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: Esseboom Jennifer Shavida

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, 6-11-2022, Paramaribo

Handtekening Esseboom

ANTON DE KOM UNIVERSITEIT VAN SURINAME

Faculteit der Juridische Wetenschappen

DE STRAFRECHTELIJKE VASTSTELLING VAN DADERSCHAP EN DEELNEMING BIJ CYBERCRIMINALITEIT

Thesis ter verkrijging van de graad van Master of Laws (LLM)

Master Surinaams Recht

Esseboom Jennifer

Begeleider: Mr. J. Kasdipowidjojo

Paramaribo, november 2022

Inhoudsopgave

Voorwoord

De thesis die voor u ligt is ter afsluiting van mijn twee jarige masteropleiding Surinaamsrecht aan de Anton de Kom Universiteit van Suriname dat verdedigt dient te worden. Hierbij heb ik als onderwerp gekozen het leerstuk van daderschap en deelneming bij cybercrime, die tevens zijn grondslag vindt in het strafrecht.

De reden voor de keuze van dit onderwerp is dat Suriname de laatste jaren met name tijdens de covid-pandemie geconfronteerd is geraakt met het fenomeen cybercrime. Tijdens de covid periode is men genoodzaakt geweest van huis uit te werken vanwege het feit dat men niet zomaar naar buiten mocht. Men moest hierdoor met het internet te werk gaan en vele zaken online volgen zodat men veilig bleef. Dit heeft natuurlijk met zich meegebracht dat cybercriminelen hun slag zijn gaan slaan voor welk rede dan ook. Omwille daarvan wil ik met mijn thesis de bewustwording creëren naar de Surinaamse autoriteiten en de samenleving ten aanzien van cybercrime.

Hierbij wil ik mijn welgemeende dank uitbrengen aan een ieder die een bijdrage heeft geleverd aan de totstandkoming van deze thesis. Een bijzondere dank gaat uit naar mijn begeleider Mr. J. Kasdipowidjojo, mijn mede-beoordelaars mr Rathipal en mr Chote en mijn dierbare ouders voor de steun en motivatie gedurende mijn studie.

Esseboom Jennifer
Paramaribo, november 2022

Lijst van afkortingen

Art	Artikel
DDoS	Distributed Denail of Service
HR	Hoge Raad
KPS	Korps Politie Suriname
NSr	Nederlands Wetboek van Strafrecht
Sr	Surinaams Wetboek van Strafrecht

Inleiding

Het jaar 2019 heeft zich internationaal gekenmerkt als het jaar van de cybersecurity crises. Enkele grote hacks, het kraken van computers, hebben zich voorgedaan waarbij privé data van miljoenen mensen is onderschept. Ook Suriname is niet bespaard van deze vorm van criminaliteit. Hackers maken voortdurend gebruik van nieuwere methoden om toegang te krijgen tot informatie, bijvoorbeeld door het plaatsen van *data breaches*, *exploits*, *backdoor hacks*, *supply-chain attacks* en dergelijke. Uit onderzoek blijkt dat Surinaamse hackers, soms uit verveling of nieuwsgierigheid, sommigen in opdracht van bepaalde lokale (politieke) organisaties bezig zijn om op een oneigenlijke manier informatie te verzamelen. Dit is aan te merken als computercriminaliteit, cybercriminaliteit of cybercrime. Dit is criminaliteit met ICT als middel en doelwit. Voor deze thesis zal gebruik worden gemaakt van het begrip cybercrime. Deze hackers zijn cybercriminelen die onder de categorie *black hat* hackers vallen. De privacy wordt geschaad en de veiligheid kan in gedrang komen. Door dit fenomeen dreigt nu een sneeuwbal effect te ontstaan. Burgers, financiële organisaties, bekende Surinaamse nieuwssites, Facebook pages, een nummer om dataplan of internet op je mobiel te activeren, regeringsfunctionarissen en anderen zijn slachtoffer van deze *black hat hackers* en hun opdrachtgevers. Sommige slachtoffers weten het, anderen niet.[1]

Met de huidige ontwikkelingen van cybercriminaliteit tijdens de Covid periode, komt het leerstuk van daderschap en deelneming ter sprake. Over deze onderwerpen is er voldoende geschreven.[2] Thans komt aan de orde in deze thesis op welke wijze invulling gegeven zal worden aan het leerstuk van daderschap en deelneming in het kader van cybercrimes oftewel computercriminaliteit. Bij deze nieuwe vorm van criminaliteit blijkt namelijk dat er een verwevenheid bestaat tussen de daders en de deelnemers. Centraal in deze thesis staat dus de vraag wie als dader en wie als deelnemer van het strafbare feit moet worden aangemerkt.

Daarnaast is door de vereiste van dubbel opzet bij deelneming het culpoos meewerken aan het vergroten van de schade veroorzaakt door cybercrime straffeloos. Dit onderzoek heeft dus mede

[1] 'Cybercrime in Suriname steeds agressiever', starnieuws.com 4-5-2022.
[2] 'Europol: grote toename cybercrime door coronavirus', rtlnieuws.nl 4-5-2022.

als doel om na te gaan of in het Wetboek van Strafrecht hiervoor een regeling kan worden getroffen.
Naar aanleiding van het bovenstaande is de volgende probleemstelling geformuleerd:
'Wat is de grondslag voor het vaststellen van daderschap en deelneming volgens het strafrecht bij cybercrime?'

Ter beantwoording van de probleemstelling zijn de volgende deelvragen geformuleerd:
1 Wat houdt daderschap in?
2 Welke deelnemingsvormen zijn er?
3 Wat houdt cybercrime in en welke vormen zijn daarvan te onderscheiden?
4 Op basis waarvan en op welke wijze in het strafrecht wordt de dader van cybercrime aangemerkt als een pleger of deelnemer van het strafbare feit?

Onderzoeksmethode

Dit onderzoek zal worden gedaan middels literatuur die zijn geanalyseerd op basis van de relevantie van het onderwerp van deze thesis. Daarnaast is ook gebruik gemaakt van rechtsbronnen zoals de Surinaamse wet- en regelgeving en jurisprudentie. Bij de jurisprudentie zijn Surinaamse maar ook Nederlandse vonnissen geanalyseerd. Bij de Nederlandse uitspraken wordt dan verwezen naar de uitspraken van de Hoge Raad en rechtbanken. Tenslotte zal ook een interview worden afgenomen met een Officier van het Openbaar Ministerie en een politie ambtenaar van de afdeling Digitale Recherche, waarbij zal worden nagegaan op welke wijze cybercrime wordt aangepakt.

Wetenschappelijke relevantie

Bij de start van dit onderzoek is duidelijk geworden dat de kans op opsporing en vervolging van cybercriminelen klein is. Dit omdat het bewijs van opzet dikwijls een probleem is. Het is van belang dat hackers en opdrachtgevers die zich schuldig maken aan cybercrime, zij die onbewust meewerken aan het verder verspreiden van informatie en daarmee schade kan veroorzaken effectief aangepakt moeten worden oftewel strafbaar gesteld moeten worden. Hierdoor kunnen een groot aantal opsporingsmiddelen worden ingezet ten behoeve van tegenhoudmaatregelen door de

daarvoor aangewezen autoriteiten. Doch is het verder aanpassen van de wetgeving de beste manier een criminele fenomeen aan te pakken. Dit onderzoek moet ertoe leiden dat middels aanpassing van de wet-en regelgeving het mogelijk wordt gemaakt om het daderschap achter cybercriminaliteit concreter vast te stellen, waardoor het mogelijk wordt om een strafvervolging in te stellen tegen deze personen. Hierbij zal gebruik worden gemaakt van de bestaande jurisprudentie met betrekking tot daderschap en deelneming en daarbij zal op basis van de criminaliteitsvormen van cybercrime de deelnemers worden geïdentificeerd.

Maatschappelijke relevantie

Dit onderzoek moet de maatschappij bewust maken over wat de schade is die cybercrime teweeg kan brengen. In bedrijven kan het leiden tot financiële verlies en erger. Bij de normale burger kan het leiden tot verlies van imago. De kennis en expertise moet er zeker zijn om dit probleem op te losse, maar het op tijd trekken aan de bel is iets wat in de burger moet worden gekweekt teneinde dit probleem in te dammen. Men moet leren niet te lang te wachten voor het treffen van maatregelen, want hoe langer men wacht hoe meer schade er wordt veroorzaakt ten gevolge van cybercrime. Mensen moeten bewust worden gemaakt dat ze soms onbewust meewerken aan cybercrime activiteiten en zelf ook strafbaar zijn.

Thesis opbouw

In hoofdstuk 1 wordt ingegaan op wat daderschap in houdt en welke vormen daaraan zijn verbonden. In dit hoofdstuk wordt ook het leerstuk deelneming ter sprake gebracht.
In hoofdstuk 2 zal besproken worden wat cybercrime inhoudt en welke vormen daarvan te onderscheiden zijn.
In hoofdstuk 3 zal uitgewerkt worden hoe men de daderschapsvorm en de deelnemingsvorm van een cybercrime delict vaststelt volgens het strafrecht.

Het geheel wordt afgesloten met een conclusie gevolgd door enkele aanbevelingen.

1 Het leerstuk daderschap

1.1 Algemene aspecten van daderschap en deelneming

Daderschap wordt in het Surinaams Wetboek van Strafrecht omschreven als: "zij die het feit plegen, zij die het feit doen plegen, zij die het feit medeplegen en zij die het feit opzettelijk uitlokken".[3] Ten aanzien van deelneming aan strafbare feiten maakt de wet een onderscheiding tussen daders en medeplichtigen. Bij medeplichtigheid gaat het erom dat personen anderen opzettelijk behulpzaam zijn bij en of opzettelijk inlichtingen of middelen verschaffen tot het plegen van één of meer misdrijven. Conform art 72 Sr is daderschap van toepassing, op zowel misdrijven als overtredingen, terwijl medeplichtigheid inzake art 73 Sr alleen toepasselijk is op misdrijven. Van deelneming is er alleen sprake bij gelijktijdige oftewel simultane of voorafgaande betrokkenheid bij het gronddelict, dus vóór of bij het plegen van het strafbare feit.[4] Deelneming na afloop van het strafbare feit levert veelal bijzondere delicten op zoals bijv. het witwassen van uit misdrijf verkregen gelden. Medeplichtigheid wordt niet zo zwaar afgestraft als daderschap. De wetgever ziet medeplichtigheid, als een minder ernstig deelnemingsvorm in vergelijking met daderschap.[5] Er zal niet worden ingegaan op daderschap van rechtspersonen, vanwege de relevantie van deze thesis. In dit onderzoek zal de nadruk hoofdzakelijk worden gelegd op het leerstuk daderschap en deelneming van natuurlijke personen.

1.2 De daderschapsvormen in het strafrecht

In het strafrecht geldt dat niet alleen degene die alle bestanddelen van een delict vervullen strafrechtelijk aansprakelijk zijn, maar ook degene die in mindere mate een aandeel aan dat delict heeft, kunnen onder bepaalde omstandigheden strafrechtelijk vervolgd worden. De handeling wordt bepaald door het type delict, de manier waarop de handeling in de delictsomschrijving is verwoord en de context waarin het delict zich afspeelt.[6]

[3] Art 72 Sr.
[4] De Hullu 2002, p.407.
[5] Rozemond 2011, p.155.
[6] De Hullu 2002, p. 149.

Art 72 Sr stelt dat als daders van een strafbare feit worden aangemerkt: '*zij die het feit plegen, zij die het feit doen plegen, zij die het feit medeplegen en zij die het feit opzettelijk uitlokken'*.

1.2.1'Plegen' als daderschapsvorm

De daderschapsvorm 'plegen' houdt in zij die het feit plegen en die zelf al de bestanddelen van het delict vervullen, dus degene die het feit materieel en persoonlijk, met of zonder rechtstreekse medewerking van anderen pleegt. Onder plegen wordt mede begrepen een fysieke handeling plegen, doch hoeft het niet zo te zijn. Ook het niet zelf plegen van een handeling of een nalaten kunnen als 'plegen' worden gekwalificeerd.[7]

In het IJzerdraad arrest heeft de HR de criteria geformuleerd waarmee bepaald kan worden of de gedraging van de ene (natuurlijke) persoon aan de andere (natuurlijke) persoon kan worden toegerekend.[8] In deze zaak ging het erom dat een eigenaar van een exportbedrijf (een eenmanszaak) vervolgd werd, omdat het aanvraagformulier voor uitvoervergunningen voor het transporteren van ijzerdraad naar Finland valse gegevens bevatte. De eigenaar van de eenmanszaak had de gegevens laten invullen door zijn exportmanager. De vergunning is vervolgens verstrekt, waardoor er bijkans 90 ton ijzer naar Finland kon worden uitgevoerd. De vraag die in dit arrest centraal stond was, of de niet feitelijk handelende eigenaar van de eenmanszaak een strafbaar feit had gepleegd, nu de handelingen opzettelijk waren verricht door de exportmanager. De Hoge Raad besliste dat: "...handelingen zoals dergelijk in strijd is met de wet. Het invullen van die formulieren en doen toekomen van die formulieren aan de Dienst van In-en Uitvoeren van goederen, slechts aangemerkt mag worden, als gedragingen van de verdachte, indien de verdachte erover mocht beschikken. Als die handelingen al dan niet plaats vonden, en deze behoorden tot de zodanige, welke plaatsvinden blijkens den loop van zaken door verdachte werd aanvaard of placht te worden aanvaard". De hiervoor geformuleerde eisen van 'beschikken' en 'aanvaarden' zijn bekend geworden als de ijzerdraad criteria. Het eerste ijzerdraad criterium, is het beschikkingscriterium, houdt in het hebben van feitelijke zeggenschap. Dit duidt een feitelijke hiërarchische relatie aan tussen de functionele dader en zijn ondergeschikte, waarbij er geen sprake hoeft te zijn van een formele zeggenschapsrelatie. De literatuur beschrijft dit als een zekere macht over anderen,

[7] De Hullu 2002, p. 149.
[8] HR 23 februari 1954, NJ 1954/378.

waarbij de functionele dader verantwoordelijk is voor de gedragingen van die ander. Het tweede ijzerdraad criterium, is het aanvaardingscriterium die een zekere bewustzijn impliceert en acceptatie van de functionele dader teweeg brengt. Kortom kan een eigenaar van een eenmanszaak niet zonder meer aansprakelijk worden gesteld voor de strafbare gedraging van zijn werknemer. De eigenaar dient onder andere een zekere zeggenschap te hebben over de werknemer en hij dient de strafbare gedraging te aanvaarden.

Ook het Slavenburgcriterium biedt voorwaarden voor het functioneel daderschap.[9]

1. Het eerste vereiste is dat de functionaris 'bevoegd en redelijkerwijs gehouden' moet zijn. De term 'bevoegd' wijst op een zekere beschikkingsmacht of zeggenschap binnen de rechtspersoon.

2. Het tweede vereiste houdt in dat de verdachte maatregelen, ter voorkoming van de strafbare gedraging, achterwege heeft gelaten.

3. Ten laatste dient de functionaris bewust de aanmerkelijke kans te aanvaarden dat de verboden gedraging zich zal voordoen. Uit beide voornoemde criteria vloeit het volgende voort:
    a. Had de verdachte zeggenschap over de gedraging?
    b. Behoorde de gedraging tot gewone bedrijfsvoering?
    c. Werd de gedraging normaliter ook toegestaan?
    d. Waren er maatregelen ter voorkoming daarvan getroffen?

1.2.2 'Medeplegen' als daderschapsvorm

Onder 'medeplegen' wordt verstaan *zij die het feit medeplegen*, het kunnen meerdere personen zijn die gezamenlijk de bestanddelen vervullen. Het gaat om zij die met anderen medewerken om het strafbare feit te vervullen.[10] In het Wormerveerse brandstichting-arrest[11] ging het erom dat twee mannen brand hadden gesticht in een schuur. De rechtsvraag dat hier naar voren kwam was

[9] HR 16 december 1986, NJ 1987/534.
[10] De Hullu 2002, p. 406.
[11] HR 29 oktober 1934, NJ 1934/1673.

of de ene comparant, als medeplichtige of als medepleger gekwalificeerd moest worden, gezien hij bij het plegen van het strafbare feit 'slechts' behulpzaam is geweest door de trap vast te houden en wat hooi aan te reiken, terwijl het de andere comparant was die het vuur had aangestoken. Volgens de Hoge Raad was de kwalificatie 'medepleger', zij overwoog dat er in casu sprake is van een bewuste, nauwe en volledige samenwerking, gelet op de gemaakte afspraken om samen brand te stichten. Het gaat er dus om dat de bijdrage van de medepleger substantieel moet zijn, dus meer moet inhouden, dan slechts enkele hulpverlening. Die gezamenlijke uitvoering vindt in de regel plaats, tijdens het plegen van het strafbare feit. Bepaalde handeling en gedragingen, voor of na afloop van het strafbare feit kunnen eveneens worden opgevat, als bedoelde, bewuste, nauwe en volledige samenwerking.[12] Het medeplegen kan dus worden omschreven als een zekere samenwerking tussen twee of meer personen bij het realiseren van één of meer strafbare feiten. Tot slot kan aangenomen worden dat medeplegen een reden voor strafverzwaring kan zijn. Bijv. in geval van diefstal in vereniging inzake art 371 lid 1 sub 4 Sr.[13] Naast de bovengenoemde voorwaarden kan medeplegen ook worden aangenomen in gevallen, waar de samenwerking ogenschijnlijk niet duidelijk is. In het Brusselse wisselkantoor-arrest kwam dit ter uiting.[14] In dit arrest ging het namelijk om een gewapende overval op een wisselkantoor door twee mannen, waarbij de ene binnen dichtbij de deur bleef staan, terwijl de andere het vuurwapen richtte op het personeel en het geld wegnam. De deelname van de passieve-rover werd ook als medeplegen gerekend. Doordat deelnemingsvormen elkaar kunnen overlappen zijn voor de bewijsvoering van medeplegen (in acht neming van de vereiste bewuste samenwerking) de volgende vragen van belang.[15]:

1. Is er afspraak gemaakt?
2. Heeft er overleg plaatsgevonden?
3. Is er van stilzwijgende overeenstemming gebleken?

Zaken die indicaties kunnen geven op een nauwe samenwerking zijn: de intensiteit van samenwerking, een taakverdeling tussen verdachten, een rol in voorbereiding en of uitvoering van het feit, de aanwezigheid op belangrijke momenten en zich niet distantiëren op geëigende

[12] De Hullu 2002, p. 421-422.
[13] Art 371 lid 1 sub 4 Sr.
[14] HR 25 maart 1975, NJ 1975/270.
[15] HR 25 maart 1975, NJ 1975/270.

momenten. Bijgeval er sprake is van deze elementen, kan dat duiden op medeplegen. Ingeval van niet dan kan dat duiden op medeplichtigheid.

Medeplegen kan ook bij lijfelijk afwezigheid plaatsvinden zoals de HR in het Moord op afstand-arrest[16] en het Containerdiefstal-arrest[17] besliste. In laatstgenoemde gevallen ging het erom dat het genius achter het misdrijf, zelf niet aanwezig was bij de uitvoering daarvan, maar desondanks als medepleger werd veroordeeld, vanwege de bewuste, nauwe en volledige samenwerking. De lijfelijke afwezigheid wordt in contrast met de lijfelijke aanwezigheid gecompenseerd door andere omstandigheden, waardoor de samenwerking zo nauw en volledig werd geacht dat de activiteiten achter de schermen als medeplegen werden aangemerkt.[18]

Zoals eerder opgemerkt houdt medeplegen dus in een gezamenlijke plan, gezamenlijke uitvoering en gezamenlijke delen in het voltooid feit. Dat wat na voltooiing geschiedt blijft buiten algemene bepalingen en wordt geregeld in bijzondere delicten.[19] Zo zijn deelnemen na voltooien of afbreken van een strafbare feit niet strafbaar, tenzij een bijzondere delict de strafbaarstelling van een dergelijk gedrag bevat. Hierbij valt te denken aan diefstal art 370 Sr[20] en heling art 480 Sr.[21]

Voor het medeplegen is gelijkerwijs *dubbel opzet* vereist, welk inhoudt dat de medeplegers opzet op het begane grondfeit moeten hebben en opzet op samenwerking moeten hebben.[22] Culpoos deelnemen is dus niet strafbaar. Als illustratie: D en F sluipen een woning binnen. D wil diefstal plegen, maar F wil brand stichten. Zij hebben elk een ander grondfeit als plan, dus er is in casu geen sprake van dubbel opzet. Indien D en F gezamenlijk de woning binnensluipen met de gedachte om diefstal te plegen, is er sprake van hetzelfde grondfeit en dan wel dubbel opzet. Dubbel opzet is opzet op het samenwerken en opzet op het doel van die samenwerking. Maar dat doel op zich is nog geen strafbaar feit. Het doel van medeplegen is niet het realiseren van een delict, maar het bewerkstelligen van een gedraging, die dan mogelijk een strafbaar feit oplevert.

[16] HR 15 april 1986, NJ 1986/740.
[17] HR 17 november 1981, NJ 1983/84.
[18] De Hullu 2002, p.223-225..
[19] 'Strafbare Deelneming- Römelingh', romelingh.com 5-5-2022.
[20] Art 370 Sr.
[21] Art 480 Sr.
[22] 'Strafbare Deelneming- Römelingh', romelingh.com 5-5-2022.

Zo kan dus een culpoos delict als 'dood door schuld' medegepleegd worden.[23] Ook bij het delict openlijke geweldpleging art 189 Sr moet het gaan om twee of meerdere personen, waarbij deze personen met verenigde krachten (oftewel inspanning) moeten hebben gehandeld. Het vereiste van 'in vereniging' in art 189 Sr en andere soortgelijke delictsomschrijvingen kan, net als het vereiste daarvan in het delict diefstal in vereniging inhouden enige mate van behulpzaamheid.[24] Hieruit afleidend hoef niet iedere deelnemer in gelijke mate betrokken te zijn geweest bij het delict. Bovendien is het zo dat bij medeplegen lijfelijk aanwezigheid geen vereiste is zoals bijv. bij het Containerdiefstal-arrest. In dit arrest is er voor 'twee of meer verenigde personen' of 'met verenigde krachten' wel vereist, dat zij aanwezig zijn op de plek van uitvoering. Die gezamenlijk aanwezigheid geeft juist het ernstige karakter van het delict weer en van die gezamenlijke aanwezigheid gaat een bijzondere dreiging uit naar de slachtoffers.[25]

Het bovengenoemde komt ter uiting in het vonnis van de Rechtbank 's Hertogenbosch.[26] In deze zaak ging het erom dat twee jongemannen het plan hadden beraamd om opzettelijk een aanrijding te veroorzaken, omdat zij zeer waarschijnlijk rekenden op de verzekeringsuitkering. Daartoe stond de tweede verdachte met een personenauto bij een T-kruising te Kraanmeer klaar, terwijl de eerste verdachte op een afstand en een plek, vanaf waar hij overzicht had op bedoelde kruising, eveneens gereedstond. De verdachten hadden telefonisch contact met elkaar, zodat de eerste verdachte zijn comparant kon waarschuwen op welk moment de auto van het slachtoffer bij genoemde T-kruising dicht genoeg genaderd zou zijn. Toen de tweede verdachte het sein kreeg, reed hij met volle vaart de kruising op en botste tegen de auto van het slachtoffer, die zelf ook op een behoorlijke snelheid reed. Ten gevolge van de botsing is het slachtoffer tegen een boom aangekomen, waarna hij kwam te overlijden. De Rechtbank overwoog dat:

'*... Naar het oordeel van de rechtbank is er mitsdien bij de uitvoering van de opzettelijke veroorzaakte aanrijding sprake van een nauwe en bewuste samenwerking tussen medeverdachte en verdachte... Uit de wijze waarop de aanrijding heeft plaatsgevonden blijkt van een planmatige aanpak. Dat naar ervaringsregels een bestuurder van een auto die met een snelheid van 60 km/u van de zijkant door een personenauto wordt aangereden, de controle over het stuur verliest, acht*

[23] Van der Neut 1999, p.106-108.
[24] Art 189 Sr.
[25] Van der Neut 1999, p. 106-108.
[26] RB 's Hertogenbosch 8 december 2011, ECLI:NL:RBSHE:2010:BN9786.

de rechtbank de kans aanmerkelijk, dat bij de door [medeverdachte] opzettelijk veroorzaakte aanrijding de door [slachtoffer] bestuurde auto van de weg zou raken en hard tegen een boom zou botsen. Naar algemene ervaringsregels is de kans dat de bestuurder daarbij dodelijk letsel oploopt. De rechtbank is van oordeel dat [medeverdachte] en [verdachte] dat ook wisten. Gelet op de hiervoor genoemde feitelijke omstandigheden—dat zijn namelijk: de aard van de gedraging, die zeer is gericht op het hier bedoelde gevolg, en de omstandigheden waaronder deze is verricht—kan het niet anders, dan dat zij deze kans hebben aanvaard, toen zij de aanrijding planden en veroorzaakten...De rechtbank is derhalve van oordeel dat het voorwaardelijke opzet van de [medeverdachte] en de [verdachte] was gericht op de dood van de bestuurder van de auto waartegen de [medeverdachte] zou zijn aangereden, te weten [slachtoffer]... Het dodelijk letsel waaraan [slachtoffer] is overleden, gelet op hetgeen omtrent het opzet is overwogen, is in redelijkheid toe te rekenen aan [medeverdachte] en [verdachte]. Het niet dragen van een gordel door [slachtoffer] doorbreekt de causale keten tussen de opzettelijke veroorzaakte aanrijding en de dood van het slachtoffer niet. De voorbedachte rade blijkt uit de gedragingen van [medeverdachte] en [verdachte]. [medeverdachte] heeft driemaal getracht een aanrijding te veroorzaken, waarbij hij werd geholpen door [verdachte]. Zowel [medeverdachte] als [verdachte] hebben gedurende die pogingen op meerdere momenten de gelegenheid gehad zich te bezinnen en op het genomen besluit een aanrijding te veroorzaken en zij zijn daarin de laatste maal ook in geslaagd. Al was er kalm beraad, al bedoelden zij een aanrijding te veroorzaken, juridisch handelden zij met de lichtste vorm van opzet op andermans dood. In plaats van de dood echt te beogen, hebben zij, kort gezegd, het aanzienlijke risico daarop bewust op de koop toegenomen..."

In de overweging van de Rechtbank in casu wordt de nadruk gelegd op de nauwe en bewuste samenwerking, het dubbele (voorwaardelijke) opzet en de redelijke toerekening.[27] De Rechtbank veroordeelde de verdachten daarom niet als pleger en medeplichtige, maar als medeplegers van moord.

[27] De Jong 2009, p. 25.

1.2.3 ‘Doen plegen’ als daderschapsvorm

De daderschapsvorm ‘doen plegen’ oftewel zij die het feit doen plegen houdt in degenen die een ander ertoe bewegen om één of meer strafbare feiten te plegen. Het betreft personen die niet persoonlijk, maar door tussenkomst van een ander, een strafbare feit plegen. Daarbij is van belang dat die andere als werktuig wordt gebruikt, vanwege de onwetendheid waarin hij zich verkeert, de dwaling waarin hij is gebracht of het geweld waarvoor hij onderdoet.[28] Hierbij is kenmerkend dat slechts de ‘doen-pleger’ strafbaar is, de pleger is niet strafbaar. Daarbij valt te denken aan iemand die een geestelijke gestoorde of een minderjarig kind een strafbare feit laat plegen. Doen plegen vereist dus straffeloosheid van de uitvoerder, anders kunnen de vereiste uitlokkingsmiddelen worden omzeild, bijv. de melkbezorger die verdunt melk met water levert of een drukker van een drukwerk.[29]

Een voorbeeld van het bovenstaande komt voor uit het Pastoor-arrest.[30] In deze zaak ging het om een pastoor die een schooltje dreef, met leslokalen die waren afgekeurd voor onderwijsactiviteiten aan het aantal kinderen dat daar zangles kreeg. De pastoor werd ten laste gelegd het doen plegen van geven van onderwijs aan teveel kinderen, in daarvoor afgekeurde lokalen. Hier werd gekozen voor het daderschapsvorm ‘doen plegen’, omdat de pastoor zelf geen onderwijs verzorgde, maar daarvoor twee onderwijzeressen in dienst had. De pastoor wist dit met succes aan te vechten. Bij ‘doen plegen’ was het namelijk noodzakelijk dat de pleger een willoos werktuig in handen van de doen-pleger is en de onderwijzeressen konden nu eenmaal niet als willoos werktuigen bestempeld worden. De Hoge Raad stelde de pastoor in het gelijk met de overweging dat ‘doen plegen’ niet van toepassing kan zijn, als degene die het delict pleegt zelf strafrechtelijk verantwoordelijk is. In het Pastoor-arrest werd dus vastgelegd dat voor ‘doen plegen’ de voorwaarde geldt dat degene die de gedraging pleegt, zelf niet gestraft kan worden. De HR meende dat, hoewel het gedrag van de pastoor verwerpelijk was, het tenlastegelegde niet was bewezen. Er was geen sprake van doen plegen, maar van uitlokking, omdat de onderwijzeressen werden betaald.

[28] De Hullu 2012, p. 406.
[29] ‘Strafbare Deelneming- Römelingh’, romelingh.com 5-5-2022.
[30] HR 27 juni 1898, W 1898/7146.

1.2.4 Medeplichtigheid

De medeplichtige neemt ten opzichte van de eerder besproken deelnemers, welke gelijkgesteld worden met de dader, een aparte positie in. Artikel 73 Sr luidt[31]:
Als medeplichtigen van een misdrijf worden gestraft:
1. Zij die opzettelijk behulpzaam zijn bij het plegen van het misdrijf;
2. Zij die opzettelijk de gelegenheid, middelen of inlichtingen verschaffen tot het plegen van het misdrijf.

Een medeplichtige levert slechts een bijdrage aan het misdrijf dat door een ander of anderen wordt gepleegd. Er is dan ook minder betrokkenheid vereist bij het misdrijf. De medeplichtige levert hulp aan, of bevordert de uitvoering van een misdrijf. De medeplichtige speelt daarmee een onderschikte rol, het gaat immers om het strafbare feit van een ander. Dat strafbare feit moet, zoals blijkt uit de wetstekst, een misdrijf zijn. Medeplichtigheid aan een overtreding is niet strafbaar. Voorts valt op dat er een onderscheid is gemaakt tussen het behulpzaam zijn bij een misdrijf (simultane of gelijktijdige medeplichtigheid) en het verschaffen van gelegenheid, middel of inlichtingen ten behoeve van een misdrijf (consecutieve of voorafgaande medeplichtigheid).[32]

Bij medeplichtigheid krijgt de pleger dus hulp aangeboden van de medeplichtige bij het plegen van een misdrijf, die de uitvoering vergemakkelijkt of bevordert. De medeplichtige pleegt het delict dus zelf niet. Medeplichtigheid moet worden afgegrensd van de deelnemingsvormen.

Medeplichtigheid is alleen strafbaar bij een misdrijf en de strafmaat is lager. De lagere strafmaat vloeit voort uit het feit dat een medeplichtige niet wordt aangemerkt, als dader van een strafbaar feit. Medeplichtigheid kan bestaan uit het opzettelijk behulpzaam zijn bij het plegen van een misdrijf of het opzettelijk verschaffen van gelegenheid, middelen of inlichtingen.[33]

Het bereik van de deelnemingsvorm medeplegen is in het verleden steeds ruimer geworden en de grens met de medeplichtige werd daarmee onduidelijker. Daar is met het overzichtsarrest uit 2014

[31] Punwasi 2019, p. 287.
[32] Punwasi 2019, p. 287.
[33] Punwasi 2019, p. 287.

een einde aangekomen. De Hoge Raad heeft aandachtspunten benoemt, waarmee de bewuste en nauwe samenwerking kan worden vastgesteld. De grens met medeplichtigheid is daarmee iets inzichtelijker geworden. Medeplegers treden in de eerste plaats op als min of meer gelijkwaardige participanten. Hun materiële of intellectuele bijdrage aan het delict is daarin van gelijkwaardige betekenis. De medeplichtige en de pleger hebben daarentegen juist geen gelijkwaardige verhouding. De medeplichtige speelt een ondergeschikte rol. Het onderscheid tussen de medepleger en medeplichtige, is onder andere van belang voor de op te leggen straf. Medeplichtigheid kent een lager strafmaximum. Medeplegen levert vaak juist een strafverzwaringsgrond op. Daarnaast is medeplichtigheid alleen strafbaar, als het een misdrijf betreft. Als de gedragingen van de deelnemer in verband gebracht kunnen worden met medeplichtigheid, dan zal de rechter nauwkeurig moeten motiveren waarom er toch sprake is van medeplegen. Bij het oordeel dat, dan sprake is van een bewuste en nauwe samenwerking, kan onder andere rekening gehouden worden met de intensiteit van de samenwerking, de onderlinge taakverdeling en de rol bij de uitvoering of de afhandeling van het strafbare feit.[34]

1.2.5 'Uitlokken' als daderschapsvorm

Onder 'uitlokking' oftewel zij die het feit opzettelijk uitlokken kan worden verstaan degene die een ander ertoe bewegen om één of meer strafbare feiten te plegen door middel van één of meer van de uitlokkingsmiddelen. Deze uitlokkingsmiddelen zijn in art 72 Sr limitatief opgesomd als[35]:

- Giften
- Beloften
- Misbruik van gezag
- Geweld
- Bedreiging
- Misleiding
- Door het verschaffen van gelegenheid
- Middelen
- Inlichtingen of een ander feitelijkheid

[34] 'Strafrecht- Specialisten in Strafrecht', fzadvocaten.nl 5-5-2022.
[35] Art 72 Sr.

Deze uitlokkers worden ook wel de auctores intellectuales oftewel de intellectuele daders genoemd.[36] Net als bij doen-plegen gaat het bij uitlokking erom dat een ander wordt bewogen om een strafbaar feit te plegen. Om van een voltooide uitlokking te spreken, is in de regel vereist dat het uitgelokte strafbare feit daadwerkelijk wordt gepleegd door de uitgelokte. Het succesvol aanzetten van de uitgelokte alleen is dus niet voldoende. Ter illustratie: Wim vraagt Jan om Kees te vermoorden en belooft hem daarvoor een bepaald bedrag. Jan gaat akkoord daarmee en vermoord Kees daadwerkelijk en ontvangt het geld van Wim. In casu is Wim de uitlokker, Jan is de uitgelokte en het geld is het uitlokkingsmiddel. Er zijn daarentegen bijzondere strafbepalingen, die in de hoedanigheid van karakter veel weghebben van uitlokking, dan wel doen-plegen, maar waarbij het gevolg niet vereist is; de aanzetting is voldoende om de delictsomschrijving te vervullen. Bijv. opruiing inzake art 177 Sr. [37]

1.3 Het Culpoos deelnemen aan strafbare feiten

Zoals eerder is aangegeven in paragraaf 1.2.2 is het culpoos deelnemen aan strafbare feiten niet strafbaar, vanwege de eis van dubbel opzet bij deelneming. Feitelijk is het wel mogelijk dat iemand door onachtzaamheid meewerkt aan het plegen van strafbare feiten. Een bankmedewerker kan bijvoorbeeld door onachtzaamheid de kluis van een bank openlaten, waardoor anderen met het geld in de kluis vandoor gaan. Deze bankmedewerker is niet strafbaar, omdat hij geen opzet heeft gehad bij het misdrijf.

Bij cybercrime zijn personen die bijvoorbeeld verboden berichten of “fake nieuws” onbewust verder verspreiden niet strafbaar, maar ze werken wel mee aan het misdrijf. Deze gedraging kan de schade die het misdrijf veroorzaakt weldegelijk vergroten. Het is dus van belang dat strafrechtelijk kan worden ingegrepen, als bijvoorbeeld personen onbewust meewerken aan het verder verspreiden van “fake nieuws”. De schuldvorm in deze is namelijk de onbewuste culpa.[38]

[36] De Hullu 2002, p. 406.
[37] Rozemond 2011, p. 153-154.
[38] “Schuld & Verwijtbaarheid in het Straf- en Bestuursrecht”, bijzonderstrafrechtacademie.nl 6-5-2022.

2 Cybercrime

2.1 Begripsomschrijving cybercrime

Onder Cybercrime of computercriminaliteit of cybercriminaliteit wordt doorgaans verstaan misdrijven die met behulp van een computer gepleegd worden.[39] Belangrijk is dat het gebruik van ICT een voorname rol speelt bij het begaan van een misdrijf. Anders gezegd gaat het bij cybercriminaliteit om misdaden gepleegd met Informatie en Communicatie Technologie (ICT), gericht op een ICT. Het strafbare feit wordt dus gepleegd met een computer, smartwatch of tablet, smartphone, dus kortom alles waar een processor in zit. Slachtoffers hoeven geen computer of internet te hebben voor het meemaken van cybercrime.[40] Dit vanwege het feit dat de meeste telefoons en bankpasjes computerchips bevatten die gemanipuleerd kunnen worden. Ook bedrijfssystemen, moderne auto's en chipkaarten zijn vatbaar voor cybercriminaliteit. Zo gebruiken criminelen speciale apparatuur en software voor het plegen van cybercrime.[41] Daarnaast worden, ook de klassieke delicten online gepleegd, middels computercriminaliteit zoals internet oplichting en afpersing via e-mail etc. Cybercrime kan zowel in brede zin, als in enge zin worden onderscheiden[42]:

- Cybercrime in enge zin betreft misdrijven, waarbij computers of netwerken een rol spelen. Er is geen strafbaar feit gepleegd, als het ICT-aspect niet voorkomt. Daarom is dat van essentieel belang.

- Cybercrime in brede zin heeft betrekking op misdrijven die zonder tussenkomst of gebruik van computers en of netwerken gepleegd kunnen worden en nog steeds strafbaar zijn. Hierbij gaat het om traditionele strafbare feiten, waarbij de computer slechts als tool wordt gebruikt om de handelingen te verrichten.

[39] Engelfriet 2016, p. 6.
[40] 'Wat is cybercrime', vraaghetdepolitie.nl 5-5-2022.
[41] ' De Wet Computercriminaliteit: Wat is computercriminaliteit', iusmentis.com 5-5-2022.
[42] ' De Wet Computercriminaliteit: Wat is computercriminaliteit', iusmentis.com 5-5-2022.

Computers of netwerken spelen een vitale rol bij cybercrime in brede zin, als onderdeel van het misdrijf. Dit heeft tot gevolg, dat ook gewone misdrijven onder de categorie zullen vallen die toevallig met de computer gepleegd worden.

Bij het inbreken in een computernetwerk is het gebruik van ICT een voorwaarde, wat inhoudt dat dit niet kan zonder gebruik te maken van computers en netwerken. Ook het verstoren van de werking van een computer, of het vernielen van elektronische gegevens kunnen tot cybercrime gerekend worden.[43]

2.2 De verscheidene vormen van cybercrime

2.2.1 Het verspreiden van een virus

Een virus is één van de bekendste vormen van cybercrime. Dit is een kwaadaardig computerprogramma die zich opslaat in je computer.[44] Het virus wordt verspreid via websites, programma's, USB-sticks, e-mail etc. Deze virus kan gevoelige informatie wissen en het onbruikbaar maken. Het doel van zo een virus hangt af waarvoor het is gemaakt. Virussen kunnen gemaakt worden om bestanden te beschadigen, websites uit de lucht te halen, spam te versturen en geld te stelen.[45]

Dikwijls kunnen virussen niet gestopt worden, omdat het aantal zich in één keer verspreidt en ze zijn moeilijk te herkennen. Antivirusprogramma's vangen maar een deel van de virussen op, dus met antivirusprogramma is de persoon of houder van een pc voor een deel beschermd.[46]

Daarenboven is het mogelijk om te voorkomen dat je een virus programma in je computersysteem krijgt, zodat het risico op het krijgen van virussen wordt verkleind. Dit kan middels enkele manieren te weten[47]:

a) Het installeren van een kwalitatieve antivirusprogramma en het up-to-date houden

[43] Engelfriet 2016, p. 8
[44] 'Welke soorten cybercrime zijn er?', veiliginternetten.nl 5-5-2022
[45] 'Welke soorten cybercrime zijn er?', veiliginternetten.nl 5-5-2022
[46] 'Methodes voor verspreiden van computervirussen en malware', kaspersky.nl 7-5-2022
[47] De Winter 2014, p. 2-5

b) Zoveel mogelijk je computer en softwaresysteem updaten
c) Vermijd het bezoeken van onbekende en onbetrouwbare sites
d) Geen onbekende mails openen, waarbij er twijfels zijn aan de bron
e) Het vermijden van onverantwoord downloaden van files

2.2.2 Phishing

Phishing is één van de bekendste vormen van internetoplichting, waarbij er gebruik wordt gemaakt van e-mails. Criminelen hebben hier toegang tot de persoonlijke gegevens van de slachtoffers of hun bankrekening. De e-mails lijken afkomstig te zijn van een officiële instantie, organisatie of bedrijf bijv. een creditcardmaatschappij, maar de daadwerkelijke afzender is een fraudeur. Dit trachten ze te doen, door het slachtoffer zijn inlog gegevens te laten invoeren. De link geeft het slachtoffer toegang tot een zogenaamde website die vaak genoeg nep blijkt te zijn en in die mate betrouwbaar lijkt.[48] Het openen van een bijlage kan ook problemen veroorzaken. Zo kan er een virus of spyware in je computer geïnstalleerd worden. Deze programma's vangen weer allerlei belangrijke persoonlijke informatie op. Het uiterste voor het hebben van de inlog gegevens van de slachtoffers door de criminelen, is om kennis en macht te krijgen over geld en persoonsgegevens. De naam ontleent zijn betekenis van het feit dat de cybercriminelen 'vissen' naar informatie, waarbij de cybercriminelen hun digitale hengel uitgooien, met name de e-mail en wachten tot een slachtoffer bijt en spelen daarbij op de angsten en emoties van de ontvangers.[49] Dit kan zich voordoen in gevallen, als een achterstallige rekening moet worden betaald, anders krijgt men een boete bij het uitblijven van de betaling. Dit zorgt voor paniek bij de slachtoffers, waardoor ze geneigd zijn in de val van de phishing-mail te trappen.

Doch zijn er een paar manieren om phishing te onderscheiden van echte e-mails zoals:

- Een gerenommeerde bank, creditcardmaatschappij of legitieme instantie vraagt nooit naar persoonlijke gegevens via de mail.
- De bank gaat bij het verzenden van een e-mail haar klant, altijd personaliseren bij de aanhef. Een phishing e-mail doet dat in geen geval.[50]

[48] 'What is phishing?', phishing.org 7-5-2022.
[49] 'What is phishing?', phishing.org 7-5-2022.
[50] 'Neem de juiste maatregelen tegen phishing', interpolis.nl 7-5-2022.

2.2.3 Identiteitsfraude

.

Er komen verschillende vormen van identiteitsfraude voor. Identiteitsfraude is het opzettelijk misbruiken van identificatiemiddelen, zoals persoonsgegevens met de bedoeling daarmee een strafbaar feit plegen. Bij het uitwisselen van informatie is voorzichtigheid vereist bij de burgers, omdat men misbruik maakt van je persoonlijke gegevens, om handelingen voor zichzelf te verrichten. Dit kan digitaal geschieden middels pincodes en inloggegevens. Identiteitsfraude is herkenbaar in gevallen te weten [51]:

1. Het ontvangen van rekeningen of ontvangstbevestigingen, voor goederen of diensten zonder ze te hebben besteld.
2. De persoon ontdekt dat zijn woonadres is veranderd zonder een wijziging te hebben doorgegeven.
3. De persoon geen bankafschriften en andere financiële post meer ontvangt.
4. De persoon brieven en contracten krijgt, waarvan hij/zij niets afweet.
5. Onbekende afschrijvingen en uitgaven staan op de persoon creditcardgegevens of bankafschriften.

Er komen drie typen identiteitsfraude voor:

1. Criminelen vervalsen hun eigen identiteit;
   Dit gebeurt in gevallen, waar de dader zijn eigen persoonsgegevens wijzigt bijv. het veranderen van de geboortedatum op het paspoort. Bij deze vorm van identiteitsfraude loopt men weinig schade op.

2. Criminelen creëren een geheel nieuwe valse identiteit;
   Deze vorm van identiteitsfraude speelt zich merendeels af op het internet. De dader maakt een nep-account op sociale media of een website zoals marktplaats. Het gaat dus om een geheel nieuwe identiteit en niet een gestolen identiteit. De dader doet zich met de nep-account voor als iemand anders, zodat hij ongestraft mensen kan oplichten. Als er aangifte wordt gedaan, wordt de vervolging ingesteld op de niet bestaande (neppe) identiteit, waarbij criminelen vaak ongestraft weg komen met fraude.

[51] 'Hoe herken ik identiteitsfraude', Rijksoverheid.nl 8-5-2022.

3. Criminelen misbruiken de gegevens van iemand anders;

   Deze vorm van identiteitsfraude is de meest gevaarlijke vorm die zich uit in identiteitsdiefstal. De reden hiervoor, is dat een persoon substantiële financiële schade kan oplopen of een strafblad of gevangenisstraf kan krijgen voor iets dat buiten zijn schuld is. Identiteitsdiefstal is het stelen van iemand persoonlijke gegevens door de cybercrimineel, waarbij vervolgens de crimineel zich probeert voor te doen, als de werkelijke bezitter van de persoonlijke gegevens. De crimineel probeert dan slachtoffers op te lichten onder de persoons(werkelijke bezitter) naam of in andere gevallen wordt de persoon (werkelijke bezitter) opgelicht. De crimineel kan soms ook toegang krijgen tot het computersysteem en of diensten van de persoon via het internet, waarbij de persoon betaalgegevens worden buitgemaakt.[52]

2.2.4 DDoS-aanvallen

DDoS oftewel Distributed Denial of Service is een aanval, dat gedaan kan worden vanuit verschillende computers en verschillende locaties. Het wordt gedaan om het servicenetwerk of een website van een bedrijf of organisatie tijdelijk slecht of helemaal onbereikbaar te maken.[53] Deze aanvalshandeling, dat middels botnets gebeurt zorgt ervoor dat de server of servicenetwerk wordt overspoeld met web verkeer. Met behulp van een botnet kan een hacker de geïnfecteerde computer besturen. Hierbij kan het om duizenden computers gaan en dit netwerk van geïnfecteerde computers dat opdrachten van een hacker uitvoert wordt een botnet genoemd.[54] Vervolgens kan zo een botnet worden ingezet om bijv. DDoS-aanvallen uit te voeren. In de volgende paragraaf wordt er besproken wat een botnet precies inhoudt.

2.2.5 Botnet

Het begrip Botnet is afgeleid van de combinatie ‘robot’ en ‘netwerk’ en omvat veel apparaten, waarvan de eigenaren vaak niet weten dat ze geïnfecteerd zijn. Deze apparaten zijn geïnfecteerd

[52] ‘Soorten identiteitsfraude- Rijksoverheid’, rijksoverheid.nl 8-5-2022.
[53] ‘Wat is een DDoS-aanval’, politie.nl 8-5-2022.
[54] ‘Wat is een DDoS-aanval’, politie.nl 8-5-2022.

met het bot-virus en betekent, dus dat de hacker de controle kan overnemen over de geïnfecteerde computer.[55] De persoon die de controle heeft over een bot-netwerk wordt dusdanig een botnet verzamelaar of botmaster genoemd, omdat deze persoon het botnet beheert via een zogenaamde 'command-and-control server'.[56] De hacker kan met zo een server alle computers tegelijk opdrachten laten uitvoeren en kan de persoon op deze manier veel apparaten tegelijk een website laten bezoeken, waardoor de servers van deze website overbelast worden. Dit verschijnsel van overbelasting van een website is een DDos-aanval.[57]

2.2.6 Hacken

Hacken wordt omschreven, als wanneer iemand in een systeem of computers van een ander probeert binnen te dringen, waarbij dit niet altijd technisch en moeilijk hoeft te zijn, het gissen van iemand wachtwoord wordt ook gezien als een vorm van hacken.[58] Er wordt toegang geboden tot iemand computer, bestanden of account. Ondanks dit, moet hacken worden uitgevoerd, waarbij er gebruik wordt gemaakt van geavanceerde software om een account te hacken dat onder andere gebruikt wordt voor internetbankieren. Dit is in dezelfde mate een vorm van hacken, maar niet de enige vorm. Ook bekende cybercrimevormen zoals phishing en het verspreiden van malware in de media worden aangeduid als hacken. Dit omdat het ten doel heeft het toegang krijgen tot data van andere personen. Vaststellend is dat een hacker iemand is die de veiligheidssystemen van computers en netwerken hackt, om op dergelijk manier heimelijk toegang te krijgen tot bestanden, waartoe ze in principe geen toegang zouden mogen hebben. Evenzo is een hacker een persoon die veel technische kennis heeft over computers en computernetwerken, die op een niet-conventionele manier een computer-gerelateerd probleem oplost.[59]

2.2.7 Grooming

Grooming is het lokken van kinderen op digitale wijze. Bij deze vorm van cybercrime doet een volwassene zich voor als een jonger persoon, dan hij of zij werkelijk is en probeert via het internet

[55] 'Wat is een botnet?', politie.nl 10-5-2022..
[56] 'Wat is een botnet?', politie.nl 10-5-2022.
[57] 'Wat is een botnet?', politie.nl 10-5-2022.
[58] 'Wat is hacken? Alles wat u moet weten- AVG', avg.com 10-5-2022.
[59] 'Wat is hacken? Alles wat u moet weten- AVG', avg.com 10-5-2022.

het vertrouwen van minderjarige kinderen te winnen. Deze persoon dwingt het kind seksuele handelingen te plegen voor een webcam.[60]

2.2.8 Skimmen

Skimmen wordt opgevat, als een op onrechtmatige wijze kopiëren van gegevens uit de ATM-machine met behulp van technische middelen.[61] De pinpas gegevens worden illegaal gekopieerd uit de magneetstrip om vervolgens een valse pinpas te maken, wat een groot financiële probleem wordt voor het slachtoffer. Skimmen kan op verschillende manieren plaatsvinden. Er worden voorzetmondjes geplaatst die de pinpas gegevens van de magneetstrip kunnen aflezen, met gebruikmaking van een camera boven de automaat, om de pincode af te kijken. [62]

Vaak genoeg zijn de slachtoffers hiervan niet op de hoogte, maar met de komst van nieuwe technologie is deze vorm van cybercrime aanzienlijk afgenomen. Door de komst van E.M.V-chips hoeven pinpassen niet door een gleuf gestopt te worden, waardoor de kans op het aflezen van de pincode sterk is teruggelopen.[63]

Echter zijn er enkele manieren om het skimmen te voorkomen namelijk[64] :

1. Voorzichtig te zijn met mensen in de buurt die pincodes kunnen aflezen.
2. Het afschermen bij het invoeren van diens pincode.
3. Het gebruik maken van een pinautomaat die binnen de bank is aangelegd, dan eentje die buiten de bank is aangelegd.

2.2.9 Cyberstalking

Cyberstalking houdt in: wanneer een crimineel één of meer slachtoffers doelbewust lastig valt en intimideert, door gebruik making van het internet of andere elektronische middelen. De intentie van de cyberstalker komt naar voren bij zijn ‘stalk’ gedrag, door bijvoorbeeld de verblijfplaats van

[60] ‘Cyber Grooming- ChildSafeNet’, childsafenet.org 11-5-2022.
[61] ‘What is skimming in cybersecurity?’, cyberexperts.com 11-5-2022.
[62] ‘Scams and Safety’, fbi.gov 11-5-2022.
[63] NICC 2008, p. 50.
[64] ‘Web skimming’, abnamro.nl 13-5-2022.

hun slachtoffers obsessief te volgen via social media of e-mails te hacken, om met de contactpersoon van het slachtoffer te communiceren, het vervalsen van foto's of het sturen van afschrikkende privé berichten.[65]

2.3 Het Cybercrime Verdrag

Het Cybercrime Verdrag hierna te noemen 'Het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken', ook het Budapest Verdrag genoemd en staat in het Engels bekend als 'Convention on cybercrime'.[66] Dit is het eerste internationale verdrag van internet en cybercrime, met als doel om cybercrime aan te pakken, door middel van een unanieme samenwerking tussen naties, een harmonisatie van strafvorderlijke bevoegdheden tot het vergaren van elektronisch bewijsmateriaal en het faciliteren van internationale rechtshulp.[67]

In art 1 sub 1 omschrijft het Cybercrime verdrag een 'computersysteem', als een apparaat of een groep van onderling verbonden of verwante apparaten, die op basis van een programma automatisch gegevens verwerken.

Het Cybercrime verdrag neemt drie aspecten in ogenschouw:

1. Het Cybercrime verdrag behelst een lijst van misdaden die elke lidstaat strafbaar moet stellen. Deze misdaden zijn: hacken, de productie, de verkoop en distributie van hackingtools en een uitbreiding van de strafrechtelijke aansprakelijkheid van schendingen van intellectuele eigendom. Deze misdaden zijn omschreven in de art 2-11 van het Cybercrime verdrag.

2. Het Cybercrime verdrag heeft als voorwaarde dat elke deelnemende natie nieuwe bevoegdheden van huiszoeking en inbeslagneming verleend aan wetshandhavingsinstanties. Deze zijn vastgesteld in de art 16-22 van het Cybercrime verdrag.

[65] 'Tips to protect yourself from cyberstalkers', Kaspersky.com 13-5-2022.
[66] Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23-11-2001.
[67] "Cyber Crime en de noodzaak van international verdragen", research.vu.nl 15-5-2022.

3. Het Cybercrime verdrag heeft als derde voorwaarde dat grensoverschrijdend opsporingsonderzoeken worden verricht m.a.w dat de rechtshandhavingsinstanties van elke deelnemend land de politie uit andere deelnemende landen te helpen. Dit is terug te vinden in de art 23 -25 van het Cybercrime verdrag.[68]

Het tweede hoofdstuk van het Cybercrime verdrag omvat de nationale maatregelen, die getroffen moeten worden. Hierbij onderscheidt het Cybercrime verdrag materieel en formeel strafrecht die bestaat uit sectie 1 en sectie 2. In het kader van deze thesis zal alleen het materieel strafrecht worden aangegeven. Het materieel gedeelte is:

- Titel 1: de strafbare feiten tegen de vertrouwelijkheid, integriteit en beschikbaarheid van computergegevens-en systemen. De strafbare feiten, die tevens te vinden zijn in art 2 en 3 zijn onder meer:
    1. onrechtmatige toegang tot
    2. onderschepping van gegevens die geautomatiseerde werken bevatten

- Titel 2: computer gerelateerde strafbare feiten. In deze titel is computer gerelateerde vervalsing van gegevens, dan wel geautomatiseerde werken strafbaar gesteld in art 7 en ten tweede is computer gerelateerde fraude van gegevens en geautomatiseerde werken strafbaar gesteld inzake art 8 van het Cybercrime verdrag.

- Titel 3: dit omvat de strafbare feiten die betrekking hebben op kinderpornografie. Dit is strafbaar gesteld in art 9.

- Titel 4: dit omvat de strafbare feiten die te maken hebben met schendingen van het auteursrecht en de aanverwante rechten. In deze titel zijn strafbare feiten gelinkt aan schendingen van het auteursrecht en de aanverwante rechten strafbaar gesteld op grond van art 10.

[68] Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23-11-2001.

- Titel 5: dit omvat de bijkomende aansprakelijkheid en sancties. De strafbare handelingen in deze titel zijn: poging, medeplichtigheid en deelneming inzake art 11. En art 12 handelt over de aansprakelijkheid van rechtspersonen.

- In art 13 worden sancties en maatregelen genoemd, die door staten moeten worden getroffen, voor de vaststelling van doeltreffende, evenredige en afschrikkende sancties, vrijheidsstraffen en schadevergoeding, ten aanzien van de strafbare feiten genoemd in de art 2 tot en met 12.[69]

2.4 De Wet Computercriminaliteit

Ten aanzien van cybercrime, heeft Nederland in het jaar 1993 de Wet Computercriminaliteit ingevoerd.[70] Bij de oprichting van het Cybercrime verdrag op 23 november 2001 heeft Nederland ter voldoening van de Verdragsvoorwaarden, de Wet Computercriminaliteit moeten bijwerken. De bijgewerkte zaken zijn te weten:

1. Bij computervredebreuk is elke vorm van wederrechtelijk binnendringen strafbaar, ook als daarbij geen beveiliging wordt doorbroken.

2. De definitie van virussen is toegespitst en de maximale straf voor deze delict is gaan verhogen. Een verdachte kan ten gevolge daarvan in voorlopige hechtenis worden genomen. Overigens is er geen grenslimit verbonden, aan de strafbaarheid van cybercrime, waardoor een burger van een lidstaat, waar cybercrime een strafbare feit is, ook strafbaar bezig is als hij/ zij het in een ander land pleegt.

3. Het delict Grooming werd ook uitgebreid inzake art 248 Sr (Ned). Grooming houdt in het door een volwassen persoon via het internet actief benaderen en verleiden van minderjarigen, met als uiteindelijk doel het plegen van seksuele handelingen of het

[69] Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23-11-2001.
[70] Van Bruggen e.a 2002, p. 157.

vervaardigen van kinderpornografisch materiaal met de minderjarige. Hierop staat een strafmaat van ten hoogste twee jaren of een geldboete.[71]

Op grond van het bovenstaande, is de wijziging van de Wet Computercriminaliteit in 2006 tot stand gekomen. Hierna heeft de desbetreffende wet wederom veranderingen moeten ondergaan namelijk[72]:

- Justitie en politie hebben nieuwe bevoegdheden gekregen, om computercriminaliteit beter te bestrijden en het toekennen van hackbevoegdheid voor de opsporingsdiensten.

- Er op afstand door justitie en politiecomputers kan worden binnengegaan, voor de opsporing van ernstige delicten zoals: kinderpornografie, drugshandel of liquidaties.

- De wet biedt overigens de mogelijkheid aan opsporingsambtenaren, om diverse onderzoek handelingen te plegen.

- De opsporingsambtenaren kunnen gegevens ontoegankelijk maken of kopiëren, maar ook communicatie aftappen, zodat de criminelen die zich schuil houden, makkelijker worden opgespoord.
- De opsporingsambtenaren worden als lokpubers ingezet, zodat het de opsporing zowel vervolging van groomers vergemakkelijkt.

- Heling van computergegevens is ook strafbaar gesteld, als zelfstandig delict. Iemand kan worden aangepakt die beschikt over de gegevens van iemand anders, zelf ingeval het niet bewezen kan worden dat de persoon die gegevens op eigen houtje heeft overgenomen.

- Malafide verkopers zijn eveneens strafbaar gesteld die herhaaldelijk goederen of diensten te koop aanbieden en die niet leveren.

[71] Van Bruggen e.a 2002, p. 160.
[72] "Wet Computercriminaliteit III", noraonline.nl op 10-5-2022.

3 Strafrechtelijk vaststelling van daderschap en deelneming bij een cybercrime delict

3.1 De strafbaarstelling van Cybercrime in Suriname

Net als in het buitenland probeert Suriname ook het fenomeen cybercrime aan te pakken, middels de nationale wetgeving. Suriname is vooralsnog geen lid bij het Cybercrime verdrag. Doch poogt de Republiek alles in te zetten om het cybercrime probleem in te dammen, door handelingen strafbaar te stellen in het Surinaams Wetboek van Strafrecht. Misdrijven zoals belaging in de wet Strafbaarstelling Belaging, bedreiging met enig misdrijf tegen het leven gericht inzake art 345 Sr (oud) mede smaad en laster inzake art 320 Sr zijn na de wijziging van het Wetboek van Strafrecht 2015 verbonden aan computercriminaliteit. Deze delicten hebben de strekking dat computergegevens ook aangemerkt kunnen worden als ‘geschrift’.

Artikelen waaruit de daderschap bij cybercrime kan worden afgeleid:

Art 187b tot en met 187j Sr[73]:
Dit artikel bevat verboden gedragingen ten aanzien van de hedendaagse mogelijkheden van misbruik van geautomatiseerde werken. Onderwerpen die te maken hebben met cybercrime zoals hacking art 187b, opwerpen blokkade art 187c, afluisteren van gesprekken art 187d en 187e, afluisteren van telefoongesprekken art 187f, afluisterapparatuur art 187g, doorgeven afgeluisterde gegevens art 187h, heimelijk fotograferen art 187i en 187j.

Art 279 lid 1 sub 7 Sr [74]:
Dit artikel legt het accent op valse betaalpassen of waardekaarten, om de gedachte uit te sluiten dat het vervalsen van deze passen en kaarten en andere kaarten niet strafbaar kan zijn. Hierbij valt te denken aan creditcards, kaarten van winkelbedrijven of van verzekeringsmaatschappijen. Immers gaat het in dit artikel om het vervalsen en het eventuele gebruik van betaalpasjes of waarde kaarten ongeacht er een mogelijke bevoordeling bestaat. De kaarten die voor beperkte kring worden afgegeven, zoals toegangspasjes van bedrijven zijn uitgesloten. In dit gekwalificeerde

[73] Memorie van Toelichting pag. 203.
[74] Memorie van Toelichting pag. 212.

artikel wordt aangeduid dat valsheid in geschriften ook wordt gepleegd, middels geknoei in geautomatiseerde werken.

Artikel 292 Sr [75]:

Deze bepaling belicht een strafmaatregel tegen degene die een afbeelding, een voorwerp of een gegevensdrager met erin een afbeelding vertonen die schadelijk kan zijn voor jeugdigen, oftewel minderjarigen beneden de leeftijd van zestien jaar.

Artikel 293 Sr [76]:

In deze bepaling vindt er een uitbreiding plaats in het kader van kinderpornografie. In dit artikel wordt degene strafbaar gesteld die een afbeelding of een gegevensdrager, met erin een seksuele getinte gedraging aan iemand toont die jonger is dan 18 jaar. Ook de gedraging tot betrokkenheid of schijnbaar betrokkenheid, het verwerven of met behulp van een geautomatiseerd werk of door gebruik making van een communicatiedienst toegang verschaft tot het bezichtigen van seksuele afbeeldingen, wordt strafbaar gesteld.

Smaad, smaadschrift art 320 Sr [77]:

Dit artikel bevat een strafmaatregel tegen degene die iemands eer of goede naam aanrandt die, door middel van beschuldigingen van een bepaalde feit om daaraan ruchtbaarheid te geven. Dit geldt ook voor degene zich schuldig maakt aan smaadschrift, door middel van het verspreiden of openlijk tentoonstellen of aanslaan of ten gehore brengen van geschriften, afbeeldingen of gegevens uit geautomatiseerde werken.

Eenvoudige belediging art 325 Sr [78]:

In dit artikel is bijgevoegd de belediging, door middel van gegevens uit geautomatiseerde werken en de mogelijkheid iemand te beledigen, door het plaatsen van teksten of afbeeldingen op het internet. De weg van directe toezending kan de computer natuurlijkerwijs worden gebruikt.

[75] Artikel 292 Sr .
[76] Memorie van Toelichting pag. 213.
[77] Artikel 320 Sr.
[78] Memorie van Toelichting pag. 214.

Art 326 Sr[79]:

Dit artikel betreft een uitbreiding op art 325 Sr, waar degene strafbaar wordt gesteld inzake belediging gedaan aan het openbaar gezag. In lid 2 zijn de ambtenaren opgenomen en in lid 3 zijn de vertegenwoordigers van bevriende staten extra beschermd.

Lasterlijke aanklacht art 327 Sr[80]:

Dit artikel bevat een strafbepaling voor degene die iemands eer of goede naam werkzaam bij de overheid aantast, door het doen van een valse klacht of een aangifte schriftelijk of met behulp van een geautomatiseerd werk.

Verspreiding beledigend geschrift art 331 Sr[81]**:**

In deze bepaling wordt de gedraging strafbaar gesteld die te maken heeft met de verspreiding, openlijke tentoonstelling of het aanslaan van beledigende of voor een overledene smadelijke geschriften of afbeeldingen of het ten voorraad aanwezig hebben van deze geschriften of afbeeldingen uit een geautomatiseerd werk om verspreid, openlijk tentoongesteld of aangeslagen te worden. In lid 2 wordt het ten gehore brengen van de inhoud van een dergelijk geschrift strafbaar gesteld.

Naast de wetgeving heeft het Korps Politie Suriname in het jaar 2015 de afdeling Digitale Recherche geïmplementeerd en bemenst met als kerntaken:

1 Het veiligstellen en analyseren van beeldmateriaal.

2 Het uitlezen van mobiele telefoontoestellen en het analyseren van de daaruit verkregen data.

3 Het doen van cybercrime onderzoekingen.

4 Het onderzoeken van digitale componenten.

5 Het veiligstellen van beeldmateriaal dat gebruikt zou kunnen worden, ten behoeve van de politie en de justitie.[82]

Uit zekere rapportages komt hacking het meest voor. Men past het toe bij hacken van Facebook profielen, e-mails en bankrekeningen. Phishing en spamming zijn na hacking de twee meest

[79] Memorie van Toelichting pag 214.
[80] Artikel 327 Sr.
[81] Nijboer & Cleiren 2006, p. 1070.
[82] "Bekendmaking>>-Korps Politie Suriname", https//politie.sr 28-8-2022.

voorkomende vormen in de Surinaamse praktijk, digitale dreigementen via WhatsApp of Facebook, Messenger, oplichting via Facebook. Volgens bronnen zijn er geen speciale daders die betrokken zijn bij dit soort criminaliteit. Het zijn veelal jeugdigen van het mannelijk geslacht die heel goed kunnen omgaan met elektronische apparaten en applicaties. Vrouwen maken zich in mindere mate schuldig aan dit soort feiten. Daders hebben geen speciale expertise. Er zijn daders in verschillende typen en soorten. Het zijn wel technische aangelegen daders ongeacht hun vooropleiding.[83] De Digitale Recherche is ook van mening dat de daders slechts gebruikmaken van de mogelijkheden die zo een platform biedt. Volgens de afdeling is niet een ieder ervan bewust dat ze een strafbaar feit begaan of hebben begaan, daarom kan er niet gesproken worden van expertise.[84]

De aanpak van een zaak begint met een aangifte en die aangifte wordt in geschrifte gesteld door de politie. Aan de hand van de zaak of de klacht wat de aangever heeft vermeld, gaat de politie daarop rechercheren.
Indien iemand een spul heeft gekocht via Facebook (al heeft betaald) en nog niks heeft gehad, gaat de politie de dader zijn Facebook profiel checken, ze gaan naar een IP- adres kijken, dus opsporen van digitale apparaten, omtrent de tijden en dagen waar ze in contact zijn geweest en telefoon uitlezen, mast gegevens, wie de advertentie heeft gezien. Hierna wordt het bewijs materiaal verzameld, doormiddel van digitaal technische methodes en worden resultaten verwerkt in een Procesverbaal. Deze worden vervolgens opgestuurd naar het Openbaar Ministerie, door tussenkomst van de onderzoekende afdeling.[85]

Ook zijn er op enkele scholen reeds sessies gedraaid, om de bewustwording bij te brengen. Er zijn thans voorbereidingen met betrekking tot voorlichting aan de gemeenschap omtrent cybercriminaliteit.[86]

De Digitale Recherche bestaande uit Natin studenten en jongens van de technische richting worden getraind, door de buitenlandse Caricom trainingen die half jaarlijks of jaarlijks één keer

[83] Intervieuw met Officier van Justitie mw Rathipal 28-8-2022.
[84] Interview met mr Schaken van de Digitale Recherche 28-9-2022.
[85] Interview met Officier van Justitie mw Rathipal 28-8-2022; interview met mr Schaken van de Digitale Recherche 28-9-2022.
[86] Interview met mr Schaken van de Digitale Recherche 28-9-2022.

terugkerend zijn en dan worden nieuwe technieken besproken, omtrent de wijze van bewijs vergaring.[87]

3.2 Jurisprudentie omtrent cybercrime

Surinaamse situatie

Kantongerecht Parketnummer: 1-1-01957

Vonnisnummer: 21-154 [2e]

Datum uitspraak: 2 maart 2021

Casus:

In onderstaande zaak gaat het om meer dan één verdachte, dan wel deelnemers van strafbare feiten die te maken hebben met cybercrime, waarvan twee verdachten zijn geïdentificeerd en aangehouden door het KPS op aangifte van de Republic Bank Suriname. Er werd al enige tijd door voornoemde bank opgemerkt dat er oneigenlijk opnamen worden gepleegd bij de ATM machines. De Republic Bank Suriname is dan met een onderzoek begonnen, toen er werd geconstateerd dat er meerdere kaarten werden opgenomen door de ATM machines die geen gelijkenissen vertoonden van originele creditkaarten, uitgezonderd het formaat en magnetische strip. De kaarten waren giftkaarten met een magnetische strip, waarop informatie van de creditkaarten worden geprogrammeerd. Na het bekijken van videobeelden is het opgevallen dat steeds vier mannen geregeld afzonderlijk geld opnamen bij verschillende Republic Bank ATM machines. Van de bekeken beelden zijn fotografische opnamen gemaakt, maar niet elk van de daders is ermee geïdentificeerd. Met behulp van het tipgeven door voornoemde bank, heeft de politie gelijk assistentie verleend, twee van de daders op te pakken met de bedoelde pinkaarten. De aan deze zaak verbonden verdachten J.F en A.T werden in verzekering gesteld en gedagvaard om de volgende feiten:

Feit 1

- Het telkens opzettelijk valselijk opmaken en of vervalsen van één of meer bankpassen en of betaalpassen en/ of pinpassen, althans één of meer geschriften, die bestemd zijn of waren om tot bewijs van enig feit te dienen.

[87] Intervieuw met Officier van Justitie mw Rathipal 28-8-2022.

- Het telkens gebruik maken van één of meer valse en of vervalste bankpassen en of betaalpassen en of pinpassen, althans één of meer geschriften, als ware die echt en onvervalst en of het telkens opzettelijk afleveren en of voor handen hebben van één of meer valse en of vervalste bankpassen en of betaalpassen en of pinpassen, althans één of meer geschriften, terwijl hij wist of redelijkerwijs moest vermoeden dat deze bestemd waren om tot bewijs van enig feit te dienen.

- Het telkens met het oogmerk van wederrechtelijke toe-eigening wegnemen van één of meer geldbedragen, althans enige gelden, geheel of ten dele toebehorende aan een ander en of anderen, waarbij de toegang tot de plaats des misdrijf werd verschaft en of het de te weg te nemen gelden onder hun bereik werd gebracht, door middel van een valse sleutel te weten één of meer valse bankpassen en of betaalpassen en of pinpassen.

- Het telkens met het oogmerk om zich en of een ander wederrechtelijk te bevoordelen, door het aannemen van een valse naam en of van een valse hoedanigheid en of door één of meer listige kunstgrepen en of een samenweefsel van verdichtsels. De Republic Bank Suriname heeft bewogen tot de afgifte van SRD2000.000 en of telkens met voren omschreven oogmerk-zakelijk weergegeven-valselijk en of listiglijk en of bedrieglijk en of in strijd met de waarheid zich voorgedaan, als rechtmatige houder van bankpassen en daardoor als gerechtigde tot de desbetreffende bankrekeningen, waardoor voornoemde bank telkens werd bewogen tot bovenomschreven afgifte.

Feit 2

- Het telkens tezamen en in vereniging met J.F, althans één of meer tot nog toe onbekende daders, althans alleen, telkens opzettelijk één of meer betaalpassen en of waarde kaarten, enige andere beschikbare dragers van identiteitsgegevens, bedoeld voor het verrichten of verkrijgen van betalingen en of andere prestaties lang geautomatiseerde weg, te weten één of meer pinpassen of bankpassen en althans betaalpassen valselijk hebben opgemaakt of vervalst, immers hebben verdachte en of zijn mededaders, toen daar telkens opzettelijk valselijk en of in strijd met de waarheid één of meer passen voorzien van gegevens, die door het skimmen/kopiëren van de gegevens van één of meer originele pinpassen of betaalpassen waren verkregen, zulks met het oogmerk zichzelf of een ander te bevoordelen.

Feit 3

- Telkens tezamen en in vereniging met J.F, althans één of meer tot nog toe onbekende daders, althans alleen opzettelijk gebruik heeft gemaakt van valse en of één of meer vervalste betaalpassen en of waarde kaarten en of enige andere voor het publiek beschikbare kaart, bestemd voor het verrichten of verkrijgen van betalingen of andere prestaties langs de geautomatiseerde weg, als ware deze pas of kaart echt en onvervalst, bestond het gebruikmaken hierin dat verdachte en of zijn mededaders met één of meer van deze passen en of kaarten telkens geldbedragen hebben gepind bij geldautomaten van de Republic Bank Suriname en bestond die valsheid of vervalsing hierin dat voornoemde passen zijn voorzien van, middels manipulatieve of fictieve verkregen magneetstrepengegevens en of pincodes.

Feit 4a

- Telkens tezamen en in vereniging met J.F althans één of meer tot nog toe onbekende daders, althans alleen telkens met het oogmerk van wederrechtelijke toe-eigening uit een geldautomaat, vanaf een aantal bankrekeningen heeft weggenomen één of meer geldbedragen tot een totaal van SRD 2000.000 (TWEE MILJOEN Surinaamse dollars), althans een ander bedrag in ieder geval enige gelden geheel of ten dele toebehorende aan de Republic Bank Suriname, in elk geval aan een ander of anderen dan aan verdachte en of zijn mededaders het weg te nemen gelden onder zijn/hun bereik heeft/hebben gebracht, door middel van een valse sleutel, te weten één of meer valse en of vervalste betaalpassen.

Feit 4b

- Telkens tezamen en in vereniging met J.F, althans één of meer tot nog toe onbekende daders, althans alleen met het oogmerk om zich en of een ander(en) wederrechtelijk te bevoordelen, door het aannemen van een valse naam en of van een valse hoedanigheid en of door één of meer listige kunstgrepen en of een samenweefsels van verdichtsels de Republic Bank Suriname heeft/hebben bewogen tot de afgifte van SRD 2000.000 (tweemiljoen Surinaamse dollars), althans enige gelden, immers heeft hij verdachte en of zijn mededaders telkens met voren omschreven oogmerk-zakelijk weergeven-valselijk en of listiglijk en of bedrieglijk en of in strijd met de waarheid zich voorgedaan als rechtmatige

houder(s) van één of meer, daardoor als gerechtigde tot de desbetreffende bankrekening(en), waardoor voornoemde bank werd bewogen tot bovenomschreven afgifte.

De deelneming van de daders bestond uit het al dan niet samen met één of meer andere deelnemers aan die organisatie telkens:

- Het huren en of betalen van één of meer woningen en of voertuigen, althans het zorgdragen voor verblijf en of vervoer in Suriname.

- Zodanige doen bewerken van één of meer kaarten, dat de magneetstrip informatie dragen aan de achterzijde voorzien werd van informatie van één of meer rekeninghouders van de Republic Bank Suriname, althans één of meer kaarten aan te passen tot één of meer bankpassen en of betaalpassen en of pinpassen.

- In ontvangst nemen en of voorhanden hebben van één of meer valse en of vervalste bankpassen en of betaalpassen en of pinpassen, althans één of meer voorwerpen bestemd, voor het plegen van voormelde misdrijven en of

- Met voormelde kaarten en of valse of vervalste bankpassen en of betaalpassen en of pinpassen, althans voormelde voorwerpen opnemen, in ieder geval verwerven van gelden bij geld-of pinautomaten van de Republic Bank Suriname.

Verdachte J.F ontkende in vereniging te hebben samengewerkt met verdachte A.T, terwijl verdachte A.T de bekentenis heeft afgelegd wel in vereniging te hebben gehandeld met verdachte J.F. Verdachte A.T heeft ook de verklaring afgelegd, dat verdachte J.F de pinpassen of betaalpassen opmaakte en aan medeverdachte verstrekte in het plegen van de opnamen bij de ATM machines. De verklaring van verdachte A.T is bekrachtigd door de verhuurder die zijn woonruimte aan beide daders zou hebben verhuurd en vervolgens als getuige heeft gediend in deze zaak.

De kantonrechter achtte feit 1 en 4a niet bewezen, omdat het volgens artikel 188 Sr moet gaan om een gestructureerd en duurzaam samenwerkingsverband van twee of meerdere personen, hetgeen in casu niet is gebleken en verdachten op grond daarvan zijn vrijgesproken. Ook de diefstal zoals feit 4a aangeeft kan niet worden afgeleid bij gebruik van een pinpas bij geldautomaten, omdat niet

is vastgesteld dat de gebruikte pinpassen gestolen waren om geld te pinnen, oftewel van diefstal afkomstig waren. Verdachten zijn op grond van feit 4a ook vrijgesproken.

De kantonrechter achtte wettig en overtuigend bewezen dat de verdachten feit 2, 3 en 4b, aldus hebben begaan met dien verstande dat verdachte J.F en A.T:

- Op één of meer niet nader aan te duiden tijdstippen vanaf januari 2020 tot en met 25 augustus 2020 te Paramaribo tezamen en in vereniging opzettelijk één of meer betaalpassen, bestemd voor het verrichten of verkrijgen van betalingen en anderen prestaties langs geautomatiseerde weg, te weten één of meer pinpassen valselijk heeft opgemaakt. Immers hebben verdachte en zijn mededader toen daar telkens opzettelijk het skimmen/ kopiëren van de gegevens, die originele pinpassen waren verkregen, zulks met het oogmerk zichzelf of een ander te bevoordelen.

- Op één of meer niet nader aan te duiden tijdstippen vanaf januari 2020 tot en met 25 augustus 2020 te Paramaribo tezamen en in vereniging opzettelijk gebruik hebben gemaakt van vervalste betaalpassen bestemd voor het verrichten of verkrijgen van betalingen en andere prestaties langs geautomatiseerde weg, als ware deze passen, echt en onvervalst, bestond het gebruikmaken hierin dat verdachte en zijn mededader met één of meer van deze passen telkens een geldbedrag hebben gepind bij geldautomaten van de Republic Bank Suriname en bestond die valsheid of vervalsing hierin dat voornoemde passen zijn voorzien van middels manipulatieve verkregen magneetstripgegevens.

- Op één of meer niet nader aan te duiden tijdstippen vanaf januari 2020 tot en met 25 augustus 2020 te Paramaribo tezamen en in vereniging met het oogmerk om zich en een ander wederrechtelijk te bevoordelen door het aannemen van een valse hoedanigheid en door één of meer listige kunstgrepen en samenweefsel van verdichtsels. De Republic Bank Suriname heeft bewogen tot de afgifte van SRD 2000.000 (TWEEMILJOEN Surinaamse Dollars). Immers hebben beide daders telkens met voren omschreven oogmerk-zakelijk weergegeven-valselijk en in strijd met de waarheid zich voorgedaan, als rechtmatige houders van één of meer valselijk opgemaakte bankpassen en daardoor als gerechtigde tot

de desbetreffende bankrekening, waardoor voornoemde bank werd bewogen tot bovenomschreven afgifte. [88]

In casu wordt opgemerkt dat er sprake is van de deelnemingsvorm medeplegen. In de bewezenverklaring van de kantonrechter zijn de gronden aangegeven die de deelnemingsvorm bevestigen tussen de verdachten en het strafbare feit skimmen. [89]

Noot: Opmerkelijk in deze twee vonnissen is dat de dader elk afzonderlijk als pleger zijn veroordeeld, omdat duidelijk vaststond dat er sprake was van betrokkenheid van de daders. Hoewel de nauwe en volledige samenwerking niet geheel tot uiting is gekomen kan worden vastgesteld dat er sprake is van deelneming van het misdrijf. Beide daders zijn dus deelnemers van elkaar in het misdrijf, hun betrokkenheid stond wel vast. En deze betrokkenheid was voldoende om beide personen elk apart als pleger te veroordelen. De rechter heeft er niet voor gekozen om ze als deelnemers van elkaar te veroordelen.

Nederlandse situatie

Toxbot-arrest van 22 februari 2011 (DDos-aanval) (ECLI:NL:HR:2011:BN9287):

In deze zaak heeft de verdachte een virus verspreid met de naam “Toxbot”. Dit resulteerde in het infecteren van 50.095 computers en deze vormden samen een botnet die op afstand via een command and control server bestuurd konden worden. Verder had de Toxbot-malware een key-logger-functionaliteit, waarmee toetsaanslagen en ook wachtwoorden konden worden onderschept. De geïnfecteerde computers konden ook worden bestuurd om een bepaalde Trojan (een Wayphisher) te downloaden en te installeren. Na de besmetting met deze nieuwe malware werden de geïnfecteerde computergebruikers omgeleid, naar een andere phishing-site waar hun financiële gegevens werd doorgegeven aan de verdachte die te gelijke tijd, de bestuurder is van de command and control server.

De verdachte werd vervolgd art 161 sexies Sr (Ned). De verdachte had allerlei computers van particulieren geïnfecteerd en dus ervoor gezorgd dat particulieren geen gebruik konden maken van telebankieren, waaronder het uitvoeren van betalingen, omdat ze geen contact kunnen maken met hun eigen bank. Het hof besliste vrijspraak voor de verdachte, omdat de computers van de

[88] Kantongerecht Parketnummer: 1-1-01957.
[89] De Hullu 2002, p. 406.

particulieren waren besmet en niet de computers van de bank. Dit artikel stelt de infectie van computers van de bank strafbaar op grond van lid 1 sub 2.

De Hoge Raad vernietigde de beslissing van het Hof en oordeelt dat het plaatsen van een virus op een computer gekwalificeerd kan worden als computervredebreuk. Daarmee maakt de verdachte zich schuldig aan computervredebreuk en de gekwalificeerde vorm daarvan bedoeld in art 138ab lid 3 Sr (Ned). Het besmetten van computer met bepaalde malware en daarna het misbruiken van die computers via een botnet kan een gekwalificeerde vorm computervredebreuk opleveren met een strafmaat van vier jaar. Volgens de Hoge Raad heeft Art 161 sexies Sr (Ned) het over geautomatiseerde werken, computer van afnemers van diensten zijn hierbij inbegrepen. Er was dus wel sprake van een gemeen gevaar van diensten.[90]

Dit arrest geeft een beeld over de pleger van een strafbare feit gelinkt met cybercrime. In casu is er sprake van de cybercrimevorm DDos-aanval die middels een botnet is gepleegd. De Hoge Raad is ertoe overgegaan het begrip ruim te interpreteren wat onder computervredebreuk mag worden verstaan conform art 161 sexies Sr (Ned).[91]

RB 28 oktober 2021 (ECLI:RBDHA:2021:11813)

Datum uitspraak: 29-10-2021
Datum publicatie: 28-10-2021
Rechtsgebied: Strafrecht
Zaaknummer: 09-039597-21
Soort procedure: Eerste aanleg
Instantie: Rechtbank Den Haag

De verdachte maakte deel uit van een groep die zich veelvuldig bezighield met oplichten via sociale media en phishing. Deze groep ging goed georganiseerd en professioneel te werk en heeft zodoende aanzienlijk grote bedragen van de slachtoffers afhandig gemaakt, door zich voor te doen als familieleden van de slachtoffers of als bankmedewerkers, of door slachtoffers via internetlinkjes om te leiden naar malafide websites om bankgegevens te achterhalen en in te breken

[90] HR 22 februari 2011, ECLI:NL:HR:2011:BN9287.
[91] Art 161 Sr (Ned).

in de internetbankierenomgeving. Daarnaast is misbruik gemaakt van de mogelijkheid tot het krijgen van extra financiële steun van de overheid, vanwege omzetverlies door de coronamaatregelen, door valselijk subsidies voor TVL aan te vragen bij de RVO.

Bij vermeende oplichting is gebruik gemaakt van bankrekeningen van geldezels die door de verdachte zijn geregeld. De verdachte is degene geweest die heeft ingespeeld op de slechte financiële situatie waarin de meeste geldezels zich bevonden en is ook degene die hen heeft misleid om snel geld te verdienen. Uiteindelijk verdiende de verdachte zelf geld eraan en als ze uit paniek contact opnamen vanwege hun geblokkeerde rekening en ze hun kinderen niet meer te eten konden geven, gaf hij aan niet thuis te zijn.

De verdachte stond terecht voor een tal van feiten, waaronder oplichting en cybercrime. Door de bevindingen in het onderzoek is jegens de verdachte de verdenking ontstaan dat hij zich, samen met anderen, heeft beziggehouden met oplichting via sociale media en computervredebreuk. De verdachte heeft bovendien bankpassen en bijbehorende gegevens van personen geregeld via misleidende advertenties op Snapchat.

Dan rijst rechtsvraag : *'Is het handelen van de verdachte aan te merken, als het medeplegen van of de medeplichtigheid aan de oplichtingen en de computervredebreuk?'*

De rechtbank is van oordeel dat het handelen van de verdachte een wezenlijk onderdeel en een onmisbare schakel is geweest in het samenstel van handelingen die de oplichtingen hebben laten lukken. Zonder het contact dat de verdachte legde met geldezels, het verwerven, en doorgeven van alle benodigde informatie en het pinnen van geld kon de opbrengst van de oplichtingen namelijk niet in handen komen van de personen die achter de oplichting zaten. Het contact met de geldezels vond plaats op dezelfde momenten, als waarop de slachtoffers het geld overmaakten naar de rekeningen. Dit impliceerde een zeer nauwe afstemming tussen de verdachte en de medeverdachten die de slachtoffers ertoe hebben bewogen om het geld over te maken.

In onderhavig geval is er sprake geweest van de deelnemingsvorm medeplegen tot het begaan van oplichting, middels cybercrime of computervredebreuk door verdachte. De rechtbank is van oordeel dat er sprake is geweest van een nauwe en bewuste samenwerking tussen verdachte en

medeverdachten. De handelingen van de verdachte waren volgens de rechtbank een dusdanig gewicht dat deze de medeplichtigheid overstegen. Medeplichtigheid is het slechts behulpzaam zijn bij het verrichten van een misdrijf zonder enige betrokkenheid en dat was in bovenstaande casu niet het geval.[92]

Arrest RB 2 oktober 2015 (ECLI:NL:RBROT:2015:7044)

Datum uitspraak: 2-10-2015
Datum publicatie: 2-10-2015
Rechtsgebied: Strafrecht
Zaaknummer: 10/960012-14
Soort procedure: Eerste aanleg-meervoudig
Zittingsplaats: Rotterdam
Instantie: Rechtbank Rotterdam

In casu heeft verdachte zich samen met anderen schuldig gemaakt aan een grootschalige en langdurige criminele activiteiten die opvallen, door professionaliteit, geraffineerdheid en de intensieve soms zelfs ook internationale-samenwerkingsverbanden.

Via een zo geheten botnet werden een groot aantal computers geïnfecteerd met malware. De malware was op maat gesneden en bestond uit webinjects, waardoor computergebruikers een ogenschijnlijk authentieke website van hun bank getoond werd, terwijl dat in werkelijkheid een bijna niet van echte te onderscheiden valse site was. De daders konden hierna beschikken over alle door de rekeninghouders ingevoerde gegevens. Daarnaast werden mobiele telefoons op maat gesneden. Het ging hier om de software genaamd Perkele. Deze software stelde de daders in staat om alle binnenkomende sms-berichten op die telefoons onzichtbaar te maken en vervolgens door te sluizen naar hun werktelefoons. Dit was een belangrijke stap die TAN-codes bevatte en noodzakelijk waren om banktransacties uit te voeren.

De daders waren in staat onbevoegd toegang tot de bankrekeningen te verschaffen om vervolgens daaruit geld over te maken. Zij hebben verschillende methoden toegepast om hun eigen rol zoveel

[92] RB 28 oktober 2021, ECLI:RBDHA:2021:11813.

mogelijk te maskeren. De daders hadden tegenover de banken een valse identiteit gepresenteerd om zo op die naam een bankrekening met bijbehorende producten zoals pinpassen te verkrijgen. Om de oplichting te laten slagen werd gebruik gemaakt van legitimatiebewijzen al dan niet in combinatie met andere documenten die soms ook waren vervalst. Echter heeft de verdachte hier niks van aangetrokken en heeft uitsluitend oog gehad voor zijn eigen financieel gewin.

De rechtbank heeft een kortere gevangenisstraf opgelegd voor de verdachte inzake medeplichtigheid voor het vervaardigen van malware ter vergemakkelijking van de te verrichte misdrijven, gekwalificeerde computervredebreuk en nog andere bijkomende feiten.[93]

In het onderhavig geval wordt er opgemerkt dat op de deelnemingsvorm medeplichtigheid geen zware straf wordt opgelegd mede door de aard ervan. Zoals tevoren te kennen is gegeven in dit onderzoek is medeplichtigheid slechts het behulpzaam zijn ter bevordering of vergemakkelijking van een te verrichte misdrijf.[94]

[93] RB 2 oktober 2015, ECLI:NL:RBROT:2015:7044.
[94] 'Strafrecht- Specialisten in Strafrecht', fzadvocaten.nl 5-5-2022.

Conclusie

Als antwoord op de probleemstelling: **“Wat is de grondslag voor het vaststellen van daderschap en deelneming volgens het strafrecht bij cybercrime?”.** Kan het volgende worden geconcludeerd.

Deelnemers kunnen als daders worden gestraft, indien het betreft de deelnemingsvormen medeplegen, doenplegen en uitlokken. Daarnaast kunnen deelnemers, ook als medeplichtigen worden aangemerkt en krijgen minder straf. De grondslag voor het vaststellen van daderschap en deelneming bij cybercrime is betrokkenheid. Daarbij kan elke vorm van betrokkenheid leiden tot het plegerschap. In de afgelopen jaren is gebleken, dat de technologie van computers en internet sterk is gaan ontwikkelen. Deze ontwikkeling komt tot uiting op alle vlakken, binnen de gemeenschap en is een onmisbare kant bij het doen van zaken. Hiernaast bestaat de kans ook, dat er groepen in de samenleving zijn die de computertechnologie op een illegale wijze zullen gebruiken, om daaruit voordeel te trekken. Deze voordeeltrekking kan zich uiten in vormen van cybercrime. Verder wordt er opgemerkt dat er talloze slachtoffers zijn die kwetsbaar zijn voor cybercrime veelal, door de onbewuste onwetendheid of onvoldoende risico bewustzijn. Evenzo is het belangrijk in acht te nemen, de plegers en deelnemers van deze strafbare handeling die moeilijk zijn te traceren. Bij cybercrime kan er sprake zijn van één of meerdere deelnemers van een strafbaar feit.

Vanuit de rechtspraktijk en arresten kan worden afgeleid dat het begrip cybercrime zich niet eenvoudig laat definiëren en daardoor diepgaand onderzoek eist. Men heeft in het buitenland getracht dit fenomeen middels strenge wetgevingen en verdragen in bedwang te houden of zwaar af te straffen, indien het zich toch afspeelt. De Hoge Raad zorgt ervoor dat cybercrime in brede en in enge zin geïnterpreteerd wordt om tot een oplossing te komen, als er geen uitweg gevonden kan worden gevonden in het Wetboek van Strafrecht. Alleen vanwege de enorme persoonlijk financiële schade die cybercrime met zich meebrengt, is het één van de riskante platforms die zoveel als mogelijk wordt bewapend door updates of andere voorzorgmaatregelen. In het Surinaams Wetboek van Strafrecht zijn er ook artikelen gewijzigd met betrekking tot cybercrime, vanwege de internationale ontwikkelingen ter bestrijding van cybercrime en het beschermen van minderjarigen op dit gebied. Het Surinaams Wetboek van Strafrecht heeft in de wijzigingen alle plegers van cybercrime strafbaar gesteld ongeacht hun betrokkenheid. Zelfs het doorgeven van

gegevens kan leiden tot het plegerschap. Dit is opmerkelijk voor het vaststellen van de daderschap, omdat alle deelnemers, als plegers worden aangemerkt. Voor het beter opsporen en vervolgen van cybercrimeplegers en-deelnemers is tenslotte de Digitale Recherche geïmplementeerd. De digitale recherche neemt maatregelen tegen cybercrime, met als doel de burger te beschermen tegen gedigitaliseerde criminaliteit.

Aanbevelingen

Tegenwoordig is sociale media en internet een ‘rond de klok’ bezigheid met een eigen marktplaats. Uit onderzoekt blijkt dat gebruikers van internet en andere computerfaciliteiten vaak niet bewust zijn van de gevolgen of het niet eens door hebben wat de risico’s kunnen zijn van cybercrime. Dit wordt deels gecreëerd door de professionele, dan wel verleidelijke houding van de cyber-criminelen, tegenover de burger waardoor een bepaald gevaar voor, bijv. oplichting niet gelijk kan worden ingezien. Naar mijn idee is het dan verstandig om enkele zaken uit te voeren gezien het internet een grote aanhang aan kijkers heeft.

Ten eerste moeten leerlingen en studenten onderwezen worden voor het nemen van beschermende maatregelen bij gebruik van internet.

Ten tweede moeten er trainingen en workshops worden verzorgd, ten aanzien van de taken en verantwoordelijkheden bij het gebruik van internet onder de gebruikers.

Ten derde moeten inwoners en vooral ondernemers gewaarschuwd worden tegen cybercrime, door verhalen van slachtoffers aan te horen. Een gewaarschuwd mens telt voor twee.

Tenslotte is het noodzakelijk dat personen die, vanwege onachtzaamheid meewerken aan strafbare feiten via het digitale netwerk, door verdere verspreiding van verboden berichten en informatie in een aparte delictsomschrijving strafbaar worden gesteld.

Met deze maatregelen kan voorkomen worden dat personen die weliswaar geen plegers zijn van het misdrijf bewust, dan wel onbewust de schade vergroten, welke door het misdrijf wordt veroorzaakt.

Bronvermelding:

Literatuurlijst:

- **Van der Neut 1999**

  J.L. Van der Neut, *Daderschap en deelneming.* Deventer: Gouda Quint 1999.

- **De Hullu 2002**

  J. de Hullu, *'Materieel strafrecht. Over algemene leerstukken van strafrechtelijke aansprakelijkheid naar Nederlands recht'*, Deventer: Kluwer 2002.

- **De Jong 2009**

  F. de Jong, *Daad-Schuld, Bijdrage aan een strafrechtelijke handelingsleer met bijzondere aandacht voor de normalisering van het delictsbestanddeel opzet*, Den Haag: Boom Juridische Uitgevers 2009.

- **De Winter 2014**

  B. de Winter, *Bescherming tegen cybercrime*, 2014.

- **Van Bruggen 2002**

  Van Bruggen R.D., Van Dun, H.A.A, De Lange E, *Juridische aspecten van de informatievoorziening*, Den Haag: Academisch Service 2002.

- **NICC 2008**

  NICC, *Publiek-Private samenwerking in het informatieknooppunt Cybercrime*, Den Haag 2008.

- **Rozemond 2011**

  Klaas Rozemond, *De methode van het materiële strafrecht*, Nijmegen: Ars Aequi Libri 2011.

- **Punwasi 2019**

  S. Punwasi, *Materieel Strafrecht in Suriname*, Paramaribo 2019.

- **Engelfriet 2010**

  A. Engelfriet, *De wet op internet*, Ius Mentis B.V, Eindhoven 2010

- **Nijboer & Cleiren 2006**

  C.P.M. Cleiren en J.F. Nijboer, *Strafrecht tekst & commentaar*, Deventer: Kluwer 2006

Wetgevingen:

- Het Surinaams Wetboek van Strafrecht (Wet van 14 oktober 1910, houdende vaststelling van een Wetboek van Strafrecht voor Suriname, zoals laatstelijk gewijzigd bij S.B. 2015 no. 44
- Het Nederlands Wetboek van Strafrecht

Verdragen:

- Het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken oftewel het Cybercrimeverdrag 23-11-2001

Intervieuws:

- Interview met Officier van Justitie mw Rathipal 28-8-2022
- Interview met mr Schaken van de afdeling Digitale Recherche 28-9-2022

Jurisprudentie:

- HR 23 februari 1954, NJ 1954/378
- HR 16 december 1986, NJ 1987/534
- HR 29 oktober 1934, NJ 1934/1673
- HR 25 maart 1975, NJ 1975/270
- HR 15 april 1986, NJ 1986/740
- HR 17 november 1981, NJ 1983/84
- RB ‘s Hertogenbosch, 8 oktober 2010, LJN: BN9786
- HR 22 februari 2011, ECLI:NL:HR:2011:BN9287
- RB 28 oktober 2021, ECLI:RBDHA:2021:11813
- RB 2 oktober 2015, ECLI:NL:RBROT:2015:7044
- Kantongerecht Parketnummer: 1-1-01957

Internetbronnen:

- ‘Cybercrime in Suriname steeds agressiever’, starnieuws.com 4-5-2022

- ‘Europol: grote toename cybercrime door coronavirus’, rtlnieuws.nl 4-5-2022
- ‘Strafbare Deelneming- Römelingh’, romelingh.com 5-5-2022
- ‘Strafrecht- Specialisten in Strafrecht’, fzadvocaten.nl 5-5-2022
- ‘Wat is cybercrime’, vraaghetdepolitie.nl 5-5-2022
- ‘De Wet Computercriminaliteit: Wat is computercriminaliteit’, iusmentis.com 5-5-2022
- ‘Welke soorten cybercrime zijn er?’, veiliginternetten.nl 5-5-2022
- ‘Methodes voor verspreiden van computervirussen en malware’, kaspersky.nl 7-5-2022
- ‘Tips over hoe je jezelf kunt beschermen tegen cybercriminaliteit’, kaspersky.nl 7-5-2022
- ‘What is phishing?’, phishing.org 7-5-2022
- ‘Neem de juiste maatregelen tegen phishing’, interpolis.nl 7-5-2022
- ‘Hoe herken ik identiteitsfraude’, Rijksoverheid.nl 8-5-2022
- ‘Soorten identiteitsfraude- Rijksoverheid’, rijksoverheid.nl 8-5-2022
- ‘Wat is een DDoS-aanval’, politie.nl 10-5-2022
- ‘Wat is een botnet?’, politie.nl 10-5-2022
- ‘Wat is hacken? Alles wat u moet weten- AVG’, avg.com 10-5-2022
- ‘Cyber Grooming- ChildSafeNet’, childsafenet.org 11-5-2022
- ‘What is skimming in cybersecurity?’, cyberexperts.com 11-5-2022
- ‘Scams and Safety’, fbi.gov 11-5-2022
- ‘Web skimming’, abnamro.nl 13-5-2022
- ‘Tips to protect yourself from cyberstalkers’, Kaspersky.com 13-5-2022
- “Bekendmaking>>-Korps Politie Suriname”, politie.sr 28-8-2022
- “Cyber Crime en de noodzaak van international verdragen”, research.vu.nl 15-5-2022
- “Schuld & Verwijtbaarheid in het Straf- en Bestuursrecht” bijzonderstrafrechtacademie.nl 6-5-2022