevel aan een persoon die de specifieke opgeslagen computergegevens in zijn bezit heeft of tot welker toegang hij gerechtigd is, te bewaren, neemt de lidstaat de wetgevende en andere maatregelen die nodig zijn om deze persoon te verplichten de integriteit van die persoonsgegevens te verzekeren en te handhaven voor een tijdsduur zolang het nodig is, met een maximum van negentig dagen, teneinde de bevoegde autoriteiten in staat te stellen de verstrekking van deze gegevens te verlangen. De staten kunnen bepalen dat zo een bevel wordt verlengd.[60] De chef van het cybercrimeteam verklaarde dat alhoewel het verdrag nog niet geratificeerd is zij altijd proberen om zo snel als mogelijk gegevens veilig te stellen.[61] De persoon belast met de bewaring is verplicht tot geheimhouding.[62] De spoedbewaring van gegevens moet mogelijk zijn ongeacht of een of meer serviceproviders bij de overdracht van die gegevens betrokken waren en te verzekeren dat de bevoegde autoriteit of een door de autoriteit aangewezen persoon,

[58] Art. 21 lid 2 Cybercrimeverdrag.
[59] Art. 16 lid 1 Cybercrimeverdrag.
[60] Art. 16 lid 2 Cybercrimeverdrag.
[61] Interview Melvin Pinas, Hoofd Digitale Recherche, 30 april 2021.
[62] Art. 16 lid 3 Cybercrimeverdrag.

onverwijld een hoeveelheid verkeersgegevens wordt verstrekt die voldoende is om de serviceproviders zijn en langs welke route de gegevens zijn overgedragen.[63]

Elke lidstaat neemt de wetgevende en andere maatregelen die nodig zijn om haar bevoegde autoriteiten de bevoegdheid te verlenen om te bevelen dat een persoon op haar grondgebied gespecificeerde computergegevens overlegt die in zijn bezit zijn of tot welker toegang hij gerechtigd is en die zijn opgeslagen in een computersysteem of op een opslagmedium voor computergegevens. De serviceprovider die zijn diensten op het grondgebied van de lidstaat aanbiedt, met betrekking tot deze diensten abonnee informatie overlegt die deze serviceprovider in zijn bezit heeft of tot welks toegang hij gerechtigd is.[64]

3.2 Het Wetboek van Strafvordering getoetst aan vereisten in Cybercrime-Verdrag

Het is opvallend dat de vaardigheden voor de opsporing van cybercrime veel verschillen van opsporingsvaardigheden die nodig zijn voor andersoortige, 'traditionele' zaken.[65] De wetten moeten wel van elkaar verschillen. Suriname heeft nog geen speciale wet die de opsporingsbevoegdheden van de politie over cybercrime beschrijft. Wij hebben geen wetgevende en andere maatregelen genomen om de politie de bevoegdheid te verlenen om op haar grondgebied te doorzoeken of op vergelijkbare wijze toegang te verschaffen tot computergegevens. De chef van het cybercrimeteam verklaarde dat zij te werk gaan met het Surinaams Wetboek van Strafvordering.[66] In het wetboek is wel aangegeven dat alle voorwerpen die kunnen dienen om de waarheid aan het licht te brengen vatbaar zijn voor inbeslagneming, maar bewijsvergaring bij cybercrime omvat zoveel meer zoals real-time vergaring van computergegevens, online infiltratie, in hoeverre mag een politieambtenaar vanaf zijn informatiesysteem bewijsmaterialen verzamelen et cetera. Het simpel te werk gaan met het Surinaams Wetboek van Strafvordering is naar mijn mening niet effectief. In deze paragraaf wordt er nagegaan of de manier van bewijsvergaring door de Surinaamse politie voldoet aan de artikelen over bewijsvergaring opgenoemd in het Cybercrime-Verdrag.

[63] Art. 17 lid 1 Cybercrimeverdrag.
[64] Art. 18 lid 1 Cybercrimeverdrag.
[65] P. Boekhoorn, 2019, p. 43.
[66] Interview Melvin Pinas, Hoofd Digitale Recherche, 30 april 2021.

3.2.1 Spoedbewaring van opgeslagen computergegevens en gedeeltelijke verstrekking van computergegevens ten aanzien van het huidige Wetboek van Strafvordering

We moeten onze autoriteiten in staat stellen de spoedbewaring te bevelen van computergegevens die vatbaar zijn voor verlies of wijziging om de integriteit van de gegevens te verzekeren en te handhaven. De Surinaamse politie probeert ten alle tijde computergegevens die belangrijk zijn voor een strafrechtelijk onderzoek in beslag te nemen. Bij de spoedbewaring van computergegevens is in het Cybercrime-Verdrag aangeduid dat de bewaarder of persoon die belast is met het bewaren van computergegevens verplicht is tot geheimhouding. Het Wetboek van Strafvordering praat wel over het bewaren van bewijs voor een bepaalde periode, maar de bewaarder is wettelijk niet verplicht tot geheimhouding.

3.2.2 Het huidige Wetboek van Strafvordering ten aanzien van het verstrekkingsbevel

Een persoon die in het bezit is van computergegevens die belangrijk zijn voor een strafrechtelijk onderzoek moet deze aan de politie overleggen. In het Surinaams Wetboek van Strafrecht zijn er bepalingen opgenomen waarbij personen of verdachten, die in het bezit zijn van middelen waarmee een strafbaar feit is gepleegd, verplicht zijn deze te overleggen.

Een serviceprovider die zijn diensten aanbiedt, moet met betrekking tot deze diensten abonnee-informatie overleggen. Zoals eerder aangegeven, bestaat er geen goede samenwerkingsverband tussen de politie en de serviceproviders. Indien deze informatie belangrijk is voor het strafrechtelijk onderzoek, moeten zij deze onmiddellijk afstaan aan de politie. Er moeten wettelijke regelingen komen die de providers verplichten om strenger te zijn bij het verkopen van simkaarten, maar ook regelingen die hun verplichten om binnen een bepaalde periode de benodigde informatie aan de politie te verschaffen.

3.2.3 Het huidige Wetboek van Strafvordering ten aanzien van doorzoeking en beslagneming van opgeslagen computergegevens

Suriname heeft geen wetgevende en andere maatregelen genomen die nodig zijn om ervoor te zorgen dat wanneer de politie een specifiek computersysteem of een onderdeel daarvan onderzoekt of zich daartoe op vergelijkbare wijze toegang verschaft en redenen heeft te vermoeden dat de gezochte gegevens zijn opgeslagen in een ander computersysteem of een onderdeel daarvan op haar grondgebied en zij deze gegevens rechtmatig kunnen verkrijgen vanuit het initiële systeem, de politie in staat is het systeem terstond te doorzoeken. De chef van het cybercrimeteam verklaarde dat zij wel op deze manier te werk gaan. Zodra zij toestemming hebben gekregen van de chef van de afdeling of de Officier van Justitie nemen zij alle

gegevensdragers in beslag.[67] Hetgeen voor een pluspunt zorgt. Het moet alleen nog in een wet worden omschreven.

In het verdrag is aangeduid dat elke lidstaat zijn bevoegde autoriteiten de bevoegdheid moet verlenen aan een persoon die kennis heeft van het functioneren van computersystemen of van de maatregelen ter bescherming van de zich daarop bevindende gegevens. Het cybercrimeteam zou de deskundigheid moeten bezitten om deze taak voor elkaar te krijgen. Behalve het vestigen van onze aandacht op het harmoniseren van onze wetgeving met de wereld, moeten de politieambtenaren de technologische ontwikkelingen bijbenen door deze regelmatig te bestuderen. De agenten worden met informatie overspoeld, zodat zij het werk naar behoren kunnen doen. Kennis en deskundigheid zijn van essentieel belang bij het aanpakken van cybercrime. Zij hebben momenteel genoeg middelen om bewijs te vergaren. Ze houden wel rekening met het feit dat er continue nieuwe ontwikkelingen zijn op het gebied van ICT. De daders zijn altijd een stapje voor, omdat zij onophoudelijk naar nieuwe manieren zoeken om niet gepakt te worden. De kunst is om ze bij te benen door constant de nieuwste middelen te gebruiken. Er wordt wel geïnvesteerd in deze middelen.

3.3 Consequentie huidige wetgeving voor Digitale Recherche

Het lukt het cybercrimeteam wel om bewijs te vergaren op grond van de huidige wetgeving, maar het zou veel makkelijker en sneller kunnen geschieden als er een bijzondere wet bestond. Zij moeten momenteel fysiek aanwezig zijn om de gegevensdragers van de verdachte in beslag te nemen voor de bewijsvergaring. Burgers krijgen nu wel de mogelijkheid om digitaal bewijs via een bepaald Whatsappnummer op te sturen naar de Digitale Recherche. Enkele van de gevolgen van de huidige wetgeving zijn:

1. Het team kan niet aan online infiltratie doen, terwijl deze vorm van bewijsvergaring zeer effectief is.

2. Het team heeft de bevoegdheden niet om snel een computer van een pedofiel of hacker te hacken om informatie veilig te stellen.

3. Het team kan serviceproviders niet wettelijk verplichten snel informatie aan de hun te verschaffen, waardoor zij maandenlang wachten op informatie.

[67] Interview Melvin Pinas, Hoofd Digitale Recherche, 30 april 2021.

4. Elke keer als zij op een ander manier eraan komt dan het wetboek van Strafvordering aangeeft, wordt deze vernietigd, omdat het onrechtmatig verkregen bewijs is. Advocaten zijn het meest hierop gefocust bij cybercrime cases, omdat zij op deze manier de verdachten kunnen helpen. Zij gaan altijd op zoek naar de vormfouten.

5. Het team kan niet via een online chatbox contact leggen met een verdachte om bewijs te vergaren.

6. Het observeren is een bijzondere opsporingsbevoegdheid waarbij de politie zaken, plaatsen, personen en gebeurtenissen waarneemt. Dit zou stelselmatig kunnen plaatsvinden, maar het is vooralsnog niet mogelijk in Suriname.

7. Het systematisch verzamelen van informatie met behulp van een software mag ook niet

8. Real time vergaring van cybercrime is hierdoor ook niet mogelijk

Het cybercrimeteam onderschrijft het belang van het Cybercrimeverdrag, omdat zij weten dat cybercrime grensoverschrijdend is. De samenwerking met andere landen is van eminent belang, maar zij geven prioriteit aan een bijzondere wet op nationaal niveau die hen meer armslag in hun werk zal bieden.[68] Daarna kan Suriname zich op hoger niveau richten op het Cybercrime-Verdrag. Mijn mening hierover is dat zij eerst met andere landen bespreken welke de belangrijke bepalingen zijn ten aanzien van opsporingsbevoegdheden in verband met cybercrime en dan pas overgaan tot het maken van de wet, zodat de wet juridisch correct in elkaar wordt gezet.

[68] Interview Melvin Pinas, Hoofd Digitale Recherche, 30 april 2021.

Conclusie

In dit onderzoek is gezocht naar een antwoord op de vraag: **Voldoet de manier van bewijsvergaring bij cybercrime door de politie in Suriname aan de vereisten die opgenoemd zijn in het Cybercrime-Verdrag?** Hiervoor is een kwantitatief onderzoek uitgevoerd naar de manier van bewijsvergaring door de politie bij het cybercrimeteam.

De meeste relevante bepalingen voor het digitaal speurwerk zijn in het Surinaams Wetboek van Strafvordering opgenomen. Volgens het cybercrimeteam is het Surinaams Wetboek van Strafvordering in tegenstelling tot het Surinaams Wetboek van Strafrecht niet voldoende om cybercrime aan te pakken, omdat de spelregels opgenomen moeten worden in een speciale wet waarbij opsporingsbevoegdheden van de politie bij cybercrime zijn vastgesteld. Het toepassen van de klassieke artikelen lukt wel, maar zij zouden meer successen boeken met een speciale wet, zodat de politie meer armslag heeft om de criminelen op te sporen en aan te houden.

Het cybercrimeteam kan momenteel bijvoorbeeld niet online infiltreren of gegevensdragers van verdachten hacken om bewijs te vergaren. Zij moeten eerst op een bepaalde plek fysiek aanwezig zijn om beslag te leggen op gegevensdragers om zodoende bewijs te vergaren. De Digitale Recherche stelt daarom voor dat Suriname eerst werkt aan deze speciale wet alvorens zij grijpen naar het Cybercrime-Verdrag. De vereisten die in het Cybercrime-Verdrag zijn opgenoemd zijn opsporingsbevoegdheden c.q. het vergaren van bewijs bij cybercrime. Indien Suriname nog geen speciale wet heeft die de opsporingsbevoegdheden van de politieambtenaren bij het opsporen van cybercrime regelt om bewijs te vergaren, kan er geconcludeerd worden dat de bewijsvergaring van cybercrime door de Surinaamse politie niet voldoet aan de vereisten opgenoemd in het Cybercrime-Verdrag.

Bronvermelding

Literatuur:

- **Boekhoorn 2019**
  P. Boekhoorn, *De aanpak van cybercrime door de regionale eenheden van de politie. Van intake van cybercrime naar opsporing en vervolging*, Den Haag: Politie & Wetenschap 2019.
- **De Poot, Lievens & Stol 2020**
  C. de Poot, E. Lievens, W. Stol, *Politie en Cybercrime*, Antwerpen: Gompel&Scavina 2020.
- **Kruisbergen, Roks & Kleermans 2019**
  E.W. Kruisbergen, R. A. Roks, E.R. Kleermans, *Georganiseerde criminaliteit in Nederland: daders, verwevenheid en opsporing: Rapportage in het kader van de vijfde ronde van de monitor Georganiseerde Criminaliteit* (Cahier; Vol. 2019, No.17) WODC 2019.
- **Leukfeldt, Domenie & Stol 2009**
  E. Leukfeldt, M. Domenie, W. Stol, *Verkenning cybercrime in Nederland 2009*, Den Haag: Boom Juridische uitgevers 2009.
- **Vermeulen 2007**
  G. Vermeulen, *Privacy en strafrecht. Nieuwe en grensoverschrijdende verkenningen*, Antwerpen: Maklu Uitgeverij 2007.

Internet

- Belangrijke Surinaamse website gehackt door Anonymous, geraadpleegd 1 april 2021 via, https://www.google.com/s/amp/s/amp.nos.nl/artikel/2144890-belangrijke-surinaamse -websites-gehackt-door-anonymous.html
- Cybercrime in Suriname steeds agressiever, geraadpleegd 18 maart 2021 via, https://www.starnieuws.com/index.php/welcome/index/nieuwsitem/56648
- Cybercrimi's & cryptonaken, geraadpleegd 28 februari 2021 via, https://economie.rabobank.com/publicaties/2018/oktober/cybercrimis-en-cryptoknaken/

- De aard en aanpak van georganiseerde cybercrime, geraadpleegd 1 april 2021 via, https://www.bjutijdschriften.nl/tijdschrift/justitieleverkenningen/2018/5/JV_0167-5850_2018_044_005_002/fullscreen
- Dit is de impact van cybercrime (op uw organisatie), geraadpleegd 14 februari 2021 via, www.kpn.com/zakelijk/blog/de-impact-van-cybercrime.html
- Naar een interventie tegen geldezels: Een pilot in de gemeente Haarlem, geraadpleegd 1 april 2021 via, https://dehaagsehogeschool.nl
- Ransomeware: voorkom dat u het volgend slachtoffer wordt, geraadpleegd 14 februari 2021 via, https://ict-as.sr/ransomware-voorkom-dat-u-het-volgende-slachtoffer-wordt/
- Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, geraadpleegd 1 april 2021 via, Wikipedia.nl.
- Voorkom dat u het volgend slachtoffer wordt, geraadpleegd 28 februari 2021 via. https://m.starnieuws.com/index.php/welcome/index/nieuwsitem/58626

Jurisprudentie:

- Rb. Rotterdam, 3 juli 2019, ECLI:NL:RBROT:2019:5339.
- Rb. Midden-Nederland, 26 augustus 2020, ECLI:NL:RBMNE:2020:3467.

Orale bronnen

Melvin Pinas, Hoofd Digitale Recherche, 30 april 2021.