Vaststelling van Geharmoniseerde Beleidsregels voor de ICT-Markt in de ACS-landen

Cybercriminaliteit / e-Misdrijven: Richtlijnen voor Model Beleid & Wetteksten

HIPCAR

Harmonisatie van Beleid, Wetgeving en Regelgevings procedures op het stuk van ICT in het Caribisch gebied

Vaststelling van Geharmoniseerde Beleidsregels voor de ICT-Markt in de ACP-landen

Cybercriminaliteit / e-Misdrijven:

Richtlijnen voor Model Beleid

& Wetteksten

HIPCAR

Harmonisatie van Beleid, Wetgeving en Regelgevings procedures op het stuk van ICT in het Caribisch gebied

Europese Commissie

CARICOM

CTU

ITU

Dit document is tot stand gekomen met de financiële ondersteuning van de Europese Unie. De standpunten die hierin tot uiting worden gebracht zijn geenszins een weergave van de officiële mening van de Europese Unie.

Denk aan het milieu voordat u dit rapport print.

Voorwoord

Informatie- en communicatietechnologie (ICT) geeft vorm aan het proces van het globalisatie. Het potentieel hiervan erkennend voor het bespoedigen van de economische integratie van de Caribische regio en daarbij haar grotere welvarendheid en sociale transformatie, heeft de CARICOM Interne Markt en Economie (CSME) een ICT-strategie ontwikkeld die gefocust is op versterkte connectiviteit en ontwikkeling.

Liberalisatie van de telecommunicatiesector is een van de sleutelelementen van deze strategie. Coördinatie binnen de gehele regio is essentieel indien beleid, wetgeving en praktijken voortvloeiend uit de liberalisatie door elk land niet dermate verschillend moeten zijn dat ze een belemmering gaan vormen voor de ontwikkeling van een regionale markt.

Het project 'Versterking van het Concurrentievermogen in het Caribisch Gebied door de Harmonisatie van Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT' (HIPCAR) was gericht op het aanpakken van deze potentiële belemmering door het samenbrengen en begeleiden van alle 15 Caribische landen in de Groep van Staten in Afrika, het Caribisch Gebied en de Stille Oceaan (ACP) terwijl zij hun geharmoniseerd Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT formuleerden en aannamen. Uitgevoerd door de Internationale Telecommunicatie-Unie (ITU), is het project ondernomen in nauwe samenwerking met de Caribische Telecommunicatie-Unie (CTU), die de voorzitter is van de HIPCAR-Stuurgroep. Een mondiaal stuurcomité bestaande uit de vertegenwoordigers van het ACP-Secretariaat en het Directoraat-generaal EuropeAid Ontwikkeling en Samenwerking (DEVCO, Europese Commissie) houdt toezicht op de totale implementatie van het project.

Het project vindt plaats in het kader van het programma ACP Informatie- en Telecommunicatietechnologie (@CP-ICT) en wordt gefinancierd uit het 9^{e} Europees Ontwikkelingsfonds (EDF), dat het voornaamste instrument is voor het verstrekken van Europese hulp voor ontwikkelingssamenwerking in de ACP-Staten, met medefinanciering van de ITU. Het @CP-ICT is gericht op het ondersteunen van de ACP-regeringen en -instituten bij het harmoniseren van hun ICT-beleid in de sector door het bieden van beleidsadvies, training en gerelateerde capaciteitsopbouw van hoge kwaliteit, met referentiepunten over de hele wereld doch van plaatselijke relevantie.

Alle projecten die meerdere belanghebbenden bij elkaar brengen worden geconfronteerd met de dubbele uitdaging van het creëren van een gevoel van gedeeld ownership en het waarborgen van optimale resultaten voor alle partijen. HIPCAR heeft bijzondere aandacht besteed aan deze kwestie vanaf het prille begin van het project in december 2008. Overeenstemming bereikt hebbend over gedeelde prioriteiten, werden werkgroepen van belanghebbenden gevormd voor het aanpakken daarvan. De specifieke noden van de regio werden vervolgens geïdentificeerd evenals potentiële succesvolle regionale praktijken, welke daarna werden getoetst aan elders gevestigde praktijken en standaarden.

Deze gedetailleerde beoordelingen, die bijzonderheden die specifiek waren voor de landen weerspiegelen, dienden als basis voor het modelbeleid en de modelwetteksten die het vooruitzicht boden van een wetgevingslandschap waarop de hele regio trots kan zijn. Het project zal zeker andere regio's tot voorbeeld strekken bij hun pogingen de katalytische kracht van ICT bruikbaar te maken voor het bespoedigen van economische integratie en sociale en economische ontwikkeling.

Ik maak gebruik van deze gelegenheid om dank uit te brengen aan de Europese Commissie en het ACP-Secretariaat voor hun financiële bijdrage. Ik breng ook dank uit aan het Secretariaat van de Caribische Gemeenschap (CARICOM) en het Secretariaat van de Caribische Telecommunicatie-Unie (CTU) voor hun bijdrage aan dit werk. Zonder de politieke wil van de zijde van de begunstigde landen zou niet veel zijn bereikt. Ik breng daarom mijn hartgrondige dank uit aan alle ACP-regeringen voor hun politieke wil welke dit project tot een groot succes heeft gemaakt.

Brahima Sanou,
BDT, Directeur

Dankwoord

Dit document vertegenwoordigt een van de resultaten van de regionale activiteiten uitgevoerd in het kader van het HIPCAR-project "Versterking van het Concurrentievermogen in het Caribisch Gebied door de Harmonisatie van Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT" officieel van start gegaan in Grenada in december 2008.

In reactie op zowel de uitdagingen als de kansen voortvloeiende uit de bijdrage van de informatie- en communicatietechnologie (ICT) aan de politieke, sociale, economische en ecologische ontwikkeling, hebben de Internationale Telecommunicatie-Unie (ITU) en de Europese Commissie (EC) hun krachten gebundeld en een overeenkomst getekend voor het geven van "Assistentie bij de vaststelling van geharmoniseerde beleidsregels voor de ICT-markt in de ACP", als onderdeel van het Programma "ACP-Informatie- en Communicatietechnologie (@CP-ICT)" in het kader van het 9e Europees Ontwikkelingsfonds (EDF), i.e. het ITU-EC-ACP-project.

Dit wereldwijd ITU-EC-ACP-project wordt geïmplementeerd via drie aparte subprojecten die zijn afgestemd op de specifieke behoeften van elke regio: het Caribisch Gebied (HIPCAR), sub-Sahara Afrika (HIPSSA) en de Stille Zuidzee Eilandstaten (ICB4PAC).

De HIPCAR-Stuurgroep - voorgezeten door de Caribische Telecommunicatie-Unie (CTU) - zorgde voor de begeleiding en ondersteuning van een team van adviseurs, onder wie Gilberto Martíns de Almeida, Kwesie Prescod en Karen Stephen-Dalton. Het concept document werd vervolgens bestudeerd, gefinaliseerd en met een ruime consensus aangenomen door de participanten van twee consultatieworkshops voor de HIPCAR-Werkgroep Kwesties de Informatiemaatschappij rakende, gehouden te Saint Lucia van 8-12 maart 2010 en Barbados van 23-26 augustust 2010 (zie Bijlagen). De toelichting bij de modelwettekst in dit document is opgesteld door Gilberto Martíns de Almeida en behandelt onder andere de punten die tijdens de tweede workshop naar voren werden gebracht.

ITU wil een bijzonder woord van dank uitbrengen aan de delegaties van de Caribische ministeries belast met ICT en telecommunicatie die hebben deelgenomen aan de workshops, alsook aan vertegenwoordigers van ministeries van justitie en juridische zaken en andere lichamen uit de publieke sector, regelgevende lichamen, de academische wereld, het maatschappelijk middenveld, aanbieders van diensten en regionale organisaties, voor hun harde werk en toewijding bij het produceren van de inhoud van dit rapport. Door deze brede participatie van de publieke sector vertegenwoordigende verschillende sectoren heeft het project kunnen profiteren van een dwarsdoorsnede van standpunten en belangen. De bijdragen vanuit het Secretariaat van de Caribische Gemeenschap en de Caribische Telecommunicatie-Unie worden ook met dank gememoreerd.

Zonder de actieve betrokkenheid van al deze belanghebbenden, zou het niet mogelijk zijn geweest documenten zoals deze te produceren, welke niet alleen de algemene vereisten en voorwaarden van de Caribische regio weergeven maar ook de internationale beste praktijk vertegenwoordigen.

De activiteiten zijn ten uitvoer gelegd door Kerstin Ludwig, verantwoordelijk voor de coördinatie van activiteiten in het Caribisch Gebied (HIPCAR-Projectcoördinator), en Sandro Bazzanella, verantwoordelijk voor het beheer van het volledig project voor de landen in Afrika ten zuiden van de Sahara, het Caribisch Gebied en de Stille Oceaan (ITU-EC-ACP-Projectmanager), met algemene ondersteuning van Nicole Darmanie, HIPCAR-Projectassistent, en van Silvia Villar, ITU-EC-ACP-Projectassistent. Het werk is uitgevoerd onder de algemene leiding van Cosmas Zavazava, Hoofd, afdeling Projectondersteuning en Kennisbeheer (PKM). Het document is verder verbeterd aan de hand van de commentaren van de ITU Telecommunication Development Bureau's (BDT) ICT-applicaties en Cybersecurity Divisie (CYB), evenals van Michael Tetelmann. Philip Cross van het ITU Regionaal Kantoor voor het Caribisch gebied verleende ondersteuning. De vooropmaak werd verzorgd door Pau Puig Gabarró. Het team van ITU's Publication Composition Service (dienst samenstelling publicaties) is verantwoordelijk voor de publicatie.

Inhoudsopgave

Bladzijde

Voorwoord ..... **iii**

Dankwoord ..... **v**

Inleiding **1**

Deel I: Richtlijnen voor model beleid – Cybercriminaliteit / e-misdrijven **11**

Deel II: Model wettekst – Cybercriminaliteit / e-misdrijven **15**

Indeling van de artikelen 15

HOOFDSTUK I – INLEIDING 17

HOOFDSTUK II – OVERTREDINGEN 19

HOOFDSTUK III – RECHTSGEBIED 24

HOOFDSTUK IV – PROCESRECHT 24

HOOFDSTUK V – AANSPRAKELIJKHEID 27

Deel III: Memorie van toelichting bij de model wettekst inzake Cybercriminaliteit / e-misdrijven **31**

INLEIDING 31

COMMENTAAR OP DE ARTIKELEN 32

HOOFDSTUK I 32

HOOFDSTUK II 35

HOOFDSTUK III 43

HOOFDSTUK IV 44

HOOFDSTUK V 48

BIJLAGEN **51**

Bijlage 1 Deelnemers in de Eerste Consultatieve Workshop voor de Werkgroep van het HIPCAR project 51

Bijlage 2 Deelnemers in de Tweede Consultatieve Workshop (fase B) voor de Werkgroep van het HIPCAR project 53

Inleiding

HIPCAR-Project – Doelstellingen en begunstigdenHet door de EU-ITU gefinancierd HIPCAR – project[1] met een looptijd van drie jaar werd door de Internationale Telecommunicatie Unie (ITU) en de Europese Unie (EU) gelanceerd in september 2008, in nauwe samenwerking met het Secretariaat van de Caribische Gemeenschap (CARICOM) en de Caribische Telecommunicatie Unie (CTU). Het maakt deel uit van een globaal ITU-EU-project voor de ACP-staten en omvat tevens de landen in Afrika ten zuiden van de Sahara en in de Stille Oceaan.

Het doel van HIPCAR is CARIFORUM[2]-landen in het Caribisch gebied te assisteren bij het harmoniseren van hun beleid en procedures voor wet- en regelgeving op het vlak van informatie- en communicatietechnologie (ICT) met het oog op het scheppen van een gunstig klimaat voor ICT-ontwikkeling en connectiviteit, om zo de marktintegratie te bevorderen, de investering in verbeterde ICT-capaciteit en -diensten aan te moedigen en de bescherming van de belangen van ICT-gebruikers in de hele regio te vergroten. Het uiteindelijk doel van het project is het versterken van het concurrentievermogen en de sociaal-economische en culturele ontwikkeling in het Caribisch gebied door middel van ICT.

Overeenkomstig artikel 67 van het Herziene Verdrag van Chaguaramas, kan HIPCAR worden beschouwd als een integrerend deel van het streven van de regio om de CARICOM Interne Markt & Economie (CSME) te ontwikkelen via de progressieve liberalisatie van zijn ICT-dienstensector. Het project biedt ook ondersteuning aan de CARICOM-Agenda voor Connectiviteit en de verplichtingen van de regio tegenover de Wereldtop over de informatiemaatschappij (WSIS), de Algemene Overeenkomst van de Wereldhandelsorganisatie inzake de Handel in Diensten (WTO-GATS) en de Millenniumdoelstellingen voor Ontwikkeling (MDG's). Het houdt tevens rechtstreeks verband met het bevorderen van het concurrentievermogen en een grotere toegang tot diensten in de context van verdragsverplichtingen zoals de Economische Partnerschapsovereenkomst van de CARIFORUM-landen met de Europese Unie (EU-EPA).

De begunstigde landen van het HIPCAR-project zijn Antigua en Barbuda, de Bahama's, Barbados, Belize, Gemenebest Dominica, de Dominicaanse Republiek, Grenada, Guyana, Haïti, Jamaica, St. Kitts en Nevis, St. Lucia, St. Vincent en de Grenadines, Suriname, en Trinidad en Tobago.

Stuurcomité en Werkgroepen van het project

HIPCAR heeft een Stuurcomité voor het project ingesteld om te zorgen voor de nodige begeleiding en supervisie. Het Stuurcomité bestaat onder andere uit vertegenwoordigers van het Secretariaat van de Caribische Gemeenschap (CARICOM), de Caribische Telecommunicatie Unie (CTU), de Oost-Caribische Telecommunicatie Autoriteit (ECTEL), de Caribische Associatie van Nationale Telecommunicatie Organisaties (CANTO), de Caribische ICT-Virtuele Gemeenschap (CIVIC), en de Internationale Telecommunicatie Unie (ITU).

Om de inbreng van de belanghebbenden en de relevantie voor elk land te garanderen, werden ook HIPCAR-Werkgroepen geïnstalleerd bestaande uit leden die zijn aangewezen door de respectieve

---

1 De volledige titel van het HIPCAR-project is "Versterking van het Concurrentievermogen in het Caribisch Gebied door de Harmonisatie van Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT". HIPCAR is deel van een mondiaal ITU-EC-ACP-project ondersteund en gefinancierd door de Europese Unie met EUR 8 miljoen en een aanvulling van USD 500,000 van de Internationale Telecommunicatie Unie (ITU). Het wordt uitgevoerd door de Internationale Telecommunicatie Unie (ITU) in samenwerking met de Caribische Telecommunicatie Unie (CTU) en met betrokkenheid van andere organisaties in de regio.
(zie **www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html**).

2 Het CARIFORUM is een regionale organisatie van vijftien onafhankelijke staten in het Caribisch gebied (Antigua en Barbuda, Bahama's, Barbados, Belize, Dominica, de Dominicaanse Republiek, Grenada, Guyana, Haïti, Jamaica, Saint Christopher en Nevis, Saint Lucia, Saint Vincent en de Grenadines, Suriname, en Trinidad en Tobago). Deze staten zijn alle ondertekenaars van de ACP-EU-verdragen.

Om de inbreng van de belanghebbenden en de relevantie voor elk land te garanderen, werden ook HIPCAR-Werkgroepen geïnstalleerd bestaande uit leden die zijn aangewezen door de respectieve overheden van de landen – met inbegrip van specialisten van ICT-agentschappen, justitie en juridische zaken en andere publieke sector lichamen, nationale regelgevende instanties, nationale ICT-contactpersonen en personen verantwoordelijk voor het ontwikkelen van nationale wetgeving. Door deze brede participatie van de publieke sector uit verschillende sectoren heeft het project kunnen profiteren van een dwarsdoorsnede van standpunten en belangen. De Werkgroepen bestaan verder uit vertegenwoordigers van relevante regionale lichamen (CARICOM-Secretariaat, CTU, ECTEL en CANTO) en waarnemers van overige belanghebbende entiteiten in de regio (zoals het maatschappelijk middenveld, de particuliere sector, aanbieders van telecommunicatiediensten, de academische wereld, enz.).

De Werkgroepen waren verantwoordelijk voor het uitdiepen van de volgende twee werkgebieden:

ICT-Beleidskader en Wetgevingskader voor Kwesties de Informatiemaatschappij rakende, omvattende zes deelgebieden: e-commerce (transacties en bewijs), persoonlijke levenssfeer & gegevensbescherming, onderschepping van berichten, cybercriminaliteit, en toegang tot publieke informatie (vrijheid van informatie).

ICT-Beleidskader en Wetgevingskader voor Telecommunicatie, omvattende drie deelgebieden: universele toegang / diensten, interconnectie, en vergunningenbeleid.

De rapporten van de Werkgroepen gepubliceerd in deze documentenreeks zijn opgebouwd rond deze twee voornaamste werkgebieden.

Projectuitvoering en – inhoud

De aanzet tot de projectactiviteiten werd gegeven door middel van een rondetafelbespreking voor de lancering van het project gehouden in Grenada, van 15 tot 16 december 2008. Tot heden hebben alle begunstigde landen van het HIPCAR-project – uitgezonderd Haïti – samen met de als partners van het project optredende regionale organisaties, regelgevende instanties, aanbieders van telecommunicatiediensten, academische wereld en het maatschappelijk middenveld actief geparticipeerd in de HIPCAR-evenementen, met inbegrip van – naast de projectlancering in Grenada – regionale workshops in Trinidad & Tobago, St. Lucia, St. Kitts en Nevis, Suriname en Barbados.

De inhoudelijke activiteiten van het project staan onder leiding van teams van regionale en internationale deskundigen die samenwerken met de leden van de Werkgroepen die zich concentreren op de twee bovengenoemde werkgebieden.

Tijdens *Fase I* van het project – net afgerond – heeft HIPCAR:

1. een beoordeling gemaakt van de bestaande wetgeving van de begunstigde landen vergeleken met de internationale beste toepassing in de praktijk en in de context van harmonisatie in de gehele regio; en
2. model beleidsregels en model wetteksten opgesteld voor de bovengenoemde werkgebieden, waaruit het nationaal ICT-beleid en de nationale ICT-wetgeving / regelgeving kunnen worden ontwikkeld.

Het is de bedoeling dat deze voorstellen worden bekrachtigd of onderschreven door CARICOM/CTU en de autoriteiten van de landen in de regio als basis voor de volgende fase van het project.

Fase II van het HIPCAR-project is erop gericht begunstigde landen die daar belangstelling voor hebben assistentie te verlenen bij het omzetten van de eerder genoemde modellen in nationaal ICT-beleid en nationale ICT-wetgeving aangepast aan hun specifieke eisen, omstandigheden en prioriteiten. HIPCAR heeft fondsen gereserveerd om te kunnen inspelen op de verzoeken van de landen voor technische bijstand – met inbegrip van capaciteitsopbouw – nodig voor dit doel.

Inleiding

Overzicht van de zes HIPCAR-richtlijnen voor model beleid en wetteksten inzake kwesties de informatiemaatschappij rakende

Wereldwijd zijn landen, ook in het Caribisch gebied, op zoek naar manieren om wettelijke kaders te ontwikkelen voor het aanpakken van de behoeften van de informatiemaatschappij met het oog op het gebruikmaken van de groeiende aanwezigheid van het wereldwijde web als een kanaal voor de levering van diensten, ter garantie van een veilige omgeving en ter verhoging van de verwerkingskracht van informatie-systemen voor zakelijke efficiëntie en effectiviteit.

De informatiemaatschappij is gebaseerd op het uitgangspunt van toegang tot informatie en diensten en het gebruik van geautomatiseerde verwerkingssystemen ter verbetering van de levering van diensten aan markten en personen *overal in de wereld*. Voor zowel gebruikers als bedrijven biedt de informatiemaatschappij in het algemeen en de beschikbaarheid van informatie- en communicatietechnologie (ICT) unieke kansen. Terwijl de belangrijkste vereisten van de handel ongewijzigd blijven, creëert de directe overdracht van commerciële informatie mogelijkheden voor verbeterde zakelijke relaties. Dit gemak van uitwisseling van commerciële informatie brengt ook nieuwe paradigma's met zich mee: ten eerste, waar informatie wordt gebruikt om transacties met betrekking tot fysieke goederen en traditionele diensten te ondersteunen, en ten tweede, waar informatie zelf het product is dat wordt verhandeld.

De beschikbaarheid van ICT en nieuwe netwerk-gebaseerde diensten bieden een aantal voordelen voor de samenleving in het algemeen, met name voor ontwikkelingslanden. ICT-toepassingen, zoals e-overheid, e-handel, e-onderwijs, e-gezondheidszorg en e-milieu, worden gezien als faciliterend voor ontwikkeling, aangezien zij een efficiënt kanaal bieden voor de levering van een breed scala aan basisdiensten in afgelegen en landelijke gebieden. ICT-toepassingen kunnen de vervulling van de millennium ontwikkelingsdoelstellingen vergemakkelijken, armoede terugdringen en de gezondheids- en milieuomstandigheden in ontwikkelingslanden verbeteren. Onbelemmerde toegang tot informatie kan de democratie ondersteunen, als de informatiestroom buiten de controle valt van overheidsinstanties (zoals is gebeurd, bij voorbeeld in Oost-Europa). Met de juiste aanpak, context en uitvoeringsprocessen, kunnen investeringen in ICT-toepassingen en -instrumenten resulteren in productiviteit en kwaliteitsverbetering.

Echter, het transformatieproces gaat gepaard met uitdagingen aangezien het bestaande wettelijk kader niet noodzakelijk de specifieke eisen van een snel veranderende technische omgeving dekt. In gevallen waar informatie de handel in traditionele goederen en diensten ondersteunt, moet er duidelijkheid zijn in de manier waarop traditionele commerciële veronderstellingen worden toegepast, en in het geval waarin informatie het product is dat wordt verhandeld, moet de maker/ eigenaar van het product worden beschermd. In beide gevallen, moet er vastgesteld worden hoe het misdrijf aan het licht wordt gebracht, vervolgd en stopgezet in de realiteit van grensoverschrijdende transacties op basis van een immaterieel product.

De zes met elkaar verbonden model kaders

Het HIPCAR-project heeft zes (6) met elkaar verbonden model kaders ontwikkeld die een alomvattend wettelijk kader vormen voor de aanpak van de hierboven genoemde veranderende omgeving van de informatiesamenleving door het begeleiden en ondersteunen van de invoering van geharmoniseerde wetgeving in de HIPCAR begunstigde landen.

In de eerste plaats werd een juridisch kader ontwikkeld om het recht van gebruikers te beschermen in een veranderende omgeving en daarmee, naast andere aspecten, te zorgen voor vertrouwen van de consument en beleggers in rechtszekerheid en bescherming van privacy, en HIPCAR model wetteksten werden ontwikkeld om overwegingen aan te pakken met betrekking tot: **de toegang tot publieke informatie (Vrijheid van Informatie)** – gericht op het stimuleren van de juiste cultuur van transparantie in regelgeving in het voordeel van alle belanghebbenden; en **privacy en gegevensbescherming** – gericht op

het waarborgen van de bescherming van de privacy en persoonlijke gegevens naar tevredenheid van het individu. Dit laatste kader is gericht op passende geheimhoudingspraktijken binnen zowel de publieke als private sector.

In de tweede plaats, werd een HIPCAR model wettekst ontwikkeld voor **elektronische handel (transacties)**, met inbegrip van elektronische handtekeningen voor het vergemakkelijken van de harmonisatie van de wetten met betrekking tot de standaardverwachtingen en rechtsgeldigheid van contract formuleringspraktijken. Dit kader is erop gericht om te voorzien in de gelijkwaardigheid van papieren en elektronische documenten en contracten en voor het leggen van een basis voor het aangaan van handel in cyberspace. Een wettekst over **Elektronische Handel (Bewijs)** – de bijbehorende tekst voor het kader voor elektronische handel (transacties) werd toegevoegd ter regulering van het wettig bewijs, in zowel civiele en criminele procedures.

Om ervoor te zorgen dat ernstige schendingen van de vertrouwelijkheid, integriteit en beschikbaarheid van ICT en de gegevens kunnen worden onderzocht door de rechtshandhaver, werden model wetteksten ontwikkeld om wetgeving te harmoniseren op het gebied van het strafrecht en het strafprocesrecht. De wettekst inzake **cybercriminaliteit** definieert strafbare feiten, onderzoeksinstrumenten en de strafrechtelijke aansprakelijkheid van de belangrijkste actoren. Een wettekst over het **onderscheppen van elektronische communicatie** verschaft een passend kader dat het wederrechtelijk onderscheppen van communicatie verbiedt en heeft een minieme mogelijkheid geschapen zodat de rechtshandhaver in staat wordt gesteld om rechtmatig communicatie te onderscheppen, indien aan bepaalde duidelijk omschreven voorwaarden is voldaan.

Ontwikkelen van de model wetteksten

De model wetteksten werden ontwikkeld rekening houdend met de belangrijkste elementen van internationale trends, alsmede juridische tradities en beste praktijken uit de regio. Dit proces werd ondernomen zodat de kaders het beste beantwoorden aan de realiteit en de behoeften van de regio van HIPCAR begunstigde landen waarvoor en waarmee zij zijn ontwikkeld. Daarom was er tijdens het proces veel interactie met belanghebbenden in elk stadium van de ontwikkeling.

De eerste stap in dit complexe proces is een evaluatie van de bestaande juridische kaders binnen de regio door middel van een beoordeling van de wetgeving betreffende alle relevante gebieden. Naast uitgevaardigde wetgeving, werd in het overzicht opgenomen, indien relevant, wetsontwerpen die waren voorbereid, maar die nog niet het proces van afkondiging hadden voltooid. In een tweede stap werden de beste internationale praktijken (bijvoorbeeld van de Verenigde Naties, OESO, EU, het Gemenebest, UNCITRAL en CARICOM), alsmede geavanceerde nationale wetgeving (bijvoorbeeld uit het Verenigd Koninkrijk, Australië, Malta en Brazilië, onder andere) geïdentificeerd. Deze beste praktijken werden gebruikt als maatstaf.

Voor elk van de zes gebieden, werden complexe juridische analyses opgesteld, die de bestaande wetgeving in de regio vergeleek met deze maatstaven. Deze rechtsvergelijkende analyse leverde een momentopname van de mate van vooruitgang op belangrijke beleidsterreinen binnen de regio. Deze bevindingen waren leerzaam, en toonden aan dat er een meer geavanceerde ontwikkeling was in wetgevingskaders met betrekking tot elektronische transacties, cybercriminaliteit (of "computermisbruik") en toegang tot publieke informatie (vrijheid van informatie) dan is gebleken in de andere kaders.

Op basis van de resultaten van de rechtsvergelijkende analyses, hebben de regionale belanghebbenden “bouwstenen” ontwikkeld voor basisbeleid, die – zodra deze zijn goedgekeurd door de betrokken partijen – de basis bepalen voor de verdere beraadslaging over het beleid en ontwikkeling van de wettekst. Deze bouwstenen voor het beleid bevestigden een aantal gemeenschappelijke thema's en trends in de internationale precedenten, maar identificeerden ook bepaalde overwegingen die moeten worden opgenomen binnen de context van een regio die bestaat uit soevereine kleine eiland-

ontwikkelingslanden. Een voorbeeld van een belangrijke overweging betreffende de situatie die de beraadslagingen beïnvloedde in deze fase en in andere fasen van het proces was de kwestie van institutionele capaciteit om adequaat beheer van deze nieuwe systemen te faciliteren.

De beleidsbouwstenen werden vervolgens gebruikt om aangepaste model wetteksten te ontwikkelen die zowel aan de internationale normen en de vraag van de HIPCAR begunstigde landen voldoen. Elke model tekst werd vervolgens opnieuw geëvalueerd door de betrokken partijen vanuit het perspectief van de levensvatbaarheid en de mogelijkheid om te worden vertaald naar de regionale context. Als zodanig, heeft de groep belanghebbenden – bestaande uit een mix van wetgevingsjuristen en beleidsdeskundigen uit de regio – teksten ontwikkeld die het beste het samenvallen van de internationale normen met lokale overwegingen weerspiegelen. Een brede betrokkenheid van vertegenwoordigers van bijna alle 15 HIPCAR begunstigde landen, regelgevers, aanbieders van telecommunicatiediensten, regionale organisaties, het maatschappelijk middenveld en de academische wereld heeft ervoor gezorgd dat de wetteksten verenigbaar zijn met de verschillende wettelijke normen in de regio. Het werd echter ook erkend dat elke begunstigde staat misschien specifieke voorkeuren heeft met betrekking tot de uitvoering van sommige bepalingen. Daarom bieden de model teksten ook een keuze in de benadering binnen de algemeenheid van een geharmoniseerd kader. Deze aanpak is gericht op het faciliteren van brede acceptatie van de documenten en het verhogen van de mogelijkheid van een tijdige uitvoering in alle begunstigde rechtsgebieden.

Interactie en het overlappen van de model teksten

Als gevolg van de aard van de kwesties die worden overwogen, weerspiegelen alle zes kaders een aantal algemene aspecten.

In eerste instantie moet aandacht worden besteed aan de kaders die zorgen voor het gebruik van elektronische middelen in communicatie en uitvoering van handel: **Elektronische handel (transacties), elektronische handel (bewijs), cybercriminaliteit** en **onderscheppen van communicatie**. Alle vier kaders handelen over kwesties in verband met de behandeling van berichten verzonden via communicatienetwerken, de vaststelling van passende testen om de geldigheid van documenten of andere bescheiden te bepalen en de integratie van systemen gericht op de gelijke behandeling van papieren en elektronisch materiaal bij bescherming tegen onheuse behandeling, consumentenzaken en procedures voor geschillenbeslechting.

Als zodanig, zijn er verschillende gemeenschappelijke definities in deze kaders die rekening moeten houden met, waar nodig, overwegingen betreffende een uiteenlopende reikwijdte van de toepasbaarheid. Gemeenschappelijke concepten zijn onder meer: “elektronisch communicatienetwerk" – wat moet worden afgestemd op de bestaande definitie van het rechtsgebied in de heersende telecommunicatiewetten; "elektronisch document" of "elektronische bescheiden" – die een brede interpretatie moeten hebben zodat bijvoorbeeld audio- en videomateriaal daaronder vallen; en "elektronische handtekeningen", "geavanceerde elektronische handtekeningen", "certificaten", "geaccrediteerde certificaten", "certificaat dienstverleners" en "certificatie-instanties" – die allemaal te maken hebben met de toepassing van encryptietechnieken voor elektronische validatie van authenticiteit en de erkenning van de technologische en economische sector, die is opgezet rond het verlenen van dergelijke diensten.

In deze context, legt **elektronische handel (transacties)**, onder andere, kernbeginselen neer van de erkenning en toekenning die nodig zijn voor de effectiviteit van de andere kaders. De nadruk ligt op het definiëren van de fundamentele beginselen die gebruikt moeten worden bij het bepalen van de gevallen van een civiele of commerciële aard. Dit kader is ook van essentieel belang bij het bepalen van een geschikte marktstructuur en een realistische strategie voor de sector toezicht in het belang van het publiek en het vertrouwen van de consument. Beslissingen over de kwesties gerelateerd aan een dergelijk

administratief systeem hebben vervolgens een invloed op hoe elektronische handtekeningen procedureel worden gebruikt ten behoeve van bewijsvoering, en hoe de verantwoordelijkheden en verplichtingen in de wet gedefinieerd op de juiste manier kunnen worden toegeschreven.

Deze veronderstelling van gelijkwaardigheid geeft de overige kaders de mogelijkheid op adequate wijze om te gaan met de vertrekpunten betreffende de passende behandeling van elektronische informatieoverdracht. Het kader voor **cybercriminaliteit**, bij voorbeeld, definieert strafbare feiten met betrekking tot de onderschepping van communicatie, verandering van communicatie- en computer-gerelateerde fraude. Het kader voor **elektronische handel (bewijs)** voorziet in een basis die elektronisch bewijsmateriaal introduceert als een nieuwe categorie van bewijs.

Een belangrijke rode draad die **e-transacties** en **cybercriminaliteit** aan elkaar verbindt is de vaststelling van de passende aansprakelijkheid en verantwoordelijkheid van dienstverleners van wie diensten worden gebruikt in situaties van elektronisch gepleegde misdrijven. Speciale aandacht werd besteed aan de samenhang bij het bepalen van de doelpartijen voor deze relevante delen en te zorgen voor de juiste toepassing van de verplichtingen en de handhaving daarvan.

In het geval van de kaders gericht op het verbeteren van gereglementeerd overzicht en vertrouwen van de gebruiker, behandelen de model teksten ontwikkeld door HIPCAR de twee uitersten van hetzelfde probleem: terwijl het model **toegang tot publieke informatie** de bevordering van de openbaarmaking van publieke informatie bevordert op specifieke uitzonderingen na, stimuleert het model **privacy en gegevensbescherming** de bescherming van een subset van deze informatie, die onttrokken is aan het vorige model. Belangrijk is dat beide kaders zijn gericht op het stimuleren van beter documentbeheer en archiveringspraktijken binnen de publieke sector en – in het geval van het laatstgenoemde kader – een aantal aspecten van de particuliere sector. Het is echter opmerkelijk dat – in tegenstelling tot de andere vier modelteksten – deze kaders niet uitsluitend van toepassing zijn op het elektronisch medium, noch voor het creëren van een gunstig kader waarbij overwegingen van een nieuw medium worden overgebracht naar bestaande procedures. Om te zorgen voor consistentie, zijn de kaders gericht op het reguleren van een passend beheer van informatiebronnen, in zowel elektronische en niet-elektronische vorm.

Er zijn een aantal structurele en logistieke overlappingen die bestaan tussen deze twee wettelijke kaders. Onder andere in de definitie van de belangrijkste concepten van "overheidsinstantie" (de personen op wie de kaders van toepassing zouden zijn), "informatie", "gegevens" en "document", en de relatie tussen deze. Een andere belangrijke vorm van overlapping betreft het gepaste toezicht op deze kaders. Beide kaders vereisen de instelling van toezichthoudende instanties, die voldoende onafhankelijk van invloeden van buitenaf moeten zijn om zo het publiek te verzekeren van de integriteit van hun beslissingen. Deze onafhankelijke instanties moeten ook de capaciteit hebben om boetes en / of sancties op te leggen tegen partijen die activiteiten ondernemen om de doelstellingen van een van deze kaders te frustreren.

Conclusie

De zes HIPCAR model wetteksten voorzien de begunstigde landen van het project met een uitgebreid kader om het meest relevante gebied van regelgeving aan te pakken met betrekking tot vraagstukken van de informatiemaatschappij. In de formulering werden zowel de meest actuele internationale normen, alsook de eisen van kleine eiland-ontwikkelingslanden in het algemeen en – meer specifiek – die van de begunstigde HIPCAR-landen opgenomen. De brede betrokkenheid van de belanghebbenden uit deze begunstigde landen in alle fasen van de ontwikkeling van de model wetteksten zorgt ervoor dat zij probleemloos en tijdig kunnen worden aangenomen. Hoewel de nadruk ligt op de behoeften van de landen in het Caribisch gebied, zijn de genoemde model wetteksten reeds geïdentificeerd als mogelijke richtsnoeren door bepaalde landen in andere regio's van de wereld.

Gezien de specifieke en nauw met elkaar verbonden aard van de HIPCAR model teksten, zal het voor de begunstigde projectlanden het voordeligst zijn wetgeving te ontwikkelen en introduceren op basis van deze modellen op een gecoördineerde wijze. De modellen voor de elektronische handel (transacties en

bewijs) zullen het meest effectief functioneren in geval van gelijktijdige ontwikkeling en adoptie van de kaders voor cybercriminaliteit en onderscheppen van communicatie, aangezien die zo nauw verbonden en afhankelijk van elkaar zijn voor het aanpakken van de zorgpunten betreffende de ontwikkeling van een gedegen regelgeving. De kaders voor toegang tot publieke informatie en privacy en gegevensbescherming bevatten ook dergelijke synergieën in de administratieve kaders en kerncompetentie vereisten dat de gelijktijdige aanname slechts beide kaders kan versterken in de uitvoering ervan.

Op deze manier zal er een optimale mogelijkheid gecreëerd worden om de holistische kaders te benutten die zijn ingesteld in de regio.

Dit rapport

Dit rapport handelt over Cybercriminaliteit, een van de werkterreinen van de Werkgroep inzake ICT-Beleidskader en Wetgevingskader voor Kwesties de Informatiemaatschappij rakende. Het omvat de Richtlijnen voor Model beleid en een Model Wettekst met Memorie van Toelichting die de landen in het Caribisch gebied zouden kunnen gebruiken wanneer zij hun eigen nationaal beleid en wetgeving op dit gebied ontwikkelen of bijwerken.

Voorafgaand aan het formuleren van dit document, heeft een team van deskundigen van HIPCAR – in nauwe samenwerking met de bovenstaande leden van de Werkgroep – een evaluatie voorbereid en beoordeeld van bestaande wetgeving in de vijftien begunstigde HIPCAR-landen in de regio die zich op zes gebieden heeft geconcentreerd: Elektronische Transacties, Elektronisch Bewijs bij e-Commerce, Bescherming van Privacy en gegevens, Onderscheppen van Communicatie, Cybercriminaliteit, en Toegang tot publieke informatie (Vrijheid van Informatie). Deze evaluatie hield rekening met geaccepteerde internationale en regionale beste praktijken.

Deze regionale evaluatie – apart gepubliceerd als bijbehorend document voor het huidige rapport[3] – betrof een vergelijkende analyse van de huidige wetgeving met betrekking tot Cybercriminaliteit in de begunstigde HIPCAR-landen en de identificatie van eventuele lacunes met betrekking hiertoe, waardoor de basis werd gelegd voor de ontwikkeling van een raamwerk voor model beleid en wetteksten dat hierin wordt gepresenteerd. Doordat de nationale, regionale en internationale beste toepassing in de praktijk en standaarden[4] worden weerspiegeld, terwijl tegelijkertijd de compatibiliteit met de juridische tradities in het Caribisch gebied zijn gegarandeerd, beantwoorden de model documenten in dit rapport aan de specifieke vereisten van de regio.

Het HIPCAR-stuurcomité – voorgezeten door de Caribische Telecommunicatie Unie (CTU) – heeft een team van consultants begeleidt en ondersteunt, waaronder Marco Gercke en Pricilla Banner. De model wettekst inzake cybercriminaliteit werd in drie fasen ontwikkeld in eerste instantie door de HIPCAR-consultants: (1) het opstellen van een evaluatierapport; (2) de ontwikkeling van richtlijnen voor model beleid; en (3) het formuleren van een model wettekst. Hierna, werden de concept documenten bekeken, besproken en aangenomen met een brede consensus door de participanten tijdens de twee consultatieworkshops voor de HIPCAR-Werkgroep inzake Kwesties de Informatiemaatschappij rakende te Saint Lucia van 8-12 maart 2010 en te St. Kitts en Nevis van 19-22 juli 2010 (zie bijlagen). De Memorie van Toelichting bij de model wettekst is opgesteld door Dr. Marco Gercke waarin onder andere de zaken die naar voren zijn gebracht in de tweede workshop worden behandeld. Dit document bevat daarom gegevens en informatie zoals bekend in juli 2010.

---

[3] Zie “ICT-Beleidskader en Wetgevingskader voor Kwesties de Informatiemaatschappij rakende – Elektronische Transacties: Evaluatierapport inzake de huidige situatie in het Caribisch gebied” beschikbaar op www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

[4] Zoals weerspiegeld in de gereedschapskist voor Wetgeving inzake Cybercriminaliteit en het Begrijpen van Cybercriminaliteit: Een gids voor ontwikkelingslanden, de *Model Wet inzake Elektronisch Bewijsmateriaal van de Gemenebest* (LMM(02)1), Directief 2002/58/EC, en nationale benaderingen zowel binnen als buiten de regio.

Volgend op dit proces werden de documenten afgerond en verspreid onder alle belanghebbenden ter overweging van de overheden van de HIPCAR begunstigde landen.

Het belang van het bestrijden van cybercriminaliteit

In de laatste decennia zijn computercriminaliteit en cybercriminaliteit uitgegroeid tot een belangrijk zorgpunt voor de rechtshandhaving in de hele wereld. Sinds het debat over crimineel misbruik van computer- en netwerktechnologie begon in de jaren 1960, is het belang van het onderwerp voortdurend opgekomen.[5] Gedurende een halve eeuw van intensieve discussies, zijn verschillende oplossingen besproken om het probleem aan te pakken. Echter, in het bijzonder als gevolg van constante technische ontwikkelingen en de veranderende methoden over hoe de misdrijven worden uitgevoerd, blijft het probleem op de agenda van zowel nationale regeringen en internationale / regionale organisaties.

Van de jaren 1960 tot de jaren 1980, waren computermanipulatie en dataspionage – vaak niet gedekt door bestaande strafwetgeving – en met name de ontwikkeling van een juridisch antwoord, vormde de focus van de discussie.[6] Dit veranderde in de jaren 1990 toen de grafische interface ("WWW") werd geïntroduceerd en het aantal websites en internet-gebruikers dramatisch begon te groeien. Daarna werd het mogelijk om informatie legaal beschikbaar te maken in een land en gebruikers overal ter wereld in staat te stellen om deze te downloaden – zelfs in landen waar de bekendmaking van dergelijke informatie strafbaar was gesteld.[7]

In de afgelopen jaren, wordt de discussie gedomineerd door nieuwe, zeer geavanceerde methoden voor het plegen van misdrijven zoals "Phishing[8]", "Botnet[9] aanvallen" en het opkomende gebruik van technologieën die moeilijker te onderzoeken zijn door de wetshandhaver, zoals "Voice-over-IP (VoIP) communicatie"[10] en" Cloud Computing"[11].

De mogelijkheid cybercriminaliteit te bestrijden is essentieel voor zowel de ontwikkelde als de ontwikkelingslanden. Met een groeiende afhankelijkheid van de beschikbaarheid van netwerken en computer systemen[12], alsook het groeiende aantal internetgebruikers, zullen misdrijven gepleegd door middel van informatie-technologie waarschijnlijk steeds vaker voorkomen en potentieel ernstiger. Met het oog op het beschermen van gebruikers die zijn begonnen met de netwerkdiensten zoals e-mail, communicatie via sociale netwerken en elektronisch bankieren te integreren, moeten landen de

5 Met betrekking tot de vroege discussie over computercriminaliteit zie: *Bequai*, Computer Crime, 1978; *Blanton*, Computer Crime, 1978; *Coughran*, Computer abuse and criminal law, 1976; *MacIntyre*, Computer and Crime, 1977; *McKnight*, Computer Crime, 1973; *Parker*, Crime by Computer, 1976; *Rose*, An analysis of computer related crime: A research study, 1977; *Sokolik*, Computer Crime: Its setting and the need for deterrent legislation, 1979; *Wilson/Leibholz*, User's Guide to Computer Crime: Its Commission, Detection and Prevention, 1969.

6 Zie bijvoorbeeld: *Nycum*, The criminal law aspects of computer abuse: Applicability of federal criminal code to computer abuse, 1976; *Sieber*, Computerkriminalitaet und Strafrecht, 1977.

7 Met betrekking tot de transnationale dimensie van cybercriminaliteit zie: *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 7.

8 De term "phishing" beschrijft een handeling die wordt uitgevoerd om aan het slachtoffer persoonlijke/ geheime informatie te ontfutselen. De term "phishing" beschreef origineel het gebruik van e-mails om te "phish" naar wachtwoorden en financiële gegevens van een zee aan internetgebruikers. Het gebruik "ph" houdt verband met populaire naamgevingsconventies van hackers. Voor meer informatie zie: Understanding Cybercrime: A Guide for Developing Countries, ITU 2009, Chapter 2.8.4.

9 Botnets is een verkorte term voor een groep van gecompromitteerde computers die software draaien die onder externe controle staat. Voor meer details, zie *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4.

10 *Simon/Slay*, "Voice over IP: Forensic Computing Implications", 2006.

11 *Velasco San Martin,* Jurisdictional Aspects of Cloud Computing, 2009; *Gercke*, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, Bladzijde 499 et seq.

12 Zie met betrekking hiertoe: Understanding Cybercrime: A Guide for Developing Countries, ITU, 2009, page 65.

mogelijkheid hebben om op te treden wanneer die diensten worden aangevallen of misbruikt op andere manieren. Maar het belang van het hebben van het vermogen om een onderzoek in te stellen om overtreders te identificeren en digitaal bewijs te verzamelen gaat verder dan consumentenbescherming. Het internet is een wereldwijde markt en bedrijven bieden diensten wereldwijd aan. Als landen een omgeving willen creëren waarin e-handel kan groeien, moeten zij op de lange termijn ervoor zorgen dat misdaden tegen dergelijke ondernemingen niet ongestraft blijven.

Als gevolg daarvan heeft cybercriminaliteit het gemaakt tot de top van de agenda in de meeste landen. Het is belangrijk te benadrukken dat – in tegenstelling tot andere onderwerpen – dit onderwerp nog jaren lang een prioriteit zal blijven aangezien het aanpakken van deze kwestie niet iets is dat voor eens en voor altijd gedaan kan worden. Cybercriminaliteit blijft zich ontwikkelen, en juridische oplossingen zullen constant van tijd tot tijd aanpassingen vereisen.

Het verminderen van de respons op technische oplossingen zal zeer waarschijnlijk de problemen niet oplossen. Sommige van de technische oplossingen die geïmplementeerd worden als onderdeel van de anti-cybercriminaliteitsstrategieën omvatten vaak ook firewalls (die illegale toegang tot computersystemen voorkomen) of codering (om illegale onderschepping van communicatie te voorkomen). Maar ervaring uit het verleden leert ons dat – naast de technische oplossingen – wetgevende maatregelen ook nodig zijn: een efficiënte strafwetgeving voor de bestraffing van bepaalde vormen van computercriminaliteit en cybercriminaliteit, alsook het bestaan van aanverwante procedurele instrumenten die de rechtshandhaver in staat stellen onderzoek uit te voeren zijn essentiële vereisten voor de betrokkenheid van rechtshandhavingslichamen in de strijd tegen computercriminaliteit en cybercriminaliteit. De landen die geen adequate wetgeving hebben, lopen het risico in de eerste plaats dat rechtshandhavingsinstanties niet in staat zullen zijn om burgers die slachtoffer zijn geworden van computercriminaliteit te ondersteunen. Maar nog ernstiger is het feit dat het ontbreken van strafbaarstelling van sommige vormen van cybercriminaliteit daders zelfs zou beschermen of hen motiveren om wederrechtelijke activiteiten te verhuizen vanuit het buitenland naar landen waar het aan wetgeving ontbreekt. Het voorkomen van "toevluchtsoorden" van waaruit criminelen straffeloos activiteiten kunnen ontplooien is daarom een belangrijke uitdaging geworden bij het voorkomen van cybercriminaliteit.[13] Overal waar "toevluchtsoorden" bestaan, is er een dreiging dat daders deze zullen gebruiken om onderzoek te ontlopen. Een bekend voorbeeld hiervan is de "Love Bug" computerworm, ontwikkeld door een verdachte in de Filippijnen in 2000[14] waarmee wereldwijd miljoenen computers werden geïnfecteerd.[15] Lokaal onderzoek werd gehinderd door het feit dat de ontwikkeling en verspreiding van kwaadaardige software op dat moment niet afdoende strafbaar was gesteld in de Filippijnen.[16]

Hoewel de ontwikkeling van nieuwe technologieën vooral is gericht op het voldoen aan de eisen van de westerse consument, hebben de ontwikkelingslanden – ondanks de nog aanwezige behoefte aan verdere verbetering – aanzienlijke vooruitgang geboekt bij het verkleinen van de kloof, in het bijzonder met

13 Deze kwestie werd aangepakt door een aantal internationale organisaties. De VN Resolutie van de Algemene Vergadering 55/63 geeft aan: “Staten moeten verzekeren dat hun wetten en praktijk veilige havens elimineren voor degenen die informatietechnologie strafrechtelijk misbruiken”. De volledige tekst van de resolutie is beschikbaar op: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. Het G8 10 punten actieplan benadrukt: “Er mogen geen veilige havens zijn voor degenen die informatietechnologie misbruiken”. Zie onder: Understanding Cybercrime: A Guide for Developing Countries, ITU 2009, Chapter 5.2.

14 Voor meer informatie, zie http://en.wikipedia.org/wiki/ILOVEYOU; met betrekking tot de invloed van een worm op bescherming van kritieke informatie infrastructuur, zie: *Brock*, “ILOVEYOU” Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000.

15 BBC News, “Police close in on Love Bug culprit”, 06.05.2000.

16 Zie bijvoorbeeld: CNN, “Love Bug virus raises spectre of cyberterrorism”, 08.05.2000; *Chawki*, “A Critical Look at the Regulation of Cybercrime”, www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, “Cyber Crime and Security – The Transnational Dimension” in *Sofaer/Goodman*, “The Transnational Dimension of Cyber Crime and Terrorism”, 2001, page 10; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Hoofdstuk 6, bladzijde 233.

betrekking tot de toegang tot informatie.[17] In 2005 is het aantal internetgebruikers in ontwikkelingslanden gestegen boven het aantal gebruikers in geïndustrialiseerde landen.[18] Met de stijgende connectiviteit en de transformatie van traditionele handel naar e-handel, is cybercriminaliteit niet langer een probleem alleen voor ontwikkelde, maar ook voor ontwikkelingslanden.[19] Echter, ontwikkelingslanden in het algemeen – en kleine eilandstaten in het bijzonder – zien zich geplaatst voor een aantal specifieke uitdagingen bij de implementatie van wetgeving. Terwijl de misdaden waarmee zij worden geconfronteerd tot op zekere hoogte dezelfde zijn als waarmee de ontwikkelde landen worden geconfronteerd, hebben de ontwikkelingslanden speciale eisen wanneer het gaat om de respons. De ontwikkelde landen kunnen bij voorbeeld in staat zijn om een zogenaamde 24 / 7 meldpunt te hebben voor internationale wederzijdse verzoeken voor rechtsbijstand. Ontwikkelingslanden hebben vaak niet de capaciteit om een dergelijke infrastructuur te onderhouden. Het is daarom essentieel dat de ontwikkelingslanden rekening houden met internationale normen en hun specifieke situatie bij het ontwikkelen van een anti-cybercriminaliteitsstrategie in het algemeen en cybercriminaliteitswetgeving in het bijzonder.

17 Met betrekking tot de mogelijkheden en de technologie beschikbaar om toegang te krijgen tot het internet in ontwikkelingslanden, zie: *Esteve/Machin*, Devices to access Internet in Developing countries, available at: www2007.org/workshops/paper_106.pdf.

18 Zie “Development Gateway’s Special Report, Information Society – Next Steps?”, 2005, beschikbaar op: http://topics.developmentgateway.org/special/informationsociety.

19 De specifieke eisen van ontwikkelingslanden worden besproken in de ITU publicatie “Understanding Cybercrime: A Guide for Developing Countries” that was published in 2009 en is gratis beschikbaar in alle zes VN-talen.

Deel I:
Richtlijnen voor model beleid – Cybercriminaliteit / e-misdrijven

Hieronder volgen de richtlijnen voor model beleid die een land kan overwegen met betrekking tot cybercriminaliteit / e-misdrijven.

1. CARICOM / CARIFORUM-LANDEN ZULLEN ZICH EROP RICHTEN OM DE NODIGE GEZAMENLIJKE INTERPRETATIES VAST TE STELLEN VOOR SLEUTELBEGRIPPEN DIE WORDEN GEASSOCIEERD MET CYBERCRIMINALITEIT.

- Er zal een passende definitie zijn van “computer”, “computersysteem”, “apparaat”, “computergegevens”, “inhoudelijke gegevens”, “verkeersgegevens”, “locatiegegevens”, “document”, “elektronische bescheiden”, “elektronisch document”, “elektronische handtekening”, “digitale handtekening” en “tijdstempel”.
- Er zal een voldoende ruime formulering van de definitie van deze termen zijn gekoppeld aan een lijst van illustratieve voorbeelden.
- Er zal een definitie zijn met betrekking tot welke terminologie wordt overgelaten aan rechterlijke interpretatie, en hoe dergelijke judiciële activiteiten opgevolgd kunnen worden zodat de bij wet neergelegde definities en judiciële definities geharmoniseerd zijn – op nationaal niveau, zal elke lidstaat besluiten welke optie het beste is voor hen.
- Vergemakkelijken van harmonisering door het delen van judiciële precedenten: het definiëren van specifieke technische termen voor zover als mogelijk.
- Trainingsmateriaal zal worden ontwikkeld om onderzoekers, officieren van justitie en rechters te voorzien van materiaal voor de nodige interpretatie van die termen, indien vereist, evenals relevante belanghebbenden.

2. CARICOM / CARIFORUM-LANDEN ZULLEN INHOUDELIJKE STRAFRECHTELIJKE WETTEN ONTWIKKELEN DIE HANDELEN OVER CYBERCRIMINALITEIT

- Er zullen bepalingen zijn die de meest algemene en internationaal geaccepteerde vormen van cybercriminaliteit, evenals die misdrijven die specifiek van belang zijn voor de regio (zoals bij voorbeeld SPAM) behandelen.
- Om de samenwerking met rechtshandhavingsinstituten te verzekeren van landen in de regio evenals buiten de regio, zal de wetgeving overeenstemmen met zowel internationale normen en beste praktijken, evenals (voor zover als mogelijk) de bestaande regionale standaarden en beste praktijken.
- Er zal een bepaling zijn die opzettelijk evenals wederrechtelijke toegang tot een computersysteem strafbaar stelt, evenals het illegaal verblijven* in een computersysteem. Een verzwaring van de straf in die gevallen waar beschermingsmaatregelen zijn omzeild om de verzending te onderscheppen kan worden overwogen.
- Er zal een bepaling zijn voor het strafbaarstellen van de opzettelijke en illegale onderschepping van niet-publieke gegevensverzending (wederrechtelijke onderschepping). Deze bepaling zou een rechtmatige onderschepping door de bevoegde autoriteiten niet in de weg mogen staan. Een verzwaring van de straf in die gevallen waar beschermingsmaatregelen zijn omzeild om de verzending te onderscheppen kan worden overwogen.

- Er zal een bepaling zijn die het opzettelijk en wederrechtelijk ingrijpen in computergegevens strafbaar stelt. Er moet verzekerd worden dat de toepassing van een procedureel instrument noodzakelijk voor onderzoek niet verhinderd wordt in gevallen waarin de overtreder verschillende overtredingen begaat en elke overtreding slechts leidt tot beperkte schade.
- Er zal een bepaling zijn die opzettelijk en wederrechtelijk ingrijpen in computersystemen strafbaar stelt (zoals aanvallen waarbij een dienst wordt geweigerd). Een verzwaring van de straf in die gevallen waar kritieke infrastructuur wordt beïnvloed kan worden overwogen.
- Er zal een bepaling zijn die opzettelijke en wederrechtelijke productie, verkoop en aanverwante daden van instrumenten die voornamelijk zijn ontworpen voor het plegen van computermisdrijven strafbaar stelt. Er moet een garantie zijn dat dergelijke wetgeving het rechtmatig gebruik van dergelijke softwareprogramma's niet strafbaar stelt.
- Er zal een bepaling zijn die opzettelijk en wederrechtelijk gebruik van computergerelateerde vervalsingen strafbaar stelt. Er moet voor worden gezorgd dat dergelijke wetgeving in het bijzonder de handelingen omvat van het versturen van phishing e-mails. Een verzwaring van de straf in die gevallen waarin een groot aantal e-mails wordt verzonden moet in overweging worden genomen.
- Er zal een bepaling zijn die opzettelijk en wederrechtelijke computer-gerelateerde fraude strafbaar stelt.
- Er moet worden verzekerd dat bestaande wetgeving die fraude strafbaar stelt ook van toepassing is in het geval dat de overtreders elektronische communicatiemiddelen gebruiken om te communiceren met het slachtoffer.
- Er moet een bepaling zijn die de opzettelijke en wederrechtelijke productie, verkoop en daaraan gerelateerde handelingen die te maken hebben met kinderpornografie strafbaar stellen. Internationale normen zouden in het bijzonder met betrekking hiertoe in acht genomen moeten worden. De wetgeving zou daarnaast de strafbaarstelling van het bezit van kinderpornografie moeten dekken, evenals het zich toegang verschaffen tot websites met kinderpornografie. Een uitzondering moeten worden opgenomen die rechtshandhavingsinstanties in staat stelt onderzoek uit te voeren.
- Er dient een bepaling te zijn die handelingen strafbaar stelt die te maken hebben met het verzenden van SPAM indien dat de mogelijkheid van de gebruikers beïnvloedt om toegang te krijgen tot het Internet.[20]
- De wetgeving moet de uitdagingen weerspiegelen die zich voordoen bij het toeschrijven.
- Er dient een bepaling te zijn die opzettelijke en wederrechtelijke handeling strafbaar stelt die te maken hebben met identiteit. De verschillende fasen van identiteitsdiefstal (het verkrijgen, overdragen en gebruiken van identiteitsgerelateerde informatie) moet in overweging worden genomen.

3. CARICOM / CARIFORUM-LANDEN ZULLEN DOELMATIGE MAAR EVENWICHTIGE PROCEDURELE INSTRUMENTEN ONTWIKKELEN DIE DE BEVOEGDE AUTORITEITEN IN STAAT STELLEN CYBERCRIMINALITEIT TE ONDERZOEKEN MAAR DE RECHTEN VAN DE VERDACHTE BESCHERMEN.

- De procedurele instrumenten zouden niet mogen komen aan de internationaal evenals regionaal geaccepteerde fundamentele rechten van de verdachte.
- Er moet een bepaling zijn die de bevoegde autoriteiten in staat stelt opdracht te geven tot de versnelde bewaring van computergegevens.
- Er moet een bepaling zijn die de bevoegde autoriteiten in staat stelt de gedeeltelijke onthulling te doen van bewaarde computergegevens.

[20] (Er blijft een zorgpunt over de evenredigheid van het rechtsmiddel)

- Er moet een bepaling zijn die de bevoegde autoriteiten in staat stelt de overlegging van computergegevens te bevelen.
- Er moet een bepaling zijn die de bevoegde instanties in staat stelt specifieke huiszoekingsinstrumenten te gebruiken met betrekking tot digitaal bewijsmateriaal en computertechnologie. De wet zal huiszoekingsprocedures reguleren op een wijze waarbij wordt vermeden dat in twijfel wordt getrokken dat de vergaring van bewijsmateriaal op een gecertificeerde wijze is geschiedt en is overlegd als materieel bewijsmateriaal van de verzamelde gegevens en van de bestaande digitale omgeving.
- Er dient een bepaling te zijn die de bevoegde autoriteiten in staat stelt de rechtmatige verzameling van verkeersgegevens en de rechtmatige onderschepping van inhoudelijke gegevens te bevelen.
- Beperkt tot gevallen van ernstige misdrijven moet er een bepaling zijn op grond waarvan de bevoegde autoriteiten geavanceerde onderzoeksinstrumenten kunnen inzetten, zoals het gebruik van key-loggers en forensische software op afstand om wachtwoorden die door de verdachte van een dergelijke misdaad worden gebruikt te verzamelen of de verbinding die wordt gebruikt door een verdachte te identificeren.

4. CARICOM / CARIFORUM-LANDEN ZULLEN INSTRUMENTEN ONTWIKKELEN VOOR TRANSNATIONALE SAMENWERKING BIJ CYBERCRIMINALITEITSONDERZOEKEN

- Het kader voor internationale samenwerking moet de internationale normen voor samenwerking weerspiegelen, evenals de specifieke behoeften met betrekking tot cybercriminaliteitsonderzoek.
- Het kader moet ook de oprichting van een aangewezen 24/7 aanspreekpunt voor verzoeken omvatten.
- Het kader moet het gebruik van versnelde communicatiemiddelen mogelijk maken (zoals email en fax).

5. CARICOM / CARIFORUM-LANDEN MOETEN EEN KADER ONTWIKKELEN VOOR DE REGULERING VAN DE VERANTWOORDELIJKHEID VAN INTERNET DIENSTVERLENERS

- Indien er aansprakelijkheid is, dan moet het kader de strafrechtelijke verantwoordelijkheid van de aanbieder van toegang beperken met betrekking tot overtredingen gepleegd door gebruikers van hun dienst, indien de aanbieder de verzending niet heeft geïnitieerd, de geadresseerde niet heeft uitgekozen en de informatie vervat in de verzending niet heeft veranderd.
- Indien er aansprakelijkheid is, dan moet het kader de strafrechtelijke verantwoordelijkheid van de aanbieder van caching diensten beperken voor automatische, tussentijdse en tijdelijke opslag van informatie.
- Indien er aansprakelijkheid is, dan moet het kader de strafrechtelijke verantwoordelijkheid van de hosting provider beperken indien de aanbieder geen feitelijke kennis heeft van het bestaan van illegale gegevens of die direct verwijdert op het moment dat die daarvan kennis krijgt.

Deel II:
Model wettekst –
Cybercriminaliteit / e-misdrijven

Onderstaand volgt een model wettekst die een land in overweging kan nemen bij de ontwikkeling van nationale wetgeving die betrekking heeft op cybercriminaliteit. Deze model tekst is gebaseerd op de richtlijnen voor model beleid hierboven aangegeven.

Indeling van de artikelen

HOOFDSTUK I – INLEIDING 17

1. Citeertitel 17
2. Doelstelling 17
3. Definities 17

HOOFDSTUK II – OVERTREDINGEN 19

4. Wederrechtelijke toegang 19
5. Wederrechtelijk verblijven 19
6. Wederrechtelijk onderscheppen 20
7. Wederrechtelijke verstoring van computergegevens 20
8. Dataspionage 20
9. Wederrechtelijke systeemverstoring 20
10. Onwettige apparaten 21
11. Computer-gerelateerde vervalsing 22
12. Computer-gerelateerde fraude 22
13. Kinderpornografie 22
14. Identiteit-gerelateerde misdrijven 22
15. SPAM 23
16. Openbaarmaking van bijzonderheden van een onderzoek 23
17. Nalaten bijstand te verlenen 23
18. Pesten door middel van elektronische communicatie 24

HOOFDSTUK III – RECHTSGEBIED 24

19. Rechtsgebied 24

HOOFDSTUK IV – PROCESRECHT 24

20. Onderzoek en inbeslagname 24
21. Bijstand 25

22. Bevel tot overlegging 25
23. Versnelde bewaring 25
24. Gedeeltelijke openbaarmaking van verkeersgege-vens 25
25. Verzamelen van verkeersgege-vens 26
26. Onderschepping van inhoudelijke gegevens 26
27. Forensische software 26

HOOFDSTUK V – AANSPRAKELIJKHEID 27

28. Geen monitoringsplicht 27
29. Aanbieder van toegang 27
30. Aanbieder van hosting diensten 28
31. Aanbieder van caching diensten 28
32. Aanbieder van hyperlinks 28
33. Aanbieder van zoekmachine 29

Deel II

HOOFDSTUK I – INLEIDING

Citeertitel 1. Deze wet wordt aangehaald als de "Wet inzake Computercriminaliteit en Cybercriminaliteit", en wordt van kracht en treedt in werking [op xxx / na publicatie in het Staatsblad].

Doelstelling 2. De doelstelling van computercriminaliteits- en cybercriminaliteitswetgeving in [vul naam van land in] zal het voorkomen en onderzoeken zijn van computer- en netwerk gerelateerde criminaliteit.

Definities 3. (1) Aanbieder van toegang: elke natuurlijke of rechtspersoon die een elektronische gegevensverzendingsdienst levert door het verzenden van informatie verstrekt door of aan een gebruiker van de dienst in een communicatienetwerk of die toegang verschaft tot een communicatienetwerk.

(2) Aanbieder van caching diensten: elke natuurlijke of rechtspersoon die een elektronische gegevensverzendingsdienst aanbiedt door automatisch, tussentijds en tijdelijk informatie op te slaan, met als enige doel de verdere verzending efficiënter te maken van de informatie naar andere gebruikers van de dienst op hun verzoek.

(3) Kind: elke persoon beneden de leeftijd van achttien (18) jaren.

(4) Kinderpornografie: pornografische materiaal dat:

a. een kind dat is betrokken in seksueel expliciet gedrag;

b. een persoon die een kind lijkt te zijn betrokken in seksueel expliciet gedrag; of

c. afbeeldingen waarin een kind wordt getoond betrokken in seksueel expliciet gedrag;

uitbeeldt, presenteert of afbeeldt. Dit omvat, maar is niet beperkt tot, ieder audio-, visueel of tekstueel pornografisch materiaal.

Een land kan de strafbaarstelling beperken door (b) en (c) niet te implementeren.

(5) Computersysteem (of informatiesysteem): een apparaat of een groep van onderling verbonden of aanverwante apparaten, waaronder het internet, waarvan een of meer, op grond van een programma, de automatische verwerking van gegevens of enige andere functie uitvoert.

(6) Computergegevens: elke weergave van feiten, concepten, informatie (zowel tekst, geluid als afbeeldingen) in een vorm die geschikt is voor de verwerking in een informatiesysteem, waaronder een programma dat geschikt is te veroorzaken dat een informatiesysteem een functie uitvoert.

(7) Opslagmedium voor computergegevens: elk artikel of materiaal (bij voorbeeld, een schijf) waarvan men informatie kan reproduceren, met of zonder de hulp van enig ander artikel of apparaat.

(8) Kritieke infrastructuur: computersystemen, apparaten, netwerken, computerprogramma's, computergegevens, zo belangrijk voor het land dat het uitvallen of de vernietiging of verstoring van dergelijke systemen en goederen een ondermijnende invloed zou hebben op de veiligheid, nationale of economische veiligheid, nationale volksgezondheid en veiligheid, of enige combinatie van die zaken.

(9) Apparaat omvat maar is niet beperkt tot

a. componenten van computersystemen, zoals grafische kaarten, geheugen, chips;

b. opslagcomponenten, zoals harde schijven, geheugenkaarten, compacte schijven, banden;

c. invoerapparaten, zoals toetsenborden, een muis, muispad, scanner, digitale camera's;

d. uitvoerapparaten, zoals printers, schermen.

(10) Hinder in relatie tot een computersysteem omvat, maar is niet beperkt tot:

a. het afsnijden van de elektriciteitstoevoer van een computersysteem; en

b. het veroorzaken van elektromagnetische storing aan een computersysteem; en

c. het aantasten van een computersysteem met alle mogelijke middelen; en

d. invoeren, verzenden, beschadigen, uitwissen, schaden, veranderen of blokkeren van computergegevens.

(11) Aanbieder van hosting diensten: elke natuurlijke of rechtspersoon die een elektronische gegevensverzendingsdienst verleend door het opslaan van informatie verstrekt door een gebruiker van de dienst.

(12) Hyperlink: een kenmerk of eigenschap van een element zoals een symbool, woord, zinsnede of afbeelding waarin informatie is vervat van een andere bron en die verwijst naar en de afbeelding veroorzaakt van een ander document wanneer het wordt uitgevoerd.

(13) Onderschepping omvat, maar is niet beperkt tot het het verwerven, bekijken en vastleggen van computergegevenscommunicatie ongeacht of die geschiedt per draad, draadloze, elektronische, optische, magnetische, mondelinge of op andere wijze tijdens de verzending met gebruik van een technisch apparaat.

(14) Meerdere elektronische berichten: een briefbericht, waaronder e-mail en instant messaging verstuurd naar meer dan duizend geadresseerden.

(15) Forensische software op afstand: onderzoekssoftware geïnstalleerd op een computersysteem en gebruikt voor het uitvoeren van taken, die inhouden maar niet beperkt zijn tot het registreren van toetsaanslagen of het verzenden van een IP-adres.

(16) Inbeslagneming omvat:

a. het activeren van elk lokaal computersysteem en opslagmedia voor computergegevens ;

b. het maken en bewaren van een kopie van computergegevens, waaronder het gebruik van lokale apparatuur;

c. het onderhouden van de integriteit van de relevante opgeslagen computergegevens;

d. het ontoegankelijk maken, of verwijderen van computergegevens op de computer waartoe men zich toegang heeft verschaft;

e. het maken van een afdruk van de uitvoer van computergegevens; of

f. het inbeslagnemen of op gelijkaardige wijze bemachtigen van een computersysteem of deel daarvan of een opslagmedium voor computergegevens.

(17) Internet dienstverlener tussen een natuurlijke persoon of rechtspersoon die aan gebruikers diensten verleent waarnaar wordt verwezen in artikelen 28-33 hiervan.

(18) Verkeersgegevens: computergegevens die:

a. verband houden met communicatie door middel van een computersysteem; en

b. zijn gegenereerd door een computersysteem dat deel is van de communicatieketen; en

c. de oorsprong van de communicatie, bestemming, route, tijd datum, grootte, duur of soort van de onderliggende diensten toont.

(19) Zaak omvat maar is niet beperkt tot:

a. een computersysteem of deel van een computersysteem;

b. een ander computersysteem, indien:

i. computergegevens van dat computersysteem beschikbaar zijn voor het eerste computersysteem dat wordt doorzocht; en

ii. er redelijke gronden zijn te geloven dat de computergegevens die gezocht worden opgeslagen zijn op het andere computersysteem;

c. een opslagmedium voor computergegevens.

(20) Gebruiken zal omvatten

a. het ontwikkelen van forensische software op afstand; en

b. het toepassen van forensische software op afstand; en

c. het kopen van forensische software op afstand.

HOOFDSTUK II – OVERTREDINGEN

Wederrechtelijke toegang 4. (1) Een persoon die opzettelijk, zonder rechtmatig excuus of rechtvaardiging, of die een rechtmatig excuus of rechtvaardiging te buiten gaat, zich tot een geheel of een deel van een computersysteem toegang verschaft begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

(2) Een land kan beslissen de loutere ongeoorloofde toegang niet strafbaar te stellen mits er andere effectieve rechtsmiddelen daarvoor beschikbaar zijn. Verder kan een land eisen dat de overtreding wordt begaan door het schenden van veiligheidsmaatregelen of met de bedoeling computergegevens te verkrijgen of met een andere oneerlijke bedoeling.

Wederrechtelijk verblijven 5. (1) Een persoon die opzettelijk, zonder rechtmatig excuus of rechtvaardiging of die een rechtmatig excuus of rechtvaardiging te buiten gaat, ingelogd blijft op een computersysteem of deel van een computersysteem of voortgaat een computersysteem te gebruiken begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

(2) Een land kan beslissen het louter ongeoorloofd verblijven niet strafbaar te stellen mits er andere effectieve rechtsmiddelen daartegen beschikbaar zijn. Verder kan een land vereisen dat de overtreding wordt begaan door het schenden van veiligheidsmaatregelen of met de bedoeling computergegevens te verkrijgen of met een andere oneerlijke bedoeling.

Wederrechtelijk onderschepen

6. (1) Een persoon die opzettelijk, zonder rechtmatig excuus of rechtvaardiging of die een rechtmatig excuus of rechtvaardiging te buiten gaat met technische middelen:

a. een niet-openbare verzending naar en van of binnen een computersysteem; of

b. elektromagnetische stralingen van een computersysteem

onderschept, begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

(2) Een land kan vereisen dat de overtreding wordt begaan met een oneerlijke bedoeling, of in verband met een computersysteem dat is verbonden met een ander computersysteem, of met omzeiling van beschermingsmaatregelen ingevoerd om te voorkomen dat men toegang heeft tot de inhoud van niet-openbare verzendingen.

Wederrechtelijke verstoring van computergegevens

7. Een persoon die opzettelijk, zonder rechtmatig excuus of rechtvaardiging, of die een rechtmatig excuus of rechtvaardiging te buiten gaat, een van de volgende handelingen uitvoert:

a. schaden of aantasten van computergegevens; of

b. verwijderen van computergegevens; of

c. veranderen van computergegevens; of

d. ongeschikt, onbruikbaar of onwerkbaar maken van computergegevens; of

e. blokkeren, onderbreken of verstoren van het rechtmatig gebruik van computergegevens; of

f. blokkeren, onderbreken of verstoren van het rechtmatig gebruik van computergegevens door een persoon; of

g. toegang weigeren tot computergegevens aan een persoon die gemachtigd is zich er toegang toe te verschaffen;

begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

Dataspionage

8. (1) Een persoon die opzettelijk zonder rechtmatig excuus of rechtvaardiging of die een rechtmatig excuus of rechtvaardiging te buiten gaat zich computergegevens die niet voor hem zijn bestemd en die speciaal zijn beschermd tegen ongeoorloofde toegang toe-eigent, voor zichzelf of voor een ander, begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

(2) Een land kan de strafbaarstelling beperken tot bepaalde categorieën computergegevens.

Wederrechtelijke

9. (1) Een persoon die opzettelijk, zonder rechtmatig excuus of rechtvaardiging of die een rechtmatig excuus of rechtvaardiging te buiten gaat:

systeemverstoring

a. het functioneren van een computersysteem hindert of verstoort; of

b. een persoon die rechtmatig een computersysteem gebruikt of beheert hindert of verstoort;

begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

(2) Een persoon die opzettelijk zonder rechtmatig excuus of rechtvaardiging of die een rechtmatig excuus of rechtvaardiging te buiten gaat een computersysteem hindert of verstoort dat uitsluitend wordt gebruikt voor het beheer van kritieke infrastructuur, of in het geval waarin dat niet uitsluitend gebruikt wordt voor het beheer van kritieke infrastructuur, maar het wordt gebruikt in het beheer van kritieke infrastructuur en dat gedrag beïnvloedt het gebruik of beïnvloedt het beheer van de kritieke infrastructuur zal er een gevangenisstraf zijn voor een periode van niet meer dan [periode], of een boete van niet meer dan [bedrag], of beide.

Onwettige apparaten

10. (1) Een persoon begaat een overtreding indien die persoon:

a. opzettelijk, zonder rechtmatig excuus of rechtvaardiging of die een rechtmatig excuus of rechtvaardiging te buiten gaat:

i. een apparaat, waaronder een computerprogramma, dat is ontworpen of aangepast voor het begaan van een overtreding gedefinieerd in andere bepalingen van Hoofdstuk II van deze wet; of

ii. een computerwachtwoord, toegangscode of gelijkaardige gegevens waarmee men toegang kan krijgen tot een geheel of enig deel van een computersysteem;

produceert, verkoopt, aanschaft voor gebruik, importeert, exporteert of distribueert of anderszins beschikbaar maakt met de bedoeling dat het wordt gebruikt door een persoon met als doel het begaan van een overtreding neergelegd in andere bepalingen van Hoofdstuk II van deze wet; of

b. een zaak vastgelegd in lid (i) of (ii) in zijn of haar bezit heeft met de bedoeling dat het wordt gebruikt door een persoon met als doel het begaan van een overtreding neergelegd in andere bepalingen van Hoofdstuk II van deze wet, begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

(2) Deze bepaling zal niet worden geïnterpreteerd als het opleggen van strafrechtelijke aansprakelijkheid in het geval dat de productie, verkoop, aanschaf voor gebruik, import, distributie of anderszins beschikbaar maken of bezitten waarnaar wordt verwezen in lid 1 niet de bedoeling heeft een overtreding te begaan neergelegd in overeenstemming met andere bepalingen van Hoofdstuk II van deze wet, zoals ten behoeve van het geautoriseerd testen of het beschermen van een computersysteem.

(3) Een land kan besluiten louter ongeoorloofde toegang niet strafbaar te stellen mits andere doelmatige rechtsmiddelen beschikbaar zijn. Verder, kan een land besluiten de strafbaarstelling te beperken tot apparaten die zijn opgenomen in een bijlage.

Deel II

Computer-gerelateerde vervalsing

11. (1) Een persoon die opzettelijk, zonder rechtmatig excuus of rechtvaardiging, of die een rechtmatig excuus of rechtvaardiging te buiten gaat, computergegevens invoert, verandert, verwijdert of blokkeert, wat resulteert in onechte gegevens met de bedoeling dat die worden beschouwd of dat daarnaar wordt gehandeld voor juridische doeleinden alsof die authentiek zijn, ongeacht of de gegevens direct leesbaar en verstaanbaar zijn, begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

(2) Indien de bovengenoemde overtreding wordt begaan door het versturen van meerdere elektronische briefberichten van of door middel van computersystemen, dan zal de straf bestaan uit een gevangenisstraf voor een periode van niet langer dan [periode], of een boete van niet meer dan [bedrag], of beide.

Computer-gerelateerde fraude

12. Een persoon die opzettelijk, zonder rechtmatig excuus of rechtvaardiging, of die een rechtmatig excuus of rechtvaardiging te buiten gaat, een verlies van eigendom van een andere persoon veroorzaakt door:

a. invoer, verandering, verwijdering of blokkering van computergegevens;

b. verstoring van het functioneren van een computersysteem,

met een frauduleuze of oneerlijke bedoeling om, onrechtmatig, een economisch voordeel te behalen voor zichzelf of een andere persoon zal worden gestraft met een gevangenisstraf voor een periode van niet langer dan [periode], of een boete van niet meer dan [bedrag], of beide.

Kinderpornografie

13. (1) Een persoon die opzettelijk, zonder rechtmatig excuus of rechtvaardiging:

a. kinderpornografie produceert met als doel het distribueren via een computersysteem;

b. kinderpornografie aanbiedt of beschikbaar maakt via een computersysteem;

c. kinderpornografie distribueert of verzendt via een computersysteem;

d. kinderpornografie aanschaft en / of verwerft door middel van een computersysteem voor zichzelf of voor een andere persoon;

e. kinderpornografie bezit in een computersysteem of op een opslagmedium voor computergegevens; en

f. bewust toegang verkrijgt, door informatie en communicatietechnologie tot kinderpornografie,

begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

(2) Het is een verdediging voor een tenlastelegging met een overtreding ingevolge lid (1) (b) tot (1)(f) indien de persoon vaststelt dat de kinderpornografie een bona fide rechtshandhavingsdoel had.

(3) Een land kan het gedrag beschreven in artikel 13 (1) (d)-(f) niet strafbaar stellen.

Identiteit-gerelateerde misdrijven

14. Een persoon die opzettelijk zonder rechtmatig excuus of rechtvaardiging of die een rechtmatig excuus of rechtvaardiging te buiten gaat door een computersysteem te gebruiken in enige fase van de overtreding, opzettelijk een identificatiemiddel van een andere persoon met de bedoeling een

wederrechtelijke daad te begaan, of daarin bij te staan of daarmee verband houdt, welke een misdrijf is, begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

SPAM

15. (1) Een persoon die opzettelijk zonder rechtmatig excuus of rechtvaardiging:

a. opzettelijk de verzending van meerdere elektronische briefberichten initieert van of door een dergelijke computersysteem; of

b. een beschermd computersysteem gebruikt voor het doorsturen of doorzenden van meerdere elektronische berichten met het oogmerk de gebruikers te bedriegen of misleiden, of een elektronisch bericht of internet dienstverlener, met betrekking tot de oorsprong van dergelijke berichten, of

c. op materiële wijze de informatie in de kop van meerdere elektronische berichten vervalst en opzettelijk de verzending van dergelijke berichten initieert,

begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

(2) Een land kan de strafbaarstelling beperken met betrekking tot de verzending van meerdere elektronische berichten binnen klanten- of bedrijfsrelaties. Een land kan beslissen het gedrag in artikel 15 onder (1) (a) niet strafbaar te stellen mits er andere doelmatige rechtsmiddelen beschikbaar zijn.

Openbaarmaking van bijzonderheden van een onderzoek

16. Een internet dienstverlener, die een bevelschrift ontvangt in verband met een strafrechtelijk onderzoek waarin expliciet is aangegeven dat geheimhouding behouden moet worden, of dergelijke verplichting is aangegeven bij wet en opzettelijk zonder rechtmatig excuus of rechtvaardiging of die een rechtmatig excuus of rechtvaardiging te buiten gaat:

a. het feit dat een bevelschrift is uitgevaardigd; of

b. om het even wat gedaan wordt onder het bevelschrift; of

c. alle gegevens verzameld of geregistreerd ingevolge het bevelschrift;

openbaarmaakt, begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

Nalaten bijstand te verlenen

17. (1) Een persoon anders dan de verdachte die opzettelijk nalaat zonder rechtmatig excuus of rechtvaardiging of die een rechtmatig excuus of rechtvaardiging te buiten gaat een persoon toe te laten of bij te staan gebaseerd op een bevelschrift zoals neergelegd in artikelen 20 tot 22 begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

(2) Een land kan besluiten de nalatigheid om bijstand toe te laten niet strafbaar te stellen mits er andere doelmatige rechtsmiddelen beschikbaar zijn.

Pesten door middel van elektronische communicatie

18. Een persoon die elektronische communicatie initieert met het oogmerk een andere persoon iets af te dwingen, te intimideren, pesten of substantiële emotionele stress te veroorzaken met behulp van een computersysteem voor het ondersteunen van ernstig, herhaald en vijandig gedrag, begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

(2) Een land kan besluiten de nalatigheid om bijstand toe te laten niet strafbaar te stellen mits er andere doelmatige rechtsmiddelen beschikbaar zijn.

HOOFDSTUK III – RECHTSGEBIED

Rechtsgebied

19. Deze wet is van toepassing op een feit begaan of een verzuim:

a. op het grondgebied van [regelgevend land]; of

b. op een schip of vliegtuig geregistreerd in [regelgevend land]; of

c. door een onderdaan van [regelgevend land] buiten het rechtsgebied van een land; of

door een onderdaan van [regelgevend land] buiten het grondgebied van [regelgevend land] indien het gedrag van de persoon ook een overtreding zou zijn krachtens de wet van het land waar de overtreding is begaan.

HOOFDSTUK IV – PROCESRECHT

Onderzoek en inbeslagname

20. (1) Indien een [rechter] overtuigd is op basis van [informatie onder ede][beëdigde verklaring] dat er redelijke gronden zijn [om te vermoeden] [om te geloven] dat er op een locatie een zaak of computergegevens kunnen zijn:

a. die van materieel belang zijn als bewijs voor het aantonen van een overtreding; of

b. die zijn verworven door een persoon als resultaat van een overtreding;

[kan] [moet] de rechter een bevelschrift uitvaardigen die een [rechtshandhavings-] [politie] functionaris machtigt, met de nodige bijstand, om een ruimte te betreden voor een onderzoek en de inbeslagname van de zaak of de computergegevens waaronder onderzoek of gelijkaardige toegang:

i. tot een computersysteem of deel daarvan en de computergegevens die daarin zijn opgeslagen; en

ii. tot een opslagmedium voor computergegevens waarin computergegevens kunnen worden opgeslagen op het grondgebied van het land.

(2) Indien de [rechtshandhavings-] [politie] functionaris die een onderzoek uitvoert op basis van artikel 20 onder (1) gronden heeft om te geloven dat de gegevens die gezocht worden zijn opgeslagen in een ander computersysteem of deel daarvan op het eigen grondgebied, en tot dergelijke gegevens kan rechtmatig toegang worden verkregen van of is beschikbaar voor het eerste systeem, dan zal hij direct in staat zijn het onderzoek uit te breiden of op gelijke wijze toegang verschaffen tot het andere systeem.

(3) De [rechtshandhavings-] [politie] functionaris die het onderzoek uitvoert, is gemachtigd de gegevens waartoe toegang is verkregen ingevolge leden 1 en 2 in beslag te nemen of op gelijkaardige wijze veilig te stellen.

Bijstand

21. (1) Elke persoon die geen verdachte is van een misdrijf maar die kennis heeft van het functioneren van een computersysteem of maatregelen toegepast voor het beschermen van de computergegevens daarin dat het onderwerp is van een onderzoek ingevolge artikel 20 moet toestaan, en bijstaan indien redelijkerwijs vereist en verzocht door de persoon die gemachtigd is het onderzoek te doen door:

a. het verstrekken van informatie die het treffen van maatregelen mogelijk maakt waarnaar wordt verwezen ingevolge artikel 19;

b. het toegang geven en gebruiken van een computersysteem of een opslagmedium met computergegevens voor het onderzoeken van computergegevens beschikbaar op of in het systeem;

c. het verkrijgen of kopiëren van dergelijke computergegevens;

d. het gebruiken van apparatuur voor het maken van kopieën; en

e. het verkrijgen van een verstaanbare uitvoer uit een computersysteem in een opmaak die toelaatbaar is voor rechtsprocedures.

Bevel tot overlegging

22. Indien een [rechter] overtuigd is op basis van een aanvraag door een politiefunctionaris dat gespecificeerde computergegevens, of een afdruk of andere informatie, redelijkerwijs vereist is voor een strafrechtelijk onderzoek of een strafrechtelijk proces, dan kan de [rechter] bevelen dat:

a. een persoon op het grondgebied van [regelgevende land] die een computersysteem beheert computergegevens of een afdruk of andere verstaanbare datauitvoer overlegt uit het systeem;of

b. een Internet dienstverlener in [regelgevende land] informatie produceert over de personen die een abonnee zijn van de dienst of de dienst op een andere wijze gebruiken.

Versnelde bewaring

23. Indien een politiefunctionaris ervan overtuigd is dat er gronden zijn om te geloven dat computergegevens die redelijkerwijs nodig zijn voor een strafrechtelijk onderzoek in het bijzonder kwetsbaar zijn voor verlies of wijziging, dan kan de politiefunctionaris in een geschreven kennisgeving afgegeven aan een persoon die de computergegevens beheert, eisen dat de persoon verzekert dat de gegevens die zijn aangegeven in de kennisgeving worden bewaard voor een periode van zeven (7) dagen zoals aangegeven in de kennisgeving. De periode kan worden verlengd buiten de zeven (7) dagen, indien op een *ex parte* aanvraag een [rechter] de verlenging toestaat voor een verder gespecificeerde tijdsperiode.

Gedeeltelijke openbaarmaking van verkeersgegevens

24. Indien een [politiefunctionaris] ervan overtuigd is dat de gegevens opgeslagen in een computersysteem redelijkerwijs zijn vereist voor een strafrechtelijk onderzoek, dan kan de politiefunctionaris met een schriftelijke kennisgeving verstrekt aan een persoon die het beheer heeft over het computersysteem, eisen dat de persoon voldoende verkeersgegevens openbaar maakt over een specifieke communicatie om:

a. de Internet dienstverleners; en/ of

b. het pad waarlangs de communicatie is verlopen

te identificeren.

Verzamelen van verkeersgegevens

25. (1) Indien een [rechter] overtuigd is op basis van [informatie onder ede/ beëdigde verklaring] dat er redelijke gronden zijn om te [vermoeden/ geloven] dat verkeersgegevens gerelateerd aan een specifieke communicatie redelijkerwijs vereist is voor een strafrechtelijk onderzoek, dan [kan/moet] de [rechter] een persoon die dergelijke gegevens beheert bevelen om:

a. verkeersgegevens te verzamelen of te registreren die zijn geassocieerd met een specifieke communicatie over een specifieke periode; of

b. een specifieke politiefunctionaris toe te staan en te assisteren bij het verzamelen en vastleggen van die gegevens.

(2) Indien een [rechter] overtuigd is op basis van [informatie onder ede/ beëdigde verklaring] dat er redelijke gronden zijn [te vermoeden] dat verkeersgegevens redelijkerwijs zijn vereist voor een strafrechtelijk onderzoek, dan [kan/ moet] de [rechter] een politiefunctionaris machtigen om de verkeersgegevens te verzamelen of te registreren die zijn geassocieerd met de specifieke communicatie tijdens een specifieke periode door toepassing van technische middelen.

(3) Een land kan besluiten artikel 25 niet te implementeren.

Onderschepping van inhoudelijke gegevens

26. (1) Indien een [rechter] overtuigd is op basis van [informatie onder ede/ beëdigde verklaring] dat er redelijke gronden zijn om te [vermoeden] [geloven] dat de inhoud van elektronische communicatie redelijkerwijs vereist is voor een strafrechtelijk onderzoek, dan [kan/moet] de rechter:

a. een Internet dienstverlener opdracht geven van wie de dienst beschikbaar is in [regelgevend land] via de toepassing van technische middelen inhoudelijke gegevens verbandhoudende met specifieke communicatie verzonden door middel van een computersysteem te doen verzamelen of registreren of bevoegde autoriteiten toe te staan of bij te staan te die te verzamelen of registreren; of

b. een politiefunctionaris machtigen die gegevens te verzamelen of registreren door de toepassing van technische middelen.

(2) Een land kan besluiten artikel 26 niet te implementeren.

Forensische software

27. (1) Indien een [rechter] overtuigd is op basis van [informatie onder ede/ beëdigde verklaring] dat in een onderzoek met betrekking tot een overtreding opgesomd in lid 5 hieronder er redelijke gronden zijn om te geloven dat essentieel bewijsmateriaal niet kan worden vergaard door het toepassen van de instrumenten opgesomd in Hoofdstuk IV maar die redelijkerwijs zijn vereist voor een strafrechtelijk onderzoek, dan [kan/ moet] de rechter op aanvraag een politiefunctionaris machtigen forensische software op afstand te gebruiken met de specifieke taak vereist voor het onderzoek en zal deze op het computersysteem van de verdachte installeren voor het verzamelen van het relevant bewijsmateriaal. De aanvraag moet de volgende informatie bevatten:

a. verdachte van de overtreding, indien mogelijk met naam en adres; en

b. beschrijving van het beoogde computersysteem; en

c. beschrijving van de beoogde maatregel, de mate en duur van het gebruik; en

d. redenen voor de noodzaak van het gebruik.

(2) Binnen een dergelijk onderzoek is het nodig te verzekeren dat veranderingen aan het computersysteem van de verdachte beperkt blijven tot wat nodig is voor het onderzoek en dat alle mogelijke veranderingen indien mogelijk ongedaan kunnen worden gemaakt na het beëindigen van het onderzoek. Tijdens het onderzoek is het nodig bij te houden

a. welk technisch middel is gebruikt en de tijd en datum van toepassing daarvan; en

b. de identificatie van het computersysteem en de bijzonderheden van de veranderingen die zijn aangebracht in het kader van het onderzoek;

c. alle informatie die is verkregen.

Informatie die is verkregen door het gebruik van dergelijke software moet worden beschermd tegen elke verandering, ongeoorloofde verwijdering en ongeoorloofde toegang.

(3) De duur van de machtiging in artikel 27 onder (1) is beperkt tot [3 maanden]. Indien de voorwaarden voor de machtiging niet langer gelden, dient de actie direct te stoppen.

(4) De machtiging tot het installeren van de software omvat het toegang verschaffen op afstand van het computersysteem van de verdachte.

(5) Indien het installatieproces fysieke toegang vereist tot panden en erven dienen de vereisten van artikel 20 te worden vervuld.

(6) Indien nodig kan een politiefunctionaris ingevolge een bevelschrift van de rechter verleend ingevolge (1) hierboven, verzoeken dat de rechter een internet dienstverlener beveelt het installatieproces te ondersteunen.

(7) [Lijst van overtredingen].

(8) Een land kan besluiten artikel 27 niet te implementeren.

HOOFDSTUK V – AANSPRAKELIJKHEID

Geen monitoringsplicht

28. Internet dienstverleners hebben geen algemene plicht voor het monitoren van informatie die zij verzenden of opslaan namens elkaar, noch hebben zij een algemene plicht om actief de feiten en omstandigheden op te sporen die wijzen op wederrechtelijke activiteiten om zo strafrechtelijke aansprakelijkheid te vermijden. Deze bepaling heeft geen invloed op de mogelijkheid die de rechter of een administratieve autoriteit heeft om te vereisen van een aanbieder van internet om een schending op grond van enige wet aangenomen door de Nationale Assemblee in [grondgebied] te beëindigen of voorkomen.

Aanbieder van toegang

29. (1) Een aanbieder van toegang is niet strafrechtelijk aansprakelijk voor het geven van toegang en het verzenden van informatie op voorwaarde dat de aanbieder:

a. de verzending niet initieert;

b. de ontvanger van de verzending niet uitkiest; of

c. de informatie vervat in de verzending niet uitkiest of wijzigt.

(2) De handelingen van verzending en het verlenen van toegang waarnaar wordt verwezen in lid 1 omvatten automatische, tussentijdse en tijdelijke opslag van de verzonden informatie in zover die plaatsheeft met als enig doel

het uitvoeren van de verzending in het communicatienetwerk, en mist de informatie niet wordt opgeslagen voor een langere periode dan redelijkerwijs nodig voor de verzending.

Aanbieder van hosting diensten

30. (1) Een aanbieder van hosting diensten is niet strafrechtelijk aansprakelijk voor de informatie die wordt opgeslagen op verzoek van een gebruiker van de dienst, op voorwaarde dat:

a. de aanbieder van hosting diensten direct toegang tot de informatie verwijdert of blokkeert nadat een bevelschrift is ontvangen van een overheidsinstantie of de rechter om specifieke wederrechtelijk opgeslagen informatie te verwijderen; of

b. de aanbieder van hosting diensten, nadat die er kennis van heeft gekregen of bewust is geworden van specifieke wederrechtelijk opgeslagen informatie op andere wijze dan op beval van een overheidsinstantie, direct een overheidsinstantie informeert om hen in staat te stellen de aard van de informatie te evalueren en indien nodig een bevelschrift uit te vaardigen voor het verwijderen van de inhoud.

(2) Lid 1 is niet van toepassing indien de gebruiker van de dienst handelt onder de machtiging of het beheer van de aanbieder van de hosting diensten.

(3) Indien de aanbieder van hosting diensten de inhoud verwijdert na een bevelschrift te hebben ontvangen ingevolge lid 1 wordt hij vrijgesteld van contractuele verplichtingen naar zijn klant om de beschikbaarheid van de dienst te verzekeren.

Aanbieder van caching diensten

31. Een aanbieder van caching diensten is niet strafrechtelijk aansprakelijk voor de automatische, tussentijdse en tijdelijke opslag van die informatie, uitgevoerd met als enig oogmerk het efficiënter maken van de verdere versturing van de informatie naar andere gebruikers van de dienst op hun verzoek, op voorwaarde dat:

a. de aanbieder van caching diensten de informatie niet verandert;

b. de aanbieder van caching diensten de voorwaarden voor toegang tot de informatie naleeft;

c. de aanbieder van caching diensten de regels met betrekking tot het bijwerken van de informatie, gespecificeerd op een wijze die breed wordt erkend en gebruikt door de industrie, naleeft;

d. de aanbieder van caching diensten niet intervenieert in het rechtmatig gebruik van technologie, die breed erkend en gebruikt wordt door de industrie, voor het verkrijgen van gegevens met betrekking tot het gebruik van informatie; en

e. de aanbieder van caching diensten direct handelt om informatie die is opgeslagen te verwijderen of toegang daartoe te blokkeren op het moment dat het werkelijke kennis heeft van het feit dat de informatie bij de oorspronkelijke bron van de verzending is verwijderd van het netwerk, of toegang daartoe is geblokkeerd, of dat een rechter of een overheidsinstantie dergelijke verwijdering of blokkering heeft gelast.

Aanbieder van hyperlinks

32. Een Internet dienstverlener die toegang tot informatie verstrekt door een derde mogelijk maakt door het verstrekken van een elektronische hyperlink is niet aansprakelijk voor de informatie indien

a. de internet dienstverlener direct de toegang verwijdert of blokkeert tot de informatie na het ontvangen van een bevelschrift van een overheidsinstantie of rechter om de link te verwijderen; en

b. de internet dienstverlener, nadat die er kennis van heeft gekregen of bewust is geworden van specifieke wederrechtelijk opgeslagen informatie op andere wijze dan op bevel van een overheidsinstantie, direct een overheidsinstantie informeert om hen in staat te stellen de aard van de informatie te evalueren en indien nodig een bevelschrift uit te vaardigen voor het verwijderen van de inhoud.

Aanbieder van zoekmachine

33. Een dienstverlener die een zoekmachine beheert die automatisch of op basis van invoer door anderen een index opstelt van Internet-gerelateerde inhoud of elektronische instrumenten ter beschikking stelt voor het zoeken van informatie verstrekt door een derde is niet aansprakelijk voor de zoekresultaten op voorwaarde dat de aanbieder:

a. de verzending niet initieert; en

b. de ontvanger van de verzending niet uitkiest; en

c. de informatie in de verzending niet uitkiest of verandert.

Deel III:
Memorie van toelichting bij de model wettekst inzake Cybercriminaliteit / e-misdrijven

INLEIDING

Deze wettekst legt een wettelijk kader vast voor de strafbaarstelling van computer- en netwerkgerelateerde overtredingen. De belangrijkste doelstellingen van deze model wettekst zijn het strafbaarstellen van bepaalde wederrechtelijke inhoud in overeenstemming met regionale en internationale beste toepassing in de praktijk, voorzien in de nodige specifieke procedurele instrumenten voor het onderzoek van dergelijke overtredingen en het definiëren van de aansprakelijkheid van de dienstverlener.

Deze toelichting is bedoeld om de inhoud van deze wet toe te lichten, en moet worden gelezen in samenhang daarmee. Het belang van de bepalingen van deze wet wordt toegelicht en, in voorkomend geval, wordt de aandacht gevestigd op bepaalde besprekingen van de HIPCAR[21] werkgroep[22] en de Richtlijnen voor model beleid van de eerste consultatie workshop van de HIPCAR werkgroep 1. Ze zijn niet, en zijn niet bedoeld, een gedetailleerde beschrijving van deze wet te geven. Dus, waar een artikel of een deel van een artikel geen uitgebreide toelichting, commentaar of verwijzing behoeft, of wanneer er geen discussie was over een bepaalde bepaling, wordt geen gedetailleerde uitleg gegeven.

De model wettekst (wet) bestaat uit vijf hoofdstukken:

Hoofdstuk I geeft de definities en legt de doelstelling van de wet neer;

Hoofdstuk II geeft een aantal inhoudelijke strafrechtelijke bepalingen die bepaalde overtredingen strafbaar stellen;

Hoofdstuk III geeft procedures voor het bepalen van de jurisdictie;

Hoofdstuk IV geeft een aantal procedurele instrumenten die nodig zijn voor het onderzoeken van Cybercriminaliteit;

Hoofdstuk V definieert de beperkingen van de aansprakelijkheid van de internet dienstverleners.

---

21 De volledige naam van het HIPCAR-project is “Versterking van het Concurrentievermogen in het Caribisch Gebied door de Harmonisatie van Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT”. Het project met een looptijd van drie jaar werd gelanceerd in september 2008 in het kader van overkoepelend project voor de ACP-landen en wordt gefinancierd door de Europese Unie (EU) en de Internationale Telecommunicatie Unie (ITU). Het project wordt geïmplementeerd door de Internationale Telecommunicatie Unie (ITU) in samenwerking met de Caribische Gemeenschap (CARICOM) en de Caribische Telecommunicatie Unie (CTU).

22 De leden van de HIPCAR Werkgroepen bestaan uit vertegenwoordigers van Ministeries en regelgevende lichamen aangewezen door hun nationale overheden, relevante regionale lichamen en waarnemers – zoals aanbieders en andere geïnteresseerde belanghebbenden. De opdracht voor de werkgroepen zijn beschikbaar op: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/docs/ToR%20HIPCAR%20WGs.pdf.
De tweede consultatie workshop (Fase B) voor HIPCAR Werkgroep 1 inzake het ICT wettelijk kader – inzake kwestie de informatiemaatschappij rakende werd gehouden in Barbados, van 23-26 augustus 2010. Participanten hebben met een brede consensus de concept model wetteksten herzien, besproken en aangenomen betreffende het betrokken werkgebied. Waar het woord “werkgroep” wordt gebruikt in dit document, verwijst het naar de voorgaande workshop.

COMMENTAAR OP DE ARTIKELEN

HOOFDSTUK I

Artikel 1.Definities

(1) Aanbieder van toegang

De opstellers van de wettekst besloten de verantwoordelijkheid van bepaalde internet dienstverleners te beperken indien hun vermogen te voorkomen dat gebruikers misdrijven begaan beperkt is. Om die reden was het nodig een onderscheid te maken tussen de verschillende typen aanbieder. Artikel 3 lid (1) benadrukt dat de term “aanbieder van toegang” zowel een rechtspersoon als een natuurlijke persoon kan zijn. Om die reden kan zelfs een eigenaar van een privé netwerk worden beschouwd als een aanbieder van toegang.

(2) Aanbieder van caching diensten

Caching van inhoud is een wijdverspreide techniek voor het verbeteren van de snelheid van toegang tot populaire informatie. Het dekt in het bijzonder de opslag van populaire websites door dienstverleners op lokale opslagmedia zodat bandbreedte vermindert kan worden en de toegang tot de gegevens efficiënter verloopt. Dit kan bij voorbeeld worden gedaan door het opzetten van proxy servers. Het proces van het kopiëren van gegevens leidt slechts naar een kwalificatie van aanbieder van caching diensten indien de aanbieder zijn systemen op dusdanige manier configureert dat het opslagproces automatisch wordt gedaan, tussentijds en tijdelijk met als enig doel het verbeteren van de efficiency van de verdere verzending. De handmatige opslag evenals de lange-termijn opslag worden om die reden niet gedekt.

(3) Kind

De term kind werd gedefinieerd in overeenstemming met artikel 1 van het VN Verdrag inzake de rechten van het kind. Bijzonderheden over de bepaling van de leeftijd, bij voorbeeld de kwestie van het uiterlijk kan worden gebruikt in gevallen waar de informatie over de werkelijke leeftijd van het kind niet achterhaald kan worden, wordt overgelaten aan de nationale wetgevers om vast te stellen in overeenstemming met de eisen van hun nationale wetten. Definitie (7) bevat met betrekking hiertoe een leidraad met betrekking tot kinderpornografie.

(4) Kinderpornografie

De definitie van kinderpornografie werd intensief besproken door de opstellers van de wettekst. Hoewel er een brede consensus was dat kinderpornografie de documentatie zou moeten dekken van echt misbruik, besloten de opstellers het over te laten aan de nationale wetgever om te bepalen of het ook personen zou moeten dekken die een kind lijken te zijn of afbeeldingen van een minderjarige. Binnen deze context hebben de opstellers rekening ermee gehouden dat in de moderne omstandigheden realistische afbeeldingen makkelijk kunnen worden gecreëerd door het gebruik van complexe computertechnologie en dat dergelijke afbeeldingen kunnen worden gebruikt om kinderen aan te moedigen of te verleiden om in dergelijke handelingen te participeren.

Met betrekking tot het feit dat kinderpornografie niet alleen wordt verspreid met foto's en video, besloten de opstellers dusdanige taal te gebruiken dat het audio, visueel of tekstueel materiaal zou omvatten.

(5) Computersysteem

Computersysteem en informatiesysteem zijn beide termen die worden gebruikt voor het beschrijven van dataverwerkingsapparaten die in het algemeen hardware en software combineren. Computersystemen omvatten daarom invoer-, uitvoer- en opslagfaciliteiten zolang die dataverwerkingscomponenten bevatten. De opstellers van de wettekst besloten de definitie te uit te breiden zodat het tevens het internet zou omvatten.

(6) Computergegevens

De opstellers besloten de definitie van computergegevens te baseren op internationale standaarden. Om te zorgen dat alle soorten inhoud worden gedekt hebben de opstellers voorbeelden gegeven tussen haakjes.

(7) Opslagmedium voor computergegevens

Niet slechts de capaciteit, maar ook de grootte en functie van de computeropslagapparaten is veranderd in de laatste decennia. De opstellers hebben besloten een open definitie te formuleren die massaopslagapparaten dekt en micro-opslagsystemen, die bij voorbeeld worden gebruikt in autosleutels. Deze bepaling is daarom zowel van toepassing op permanente en korte-termijn opslagapparaten (zoals RAM).

(8) Kritieke infrastructuur

Vandaag worden computersystemen niet slechts gebruikt door privépersonen en bedrijven, maar ook door beheerders van kritieke infrastructuur, zoals energievoorziening of verkeersbeheersing. Aangezien infrastructuur die als kritiek wordt beschouwd van land tot land verschilt, hebben de opstellers besloten een brede definitie van kritieke infrastructuur op te nemen.

(9) Apparaten

De opstellers hebben besloten een open benadering te hebben voor de toepassing van bepalingen die naar een apparaat verwijzen door het geven van een aantal voorbeelden. Deze lijst van voorbeelden is daarom niet finaal of beperkt, maar is open voor nieuwe ontwikkelingen.

(10) Hinder

Sommige internationale benaderingen bij het aanpakken van Cybercriminaliteit stellen het onrechtmatig hinderen van computersystemen strafbaar zonder een precieze definitie te geven van wat wordt gedekt door de wet. De opstellers hebben besloten te verzekeren dat de term hinderen aanvallen vanuit een netwerk omvat (zoals de verzending van computergegevens) evenals fysieke aanvallen. Toevallige verbreking van de energietoevoer wordt gedekt door de definitie, maar zijn uitgesloten van strafrechtelijke aansprakelijkheid aangezien de verwante bepaling (artikel 9) het plegen van het feit vereist evenals de intentie.

(11) Aanbieder van hosting diensten

Net als bij de definitie van andere categorieën van internet dienstverleners, omvat de term aanbieder van hosting diensten niet alleen een rechtspersoon, maar ook een natuurlijke persoon. Het is niet nodig dat een aanbieder van hosting diensten opslagapparaten bezit. De beheerder van een website waarop de gebruikers in staat worden gesteld berichten achter te laten, handelt ook als een aanbieder van hosting diensten.

(12) Hyperlink

De opstellers hebben besloten de strafrechtelijke verantwoordelijkheid te regelen van een aanbieder van hyperlink diensten. Binnen deze context geeft de wet een brede definitie van hyperlink zodat de verschillende technische oplossingen worden gedekt.

(13) Onderschepping

De onderschepping van gegevensoverbrengingsprocessen is een procedureel instrument dat kan worden aangetroffen in verschillende internationale benaderingen om cybercriminaliteit aan te pakken. Echter, de meeste van deze instrumenten specificeren de handelingen niet of geven bijzonderheden over de rechtmatige onderzoeksprocedures. De opstellers hebben besloten enkele voorbeelden te geven van zowel rechtmatige handelingen en van de soorten communicatie die onderschepping kunnen uitmaken.

(14) Meerdere elektronische briefberichten

De opstellers erkennen de mogelijk negatieve invloed van SPAM op ontwikkelingslanden. Een essentieel onderdeel van de strafbaarstelling van SPAM is de definitie van meerdere berichten. In dit licht bezien, hebben de opstellers besloten tenminste een vereiste van een duizend (1000) berichten te vereisen.

(15) Forensische software op afstand

Een van de aspecten die intensief werd besproken tijdens de onderhandeling van de wettekst was het voeren van ingewikkelde opsporingsprocedures. De opstellers hebben kennis genomen van verslagen over het gebruik van forensische software op afstand tijdens nationale onderzoekingen. Met betrekking tot de definitie van forensische software op afstand besloten zij de mogelijke velden waar dergelijke software gebruikt zou kunnen worden aan te geven (registreren van toetsaanslagen en verzending van IP-adressen), maar de reikwijdte van deze software niet te beperken tot deze functies.

(16) Inbeslagneming

Het in beslag nemen van bewijsmateriaal is een traditioneel onderzoeksproces. Rekening ermee houdende dat naast het in beslag nemen van apparatuur er verschillende wijzen zijn waarop bewijsmateriaal kan worden verzameld. De opstellers hebben besloten verder deze definitie uit te werken door het geven van voorbeelden van activiteiten die kunnen worden beschouwd als deel van het in beslag nemen van bewijsmateriaal. Een voorbeeld dat was inbegrepen in de definitie was de bevoegdheid voor het activeren van het computersysteem van de verdachte. De opstellers vonden het de moeite waard om aan te geven dat dit een essentiële vereiste is in geval van een complex onderzoek.

(17) Internet dienstverlener

In plaats van het geven van een enkele definitie van internet dienstverlener hebben de opstellers besloten een onderscheid te maken tussen de soorten dienstverleners.

(18) Verkeersgegevens

De onderschepping van verkeersgegevens is een belangrijk onderzoeksproces. De opstellers hebben besloten een reeks criteria te geven die duidelijk de toepasselijkheid van de bepaling definieert en daarmee de beperking met betrekking tot relevante categorieën gegevens.

(19) Zaken

Zaken zijn het onderwerp van een inbeslagname. Hoewel de interpretatie van de term wordt overgelaten aan de nationale rechter, hebben de opstellers besloten een reeks voorbeelden te geven.

(20) Gebruiken

De definitie van de term “gebruiken” is relevant voor het gebruik van forensische software op afstand. Als gevolg van een intensieve discussie tijdens de werkgroepsessie, hebben de opstellers besloten uit te leggen dat niet slechts het gebruik van dergelijke software, maar ook de voorbereidende handelingen worden gedekt door de bepaling.

HOOFDSTUK II

Inleiding tot artikelen 4 – 15

De bedoeling van artikelen 4-15 van de wettekst is het verbeteren van de middelen voor het voorkomen en onderzoeken van computer- en netwerkgerelateerde misdrijven door het definiëren van een gemeenschappelijke minimumstandaard van relevante overtredingen gebaseerd op de beste praktijken die voorkomen in de regio evenals internationale standaarden. Binnen dit kader zal de definitie van standaarden in artikelen 4-15 de nationale wetgevers helpen mogelijke hiaten in de nationale wetgeving te ontdekken en het vormt tevens de basis voor een nauwere internationale samenwerking die in het algemeen een gelijke mate van strafbaarstelling vereist als gevolg van de dubbele criminaliteitsvereiste. Artikelen 4-15 geven een definitie van de minimumstandaarden en sluiten daarom een uitgebreidere strafbaarstelling op nationaal niveau niet uit.

Tijdens de discussie heeft de werkgroep besloten bepaalde kwalificerende omstandigheden toe te voegen om de strafbaarstelling te beperken die een weerspiegeling vormt van de verschillende beoordelingen van de gevaarlijke aard van het betrokken gedrag of van de noodzaak strafrecht te gebruiken als tegenmaatregel binnen de regio. Deze benadering verleent flexibiliteit aan de verschillende staten voor het bepalen van hun strafrechtelijk beleid op dit gebied.

Artikel 4: Wederrechtelijke toegang

Deze bepaling stelt het toegang verschaffen strafbaar. Het beschermde juridisch belang is de integriteit van het computersysteem. De noodzaak voor criminalisering van dergelijke handelingen weerspiegelt de belangen van de beheerders van computersystemen om hun systemen op ongestoorde wijze te kunnen laten draaien. De loutere ongeoorloofde inbreuk en niet slechts daaropvolgende misdrijven, zoals verstoring van computergegevens moeten daarom worden strafbaar gesteld aangezien het kan leiden tot belemmeringen voor legitieme gebruikers van de systemen en gegevens en kan leiden tot hoge reconstructiekosten. De bepaling vult de technische benaderingen in die dergelijk gedrag kunnen voorkomen (bv. Wachtwoord beschermingsmaatregelen) en het stelt rechtshandhavingsinstanties in staat onderzoek uit te voeren in die gevallen waarin overtreders erin slagen op succesvolle wijze de overtreding te begaan.

Toegang specificeert niet een bepaalde manier van communicatie, maar is open en vergemakkelijkt verdere technische ontwikkelingen. Het omvat alle manieren voor het zich toegang verschaffen tot een ander computersysteem, waaronder internetaanvallen, evenals wederrechtelijke toegang tot draadloze netwerken. Zelfs de wederrechtelijke toegang tot computers die niet zijn verbonden aan een netwerk (bv. door het omzeilen van wachtwoordbescherming) worden gedekt door de bepaling. Net als andere overtredingen die zijn neergelegd in dit document vereist artikel 4 dat de overtreder de overtreding met opzet begaat. Roekeloze handelingen worden daarom niet gedekt.

Toegang tot een computersysteem kan slechts worden vervolgd onder artikel 4, indien het plaatsheeft “zonder rechtmatig excuus of rechtvaardiging”. Dit vereist dat de overtreder handelt zonder bevoegdheid (ongeacht of dat wetgevend, uitvoerend, administratief, judicieel, contractueel of met wilsovereenstemming gebeurt) en het gedrag wordt anderszins niet gedekt door een vastgestelde

juridische verdediging, verschoningsgronden, rechtvaardigingen of relevante principes. Toegang tot een systeem dat vrije en open toegang verschaft aan het publiek of toegang tot een systeem met toestemming van de eigenaar of andere rechthebbende is dientengevolge niet strafbaar gesteld. Netwerkadministrateurs en veiligheidsbedrijven die de bescherming van computersystemen testen voor het identificeren van mogelijke hiaten in de beschermingsmaatregelen begaan geen misdrijf.

Het feit dat het slachtoffer van een misdrijf een wachtwoord of gelijkaardige toegangscode heeft aangereikt aan de overtreder, bv. omdat de overtreder het slachtoffer ervan overtuigde een wachtwoord of toegangscode te onthullen als gevolg van geslaagde social engineering technieken, betekent niet noodzakelijkerwijs dat de overtreder rechtmatig handelde toen hij zich toegang verschafte tot het computer systeem van het slachtoffer.

Artikel 5: Illegaal verblijven

Deze bepaling stelt het illegaal verblijven in een computersysteem strafbaar. Gelijk aan artikel 4 is het beschermde juridisch belang de integriteit van het computersysteem. De bepaling, die op deze wijze noch in de Gemenebest modelwet noch het Verdrag van de Raad van Europa inzake Cybercriminaliteit is opgenomen, weerspiegelt het feit dat de integriteit van een computersysteem niet slechts kan worden verbroken door het zich onrechtmatig toegang verschaffen tot het systeem maar ook door het verblijven in het systeem nadat toestemming daarvoor is verstreken. Dit gedrag kan niet worden gedekt door artikel 4 aangezien in dergelijke gevallen de overtreder zich niet onrechtmatig toegang heeft verschaft tot het systeem.

Verblijven vereist dat de overtreder nog steeds toegang heeft tot het computersysteem. Dit kan bij voorbeeld het geval zijn indien de overtreder ingelogd blijft of voortgaat met het doen van werkzaamheden. Het feit dat hij de theoretische mogelijkheid heeft om in te loggen op een computersysteem is niet voldoende.

Artikel 4 vereist dat de overtreder de overtredingen met opzet begaat. Roekeloze daden worden niet gedekt door dit artikel. Artikel 4 stelt alleen die handelingen strafbaar die zijn begaan “zonder rechtmatig excuus of rechtvaardiging”.

Artikel 6: Wederrechtelijke onderschepping

Deze bepaling richt zich op het gelijkstellen van bescherming van elektronische overdrachten met de bescherming van mondelinge conversaties tegen onrechtmatig afluisteren en/of opnemen die reeds bestaan in de meeste rechtssystemen. De overtreding is in het algemeen van toepassing op alle vormen van elektronische gegevensoverdracht (bv. telefoon, fax, bestandsoverdracht of email).

De toepasselijkheid van artikel 3 is beperkt tot de onderschepping van verzendingen volbracht met behulp van technische maatregelen. Onderschepping in verband met elektronische gegevens kan worden gedefinieerd als elke handeling voor het verwerven van gegevens tijdens een verzendingsproces. Onderschepping in verband met elektronische gegevens kan worden gedefinieerd als elke handeling voor het verwerven van gegevens tijdens het verzendingsproces. Dit kan worden gedaan door te luisteren, monitoren of controleren van de inhoud van communicatie. Deze bepaling is slechts van toepassing op de onderschepping van verzendingen, daarom wordt het toegang verschaffen tot opgeslagen informatie niet gezien als een onderschepping van een verzending.

De term “verzending” dekt alle dataverzendingen, of die nou per telefoon, fax, email of bestandsoverdracht plaatshebben. De overtreding neergelegd onder artikel 6 is slechts van toepassing op niet-openbare verzendingen. Een verzending is “niet-openbaar”, indien het verzendingsproces confidentieel is. Het belangrijke element om een onderscheid te maken tussen publieke en niet-publieke verzendingen is niet de aard van de gegevens die worden verzonden, maar de aard van het verzendingsproces zelf. Zelfs de onderschepping van publiek beschikbare informatie kan als crimineel worden beschouwd, indien de partijen die betrokken zijn bij de verzending van plan zijn de inhoud van hun communicatie geheim te houden. Het gebruik van een openbaar netwerk sluit nog geen “niet-openbare” communicatie uit.

Het opnemen van elektromagnetische uitstralingen in de wettekst zorgt ervoor dat een alomvattende benadering wordt gevolgd, vooral omdat oudere computers elektromagnetische uitstralingen veroorzaken tijdens hun werking. Dergelijke uitstralingen die niet worden gedekt door de term gegevens in de wettekst moesten specifiek strafbaar worden gesteld.

Artikel 6 vereist dat de overtreder de overtredingen opzettelijk uitvoert of begaat en zonder rechtmatig excuus of rechtvaardiging. Dit is niet het geval indien de onderschepping plaatsheeft op basis van instructies of met de toestemming van de deelnemers aan de verzending of indien het een rechtmatige onderschepping is op basis van strafrechtelijke bepalingen.

Artikel 7: Wederrechtelijke verstoring van computergegevens

Artikel 7 is erop gericht bestaande hiaten te vullen in nationale strafwetgeving, evenals het voorzien van gelijkaardige bescherming aan computergegevens en computerprogramma's die wordt genoten door tastbare voorwerpen tegen de opzettelijke toebrenging van schade.

De termen schaden en aantasten betekenen elke handeling die verband houdt met de negatieve verandering van de integriteit van gegevens en software. Tot op zekere hoogte overlappen deze termen elkaar. “Verwijderen” dekt handelingen zoals het verwijderen van gegevens van opslagmedia en wordt beschouwd als vergelijkbaar met de vernietiging van een tastbaar object. Het verplaatsen van het bestand naar de virtuele vuilnisemmer verwijdert het bestand niet van de harde schijf en wordt daarom niet beschouwd als een verwijdering, maar kan worden gedekt door de term weigeren van toegang. Het veranderen van gegevens dekt de wijziging van bestaande gegevens, zonder dat noodzakelijkerwijs de bruikbaarheid van de gegevens wordt verminderd. Deze wet dekt in het bijzonder de installatie van schadelijke software, zoals spyware, virussen of adware op de computer van het slachtoffer, zelfs als die achteraf niet blijken te functioneren.

De term “ongeschikt maken” dekt alle verstorende handelingen die gegevens onverwerkbaar maken voor het bedoelde gebruik. Deze wet vereist dat de gegevens bruikbaar of werkzaam was voor dergelijke verstoring.

“Het rechtmatig gebruik of het rechtmatig gebruik door een persoon blokkeren, onderbreken en verstoren” dekt elke actie die een rechtmatig dataverwerkingsproces negatief beïnvloedt De toepassing van de bepaling wordt speciaal besproken met betrekking tot de aanvallen “Weigering-van-dienstverlening”. Tijdens de aanval zijn de gegevens verstrekt op de computersysteem dat het doelwit is niet langer beschikbaar voor de potentiële rechtmatige gebruikers, evenals de eigenaar van het computersysteem. Echter, een specifiekere bepaling (artikel 9) is inbegrepen om te strafbaarstelling van dergelijke handelingen te verzekeren.

De onderdrukking van computergegevens verwijst naar een actie waarbij de beschikbaarheid van gegevens voor de persoon die toegang heeft tot het medium waarop de informatie is opgeslagen negatief wordt beïnvloed

Artikel 6 vereist dat de overtreder de overtredingen opzettelijk en zonder rechtmatig excuus of rechtvaardiging uitvoert. Het recht om gegevens te wijzigen werd besproken, vooral binnen de context van “remailers” die worden gebruikt voor het wijzigen van bepaalde gegevens met als doel het vergemakkelijken van anonieme communicatie. Het opzettelijke gebruik van dergelijke diensten wordt beschouwd als een toestemming voor de noodzakelijke wijzigingen.

Artikel 8: Dataspionage

Het verdrag inzake cybercriminaliteit evenals de Gemenebest model wet en het concept verdrag van Stanford voorzien in wettelijke oplossingen voor wederrechtelijke onderschepping, maar niet voor het wederrechtelijk verwerven van gegevens. Het is de vraag of artikel 3 van het verdrag inzake cybercriminaliteit van toepassing is op andere zaken dan die waarbij overtredingen worden begaan door het onderscheppen van dataverwerkingsprocessen.

Artikel 8 beschermt de geheimhouding van opgeslagen en beschermde computergegevens. In tegenstelling tot andere benaderingen dekt dit artikel niet slechts economische geheimen, maar ook opgeslagen computergegevens in het algemeen. Met betrekking tot de beschermingsdoelen, is deze aanpak ruim van aard, maar de toepassing van de bepaling is beperkt aangezien het verwerven van gegevens slechts strafbaar is gesteld wanneer de gegevens speciaal zijn beschermd tegen wederrechtelijke toegang. De speciale bescherming vereist dat de persoon die de informatie host beschermingsmaatregelen heeft ingevoerd die aanzienlijk de moeilijkheid vergroten voor het krijgen van toegang tot de gegevens zonder toestemming. Voorbeelden zijn wachtwoordbescherming en codering. Het is noodzakelijk dat de beschermingsmaatregelen verder gaan dan standaardbeschermingsmaatregelen die van toepassing zijn op gegevens evenals op andere eigendommen, bij voorbeeld beperking van toegang tot bepaalde delen van overheidsgebouwen. Aan de andere kant is het niet nodig dat de maatregelen gerelateerd zijn aan computertechnologie. Zelfs fysieke maatregelen zoals sloten maken de toepassing van de bepaling mogelijk.

De handeling van het verwerven dekt elke activiteit ondernomen door de overtreder voor het in bezit krijgen van relevante gegevens. Dit kan bij voorbeeld worden gedaan door het verwijderen van een opslagapparaat of het kopiëren van bestanden van de oorspronkelijke locatie naar het apparaat van de overtreder.

Artikel 9: Systeemverstoring

Voor het beschermen van toegang van beheerders en gebruikers tot ICT's werd een bepaling opgenomen die het opzettelijk verstoren van het rechtmatig gebruik van een computersysteem strafbaar stelt. Deze bepaling is om die reden erop gericht om de integriteit van computersystemen te beschermen. De toepassing van de bepaling vereist dat de overtreder het functioneren van een computersysteem verhindert of verstoort.

“Verhinderen” betekent elke handeling die de behoorlijke functionering van een computersysteem verstoort. De term wordt verder gedefinieerd in artikel 3. De werkgroep besprak of het probleem van spam email kon worden behandeld onder artikel 5, aangezien spam computersystemen kan overbelasten. Als gevolg van het feit dat de toepassing van een gelijkaardige bepaling in het Verdrag inzake Cybercriminaliteit met betrekking tot SPAM uitdagingen aan de dag legt, besloten de opstellers een specifieke bepaling op te nemen die SPAM behandel in artikel 15. Artikel 9 vereist dat de overtreder de overtredingen opzettelijk begaat en zonder rechtmatig excuus of rechtvaardiging. Daarom volgt daaruit dat toegestane computertesten niet strafbaar zullen worden gesteld.

Lid 2 bevat een regeling die betrekking heeft op een strafverzwaring indien de overtredingen kritieke infrastructuur beïnvloeden Het functioneren van een computersysteem is essentieel geworden voor het beheren van kritieke infrastructuur, zoals gezondheidszorg, transport en energietoevoer. Lid 2 neemt on die reden deze dreiging in overweging door te voorzien in een mogelijkheid om naar zwaardere straffen te verwijzen.

Twee verschillende zaken worden genoemd in lid 2, te weten (1) die invloed hebben op computersystemen die exclusief worden gebruikt voor kritische infrastructuur werkzaamheden en (2) die invloed hebben op computersystemen die niet exclusief kritieke infrastructuur besturen, maar die onder andere worden gebruikt voor bescherming van kritieke infrastructuur. In het laatste geval is het nodig te bewijzen dat het gedrag plaatshad op een tijd dat het computersysteem kritieke infrastructuur werkzaamheden aanstuurde.

Artikel 10: Onwettige apparaten

Lid 1(a) identificeert zowel de apparaten die zijn ontworpen voor het begaan en bevorderen van cybercriminaliteit evenals wachtwoorden die toegang tot een computersysteem mogelijk maken. De term apparaten dekt oplossingen gebaseerd op hardware en software die zijn gericht op het begaan van een

van de genoemde overtredingen. Voorbeelden van dergelijke software zijn virusprogramma's, of programma's die zijn ontworpen of aangepast voor het zich toegang verschaffen tot computersystemen. Computerwachtwoorden, toegangscodes of gelijkaardige gegevens voeren in tegenstelling tot apparaten geen activiteiten uit maar toegangscodes. Voorbeelden zijn gepubliceerde wachtwoorden die toegang voorzien tot betaalde diensten en databanken. De publicatie van systeemkwetsbaarheden die kunnen dienen als een instructie hoe men beschermingsmaatregelen omzeilen zijn niet gedekt in deze bepaling, zolang die geen toegangscodes omvatten. In tegenstelling tot klassieke toegangscodesysteemkwetsbaarheden geeft maakt het niet directe toegang tot een computersysteem mogelijk, maar het stelt de overtreder in staat gebruik te maken van de kwetsbaarheden zodat een computersysteem met succes kan worden aangevallen.

“Productie” betekent elk proces van het creëren van een apparaat of wachtwoord. De productie van niet-uitvoerbare delen software zal niet worden gedekt. “Verkoop” beschrijft activiteiten betrokken in het verkopen van apparaten en wachtwoorden voor geld of een andere vergoeding. “Aanschaf voor gebruik” dekt handelingen die gerelateerd zijn aan het actief verwerven van wachtwoorden en apparaten. Het feit dat de handeling van verwerven is gerelateerd aan het gebruik van dergelijke gereedschappen in het algemeen vereist de intentie van de overtreder voor het aanschaffen van gereedschappen met het doel die te gebruiken op een wijze die verder gaat dan “reguliere” opzet en “dat die wordt gebruikt met als doel het aangaan van enige van de overtredingen vastgelegd ingevolge hoofdstuk II.

“Import” heeft betrekking op handelingen voor het verwerven van apparaten en toegangscodes uit het buitenland. Als gevolg daarvan kunnen overtreders die dergelijke instrumenten importeren met als doel het verkoop daarvan, worden vervolgd zelfs nog voor zij deze gereedschappen ter verkoop aanbieden. Met betrekking tot het feit dat de aanschaf van dergelijke gereedschappen slechts wordt strafbaar gesteld indien die in verband kan worden gebracht met het gebruik, is het de vraag of de eenvoudige import zonder de intentie de gereedschappen te verkopen of the gebruiken wordt gedekt door artikel 10.

“Export” betekent de werkelijke verzending, overdracht of overbrenging van apparaten of toegangscodes buiten een land evenals een overdracht van apparaten of toegangscodes binnen een land in de wetenschap of met de intentie dat de apparaten of toegangscodes zullen worden verzonden, overgedragen of overgebracht buiten het land. “Distributie” dekt dergelijke handelingen zoals het doorsturen van apparaten of wachtwoorden naar anderen. De aanschaf voor gebruik dekt handelingen die zijn gerelateerd aan het actief verwerven van wachtwoorden en apparaten. “Beschikbaar stellen” verwijst naar een handeling die andere gebruikers in staat stelt toegang te verkrijgen tot artikelen. Het is ook bedoeld voor het dekken van de creatie of compilatie van hyperlinks zodat toegang mogelijk kan worden gemaakt tot dergelijke dienst.

Deze bepaling is in het algemeen van toepassing niet slechts op apparaten die exclusief zijn ontworpen voor het vergemakkelijken van het begaan van cybercriminaliteit, maar dekt tevens apparaten die over het algemeen worden gebruikt voor rechtmatige doelstellingen, terwijl de specifieke intentie van de overtreders is het begaan van cybercriminaliteit. De beperking tot apparaten die slechts zijn ontworpen voor het begaan van misdrijven is te eng in de reikwijdte en kan leiden tot onoverkomelijke moeilijkheden voor de bewijsvoering in strafrechtelijke processen, waardoor de bepaling virtueel niet van toepassing is of slechts van toepassing in zeldzame gevallen. Een verduidelijking dat toegestane testen niet worden getroffen werd toegevoegd in lid 3.

Artikel 10 vereist dat de overtreder de overtredingen opzettelijk begaat. Naast de reguliere intentie met betrekking tot de handelingen gedekt vereist artikel 10 een toevoeging van speciale intentie dat het apparaat wordt gebruikt met als doel het begaan van een van de overtredingen neergelegd in hoofdstuk II.

Lid 2 bevat een wettelijke veronderstelling dat een verdachte die in het bezit is van een of meer artikelen waarnaar wordt verwezen in lid 1 onder (i) en (ii) wordt verondersteld het artikel te bezitten met de vereiste criminele oogmerk totdat het tegendeel is bewezen.

Artikel 10 vereist dat de overtreder handelt zonder rechtmatig excuus of rechtvaardiging. Binnen deze context moet de verheldering in deze leden in overweging worden genomen. Als gevolg daarvan zal het rechtmatige beheer van softwaregereedschappen binnen de context van zelfbeschermende maatregelen niet worden beschouwd te worden uitgevoerd zonder rechtmatig excuus.

Artikel 11: Computer-gerelateerde vervalsing

In de meeste strafrechtsystemen is de handeling van vervalsing van tastbare documenten strafbaar gesteld. De dogmatische structuur van de nationale wettelijke benaderingen varieert afhankelijk van het rechtsgebied. Terwijl een concept is gebaseerd op de authenticiteit van de auteur van het document, is de ander gebaseerd op de authenticiteit van de verklaring. Artikel 11 is gericht op het beschermen van de veiligheid en betrouwbaarheid van elektronische gegevens door het creëren van een parallelovertreding naast de traditionele vervalsing van tastbare documenten en vult het hiaat in het strafrecht, aangezien de traditionele wettelijke bepalingen die betrekking hebben op vervalsing niet van toepassing zouden kunnen zijn op elektronisch opgeslagen gegevens.

Het doel van computer-gerelateerde vervalsing is computergegevens zoals gedefinieerd in artikel 3. Binnen deze context is het ongeacht of die direct leesbaar zijn en/of verstaanbaar. De bepaling verwijst niet slechts naar computergegevens als het doel van een van de handelingen waarnaar wordt verwezen, maar het is ook nodig dat de handelingen resulteren in niet-authentieke gegevens. Artikel 11 vereist tenminste dat met betrekking tot het mentale element van de overtreding, de gegevens gelijk zijn aan een publiek of privédocument.

De invoer van gegevens moet overeenstemmen met de productie van een vals tastbaar document. Verandering verwijst naar de wijziging van bestaande gegevens. Blokkeren van computergegevens verwijst naar een handeling die de beschikbaarheid van gegevens beïnvloedt Dit kan bij voorbeeld relevante informatie zijn van een databank die wordt geblokkeerd tijdens de creatie van een elektronisch document. Verwijdering correspondeert met de definitie van de term in artikel 4 waarin handelingen worden gedekt waarbij informatie wordt verwijdert.

Artikel 11 vereist dat de overtreder de overtredingen opzettelijk en zonder rechtmatig excuus of rechtvaardiging begaat.

Artikel 12: Computer-gerelateerde fraude

Fraude is een populair misdrijf in de cyberruimte en de toepassing van bestaande bepalingen op internet-gerelateerde zaken kan lastig zijn, waar de traditionele nationale strafrechtbepalingen zijn gebaseerd op de leugens van een persoon, het is met het oog hierop dat de werkgroep heeft besloten een bepaling op te nemen die computer-gerelateerde fraude strafbaar stelt.

Artikel 12 omvat een lijst van de meest relevant handelingen van computer-gerelateerde fraude. Het is noodzakelijk dat de manipulatie van de overtreder een direct economisch of bezitsverlies van het eigendom van andere persoon tot gevolg heeft, waaronder geld, activa en passiva met een economische waarde.

Invoer van computergegevens dekt alle soorten van invoermanipulatie, zoals het invoeren van incorrecte gegevens in de computer evenals manipulatie van computersoftware en andere verstoringen van het verloop van de dataverwerking. Verandering verwijst naar de wijziging van bestaande gegevens. Blokkeren van computergegevens verwijst naar een handeling die de beschikbaarheid van gegevens beïnvloedt Verwijdering verwijst naar de verwijdering van computergegevens.

Ingrijpen (Interference) in het functioneren van een computersysteem zoals genoemd in b) dekt handelingen zoals hardwaremanipulatie, handelingen waarbij afdrukken worden geblokkeerd en handelingen die het opnemen of de toevoer van gegevens beïnvloeden, of de volgorde waarin de programma's verlopen.

Gelijk aan de werking van de andere bepalingen van de wettekst vereist artikel 11 dat de overtreder opzettelijk handelt. Deze intentie verwijst naar het manipuleren evenals naar het optreden van financiële gevolgschade. Daarnaast vereist artikel 12 dat de overtreder handelde met een frauduleuze of oneerlijke intentie voor het verkrijgen van economische of andere voordelen voor zichzelf of een ander. Een voorbeeld van handelingen die zijn uitgesloten van strafrechtelijke aansprakelijkheid als gevolg van de afwezigheid van een speciale intentie zijn de commerciële praktijken die voortkomen uit marktconcurrentie die economische nadelige gevolgen kan hebben voor een persoon en een ander tot voordeel kunnen strekken, maar die niet worden uitgevoerd met een frauduleuze of oneerlijke bedoeling.

Daarnaast, vereist artikel 12 dat de overtreder handelt zonder rechtmatig excuus of rechtvaardiging.

Artikel 13: Kinderpornografie

Artikel 13 omvat een brede strafbaarstelling van handelingen die betrekking hebben op kinderpornografie. De strafbaarstelling van kinderpornografie heeft de bedoeling het beschermen van verschillende juridische belangen. Door de strafbaarstelling van de productie van kinderpornografie richt de bepaling zich op het beschermen van kinderen tegen seksueel misbruik. Met betrekking tot het verbod op handelingen die zijn gerelateerd aan de uitwisseling van kinderpornografie (aanbieden, distribueren), evenals het bezitten van kinderpornografie, richt de strafbaarstelling van dergelijke handelingen zich op het vernietigen van de markt voor dergelijk materiaal, zoals de constante vraag naar nieuw materiaal overtreders kan motiveren voort te gaan met het misbruik van kinderen. Daarnaast, richt het verbod op uitwisseling zich erop personen te verhinderen toegang te krijgen tot dergelijk materiaal en daarbij een trigger-effect te voorkomen met betrekking tot het seksueel misbruik van kinderen.

“Productie” betekent een proces van het creëren van kinderpornografie. Het is nodig dat de productie van kinderpornografie wordt uitgevoerd met als doel het distribueren via een computersysteem. Indien de overtreder het materiaal produceert voor eigen gebruik of van plan is het in niet-elektronische vorm te distribueren, dan is artikel 9 van het Verdrag inzake Cybercriminaliteit niet van toepassing.

“Aanbieden” dekt de handeling van het benaderen van anderen voor het aanschaffen van kinderpornografie. Het is niet nodig dat dergelijk materiaal wordt aangeboden op een commerciële basis, maar het impliceert dat de overtreder die het materiaal aanbiedt in staat is het te verstrekken. “Beschikbaar maken” verwijst naar de handeling die anderen in staat stelt toegang te krijgen tot kinderpornografie. Deze handeling kan worden begaan door het plaatsen van kinderpornografie op websites of door een verbinding tot stand te brengen met systemen voor het delen van bestanden en het in staat stellen van anderen toegang te krijgen tot dergelijk materiaal op niet-geblokkeerde geheugencapaciteit of mappen.

“Distributie” dekt de handeling van het doorsturen van kinderpornografie aan anderen. “Verzenden” dekt alle communicatie door middel van verzonden signalen. “Aanschaffen voor zichzelf of voor een ander” dekt elke handeling waarbij actief kinderpornografie wordt verworven. Bezit is de controle die een persoon met opzet uitoefent in relatie tot kinderpornografie. Het vereist dat de overtreder beheer heeft wat niet alleen het geval is met betrekking tot lokale opslagapparaten, maar ook tot opslagapparaten op afstand, waartoe hij toegang heeft en waarover hij het beheer uitoefent. Verder vereist bezit in het algemeen een mentaal element zoals aangegeven in de bovenstaande definitie. “Toegang verkrijgen” dekt elke handeling van het initiëren van het proces van het afbeelden van informatie die beschikbaar is gemaakt door middel van informatie- en communicatietechnologie. Dit is bij voorbeeld het geval indien de overtreder de domeinnaam invoert van een bekende kinderpornografiewebsite en het proces op gang brengt van het ontvangen van informatie van de eerste pagina wat samengaat met het noodzakelijke geautomatiseerde downloadproces. Dit stelt rechtshandhavingsinstituten in staat overtreders te vervolgen in gevallen waarbij zij in kunnen aantonen dat de overtreder websites heeft geopend met kinderpornografie, maar niet kunnen aantonen dat de overtreder materiaal heeft gedownload. Deze moeilijkheden bij het verzamelen van bewijsmateriaal, bij voorbeeld indien de overtreder coderingstechnologie gebruikt om de bestanden die zijn gedownload op zijn opslagmedium te

beschermen. Deze bepaling is ook van toepassing in gevallen waar de consumptie* van kinderpornografie kan plaatshebben zonder het downloaden van materiaal. Dit kan het geval zijn waar een website het mogelijk maakt video's te bekijken, en door de technische instelling van het streamingsproces de ontvangen informatie niet wordt gebufferd maar direct wordt gewist nadat informatie is verzonden.

De opstellers besloten de landen in staat te stellen het gedrag beschreven in artikel 13 onder 1 (d)-(f) niet te strafbaar te stellen.

Artikel 14: Misdrijven gerelateerd aan de identiteit

Deze bepaling dekt belangrijke fasen van typische identiteit-gerelateerde misdrijven. Slechts de fase van het verwerven van identiteit-gerelateerde informatie wordt niet gedekt door deze bepaling, die handeling wordt gedekt door andere bepalingen gedekt in Hoofdstuk II van de wettekst.

De term “overdracht” dekt dataverzendingsprocessen van een computer- naar een ander computersysteem. Dit is relevant indien databanken met identiteit-gerelateerde informatie die onrechtmatig zijn verkregen worden overgedragen aan criminele groepen die de verkoop van dergelijke informatie organiseren. “Bezitten” is het beheer dat een persoon opzettelijk uitoefent met betrekking tot identiteit-gerelateerde informatie. “Gebruik” dekt een breed scala aan praktijken, zoals het indienen van dergelijke informatie voor online aankopen.

Het is nodig dat de overtreder opzettelijk de handeling uitvoert en daarbij speciaal de intentie heeft een overtreding te begaan of daarin bij te staan.

Artikel 15: SPAM

Deze bepaling handelt over de kwestie van SPAM door het strafbaar stellen van drie (3) van de belangrijkste handelingen die de meeste SPAM verspreidingen gemeen hebben. Naast het beperken van de strafbaarstelling tot drie belangrijke handelingen, kan de overtreder slechts worden vervolgd, indien de handeling de handel beïnvloeden Variant a) dekt het initiëren van de verzending van meerdere elektronische mails. Dit stelt de verzending van massamail zonder de toestemming van de ontvanger strafbaar. De beperking van de strafbaarstelling tot handelingen die zijn uitgevoerd zonder rechtmatig excuus of rechtvaardiging, speelt een belangrijke rol in het onderscheid maken tussen rechtmatige massmail (zoals nieuwsbrieven) en wederrechtelijke SPAM. Variant b) stelt het omzeilen van anti-SPAM technologie strafbaar die beschermde computersystemen misbruikt voor het doorzenden of verzenden van elektronische berichten. Het is nodig dat de overtreder opzettelijk handelt met betrekking tot het bedriegen of misleiden van de ontvanger of de betrokken dienstverleners. Variant c) dekt het omzeilen van anti-SPAM technologie door het vervalsen van de kopinformatie. Afhankelijk van de manier van manipulatie, kan dergelijke handeling ook gedekt worden door artikel 11 van de wettekst.

Artikel 15 vereist dat de overtreder de overtredingen opzettelijk en zonder rechtmatig excuus of rechtvaardiging begaat. Daarom wordt het toegestane computertesten niet strafbaar gesteld. Door de verschillende meningen over de noodzaak de verspreiding van SPAM strafbaar te stellen, hebben de opstellers besloten de landen de gelegenheid te geven dergelijk gedrag strafbaar te stellen in Artikel 15 onder (2) (a) mits er andere effectieve rechtsmiddelen beschikbaar zijn.

Artikel 16: Openbaarmaking van bijzonderheden van een onderzoek

Geheimhouding van het onderzoek kan van groot belang zijn met betrekking tot het doel en de strategieën die worden gebruikt voor dergelijke activiteiten. Dit is vooral van belang indien het onderzoek nog niet is afgerond en het relevante bewijs in kwestie kon worden veranderd. Met betrekking hiertoe voorziet deze maatregel ook in de behoeften van de rechtshandhaving voor het verzekeren dat de

verdachte van het onderzoek niet op de hoogte is gesteld van het onderzoek, evenals het recht van individuen op privacy. Het laatste is inbegrepen voor de bescherming van de privacy van de gegevens die het onderwerp of andere personen die genoemd of geïdentificeerd kunnen worden in die gegevens.

Artikel 17: Nalaten bijstand te verlenen

In veel gevallen zijn rechtshandhavingsinstituten afhankelijk van de bijstand van systeemadministrateurs en andere personen met specifieke kennis voor het identificeren van de opslaglocatie van relevant bewijsmateriaal of voor het verkrijgen van toegang tot de opgeslagen informatie. Artikel 20 legt een dwingende maatregel neer voor het vergemakkelijken van het onderzoeken en in beslag nemen van computergegevens. Artikel 17 legt de consequenties van het falen om een dergelijke verplichting na te leven neer. Het “nalaten” in deze context vereist dat de overtreder objectief en persoonlijk in staat was de opdracht te volgen.

Artikel 18: Pesterij door middel van elektronische communicatie

Als gevolg van de toenemende relevantie voor de Caribische landen hebben de opstellers besloten een bepaling op te nemen die pesterij door middel van elektronische communicatie strafbaar stelt. De strafbaarstelling vereist dat de overtreder een elektronische communicatie initieerde. Een elektronische communicatie wordt bij voorbeeld geïnitieerd indien de overtreder een email verstuurt of een bericht via de babbelbox. De bepaling vereist verder dat de overtreder een computersysteem gebruikt voor het ondersteunen van ernstig, herhaald en vijandig gedrag. Tenslotte, vereist de bepaling dat de overtreder handelt met een specifieke bedoeling (de bedoeling om af te dwingen, te intimideren, pesten of substantiële emotionele stress te veroorzaken).

HOOFDSTUK III

Artikel 19: Rechtsgebied

Dit artikel geeft een aantal criteria voor het vaststellen van jurisdictie betreffende de strafrechtelijke overtredingen die worden opgesomd in artikelen 4-17. Artikel 19 a) is gebaseerd op het principe van territorialiteit. De territoriale jurisdictie wordt ingezet indien zowel de persoon die een computersysteem aanvalt en het slachtoffersysteem zich bevinden binnen hetzelfde rechtsgebied of land. Het principe zal ook van toepassing zijn indien het computersysteem dat wordt aangevallen binnen het grondgebied is, zelfs als de aanvaller dat niet is.

Artikel 19 b) bevat varianten op het principe van territorialiteit. Dit vereist dat elke partij een strafrechtelijke jurisdictie instelt met betrekking tot overtredingen begaan op schepen die onder hun vlag varen of vliegtuigen die zijn geregistreerd volgens hun wetten. Beide principes zijn al deel van beginselen van jurisdictie buiten cybercriminaliteit, omdat schepen en vliegtuigen vaak worden beschouwd als een extensie van het grondgebied van een staat. Indien een misdrijf wordt begaan op een boot of in een vliegtuig dat zich buiten het territorium van de partij ligt onder wiens vlag men vaart, dan is er in het algemeen geen uitoefening van jurisdictie. Rekening houdend met de toenemende connectiviteit aangeboden aan boord van vliegtuigen en schepen, heeft dit beginsel het potentieel relevanter te worden in de toekomst.

Artikel 19 c) is gebaseerd op het beginsel van nationaliteit. Het beginsel van nationaliteit wordt het vaakst toegepast in landen met een gecodificeerd rechtssysteem (*civil-law* landen). Het definieert de jurisdictie indien een onderdaan een overtreding begaat in het buitenland, de staat moet de mogelijkheid hebben het te vervolgen indien het gedrag tevens een overtreding is ingevolge de wet van de staat waarin het was begaan of het gedrag heeft plaatsgehad buiten de territoriale jurisdictie van welke staat dan ook.

HOOFDSTUK IV

Artikelen 20 – 27

Het succesvol onderzoeken van cybercriminaliteit vereist dat rechtshandhavingsinstituten toegang hebben tot de juiste instrumenten die nodig zijn voor het uitvoeren van een onderzoek. De identificatie van overtreders evenals de bescherming van de integriteit van computergegevens tijdens een onderzoek omvat verschillende inherent unieke uitdagingen voor de rechtshandhavingsautoriteiten. Het doel van Hoofdstuk 4 is het verbeteren van de nationale procedurele instrumenten door het definiëren van algemene minimumstandaarden gebaseerd op de beste praktijken in de regio evenals internationale standaarden. Binnen deze context zal de definitie van standaarden nationale wetgevers helpen mogelijke hiaten te ontdekken in het nationale procesrecht. Artikelen 20-27 definiëren slechts minimumstandaarden en sluiten daarom de creatie van uitgebreidere strafbaarstelling op nationaal niveau niet uit.

Hoofdstuk 4 introduceert nieuwe onderzoeksinstrumenten (zoals artikel 27) en is er ook op gericht traditionele procedurele maatregelen aan te passen (zoals artikel 20). Alle instrumenten waarnaar wordt verwezen zijn erop gericht het verwerven en of verzamelen van gegevens toe te staan met als doelstelling het uitvoeren van specifieke strafrechtelijke onderzoeking of processen. De instrumenten beschreven in Hoofdstuk 4 zullen niet slechts worden gebruikt voor traditionele onderzoek naar computercriminaliteit, maar voor elk onderzoek dat computergegevens en computersystemen omvat.

De opstellers hebben uitgebreid gesproken over het belang van waarborgen. Er was consensus dat de toepassing van procedurele instrumenten waarin artikelen 20-27 voorzien onderworpen moeten worden aan voorwaarden en waarborgen. De opstellers bespraken de optie of zij een uitgebreide serie van waarborgen moeten opnemen of gebruik moeten maken van de bestaande waarborgen in de nationale wetgeving. Aangezien deze wettekst niet direct van toepassing is, maar slechts een richtlijn geeft voor de aanpassing en harmonisering van de nationale wetten en waarbij de verschillen in overweging worden genomen die in de nationale wetten van elk Caribisch land kunnen bestaan, besloten de opstellers de waarborgen niet te definiëren, maar het over te laten aan het nationale implementatieproces dat alle voorwaarden of waarborgen, die constitutioneel, wettelijk, of judicieel of anderszins worden voorzien van toepassing zijn met betrekking tot de instrumenten in Hoofdstuk 4. Wanneer nieuwe instrumenten kunnen worden neergelegd tijdens het implementatieproces, kan een uitbreiding van de bestaande waarborgen nodig zijn voor het in evenwicht brengen van de vereisten van de rechtshandhaving met de bescherming van mensenrechten en menselijke vrijheden.

De verschillen binnen het wetssysteem in het Caribisch gebied zijn niet slechts in overweging genomen met betrekking tot waarborgen, maar ook met betrekking tot de definitie van de voorwaarden voor de toepassing van de instrumenten. De bepalingen voorzien in opties voor de aanpassing met betrekking tot de autoriteit die de toepassing van een instrument kan gelasten (bij voorbeeld de rechter, rechtshandhaving, politie), de basis van de actie (bij voorbeeld informatie onder beëdiging of volgens beëdigde verklaring), de mate van zekerheid (bij voorbeeld verdacht of vermoeden), evenals de noodzaak om te reageren (bij voorbeeld kan of moet). Tenslotte, besloten de opstellers de landen in staat te stellen af te wijken van de implementatie van bepaalde procedures. Rekening houdend met verschillende standaarden die betrekking hebben op het vermogen communicatie te onderscheppen, werd specifiek binnen deze context de mogelijkheid voorzien de procedurele instrumenten te beperken.

Alle instrumenten opgenomen in de artikelen 20-27 zijn niet alleen van toepassing op onderzoek binnen het grondgebied van de staat. Met betrekking tot de transnationale dimensie van cybercriminaliteit bespraken de opstellers de noodzaak voor het toevoegen van een aparte serie bepalingen die specifiek handelen over internationale samenwerking voor het onderzoek van transnationale cybercriminaliteit. Echter, de opstellers besloten dat als gevolg van het specifieke mandaat van de werkgroep de regelgeving over internationale samenwerking niet moest worden opgenomen.

Artikel 20: Onderzoek en Inbeslagname

Zelfs bij misdrijven begaan met hoogstaande technologie, blijft onderzoek en inbeslagname een belangrijk onderzoeksproces. Over het algemeen, omvatten de belangrijkste strafrechtelijke procedurele wetten bevoegdheden voor het onderzoek en de inbeslagname van tastbare objecten. Maar aangezien sommige rechtsgebieden computergegevens niet als objecten behandelen, en slechts de inbeslagname van tastbare zaken toestaan, is dit hoofdstuk gericht op het moderniseren van nationale wetten betreffende onderzoek en inbeslagname van opgeslagen computergegevens door het neerleggen van een gelijkaardige bevoegdheid met betrekking tot opgeslagen gegevens.

De bedoeling van artikel 20 (1) is het vergemakkelijken van het proces van het verzamelen van digitaal bewijs. De bepaling verduidelijkt dat een bevelschrift nodig is voor het doen van ieder zoekactie. Dit is van toepassing op opgeslagen computergegevens. Indien een dergelijk bevelschrift wordt uitgegeven machtigt het de rechtshandhavingsinstanties niet alleen om een computersysteem te activeren, of op andere wijze toegang to te verschaffen, maar ook om de ruimte van de verdachte te betreden. De toepassing van het proces is niet beperkt tot zaken waar beslissend bewijs van het begaan van een overtreding kan worden verzameld, maar is ook van toepassing op gevallen waar de computergegevens zijn verkregen door een persoon als gevolg van een overtreding.

Om te verzekeren dat de formulering van de bepaling de toepassing van gesofisticeerde onderzoekstechnieken niet in de weg staat, besloten de opstellers de technieken niet te specificeren die gebruikt kunnen worden voor het onderzoeken of toegang verschaffen tot een computersysteem. De term “onderzoek omvat” maar is niet beperkt tot het onderzoeken, lezen, inspecteren of beoordelen van gegevens.

Artikel 20 onder (2) stelt onderzoeksautoriteiten in staat hun onderzoek uit te breiden, of gelijkaardige toegang te krijgen tot een ander computersysteem of deel daarvan, indien aan bepaalde voorwaarden is voldaan. De opstellers besloten dat dergelijke machtiging nodig is omdat opslagsystemen op afstand nu worden gebruikt in toenemende mate. Met betrekking tot de beperking van procedurele instrumenten voor nationaal onderzoek, is de bepaling niet van toepassing indien relevante informatie is opgeslagen op een computersysteem buiten het grondgebied (zelfs als technisch gezien men toegang ertoe kan krijgen. De bepaling schrijft niet voor hoe een uitbreiding van een onderzoek zal worden ondernomen aangezien de vaststelling van dit aspect wordt overgelaten aan nationale wetgeving.

Artikel 20 onder (3) machtigt de bevoegde autoriteiten digitaal bewijsmateriaal in beslag te nemen en veilig te stellen. De term in beslag nemen wordt gedefinieerd in artikel 3. Naast de traditionele benaderingen zoals de inbeslagname van computerhardware (waaronder opslagmedia voor computerdata) stelt de bepaling de onderzoeksautoriteiten in staat gesofisticeerde en minimalistische onderzoeken uit te voeren zoals de productie van de kopie van de relevante gegevens. Aangezien dergelijke maatregelen kunnen leiden tot de productie van meerdere kopieën, zijn er bijkomende maatregelen vereist. Dus kunnen de bevoegde autoriteiten de mogelijkheid om gegevens te verwijderen van de oorspronkelijke bron opnemen en de integriteit van de gegevens bewaren om te verzekeren dat het niet wordt veranderd tijdens het onderzoeksproces.

Artikel 21: Bijstand

De identificatie van het relevante digitale bewijsmateriaal gaat vergezeld van unieke uitdagingen. Dit is vooral relevant voor de identificatie van fysieke opslagruimte gezien de kwantiteit aan gegevens die verwerkt en opgeslagen kan worden, evenals de mogelijke veiligheidsmaatregelen die zijn ingevoerd. Bijstand ban personen met specifieke kennis (zoals systeemadministrateurs) over het functioneren van een computersysteem kan daarom onmisbaar zijn voor een onderzoek. Dergelijke samenwerking is niet alleen goed voor de onderzoeksautoriteiten maar ook voor de bedrijven, aangezien zonder die bijstand de onderzoeksautoriteiten gedwongen kunnen zijn in de ruimte te blijven waar de huiszoeking plaatsvindt en

voorkomen dat er toegang wordt gekregen tot het computersysteem voor lange perioden terwijl zij het onderzoek uitvoeren. Dergelijke lange duur van een onderzoek kan een economische last creëren voor legitieme bedrijven. De opstellers hebben daarom besloten een verplichting te creëren voor dergelijke relevante personen die kennis hebben betreffende het functioneren van een computersysteem of maatregelen toegepast voor de bescherming van de computergegevens daarin. Dergelijke bijstand is echter beperkt tot wat redelijkerwijs vereist is. Artikel 21 legt de vijf (5) gebieden van bijstand neer. Echter, de opstellers vonden het belangrijk te benadrukken dat de regel tegen het zichzelf incrimineren de toepassing van de bepaling met betrekking tot de verdachte van het misdrijf in de weg staat.

Artikel 22: Bevel tot overlegging

De bevoegde autoriteiten hebben verschillende krachtige processen en procedures voor het verzamelen van relevant elektronisch bewijsmateriaal. Een van de meest krachtige processen is het onderzoeken en in beslag nemen van computergegevens. Dit kan van speciaal belang blijken te zijn wanneer een onderzoek wordt ingesteld naar bewijsmateriaal opgeslagen op de server van een aanbieder van hosting diensten want dergelijke procedures kunnen de bedrijfsvoering beïnvloeden (zelfs als de aanbieder de rechtshandhavers bijstaat in het identificeren van de fysieke locatie). In dit licht bezien besloten de opstellers een proces op te nemen in artikel 22 onder (a) dat een persoon in zijn grondgebied verplicht de specifieke opgeslagen computergegevens te verstrekken. Deze bepaling zal niet worden geïnterpreteerd als een verplichting voor het bewaren van gegevens. De toepassing van de bepaling is niet beperkt tot bepaalde categorieën van gegevens en is van toepassing met betrekking tot inhoudelijke en verkeersgegevens. Met betrekking tot de specifieke regulering van abonneeinformatie in artikel 22 onder (b), wordt deze categorie van gegevens niet inbegrepen in artikel 22 onder (a). Om misbruik van het proces te voorkomen, hebben de opstellers verzoeken beperkt tot die waar deze informatie redelijkerwijs vereist is. Naast dit criterium, wordt een bevelschrift van de bevoegde autoriteit (rechter) vereist.

In die gevallen waarin onderzoekers proberen een verdachte te identificeren kunnen zij niet concentreren op gegevens die wordt gegenereerd tijdens de elektronische communicatie, maar eerder op de abonneeinformatie die hen in staat stelt crimineel gedrag in verband te brengen met een persoon. De opstellers besloten deze kwestie te behandelen in een specifiek lid (artikel 22 onder (b)). Artikel 22 onder (b) is van toepassing met betrekking tot alle persoonlijke informatie over een abonnee of een persoon die anderszins een internetdienst gebruikt. Aangezien abonneeinformatie slechts beschikbaar zal zijn als een dienst wordt aangeboden, is de verplichting voor het overleggen van dergelijke gegevens beperkt tot de Internet dienstverlener. De bepaling is niet beperkt tot abonneeinformatie die elektronisch is opgeslagen maar dekt ook niet-elektronische bescheiden.

Artikel 23: Versnelde bewaring

Computergegevens die nodig zijn voor het identificeren van een overtreder of om te bewijzen dat een misdrijf is begaan kan gemakkelijk worden gewist of gewijzigd voordat de onderzoekers in staat zijn het bewijsmateriaal veilig te stellen. De wijziging of verwijdering gebeurt niet noodzakelijkerwijs met de bedoeling de overtreder te beschermen (bij voorbeeld, verkeersgegegens die relevant zijn voor de identificatie wordt vaak automatisch verwijdert binnen een nogal korte periode na de beëindiging van de communicatie aangezien het niet langer nodig is). In tegenstelling tot internationale benaderingen (zoals de EU databewaringsrichtlijn) besloten de opstellers de implementatie van een databewaarplicht niet voor te schrijven, maar een proces vast te stellen dat rechtshandhavingsinstanties in staat stelt de bewaring van dergelijke gegevens te bevelen indien nodig.

Op basis van een bevelschrift gegeven ingevolge artikel 23 is elke persoon die daartoe een bevel wordt gegeven (met uitzondering van de verdachte) verplicht de gegevens te bewaren die werd verwerkt tijdens de verlening van de dienst. Artikel 23 houdt geen verplichting in voor de persoon die de gegevens beheert de relevante gegevens te verzenden naar de bevoegde autoriteiten. De verzendingsplicht wordt geregeld

in artikelen 22 en 24. Na het ontvangen van het bevelschrift is de beheerder van dergelijke informatie niet toegestaan handmatig of automatisch de gegevens aangegeven in het bevelschrift te verwijderen voor een periode van zeven (7) dagen. De opstellers waren het eens dat deze periode voldoende is voor het verkrijgen van een bevelschrift om de verzending van de relevante gegevens te verzoeken. Indien het bevelschrift voor de versnelde bewaring niet tijdig wordt gevolgd door of een bevelschrift voor de verlenging van die periode, of een bevelschrift tot overlegging, dan kan de beheerder van de gegevens die opgeslagen informatie verwijderen.

Om ervoor te zorgen dat onderzoekers een efficiënt proces ter beschikking hebben voor het voorkomen van de verwijdering van relevant bewijsmateriaal en er rekening mee houdende dat artikel 23 slechts de verwijdering van informatie voorkomt en de rechtshandhavers geen toegang geeft tot dergelijke informatie, hebben de opstellers besloten geen bevelschrift te vereisen van een rechter, maar dit artikel stelt een politiefunctionaris in staat versnelde bewaring te bevelen. Gezien het feit dat het bevelschrift tot overlegging (artikel 22) vereist dat een bevelschrift afkomstig is van de bevoegde autoriteit daartoe, wordt verzekerd dat de rechten van de verdachte van het onderzoek voldoende zijn beschermd.

De duur van de bewaring kan een (1) keer worden verlengd. Dergelijke verlenging zal worden gelast door de rechter.

Artikel 24: Gedeeltelijke openbaarmaking

Hoewel de opstellers in principe overeenstemming hadden bereikt over een strikt onderscheid tussen de goedkeuring voor het bevelen van bewaring van gegevens (die kan worden gegeven door elke politieofficier) en het bevel voor het verzenden van de gegevens (wat een bevelschrift vereist van een rechter) hebben zij de noodzaak onderstreept om te verzekeren dat de onderzoekers in staat zijn directe toegang te krijgen tot bepaalde verkeersgegevens. Zonder dergelijke gedeeltelijke openbaarmaking zouden onderzoekers, in sommige gevallen, niet in staat zijn de overtreder terug te vinden en de meer relevante gegevens te bewaren wanneer meer dan een aanbieder erbij betrokken is. In tegenstelling tot het bevelschrift tot overlegging, is dit instrument beperkt tot verkeersgegevens.

Artikel 25: Verzamelen van verkeersgegevens

De opstellers hebben erkend dat verkeersgegevens een belangrijke rol spelen in cybercriminaliteitsonderzoek. Het monitoren van de verkeersgegevens die zijn gegenereerd tijdens het gebruik van de Internet diensten stelt de onderzoekers in staat het IP-adres te identificeren van een overtreder en daarna kan men pogen de fysieke locatie van hem vast te stellen. Artikel 25 bevat twee (2) verschillende benaderingen: gebaseerd op artikel 25 onder (1) kan elke persoon die verkeersgegevens beheert worden bevolen dergelijke gegevens te verzamelen of te registreren of een politieofficier toestaan of bijstaan bij het verzamelen of registreren van dergelijke gegevens. Artikel 25 onder (2) omvat een bevelschrift waarin een politieofficier wordt toegestaan verkeersgegevens te verzamelen. Aangezien het verzamelen van verkeersgegevens op dezelfde controversiële wijze werd besproken als de onderschepping van inhoudelijke gegevens besloten de opstellers te benadrukken dat de landen naar hun eigen oordeel kunnen besluiten artikel 25 niet te implementeren.

Artikel 26: Onderschepping van inhoudelijke gegevens

In sommige gevallen is het verzamelen van verkeersgegevens onvoldoende voor het veiligstellen van een succesvolle veroordeling van de verdachte. Dit is vooral relevant in die gevallen waarbij onderzoekers reeds de communicatiepartner kennen en de diensten gebruikt, maar waar zij onvoldoende informatie hebben over de informatie die is uitgewisseld. De opstellers besloten een bepaling op te nemen die de onderschepping van gegevenscommunicatie mogelijk maakt. Om een geharmoniseerde aanpak te verzekeren werd de bepaling opgesteld in overeenstemming met de model wettekst inzake onderschepping van communicatie.

Artikel 26 bevat twee (2) verschillende benaderingen. Op basis van artikel 26 onder (a) kan een ISP worden bevolen inhoudelijke gegevens op te nemen en te verzamelen. Artikel 26 onder (b) stelt rechtshandhavingsinstanties in staat de onderschepping uit te voeren. Aangezien er een controversiële discussie was binnen de werkgroep, hebben de opstellers besloten dat landen kunnen besluiten artikel 26 niet te implementeren.

Artikel 27: Forensische software

Tijdens de discussie binnen de werkgroep hebben de opstellers gesofisticeerde onderzoeksmethoden geanalyseerd. Na een intense discussie besloten de opstellers een bepaling op te nemen die de onderzoekers machtigt forensische software op afstand te gebruiken voor het verzamelen van relevant bewijsmateriaal. De opstellers erkenden dat het proces bijzonder indringend is en potentieel de fundamentele rechten van de verdachte zou kunnen belemmeren en besloten daarom een aantal beperkingen in te bouwen. Ten eerste, het gebruik van dergelijke software vereist dat bewijsmateriaal niet kan worden verzameld door het toepassen van andere processen. Ten tweede, is een bevelschrift van de rechter vereist. Ten derde, moet de aanvraag informatie bevatten op vier belangrijke gebieden (artikel 27 onder (1)(a)-(d). Daarnaast zijn de toegestane handelingen beperkt door zowel paragraaf 1 en 2. De opstellers besloten landen in staat te stellen verdere beperkingen in te voeren door het beperken van de toepassing van het instrument voor misdrijven opgenomen in een lijst in artikel 27 onder (7) of deze bepaling niet te implementeren (artikel 27 onder (8)).

HOOFDSTUK V

Artikel 28: Geen monitoringplicht

Internet aanbieders hebben tot op zekere hoogte de theoretisch technische mogelijkheid voor het monitoren van activiteiten die zijn gerelateerd aan hun diensten. Zonder een duidelijke regeling is er onzekerheid of er een verplichting is voor het monitoren van activiteiten en of de aanbieders kunnen worden vervolgd op basis van een schending van de plicht gebruikersactiviteiten te monitoren. Naast de mogelijke conflicten met de databeschermingsregels en de geheimhouding van telecommunicatie, zal dergelijke verplichting vooral moeilijkheden veroorzaken voor aanbieders van hosting diensten die duizenden websites opslaan. Om deze conflicten te voorkomen sluit artikel 28 een algemene plicht voor het monitoren van verzonden of opgeslagen informatie uit. De bepaling beperkt slechts de aansprakelijkheid van aanbieders met betrekking tot strafrechtelijke aansprakelijkheid.

Artikel 29: Aanbieder van toegang

Op basis van artikel 29 is de aansprakelijkheid van aanbieders van toegang (Artikel 29 onder (1)) en beheerders van routers (artikel 29 onder (2)) wordt volledig uitgesloten, zolang zij de drie voorwaarden neergelegd in artikel 29 naleven. Als gevolg daarvan, is de aanbieder van toegang in het algemeen niet verantwoordelijk voor strafrechtelijke overtredingen begaan door de gebruikers. Deze volledige uitsluiting van aansprakelijkheid stelt de aanbieder niet vrij van de plicht verdere overtredingen te voorkomen indien de rechter of een administratieve autoriteit dat beveelt.

Artikel 30: Aanbieder van hosting diensten

De opsteller heeft er kennis van genomen dat het identificeren van wederrechtelijke inhoud een grote uitdaging vormt voor de aanbieder van hosting diensten. In het bijzonder voor populaire aanbieders die duizenden website opslaan zou het manueel zoeken naar wederrechtelijke inhoud onmogelijk zijn. Als gevolg, hebben de opstellers besloten de aansprakelijkheid van de aanbieders van hosting diensten te

beperken. Echter, in tegenstelling tot het geval van de aanbieder van toegang, wordt de aansprakelijkheid van de aanbieder van hosting diensten niet in het algemeen uitgesloten, maar slechts indien aan bepaalde voorwaarden is voldaan.

Artikel 30 onder (1)(a) beperkt de aansprakelijkheid indien de aanbieder van hosting diensten direct de inhoud verwijdert na daartoe een bevelschrift te hebben ontvangen van een overheidsinstantie of de rechter. Direct betekent in het algemeen in minder dan 24 uur.

Artikel 30 onder (1)(b) definieert dat zolang de aanbieder van hosting diensten geen werkelijk kennis heeft van wederrechtelijke activiteiten of wederrechtelijke inhoud opgeslagen op zijn servers, hij niet aansprakelijk is. De opstellers vonden het belangrijk aan te geven dat een veronderstelling dat wederrechtelijke inhoud opgeslagen zou kunnen zijn op de servers niet hetzelfde wordt beschouwd te zijn als werkelijk kennis hebben van de kwestie. Indien de aanbieder wordt geïnformeerd dan moet die informatie concreet en specifiek genoeg zijn zodat hij de locatie van de wederrechtelijke inhoud kan identificeren. Indien de aanbieder concrete kennis heeft over wederrechtelijke activiteiten of wederrechtelijke inhoud kan hij slechts aansprakelijkheid vermijden, indien hij een overheidsinstantie in kennis stelt over de potentieel wederrechtelijke inhoud. In tegenstelling tot de richtlijn van de Europese Unie over E-handel, die aansprakelijkheid vaststelt indien de aanbieder van hosting de wederrechtelijke inhoud niet verwijdert nadat er informatie is ontvangen over het bestaan daarvan, hebben de opstellers besloten het besluit indien de inhoud illegaal is over te laten aan de bevoegde overheidsinstanties. Landen kunnen specifiek aangeven aan welke bevoegde autoriteit dergelijke inhoud moet worden gerapporteerd.

Artikel 30 is niet slechts toepasselijk op de aanbieders die hun diensten beperken tot het verhuren van technische dataopslaginfrastructuur. Populaire internetdiensten zoals de veilingplatforms bieden ook hosting diensten aan. Landen kunnen besluiten een speciale telefoonlijn in te stellen waar de wederrechtelijke inhoud kan worden gerapporteerd. Aangezien de verwijdering van de wederrechtelijke inhoud, ondanks de wederrechtelijke aard van de inhoud, in botsing kan komen met de contractuele verplichtingen van de aanbieder naar zijn klant toe. Daarom hebben de opstellers besloten een verduidelijking op te nemen in artikel 30 onder (3) dat in die gevallen dat een bevelschrift was ontvangen ingevolge lid 1.

Artikel 31: Aanbieder van caching diensten

Artikel 31 beperkt de aansprakelijkheid van de aanbieder van caching diensten. De term caching binnen deze context wordt gebruikt voor het beschrijven van de opslag van populaire website op lokale opslagmedia voor het beperken van de bandbreedte en de toegang tot gegevens efficiënter te maken – bij voorbeeld door het implementeren van proxy servers. Binnen dit bestek kan een proxy server verzoeken verwerken zonder de gespecificeerde server te benaderen door het opvragen van de inhoud opgeslagen op lokale opslagmedia naar aanleiding van een eerder verzoek te halen. De opstellers erkenden het economisch belang van caching en besloten de aansprakelijkheid uit te sluiten voor automatische tijdelijke opslag indien de aanbieder de voorwaarden neergelegd in artikel 31 naleeft.

Artikel 32: Aanbieder van hyperlink diensten

Hyperlinks spelen een belangrijke rol in het verbinden en beschikbaar maken van inhoud op het internet. Zij stellen een aanbieder van de hyperlink in staat de gebruiker naar specifieke informatie te leiden die beschikbaar is online. De hyperlink geeft het commando aan de webbrowser om het internetadres dat is ingevoerd to openen. Door de overeenkomsten met het aanbieden van hosting diensten voor inhoud hebben de opstellers besloten de aansprakelijkheid van de aanbieder van hyperlink diensten te reguleren in overeenstemming met de aansprakelijkheid van de aanbieder van hosting diensten (artikel 30).

Artikel 33: Aanbieder van zoekmachine

Aanbieders van zoekmachines bieden zoekdiensten aan voor het identificeren van belangwekkende documenten door het specificeren van bepaalde criteria. De zoekmachine zal de relevante documenten zoeken die overeenkomen met de criteria ingevoerd door de gebruiker. Zoekmachines spelen een belangrijke rol in de succesvolle ontwikkeling van het internet. Tot inhoud die beschikbaar wordt gemaakt op een website maar niet voorkomt in de index van de zoekmachine kan slechts worden toegang worden gekregen indien de persoon die toegang wil krijgen de volledige URL kent. Door de overeenkomsten met de aanbieder van toegang besloten de opstellers de aansprakelijkheid van de zoekmachines te reguleren in overeenstemming met de aansprakelijkheid van de aanbieder van toegang (artikel 29).

BIJLAGEN

Bijlage 1

Deelnemers in de Eerste Consultatieve Workshop voor de Werkgroep van het HIPCAR project, van de Werkgroep inzake ICT Wetgevingskader voor Kwesties de Informatiemaatschappij rakende Gros Islet, Saint Lucia, 8-12 Maart 2010

Officieel Benoemde Deelnemers en Waarnemers

Land	Organisatie	Familienaam	Voornaam
Antigua and Barbuda	Ministry of Information, Broadcasting, Telecommunications, Science & Technology	SAMUEL	Clement
Bahamas	Utilities Regulation & Competition Authority	DORSETT	Donavon
Barbados	Ministry of Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Ministry of Trade, Industry and Commerce	COPPIN	Chesterfield
Barbados	Cable & Wireless (Barbados) Ltd.	MEDFORD	Glenda E.
Barbados	Ministry of Trade, Industry and Commerce	NICHOLLS	Anthony
Belize	Public Utilities Commission	SMITH	Kingsley
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Grenada	National Telecommunications Regulatory Commission	ROBERTS	Vincent
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Guyana	Office of the Prime Minister	RAMOTAR	Alexei
Guyana	National Frequency Management Unit	SINGH	Valmikki
Jamaica	University of the West Indies	DUNN	Hopeton S.
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts and Nevis	Ministry of Information and Technology	BOWRIN	Pierre G.
Saint Kitts and Nevis	Ministry of the Attorney General, Justice and Legal Affairs	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FELICIEN	Barrymore
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FLOOD	Michael R.
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	JEAN	Allison A.
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	ALEXANDER	K. Andre
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel

Bijlage 1

Land	Organisatie	Familienaam	Voornaam
Suriname	TelecommunicatieAutoriteit Suriname / Telecommunication Authority Suriname	LETER	Meredith
Suriname	Ministry of Justice and Police, Department of Legislation	SITALDIN	Randhir
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PHILIP	Corinne
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon

Regional / Deelnemers vanuit Regionale en / of Internationale Organisaties

Organisatie	Familienaam	Voornaam
Caribbean Community Secretariat (CARICOM)	JOSEPH	Simone
Caribbean ICT Virtual Community (CIVIC)	GEORGE	Gerry
Caribbean ICT Virtual Community (CIVIC)	WILLIAMS	Deirdre
Caribbean Telecommunications Union(CTU)	WILSON	Selby
Delegation of the European Commission to Barbados and the Eastern Caribbean (EC)	HJALMEFJORD	Bo
Eastern Caribbean Telecommunications Authority (ECTEL)	CHARLES	Embert
Eastern Caribbean Telecommunications Authority (ECTEL)	GILCHRIST	John
Eastern Caribbean Telecommunications Authority (ECTEL)	HECTOR	Cheryl
International Telecommunication Union (ITU)	CROSS	Philip
International Telecommunication Union (ITU)	LUDWIG	Kerstin
Office of Trade Negotiations (formerly CRNM) Caribbean Community Secretariat (CARICOM)	BROWNE	Derek E.
Organization of Eastern Caribbean States Secretariat (OECS)	FRANCIS	Karlene

Experts voor het HIPCAR Project

Familienaam	Voornaam
MARTÍNS DE ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[23]	J Paul
PRESCOD	Kwesi

[23] Workshop voorziter

Bijlage 2

Deelnemers in de Tweede Consultatieve Workshop (fase B) voor de Werkgroep van het HIPCAR project, van de Werkgroep inzake ICT Wetgevingskader voor Kwesties de Informatiemaatschappij rakende Frigate Bay, Saint Kitts and Nevis, 19-22 Juli 2010

Officieel Benoemde Deelnemers en Waarnemers

Land	Organisatie	Familienaam	Voornaam
Antigua and Barbuda	Ministry of Information, Broadcasting, Telecommunications, Science & Technology	SAMUEL	Clement
Bahamas	Utilities Regulation and Competition Authority	DORSETT	Donavon
Barbados	Ministry of Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Office of Trade Negotiations	BROWNE	Derek
Barbados	Ministry of Trade, Industry and Commerce	NICHOLLS	Anthony
Belize	Ministry of Finance	LONGSWORTH	Michelle
Belize	Public Utilities Commission	PEYREFITTE	Michael
Dominica	Ministry of Information, Telecommunications and Constituency Empowerment	CADETTE	Sylvester
Dominica	Ministry of Legal Affairs	RICHARDS-XAVIER	Pearl
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Grenada	National Telecommunications Regulatory Commission	ROBERTS	Vincent
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Guyana	Office of the President	RAMOTAR	Alexei
Guyana	National Frequency Management Unit	SINGH	Valmikki
Jamaica	Digicel Group	GORTON	Andrew
Jamaica	Office of the Prime Minister	MURRAY	Wahkeen
Jamaica	Attorney General's Chambers	SOLTAU-ROBINSON	Stacey-Ann
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts and Nevis	Ministry of National Security	ARCHIBALD	Keisha
Saint Kitts and Nevis	Department of Technology	BOWRIN	Pierre
Saint Kitts and Nevis	ICT4EDC Project	BROWNE	Nima
Saint Kitts and Nevis	Government of St. Kitts and Nevis	CHIVERTON	Eurta
Saint Kitts and Nevis	Department of Technology	HERBERT	Christopher
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	LAZAAR	Lloyd
Saint Kitts and Nevis	Ministry of Finance, Financial Intelligence Unit	MASON	Tracey
Saint Kitts and Nevis	Ministry of Sustainable Development	MUSSENDEN	Amicia

Bijlage 2

Land	Organisatie	Familienaam	Voornaam
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	PHILLIP	Glen
Saint Kitts and Nevis	Attorney General's Chambers	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Ministry of Finance, Financial Intelligence Unit	SOMERSALL-BERRY	Jacqueline
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Ministry of Communication, Works, Transport and Public Utilities	DANIEL	Ivor
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FELICIEN	Barrymore
Saint Lucia	Cable & Wireless (St. Lucia) Ltd.	LEEVY	Tara
Saint Lucia	The Attorney General's Chambers	VIDAL-JULES	Gillian
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	ALEXANDER	K. Andre
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel
Suriname	Telecommunicatiebedrijf Suriname (TELESUR)	JEFFREY	Joan
Suriname	TelecommunicatieAutoriteit Suriname	LETER	Meredith
Suriname	Ministry of Justice and Police	SITLADIN	Vyaiendra
Suriname	Ministry of Transport, Communication and Tourism	SMITH	Lygia
Trinidad and Tobago	Office of the Prime Minister, Information Division	MAHARAJ	Rishi
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PHILIP	Corinne
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon

Regional / Deelnemers vanuit Regionale en / of Internationale Organisaties

Organisatie	Familienaam	Voornaam
Caribbean Community Secretariat (CARICOM)	JOSEPH	Simone
Caribbean ICT Virtual Community (CIVIC)	HOPE	Hallam
Caribbean ICT Virtual Community (CIVIC)	ONU	Telojo
Eastern Caribbean Telecommunications Authority (ECTEL)	WRIGHT	Ro Ann
International Telecommunication Union (ITU)	CROSS	Philip
International Telecommunication Union (ITU)	LUDWIG	Kerstin
Organization of Eastern Caribbean States Secretariat (OECS)	FRANCIS	Karlene

Bijlage 2

Experts voor het HIPCAR Project

Familienaam	Voornaam
GERCKE	Marco
MORGAN[24]	J Paul
PRESCOD	Kwesi

[24] Workshop voorziter.

International Telecommunication Union
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Geneva, 2013