Mercuriale 2016 uitgesproken door PG A met dank voor de medewerking van SPG Dirk Schoeters en SPG met opdracht Robrecht De Keersmaecker .

Uitdagingen voor de rechtshandhaving in cyberspace.

Inhoud

Actualiteit – introductie

Er gaat geen dag, week of maand voorbij of onze samenleving wordt geconfronteerd met één of andere vorm van “cybercriminaliteit”. Men hoeft enkel maar de media te volgen om te beseffen dat er steeds vaker misbruik wordt gemaakt van de digitale wereld om een brede waaier van misdrijven te plegen:

Bv. 09.06.2016: Downsec legt Tax-on-web namiddag plat (http://www.hln.be/hln/nl/943/Consument/article/detail/2728061/2016/06/08/Tax-on-Web-platgelegd-door-hackerscollectief-Down-Sec.dhtml).

Bv. 09.06.2016: België scoort slecht op vlak van cyberveiligheid (http://www.standaard.be/cnt/dmf20160608_02329845).

Bv. 29.06.2016: hackers vallen steeds vaker dokters en zorginstellingen aan (http://www.gva.be/cnt/dmf20160628_02361089/hackers-vallen-steeds-vaker-dokters-en-zorginstellingen-aan).

Dit hoeft ook niet te verwonderen. Het internet en de daarbij horende moderne communicatiemiddelen (sociale media, Voice over IP (VoIP), cloud-services, messenger-diensten …) zijn niet meer weg te denken uit het dagdagelijkse leven van de burgers, bedrijven en overheden. Het internet is daarbij uitgegroeid tot het belangrijkste informatiemedium en communicatiekanaal.

Deze digitale revolutie biedt ongetwijfeld enorme kansen voor economische en maatschappelijke vooruitgang en zal de volgende jaren één van de sterkste motoren zijn van groei, jobs en welzijn.

Het is dan ook niet meer dan logisch dat de regering met haar actieplan “Digital Belgium” deze kansen wil grijpen en een digitale langetermijnvisie heeft ontwikkeld om de positie van België op de digitale kaart te versterken[1]. Eén van de prioriteiten hierbij is ‘digitaal vertrouwen en digitale veiligheid’.

We moeten ons echter bewust zijn dat er ook een keerzijde is aan de toenemende impact van deze digitale technologieën. Er dient te worden vastgesteld dat ook de criminaliteit nieuwe kansen heeft gekregen. Dit stelt zeer reële uitdagingen op het vlak van de rechtshandhaving waardoor nieuwe mogelijkheden op het vlak van opsporing en vervolging moeten worden aangesneden.

[1] Zie www.digitalbelgium.be.

Beleidsdocumenten

De regering, het Openbaar Ministerie en de politiediensten zijn zich bewust van deze nieuwe uitdagingen.

De **Kadernota Integrale Veiligheid** (KIV) 2016-2019 weerhoudt terecht "cybercrime en cybersecurity" als één van de 10 prioritaire clusters inzake veiligheid.

Tevens worden meerdere uitdagingen gedefinieerd die doorheen de aanpak van meerdere criminele fenomenen lopen en dus een transversaal karakter hebben: het gebruik van het internet en ICT als facilitator voor criminaliteit maar ook de aanpak voor veiligheidshandhaving en opsporing is er één van. In de KIV wordt bijgevolg gesteld dat een integrale en geïntegreerde aanpak voor deze materie absoluut prioritair is.

Ook het **College van Procureurs-generaal** heeft in zijn **jaarverslag** 2013-2015 "cybercrime" als één van de vijf belangrijkste criminaliteitsfenomen bepaald voor het komende jaar.[2]

Het betreft hier enerzijds de informaticacriminaliteit in de strikte zin (aanvallen op informaticasystemen, met inbegrip van de kwetsbaarheid van de kritieke infrastructuren en "cybercrime as a service") en anderzijds in de ruime zin (het gebruik van het internet en nieuwe technologieën om klassieke criminele feiten te plegen). Bij dit laatste punt zal in het bijzonder gefocust worden op de strijd tegen terrorisme, cyberhate en kinderpornografie.

Het College van Procureurs-generaal heeft in 2015 een **nieuw expertisenetwerk Cybercrime** opgericht dat belast is met de uittekening van het strafrechtelijk beleid vanuit drie invalshoeken: de informaticacriminaliteit in de strikte zin, de mogelijkheden en moeilijkheden met betrekking tot het onderzoek op internet of andere elektronische communicatienetwerken alsook de middelen en struikelblokken betreffende de interceptie van de communicatie.

Het heeft ook als doelstelling de expertise binnen het OM te bundelen en te verspreiden.

In het **advies** met betrekking tot de **Kadernota Integrale Veiligheid** wijst het College van Procureurs-generaal op de moeilijkheden die de politiediensten ondervinden inzake lokalisatie en onderscheppen van communicatie ten gevolge de niet te stuiten technologische evoluties.

Het College formuleerde drie voorstellen: het aanpassen van het wettelijk kader, investeringen in middelen en een dringende verhoging van de capaciteit van de federale politie.

[2] www.om-mp.be: Jaarverslag 2013-2015 College van Procureurs-generaal.

Deze beleidsteksten en visies dienen ook in de praktijk omgezet te worden.

Tijd om even stil te staan wat de begrippen “cyberveiligheid” en “cybercrime” inhouden, welke hinderpalen het Openbaar Ministerie ondervindt die een efficiënte aanpak van deze vormen van criminaliteit bemoeilijken en de mogelijke oplossingen die zich kunnen aandienen met een blik vooruit naar nieuwe aankomende wetgeving.

Wat “cyberveiligheid” betreft werd bij Koninklijk Besluit van 10 oktober 2014 eindelijk het reeds lang aangekondigde **Centrum voor Cybersecurity België (CCB)** opgericht. De oprichting hiervan betekent voor deze problematiek een belangrijke stap: het CCB zal immers als centrale autoriteit optreden voor de cyberveiligheid in België.

Niets te vroeg blijkt. Op 8 juni 2016 bracht De Standaard nog de krantenkop dat België de slechtste leerling op vlak van cyberveiligheid zou zijn[3]. Meer concreet zou België het land zijn dat het meest kwetsbaar is voor aanvallen van hackers op computerservers, gelet op het aantal openstaande poorten. Dat zou blijken uit een rangschikking die het internetbeveiligingsbedrijf Rapid7 publiceerde en die The Guardian publiekelijk naar buiten bracht[4].

Beide begrippen “Cybercrime en “Cybersecurity” worden vaak in één adem genoemd en gaan ook hand in hand. Hoe veiliger de systemen hoe moeilijker misdrijven kunnen gepleegd worden.

Evident dus dat het Openbaar Ministerie zich op de eerste plaats focust op de opsporing en de vervolging van de misdrijven. Dit wil echter niet zeggen dat het Openbaar Ministerie haar steentje niet zal bijdragen aan de werkzaamheden van het Centrum voor Cybersecurity België en daar waar nodig en nuttig zal samenwerken.

[3] http://www.standaard.be/cnt/dmf20160608_02329845.
[4] https://www.theguardian.com/technology/2016/jun/08/belgium-nations-vulnerable-hacking-exposed-servers-rapid7-heat-map-internet.

Situering cybercrime

Definitie

Tijd om even stil te staan wat de begrippen “Cyberveiligheid, Cybercrime” inhouden.

Cyberveiligheid is “de gewenste toestand waarbij de beveiliging van cyberspace in verhouding staat tot de cyberdreiging en de mogelijke gevolgen van cyberaanvallen”. Cyberveiligheid houdt ook in het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT.

De gevolgen door misbruik, verstoring of uitval kunnen bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van informatie of schade aan de integriteit van die informatie (onrechtmatig wijzigen, wissen of toevoegen)[5].

Kortom alles wat ICT maatschappelijk en economisch voor ons betekent.

Cyberveiligheid is de meest effectieve manier om cybercrime te bestrijden. Voorkomen is immers beter dan genezen.

Het komt vooreerst neer op een gedegen digitale hygiëne bij de gebruiker.

Die digitale hygiëne laat zich misschien nog het best vatten in de principes “Doe niets online wat u ook niet offline zou doen” en “als iets te mooi lijkt om waar te zijn, is het doorgaans niet waar”.

Cyberveiligheid gaat echter verder. Een doorgedreven cyberveiligheidsbeleid begint immers reeds bij het ontwerpen van nieuwe IT-systemen, bij het voorzien van minimale veiligheidsvoorschriften. Dit zal almaar belangrijker worden naarmate er steeds meer zaken aangesloten en geïnterconnecteerd worden.

Het Openbaar Ministerie is er zich terdege van bewust dat cyberveiligheid niet zal kunnen beletten dat er toch nog misdrijven gepleegd worden, maar meent dat het een eerste en cruciaal front is in de strijd tegen cybercrime.

Cybercrime of informaticacriminaliteit neemt een hoge vlucht. Dit is een logisch gevolg van de toenemende rol die informatica binnen de maatschappij speelt. Elke criminele activiteit die informatietechnologie als middel of als doelwit omvat, valt binnen de brede definitie van cybercrime.

[5] Nationale Cyber Security Strategy België d.d. 23.11.2012, https://www.b-ccentre.be/wp-content/uploads/2013/03/cybersecustra_nl.pdf, p. 15.

Een engere definitie behelst de bijzondere misdrijven zoals ingevoerd in de wet van 28 november 2000: de informaticavalsheid, het informaticabedrog, de hacking en de informaticasabotage.

Dat de gewone crimineel bovendien steeds vaker informatietechnologie gebruikt om zijn gewone misdrijven te plegen of de straffeloosheid ervan te bewerkstelligen, bezorgt menig rechtshandhaver een nachtmerrie en doet de grens tussen klassieke misdrijven en informaticacriminaliteit steeds vager worden.

Evolutie en beeldvorming

Doorheen de jaren negentig bleef cybercrime in het algemeen en hacking in het bijzonder doorgaans een vrijetijdsbezigheid van occasionele, technisch zeer beslagen zonderlingen, maar vanaf de jaren 2000 begon er iets te roeren vanuit Oost-Europa.

Die verandering bleek in eerste instantie uit de soort van websites die geviseerd werden, de hoeveelheid spam en phishing mailverkeer en de remonte van kredietkaartfraude. Cybercrime ontwikkelde zich tot een professionele en winstgerichte onderneming[6], aangewend door internationale criminele organisaties[7].

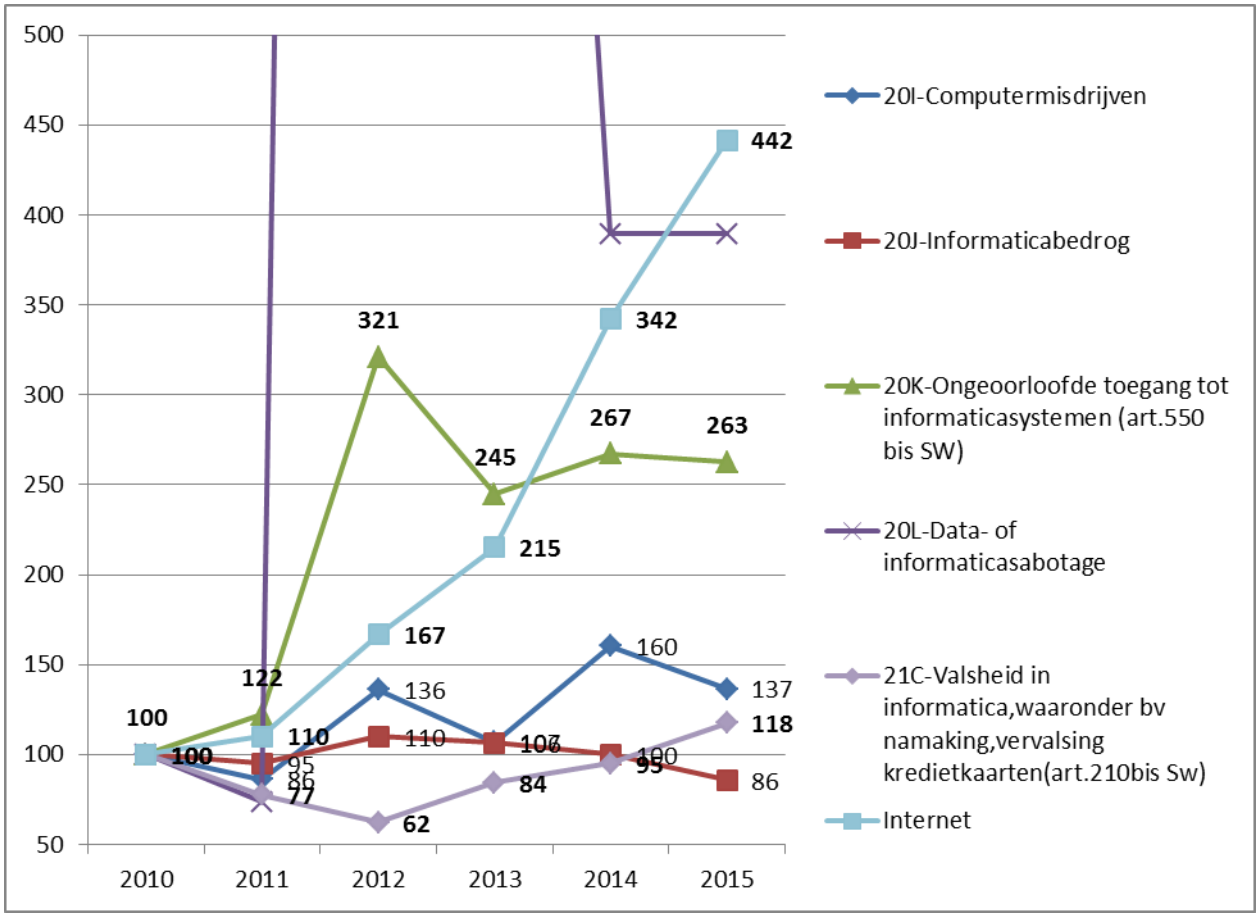
Cybercrime verschilt van klassieke criminaliteit op enkele wezenlijke punten: cybercrime is niet lokaal, maar globaal, niet persoonlijk, maar doorgaans anoniem, niet individueel, maar massaal.

Cybercrime is bovendien in wezen een technology-driven sector en kent bijgevolg een exponentiële groei.

Zo zagen we in België tussen 2010 en 2015 een stijging van de misdrijven gepleegd via of middels het internet met 342%.

[6] https://www.wired.com/2016/05/maksym-igor-popov-fbi/.

[7] Op 25 juni 2015 deelde het Federaal Parket mee dat het meegewerkt had aan een internationale operatie waarbij een dergelijke internationale bende werd onthoofd: in 2010 hadden verschillende Belgische banken te kennen gegeven dat het internetbankieren-platform van hun klanten besmet was met Zeus en SPyEye malware. Op deze wijze werden grote sommen geld getransfereerd van de rekeningen van de besmette klantenaccounts naar rekeningen in Spanje en Portugal. Vandaar gingen de gelden naar zogenaamde “moneymules”, wiens rol erin bestond de illegaal verworven gelden meermaals rond te laten gaan en uiteindelijk tot bij de opdrachtgevers te brengen. In totaal werden er een 1500 klanten voor bijna 5 miljoen euro opgelicht, waarvan ongeveer 2 miljoen gerecupereerd kon worden. Het onderzoek werd in samenwerking met Eurojust en Europol gevoerd en bracht de onderzoekers naar Duitsland, Frankrijk, Nederland, Finland, Moldavië, Polen, Letland, Estland, Oekraïne en Rusland, waar men uiteindelijk de leidende personen kon vatten. Hierbij was het doorgedreven onderzoek van het daartoe nieuw opgerichte “NewTech”-team in de schoot van de Federal Computer Crime Unit (FCCU) van cruciaal en baanbrekend belang.



Ook is het verontrustend te noemen dat de drempel steeds lager wordt. Waar de hacker in de jaren 80-90 nog over een zeer grote technische bagage diende te beschikken, duiken er thans steeds meer programma's op (de zogenaamde *hackertools*), die het hacken binnen eenieders handbereik brengen ongeacht de voorkennis van de gebruiker[8].

De voorbeelden opgenomen in de rand tonen aan dat België zijn rol op internationaal vlak ter harte heeft genomen en dit ook naar de toekomst toe wil blijven doen.

[8] Een voorbeeld hiervan is de hackersoftware *Blackshades*, een *remote access tool (RAT)* dat toelaat om een besmet systeem te bespioneren of zelfs over te nemen met het oog op het verwerven van vertrouwelijke informatie of te encrypteren met oog op het verkrijgen van een losgeld. De Amerikaanse FBI kwam deze malware op het spoor en ontdekte een criminele organisatie aangevoerd door een Zweed en een Amerikaan. Zij hadden verschillende versies van de malware ontwikkeld, die door andere cybercriminelen online gekocht kon worden voor een luttele $40 voor een basisversie, maar die eveneens geheel aan de wensen van de crimineel kon worden aangepast. De organisatie werd als een bedrijf gerund: personeel werd aangeworven, lonen betaald, updates van de malware geleverd op vraag van klanten. Er was een marketing directeur, een website-ontwikkelaar, een klantendienst en een team van vertegenwoordigers. Opnieuw in een internationale actie ingevolge samenwerking tussen de FBI, EUROPOL en EUROJUST werden er wereldwijd 359 huiszoekingen gedaan in België, Nederland, Frankrijk, Duitsland, Verenigd Koninkrijk, Finland, Oostenrijk, Estland, Denemarken, Italië, Kroatië, de VSA, Canada, Chili, Zwitserland en Moldavië. Er werden 97 personen aangehouden.

Deze cijfers zijn echter maar het topje van de ijsberg. De niet gekende feiten – het zogenaamde *dark number* – is vele malen groter. Doorgaans zijn slachtoffers van informaticamisdrijven immers niet snel geneigd hiervan aangifte te doen. Men vreest – terecht – een bijkomende reputatieschade wanneer de buitenwereld lucht zou krijgen van hun tegenspoed. Cybercriminelen rekenen hierop en voelen zich gerustgesteld door de daaruit volgende straffeloosheid. Hierbij moet echter vermeld worden dat niet enkel de mogelijke reputatieschade voor de geviseerde ondernemingen op het spel staat. Uiteraard worden ook de belangen van de klanten van deze ondernemingen wiens gegevens desgevallend ten prooi vielen aan cybercriminelen, afgewogen.

In deze zin zal de Algemene Verordening Gegevensbescherming ondermeer voorzien in een verplichting[9] voor bedrijven om gebeurlijke *data breaches* te melden, niet alleen aan de betrokken klanten, maar zelfs aan de toezichthouder, indien deze inbreuk risico's voor de rechten en vrijheden met zich mee brengt[10]. Het niet naleven van deze verplichtingen zal zelfs middels administratieve geldboetes[11] kunnen worden beteugeld.

Deze sector staat allerminst stil. Het is onrustwekkend te zien hoe informaticacriminaliteit zich ontwikkelde de voorbije 20 jaar. Zo is er een bloeiende zwarte economie ontstaan op het internet, die toelaat aan geografisch sterk verspreide individuele actoren om zich te specialiseren in bijzondere kennis, diensten of middelen, waar nagenoeg alles beschikbaar is voor de juiste prijs. De bijgaande schaalvergroting zorgt ervoor dat een informaticamisdrijf mogelijks door een dozijn verschillende mededaders gepleegd wordt, waarbij elk een apart deel van de keten voor zijn of haar rekening neemt zonder zich te moeten bekommeren om het overige en hiervoor een vaste prijs of commissie betaald krijgt[12].

Deze ondergrondse marktplaats reguleert zich bovendien steeds meer zelf als een sociaal netwerk, in de zin dat men elkaar online gaat beoordelen al naargelang tevredenheidsgraad, dat er referenties gegeven moeten worden tot zelfs het afnemen van echte interviews alvorens toetreding mogelijk is.

[9] Verordening 2016/679, *EU Publ*., L 119/33, art. 33 en 34.
[10] Verordening 2016/679, *EU Publ*., L 119/17, overweging 85.
[11] Verordening 2016/679, *EU Publ*., L 119/82, art. 83.
[12] Een voorbeeld: handel in namaak (kledij, geneesmiddelen, software, etc.). Vroeger geschiedde deze handel deur-aan-deur, op markten, in schimmige winkels. Thans zoekt een verkoper van namaak een afzetmarkt. Twitter, maar evengoed kapaza of 2dehands.be, lijkt een goed kanaal om zijn producten aan te bieden. Hij doet beroep op een spammer met toegang tot een veelheid aan Twitter-contacten, met afscherming van zijn eigen IP-adressen. Hierbij gebruikt hij een grote hoeveelheid valse accounts. Die accounts worden aangemaakt door weer andere partijen, die hierbij op hun beurt beroep doen op fysieke ondersteuning om de CAPTCHA en sms-verificaties te verrichten. Zo belanden de reclame-links in de brievenbus van mogelijke argeloze kandidaat kopers. Zodra ze op de links klikken, treedt een tweede luik in werking. De koper wordt verwezen naar een webpagina, gemaakt en gehost door nog andere dienstverleners. Daar wordt de bestelling opgenomen, de betaling afgehandeld en de gegevens mogelijks nog bewaard om in de toekomst verder illegaal ten gelde te maken. Ten slotte krijgt de klant zijn namaak product en krijgen de dienstverleners een deel van de koek.

Cruciale schakel voor deze netwerken zijn steeds vaker de besmette systemen van onwetende gebruikers. Die systemen blijken een schat aan informatie (keyloggers) te bieden, alsook de noodzakelijke middelen (rekenkracht, bandbreedte, toegang tot contacten, schijn van waarachtigheid, etc.) waarbij de besmette systemen als kip met de gouden eieren niet langer zelf uitgemolken worden, doch worden ingezet als kapitaal om andere systemen te viseren.

De uitbetaling is een flessenhals voor de criminele economie. Inderdaad, het internationale betaalverkeer is sterk gereglementeerd en wordt nauwgezet opgevolgd, zodat cybercriminelen hun toevlucht moeten zoeken tot money-mules, prepaid-diensten en digitale en/of cryptocurrencies (Bitcoin, WebMoney, Ukash, paysafecard, Paypal, etc.)[13]. Klassieke rechtshandhaving lijkt hier weinig zoden aan de dijk te kunnen brengen gelet op de anonimiteit die dergelijke diensten al te vaak vergezelt. Innovatievere vormen van bestrijding zijn noodzakelijk, benevens uiteraard een versterking van de bescherming en responsabilisering van de gebruikers. Hierbij kan in eerste instantie gedacht worden aan de verstoring van het criminele betaalverkeer, dat een groter effect heeft dan het vatten van de daders. Maar ook hier blijkt het zeer moeilijk om gelijke tred te houden met de ontwikkelingen en lijken rechtshandhavers op achternahollen aangewezen.

Nochtans konden EUROJUST, EUROPOL en diverse Amerikaanse rechtshandhavingsdiensten in november 2014 de ondergrondse economie een gevoelige slag toedienen via Operation Onymous, waarbij het Darknet handelsplatform Silk Road 2.0 werd onderuit gehaald en diens beheerder gearresteerd.

Criminelen zijn aldus niet onvindbaar op het Darknet en het effect van deze actie liet zich voelen[14].

De motieven van de cybercrimineel blijken dus aloud: het gros van de cyberverdachten doet het voor het geld (65%).

Anderen doen het om zijn of haar boodschap kracht bij te zetten, het zogenaamde hacktivisme (25%). Hierbij kan verwezen worden naar de recente praktijken van het hackercollectief Down-sec[15] in het voorbije jaar: het publiek maken van foto's van de vermeende pestkoppen van de 14-jarige Madison, het meisje uit Herstal dat ingevolge de voortdurende pesterijen geen andere uitweg zag dan zelf uit het leven te stappen, of het platleggen van overheidswebsites. Internationaal kan er gewezen worden op het hackerscollectief Anonymous.

[13] The Internet Organized Crime Threat Assessment (IOCTA) 2015, p. 46, https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.
[14] https://www.europol.europa.eu/print/content/global-action-against-dark-markets-tor-network.
[15] http://www.lecho.be/economie_politique/belgique_general/Qui_se_cache_derriere_Down_Sec.9784581-4003.art?ckc=1&ts=1467618796 ; https://twitter.com/downsecbelgium?lang=nl.

Zelden handelt het, althans volgens de gekende gegevens, om spionage (7%) en oorlogsvoering (3%), hoewel de mogelijke gevolgen van dergelijke aanvallen uiteraard des te desastreuzer zijn.

Zo zagen het Amerikaanse FBI en Homeland Security in februari 2016 hun lijsten met werknemersgegevens ontvreemd en openlijk op het internet verspreid door een Pro-Palestijnse groepering, waardoor deze personen geviseerd dreigen te worden door malafide spelers, net omwille van hun bijzondere hoedanigheid[16].

Ook naar de onmiddellijke toekomst toe toont de cybercrimineel zich stoutmoediger en gesofisticeerder dan ooit[17]. Hierbij dient eveneens verwezen te worden naar de recente dreigingsanalyse[18] van EUROPOL met een beeldvorming rond de bedreigingen voor de kritieke infrastructuren, ransomware aanvallen, informatiemanipulatie en het “Internet of things”.

Kritieke infrastructuur staat in voor de vitale productie en transport van energie, behelst de vitale knooppunten van het vervoer, betreft de onontbeerlijke schakels in het elektronische betalingsverkeer en de vitale verbindingen van de elektronische communicatie.

De definitie van kritieke infrastructuur staat vermeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren. De burger kent het beter als de elektriciteit die uit het stopcontact komt, het water dat uit de kraan komt, het openbaar vervoer dat ons naar onze bestemming brengt, de winkels waar we onze levensmiddelen kopen en de communicatiekanalen waar we op vertrouwen om contact te houden met vrienden en familieleden. Deze systemen zijn zeer complex, samengesteld uit een veelheid aan hardware en software, soms oeroud, vaak ontworpen met weinig aandacht voor cyberveiligheid.

Nochtans wordt de kritieke infrastructuur in toenemende mate geautomatiseerd en via netwerken gekoppeld, zodat deze ook vatbaarder wordt voor cyberaanvallen[19].

Na de *ransomware* aanvallen, waarbij de *malware* de toegang tot de systemen en bestanden van de gebruiker versleutelt totdat men een losgeld betaalt, zal men verregaandere afpersing zien opduiken. De cybercrimineel zal ermee dreigen gevoelige informatie over het slachtoffer publiek te maken indien er niet betaald wordt. Dit houdt in dat het geregeld maken van een back-up niet langer afdoende bescherming zal bieden. Bovendien is het nog maar de vraag of het slachtoffer van dergelijke feiten deze zal durven aan te geven aan de overheden, uit schrik nog

[16] http://www.zdnet.com/article/hacker-gains-access-to-20000-fbi-9000-dhs-employees-contact-details/.
[17] https://www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016/.
[18] The Internet Organized Crime Threat Assessment (IOCTA) 2015, https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.
[19] The Internet Organized Crime Threat Assessment (IOCTA) 2015, p. 44, https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.

meer schade te ondervinden als imagoschade of voor aansprakelijkheidsvorderingen van klanten wiens informatie gelekt werd.

Voorbeelden hiervan zagen we reeds in mei en juli 2015, toen datingsites *AdultFriendFinder* en *AshleyMadison*, zogezegd discrete websites waar men terecht kon voor een buitenhuwelijkse verhouding, gehackt werden en persoonlijke en vertrouwelijke gegevens over miljoenen van hun klanten gelekt werden, zodat ze mogelijks zeer kwetsbaar werden voor verdere afpersing. 1400 van die klanten werden immers geïdentificeerd als hooggeplaatste leidinggevenden binnen Fortune500 bedrijven[20].

Verwacht wordt dat cybercriminelen niet alleen gevoelige informatie zullen stelen, maar ook steeds vaker deze informatie zullen manipuleren en wijzigen. In een maatschappij die steeds meer informatie digitaal opslaat en papieren dossiers achter zich laat, brengt dit immer grotere risico's met zich mee.

Het toevoegen van een chip en pincode aan kredietkaarten heeft het misbruik (skimming) van betaalkaarten teruggedrongen. Cybercriminelen zullen zich meer richten op online handel, waarbij via *(spear)phishing* en onvoldoende zorgvuldigheid van de gebruiker deze bescherming te omzeilen valt[21].

De opkomst van het *Internet of Things* en *Internet of Everything*, waarbij zaken steeds meer via het internet met elkaar verbonden worden, brengt ook het risico met zich mee dat deze voorwerpen (auto's, IP-camera's, huishoudtoestellen, etc.) onvoldoende beveiligd worden, wegens mogelijks verwaarloosbare inhoud, en dienvolgens misbruikt zullen worden als *vectors* in cyberaanvallen (bv. botnets)[22]. Bovendien brengen deze zaken een enorme bijkomende toestroom aan gegevens met zich mee, waarbij rechtshandhavers het steeds moeilijker zullen krijgen om de spreekwoordelijke naald in de hooiberg te vinden, spijts er ook krachtigere zoek- en analysetools ontwikkeld worden.

Ook bleken in 2016 enkele informaticatoestellen reeds van bij ontwikkeling achterdeurtjes te bevatten, waarlangs onbevoegden toegang konden krijgen tot de informatica-systemen waar ze deel van uitmaakten[23]. Dit hangt nauw samen met het debat inzake encryptie en universele toegang voor rechtshandhavers, waarover verder meer.

[20] http://www.ibtimes.co.uk/john-mcafee-adult-friendfinder-hack-major-threat-national-security-1504070.
[21] The Internet Organized Crime Threat Assessment (IOCTA) 2015, p. 34, https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.
[22] The Internet Organized Crime Threat Assessment (IOCTA) 2015, p. 43, https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.
[23] KAIYUAN, Y. e.a., "*A2: Analog Malicious Hardware",* http://static1.1.sqspcdn.com/static/f/543048/26931843/1464016046717/A2_SP_2016.pdf?token=N4pJSSoqL4kE4V4JXpTwx7qDRX4%3D.

Hinderpalen

1. Internationaal karakter, veelheid spelers

Internationaal

Een eerste en belangrijke hinderpaal voor de rechtshandhavingsinstanties in de strijd tegen cybercriminaliteit en de strijd tegen het criminele gebruik van informatietechnologieën is uiteraard de internationale dimensie van de huidige informatie- en communicatietechnologie (ICT).

Het internet is een netwerk van netwerken, via hetwelk een gebruiker door middel van een informaticasysteem toegang heeft tot een enorm aantal andere computernetwerken of -aansluitingen wereldwijd.

“Cyberspace”, de virtuele wereld van computers, is uitgegroeid tot een tweede wereld, een plaats waar gebruikers vanop afstand informatie (in alle mogelijke vormen) kunnen opzoeken, documenten en afbeeldingen kunnen bewaren in virtuele opslagplaatsen (dropbox of andere cloud-diensten), contacten en conversaties kunnen houden op sociale media en in chatrooms, op een geëncrypteerde en anonieme wijze kunnen communiceren en illegale bestanden (bv kinderpornografie) kunnen uitwisselen.

Het digitale bewijsmateriaal (“e-evidence”) verplaatst zich meer en meer naar servers elders in de wereld, vaak beheerd door derden. De locatie van opgeslagen gegevens is tevens niet langer een statisch gegeven maar is ook een dynamisch gebeuren geworden waarbij een derde, als het ware met één klik, een massa gegevens kan verplaatsen van het ene land naar het andere. Vaak is daarenboven de effectieve locatie zelfs niet gekend.

Zo kiezen cybercriminelen voor het gebruik van ICT om hun misdrijven te plegen bewust landen uit waarvan zij menen dat dit voor hen “veilige safehavens” zijn; landen waarmee de internationale samenwerking in strafzaken op zijn minst moeizamer verloopt, zo niet soms onbestaande is.

Deze internationale dimensie werpt rechtsvragen op omtrent de lokalisering van de misdrijven en de opsporings- en vervolgingsbevoegheden van nationale overheden.

De territoriale aanknopingspunten en de traditionele rechtshulpmechanismen zijn dan ook niet altijd adequaat om cybercriminaliteit doeltreffend te vervolgen en te bestraffen. Daardoor ontstaat de neiging om brede lokalisatiecriteria te gebruiken en ruime onderzoeksbevoegdheden te hanteren.

De vraag kan dan ook gesteld worden hoe moet omgegaan worden met de principes van soevereiniteit en territorialiteit in de huidige geïnformatiseerde samenleving en hoe de rechtshulpinstrumenten verbeterd kunnen worden om e-evidence op snelle en effectieve wijze te bewaren en te verzamelen?

Privaat-publiek

Naast deze strafprocedurele vraagstukken worden de rechtshandhavingsinstanties geconfronteerd met grote internationale dienstenverstrekkers (Apple, Microsoft, Google, Yahoo, Facebook, Twitter, Viber, Whatsapp, Skype, Telegram …) die er elk hun eigen policy op nahouden als het gaat over de samenwerking met gerechtelijke overheden. Dit zal mogelijks nog erger worden wanneer in 2017 de roamingkosten voor mobiel internet zullen wegvallen en de aanbieders vlotter consumenten over de grenzen heen zullen kunnen bedienen.

Voor deze internationale spelers is het vaak een huzarenstuk om een weg te vinden tussen de verplichtingen opgelegd door verschillende rechtssystemen, waarbij het risico op tegenstrijdige opvattingen inzake toepasselijkheid niet onderschat mag worden. De multinationals tonen zich vaak weigerachtig om mee te werken, zich hierbij verschuilend achter de vermeende extraterritoriale aanmatiging van onderzoeksbevoegdheden door het Openbaar Ministerie of de onderzoeksrechter wanneer deze hun medewerking vorderen met oog op achterhalen van de identiteit van cybercriminelen.

Het kan echter moeilijk ontkend worden dat deze internationale spelers, hoewel de meesten geen “fysieke” vestigingsplaats in België hebben, wel degelijk actief aanwezig zijn op ons Belgisch grondgebied en hier hun diensten online aanbieden. Dienen zij zich dan niet te conformeren naar onze Europese of Belgische wetgeving?

Een studie uitgevoerd voor de Europese commissie[24] wijst uit dat de E-Privacy richtlijn (richtlijn 2002/58/EC van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector van elektronische communicatie), inzonderheid wat betreft het toepassingsgebied van deze richtlijn, dringend aan herziening toe is en leidt tot een ongelijke behandeling indien zij enkel van toepassing zou zijn op de klassieke providers van elektronische communicatie en zich niet zou uitstrekken op andere dienstenverstrekkers die elektronische communicatiediensten aanbieden via het internet.

[24] https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.

Indien we cybercrime effectief willen bestrijden, is de samenwerking met de private sector van cruciaal belang. Het merendeel van de gegevens die noodzakelijk zijn om cybercriminelen op te sporen zit immers bij private partijen, zoals de internet access providers en de internet service providers. Zonder deze gegevens is het identificeren en lokaliseren van de cybercrimineel, laat staan vatten, simpelweg onmogelijk. Bovendien is de medewerking van de private sector primordiaal wil men cybercriminaliteit bij de bron bestrijden. Hierbij kan gedacht worden aan het blokkeren of verwijderen van websites waarop illegale *content* aangeboden worden.

Overleg met de private spelers is dan ook een must. Alleen dan kunnen we onze middelen bundelen om cybercrime te bestrijden.

Dit werd begin 2016 eveneens duidelijk benadrukt door het World Economic Forum[25].

2. Privacy en Dataretentie

Kenmerkend aan de informatie- en communicatietechnologie van heden ten dage is het feit dat elke vorm van telecommunicatie en internetverkeer digitale sporen nalaat die kunnen gelogd worden.

Al jarenlang steunen speurders en gerechtelijke autoriteiten sterk op deze gegevens om digitale sporen van misdrijven te verzamelen en verdachten te identificeren, maar ook om personen a décharge uit te sluiten van de lijst van verdachten of de slachtoffers van misdrijven op te sporen en te lokaliseren.

Bij arrest van 11 juni 2015[26] vernietigde het Grondwettelijk Hof de Belgische wetgeving die de operatoren zoals Telenet en Proximus en andere dienstverleners op het internet verplicht om de elektronische identificatie- en verkeersgegevens van al hun klanten bij te houden gedurende twaaf maanden. In het vernietigde artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie (WEC) werd voorzien in de verplichting voor aanbieders van aan het publiek aangeboden vaste telefoniediensten, mobiele telefoniediensten, internettelefoniediensten, internettoegangdiensten en internet e-maildiensten om bepaalde gegevens[27] te bewaren gedurende een termijn van twaalf maanden opdat die gegevens beschikbaar zouden zijn voor bepaalde specifieke doeleinden en in het bijzonder voor de strafonderzoeken of onderzoeken met het oog op inlichtingen.

De Belgische wetgeving zou onevenredig inbreuk plegen op het recht op privacy van elke burger. De wet is immers zonder onderscheid van toepassing op de gegevens van alle personen en alle communicatiemiddelen.

[25] http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf; http://www.eurojust.europa.eu/press/PressReleases/Pages/2016/2016-03-04.aspx.
[26] Arrest GWH nr. 84/2015 van 11 juni 2015.
[27] In de artikelen 3 tot en met 6 van het Koninklijk Besluit van 19 september 2013 tot uitvoering van artikel 126 WEC werd gedetailleerd vervat welke gegevens dienen te worden bijgehouden.

Volgens het Hof mogen enkel de gegevens worden bijgehouden van personen voor wie er een aanwijzing bestaat dat hun gedrag, zelfs al is het maar indirect of van ver, een verband vertoont met strafbare feiten. De bewaring moet ook beperkt blijven “tot een bepaalde periode of een bepaalde geografische zone of nog tot een kring van personen die betrokken kunnen zijn bij een inbreuk, of die zouden kunnen helpen, door het bewaren van gegevens, bij het voorkomen, opsporen of vervolgen van die inbreuken”. Een derde vorm van kritiek betreft de afwezigheid in de WEC van enige materiële of procedurele voorwaarde voor de toegang door de autoriteiten tot de bewaarde gegevens.

Door dit arrest van het Grondwettelijk Hof lijkt echter het evenwicht tussen het recht op privacy en het recht van de burger op effectieve veiligheid in het gedrang te komen.

Hoewel het arrest van het Grondwettelijk Hof in het verlengde lag van de vernietiging door het Hof van Justitie[28] van richtlijn 2006/24/EG (de zogenaamde “dataretentierichtlijn”), die in het vernietigde artikel 126 WEC ten uitvoer werd gelegd, was het Openbaar Ministerie toch enigszins verrast door deze uitspraak.

Het Grondwettelijk Hof lijkt te eisen dat enkel gegevens bewaard kunnen worden van mogelijke verdachten of van personen die kunnen bijdragen bij de opheldering van strafbare feiten.

De raadpleging van bewaarde gegevens bij operatoren is echter in de meeste gevallen de eerste noodzakelijke stap om op te sporen wie mogelijke verdachten zijn van een misdrijf. Het is evident dat politie noch justitie op voorhand weten welke personen in de toekomst mogelijke verdachten kunnen zijn in latere strafonderzoeken of wie het slachtoffer zal worden van een misdrijf. Telefonie- en internetgegevens kunnen juist richtinggevend zijn in de identificatie van mogelijke verdachten in bepaalde criminele netwerken of terroristische groepen.

Ons land heeft al jarenlang wettelijke waarborgen en voorwaarden ingebouwd voor de toegang van speurders tot communicatiegegevens. De strikte regels in het Wetboek van Strafvordering (artikelen 46bis en 88bis Sv) bepalen daarbij wie welke informatie voor welke misdrijven mag opvragen bij de operatoren. Zo is bijvoorbeeld bepaald dat identificatiegegevens slechts mogen worden opgevraagd, mits machtiging van de procureur des Konings. Voor oproepgegevens (incluis een zendmastbepaling) is er een bevelschrift van de onderzoeksrechter nodig.

Deze waarborgen lijken door het Grondwettelijk Hof buiten beschouwing gelaten te zijn. Zoals de voorzitter van de Privacycommissie trouwens opmerkt:

[28] Europees Hof van Justitie, 8 april 2014, C-293/12 en C-594/12.

"... het (is) vreemd dat de rechters in dit arrest niet dieper ingaan op de waarborgen die ons land al decennia heeft ingebouwd voor de toegang van speurders tot communicatiegegevens. ... Nog nooit is er een ernstig probleem vastgesteld. Merkwaardig dat het Grondwettelijk Hof daar geen rekening mee houdt." (De Standaard, maandag 15 juni 2015)".

Onmiddellijk na het arrest van het Grondwettelijk Hof heeft het Openbaar Ministerie als standpunt ingenomen dat nog steeds, zoals voorheen, op rechtsgeldige wijze toepassing kan gemaakt worden van de medewerkingsverplichtingen voorzien in de vermelde artikelen 46bis en 88bis Sv. In een vonnis van 20 juni 2014 aanvaardde de correctionele rechtbank van Antwerpen dat de gegevens, die bekomen worden via de vermelde artikelen 46bis en 88bis, nog rechtsgeldig kunnen worden gebruikt. De rechtbank kwam tot dit oordeel, zelfs nadat de vernietiging van de Europese Dataretentierichtiijn 2006/24/EG door het Europees Hof van Justitie (arrest van 8 april 2014) werd opgeworpen.

Naast de reeds vermelde artikelen 46bis en 88bis Sv, blijven ook de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de werking van persoonsgegevens (de Privacywet) en de artikelen 114, 122, 123, 124, 125 en 127 van de wet van 13 juni 2005, relevant en bieden zij een houvast.

Ondertussen werden reeds meerdere vonnissen en arresten geveld die het gebruik van de bekomen communicatiegegevens toelaten.

Het arrest van het Grondwettelijk Hof van 11 juni 2015 bracht echter voor alle spelers op het terrein een factor van rechtsonderzekerheid.

In de nasleep van de “Snowden-affaire” lijkt bij bepaalde belangengroepen het gevoel te leven dat de privacy van de burgers van geen tel meer is en dat de bestrijding van zware criminaliteit en terrorisme van de massacontrole een politiek haalbare kaart maakt.

De bescherming van de privacy en van de grondwettelijke rechten en vrijheden van de burger, net als zijn recht op veiligheid, zijn wel degelijk fundamentele waarden die het Openbaar Ministerie hoog in het vaandel draagt.

Het is echter een realiteit dat die rechten meer en meer onder druk komen te staan door allerlei vormen van criminaliteit, zoals de cybercriminaliteit, de zware en georganiseerde criminaliteit, het gewelddadig extremisme en terrorisme.

Het evenwicht tussen deze rechten is van cruciaal belang in een democratische rechtstaat.

Zonder het debat te willen polariseren, dienen enkele elementen in dit kader in het juiste daglicht te worden geplaatst.

Het Europees Hof stelde dat de dataretentie-richtlijn een zeer ruime en bijzonder zware inmenging vormt in de door artikelen 7 en 8 van het EU-Handvest gewaarborgde rechten, maar dat deze dataretentie wel degelijk beantwoordt aan een doel van algemeen belang, en een waardevol instrument vormt bij strafonderzoeken.

Er dienen evenwel duidelijke en precieze regels te bestaan die minimale vereisten opleggen betreffende de draagwijdte en de toepassing van de betrokken maatregelen, zodat de personen van wie de gegevens bewaard zijn voldoende garanties hebben dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en onrechtmatig gebruik van deze gegevens.

Het belang van communicatiegegevens voor strafonderzoeken kan niet voldoende onderstreept worden. Zoals reeds gesteld zijn identificaties en retro-actief telefonie-onderzoek in zowat elk belangrijk strafonderzoek naar feiten van zware en georganiseerde criminaliteit, terrorisme-onderzoeken, onderzoeken naar kinderpornografie, ontvoeringen, cyberlokkers, illegale wapenhandel, handel in verdovende middelen, aanzetten tot haat en discriminatie, hackings, vaak de eerste en enige stap zijn om de misdrijven op te helderen en de daders te identificeren in een tijdperk waar deze criminelen meer en meer gebruik maken van de moderne communicatietechnologieën om deze misdrijven voor te bereiden en te plegen, en onderling op geëncrypteerde wijze te communiceren.

Dataretentie is inderdaad van algemeen belang.

“Dataretentie” is overigens geen “massasurveillance” en heeft daarenboven niets te maken met de bewaring van inhoud (“content”) van elektronische communicatie.

Een ander belangrijk element in het debat is artikel 8 EVRM dat de bescherming van het privé-leven waarborgt, houdt tevens een positieve verplichting in voor de lidstaten om inbreuken op dit recht op privacy ook daadwerkelijk te kunnen onderzoeken, de daders te kunnen identificeren en te vervolgen.

Vermeldenswaardig in deze context is het arrest van het Europees Hof voor de Rechten van de Mens inzake K.U. v. Finland van 2 december 2008.

De feiten van deze zaak dateren van 1999 maar zijn nog steeds zeer actueel: een onbekende had een vals profiel aangemaakt op een datingsite met de naam van een onwetend minderjarig (12-jarig) slachtoffer, hierbij aangevend dat het op zoek was naar intieme contacten met minder- of meerderjarigen.

Er werd tevens een webpagina aangemaakt met foto’s van het slachtoffer en het e-mailadres. De vader van de benadeelde kwam dit te weten doordat er reacties kwamen via e-mail van mannen die het slachtoffer wensten te ontmoeten.

Hoewel de houder van het IP-adres waarmee de advertentie was aangemaakt gekend was bij de internet service provider, liet de Finse wetgeving, om reden van privacy en geheimhoudingsplicht, niet toe dat de internet service provider (ISP) diens identiteit vrij gaf aan de gerechtelijke autoriteiten.

Finland werd in deze zaak veroordeeld voor een schending van artikel 8 EVRM omdat haar wetgeving niet toeliet om over te gaan tot de nodige identificaties.

In bovenvermeld arrest van het Europees Hof voor de Rechten van de Mens wordt eveneens dieper ingegaan op reeds lang bestaande internationale aanbevelingen en rechtsinstrumenten in het domein van de strijd tegen cybercrime[29].

Meer dan twintig jaar geleden nam de Raad van Europa op 11 september 1995 aanbeveling R (95)13 aan. Deze aanbeveling is cruciaal voor het strafprocedurele luik van de strijd tegen cybercrime. In punt 12 van de appendix aan de aanbeveling werd ondermeer het volgende bepaald: *"Specific obligations should be imposed on service-providers who offer telecommunication services to the public, either through public or private networks, to provide information to identify the user when so ordered by the competent investigation authority".*

Verder stipuleerde de appendix onder punt V.14.: "*Use of encryption. Measures should be considered to minimize the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary".*

Hoewel het document reeds werd opgesteld in de vorige eeuw, dient vandaag nog steeds vastgesteld te worden dat de voorliggende procedurele problematieken ongewijzigd zijn.

Ook het Verdrag van Budapest van 23 november 2001 betreffende computercriminaliteit ("Cybercrime conventie"), geratificeerd door België[30] in 2013, bepaalt eveneens het minimum wettelijk procedureel arsenaal dat door de lidstaten dient te worden voorzien om cybercrime "sensu lato" te bestrijden.

Verder verwijst het arrest van het Europees Hof in dit verband ook nog naar de resoluties van de Verenigde Naties 55/63 van 4 december 2000 en 56/121 van 19 december 2001 betreffende de strijd tegen het crimineel gebruik van informatietechnologieën.

Er dient dus vastgesteld dat de tegenstanders van dataretentiewetgeving er nog steeds niet in slagen om te verantwoorden hoe aan deze essentiële aanbevelingen en internationale verplichtingen kan voldaan worden zonder wettelijk opgelegde dataretentieverplichtingen.

[29] Zie dienaangaande ook: KERKHOFS, J., VAN LINTHOUT, P., *Cybercrime*, Politeia, 2013, p. 21-33.
[30] Wet van 3 augustus 2013 houdende instemming met het Verdrag betreffende de computercriminaliteit gedaan te Budapest op 23 november 2001.

De regering heeft na het arrest van het Grondwettelijk Hof onmiddellijk de nodige initiatieven genomen om de rechtsonzekerheid weg te werken, wat geleid heeft tot de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van gegevens in de sector van de elektronische communicatie.

De uitkomst was een moeilijke evenwichtsoefening tussen de fundamentele rechten en vrijheden. Van deze huidige dataretentiewetgeving kan op zijn minst gezegd worden dat zij klaar en duidelijk is en tal van waarborgen, checks and balances, wettelijk versterkt.

De wet gaat uit van het standpunt dat de rechtspraak van het Hof van Justitie en het Grondwettelijk Hof niet verhindert dat de gegevens van alle personen op ongedifferentieerde wijze worden bewaard. In de memorie van toelichting wordt er op gewezen dat een meer gerichte opslag van data onwerkbaar is en een keuze voor ‘profiling’ van individuen impliceert, met daarmee samenhangende risico’s op discriminatie en ongelijke behandeling.

Het gehuldigde principe van de algemene dataretentie wordt wel gecompenseerd door een striktere regeling van andere (procedurele) aspecten.

De nieuwe dataretentiewet biedt als voordeel dat de burger perfect op de hoogte is welke gegevens bewaard worden, hoe lang, voor welke doeleinden en door welke overheden zij kunnen opgevraagd en gebruikt worden. Ook wordt voorzien in een traceerbaarheid van de exploitatie van de bewaarde gegevens ingevoerd met behulp van een logboek, met een controlemogelijkheid door de Privacycommissie en het BIPT.

Anderzijds worden in de nieuwe wetgeving de mogelijkheden van het retro-actief telefonieverkeer (artikel 88 bis Sv) voor de opsporings- en onderzoeksinstanties beperkt ten aanzien van de vorige toestand door het inbouwen van een strafdrempel en het voorzien in drie periodes voor de bewaringstermijnen afhankelijk van het soort misdrijf.

De toekomst zal uitwijzen of het gevonden evenwicht niet in de verkeerde richting doorslaat.

Hoewel de wetgever voorziet in een evaluatie bestaat de vrees dat er de facto geen relevante gegevens voorhanden zullen zijn om een degelijke kwalitatieve evaluatie te maken en de evaluatie herleid zal worden tot het aanleveren van kwantitatieve gegevens zonder dat hieruit enige conclusie kan getrokken worden. Het lijkt immers een quasi onmogelijke opdracht om aan te tonen dat een bepaalde strafzaak wel of niet kon opgelost worden onder het regime van de nieuwe wetgeving als de maatregel zelf niet kan genomen worden.

In een tijdperk waar de burgers hun eigen privacy grotendeels opgeven en hun gegevens als het ware te grabbel gooien op het internet en vrijgeven aan alle grote private spelers (bv Facebook, Twitter, Instagram…) en waarbij de burgers vaak niet of onvoldoende bewust zijn welke gegevens door deze spelers bewaard worden, hoe deze worden aangewend en voor welke doeleinden ze kunnen aangewend worden, is het wantrouwen dat in dit debat gevoed werd tegenover de gerechtelijke overheden, die juist als taak hebben de burger te beschermen tegen inbreuken op hun fundamentele rechten en vrijheden, moeilijk te vatten.

3. Middelen en mensen

Voor een efficiënte en daadwerkelijke aanpak van "het internet als facilitator voor criminaliteit" dient de nodige capaciteit (zowel personele als operationele middelen) voorzien te worden en dienen de nodige investeringen ook daadwerkelijk te gebeuren.

De opbouw en instandhouding van de nodige gespecialiseerde kennis, het opvolgen en in kaart brengen van de nieuwste technologische evoluties die zich voordoen in de digitale informatie- en communicatietechnologieën, alsmede doorgedreven opleidingen van de politiediensten en magistraten zijn eveneens noodzakelijk.

In deze zin[31] vestigde het College van Procureurs-generaal in zijn advies van 1 februari 2016 inzake de Kadernota Integrale Veiligheid reeds de aandacht op de moeilijkheden van onze politiediensten inzake lokalisatie en onderscheppen van communicatie, mede ten gevolge de technologische evoluties inzake de informatie- en communicatietechnologie.

Het advies bevatte voorstellen inzake het aanpassen van het wettelijk kader, investeringen in middelen en de vraag om een dringende verhoging van de capaciteit van de federale politie door te voeren.

Er dient tevens een efficiënte en **gecoördineerde samenbundeling** te gebeuren van de middelen die thans, soms op ongecoördineerde wijze, over verschillende diensten heen verspreid worden (expertise bij de veiligheidsdiensten en politiediensten). De samenwerking met de academische wereld én met de private sector (inzonderheid de grote internetbedrijven) zou eveneens op een meer gestructureerde wijze dienen te verlopen.

Daarom is het onthutsend te moeten vaststellen dat, hoewel de kaders van Regionale Computer Crime Units (RCCU) en Federale Computer Crime Unit (FCCU) recent licht werden uitgebreid in de nieuwe Organieke Tabel[32], de daadwerkelijke invulling ervan problematischer blijkt te zijn, met slechts 5 van de 14 RCCU's volledig opgevuld en het FCCU slechts voor 64% ingevuld.

[31] Advies College van Procureurs-generaal inzake Kadernota Integrale Veiligheid d.d. 01.02.2016, p. 7
[32] Koninklijk besluit d.d. 27 oktober 2015 tot vaststelling van de personeelsformatie van de federale politie.

CCU	Vereiste capaciteit			Werkelijke capacteit		
	OT2 Ter	OT3	uitbreiding	Maart 2016	%OT2Ter	%OT3
FGP Antwerpen	23	24	4%	19	83%	79%
FGP Brussel	43	56	30%	34	79%	61%
PJF Charleroi	15	22	47%	11	73%	50%
PJF Eupen	2	2	0%	2	100%	100%
FGP Halle-Vilvoorde	2	5	150%	3	150%	60%
FGP Leuven	6	6	0%	5	83%	83%
PJF Liège	15	30	100%	19	127%	63%
FGP Limburg	5	9	80%	10	200%	111%
PJF Luxembourg	6	8	33%	8	133%	100%
PJF Mons/Tournai	10	12	20%	11	110%	92%
PJF Namur	7	10	43%	10	143%	100%
PJF Nivelles	3	4	33%	4	133%	100%
FGP Oost-Vlaanderen	19	22	16%	16	84%	73%
FGP West-Vlaanderen	18	17	-6%	12	67%	71%
DJSOC - FCCU	39	44	13%	28	72%	64%
Totaal	**213**	**271**	27%	**192**	90%	71%

Bovendien volstaat het niet om extra mensen aan te werven, doch deze moeten ook beschikken over de noodzakelijke uitrusting en training, hierbij terdege rekening houdend met de snelle technologische evoluties, wil men pretenderen minstens gelijke tred te houden met de cybercriminaliteit. Gelet op de huidige cijfers dreigt dit een illusie te worden.

Dit klemt des te meer gelet op de prioriteiten gesteld in de Kadernota Integrale Veiligheid en het Nationale Veiligheidsplan.

Ook zal hierbij de vraag gesteld moeten worden welke politiediensten welke taken voor zich zullen nemen.

Steeds meer lokale politiediensten zullen immers geconfronteerd worden met cybercriminaliteit, zonder dat zij hiervoor de expertise van een FCCU of zelfs RCCU in huis hebben. Het ontwikkelen van een lokale computer crime unit, LCCU, in nauwe samenwerking en met ondersteuning van de RCCU/FCCU als kennishubs is een mogelijke piste om hieraan tegemoet te komen.

4. Encryptie

Encryptie, cryptografie, ook wel de versleuteling van data, is een tweesnijdend zwaard.

Enerzijds is de versleuteling van communicatie en opgeslagen gegevens primordiaal opdat hun vertrouwelijkheid en integriteit gewaarborgd kan worden in de digitale maatschappij van heden.

Overheid, bedrijven en burgers rekenen op encryptie om hun digitale producten en diensten te beveiligen tegen mogelijke cybercriminelen. Zonder encryptie is er geen internetbankieren of bestaan geen webshops.

Bovendien is de sector van encryptie per definitie altijd in beweging, waarbij gezocht wordt naar almaar sterkere encryptie. Vandaag de dag gebeurt dit nog doorgaans op basis van wiskundige berekeningen die onnoemelijk veel berekeningen zouden vragen wil men ze zonder de sleutel kraken. Aan de horizon verschijnt echter alweer de volgende versleuteling aan de hand van de wetten van de fysica[33], gelet op de almaar sneller voortschrijdende ontwikkeling van computertechnologie. Deze ontwikkeling biedt veel kansen voor bedrijven in een kenniseconomie.

Ook de overheden willen almaar meer diensten digitaal aanbieden aan de burgers, waarbij de vertrouwelijkheid van de onderliggende gegevens noodzakelijk is.

Anderzijds bemoeilijkt encryptie de opsporing van en bewijsvergaring inzake misdrijven in zeer ernstige mate. In 75% van de cybercrime onderzoeken stoot de rechtshandhaver immers op encryptie.

Hoewel het legitiem gebruik van encryptie aangemoedigd moet worden om persoonlijke, klanten- of andere bedrijfsdata of intellectuele eigendom te beveiligen, stelt het gebruik ervan door criminelen en terroristen de ordediensten voor niet te onderschatten problemen[34].

Ook hier rijst de vraag hoe een evenwicht te vinden tussen enerzijds privacy en bescherming van persoonlijke gegevens en anderzijds de noodzaak voor de rechtshandhavers om toegang te krijgen tot die gegevens in de bestrijding van misdrijven en terrorisme.

[33] Quantum-encryptie, op basis van het gedrag van fotonen; http://www.computerworld.com/article/3092954/security/google-hopes-to-thwart-quantum-computers-from-cracking-internet-encryption.html.
[34] The Internet Organized Crime Threat Assessment (IOCTA) 2015, p. 50, https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.

Het valt echter te vrezen dat deze vraag geen eenvoudig antwoord heeft.

Het meest simplistische antwoord betreft een verbod op gebruik van encryptie *tout court* of toch minstens van de zwaarste (onbreekbare) vorm van encryptie.

Men gaat er hierbij vanuit dat de burger niets te verbergen heeft en dat enkel criminelen zaken wensen te versleutelen. Deze logica gaat echter voorbij aan de recente ontwikkelingen, zeker in een post-Snowden tijdperk, en miskent het recht op bescherming van de persoonlijke levenssfeer[35]. Overigens, deze encryptie bestaat reeds en wetgeving die het gebruik ervan aan banden legt, zou criminelen er niet van weerhouden deze te gebruiken of verder te ontwikkelen. De burger zou in deze situatie des te kwetsbaarder worden voor de criminelen die dergelijk verbod zouden omzeilen.

Dergelijk verbod zou ook internationaal moeten gehandhaafd worden, maar de garantie dat elke overheid hetzelfde zou doen is quasi onbestaand.

Anderen stellen dat eenieder die zich bedient van encryptie, verplicht zou moeten worden om de sleutel ervan in bewaring te geven bij een te vertrouwen derde partij, waar de rechtshandhavers dan voorzien van de nodige gerechtelijke mandaten de sleutel kunnen ophalen indien nodig. Ook deze oplossing biedt weinig soelaas en lijkt ook technisch niet haalbaar, gelet op het feit dat nagenoeg elke transactie een eigen sleutel heeft. Trouwens zouden de criminelen zo vriendelijk zijn om hun sleutels netjes aan te bieden?

Bovendien dreigt de te vertrouwen derde partij zelf een gedroomd doelwit te worden van dergelijke criminelen, die alle eitjes in één mand zouden vinden.

Ten slotte is het nog maar de vraag of er internationaal een organisatie gevonden kan worden die door alle overheden vertrouwd wordt om de sleutels van hun burgers, bedrijven of instellingen, te bewaren.

Dezelfde bezwaren gelden voor de door sommigen bepleite verplichting voor ontwikkelaars om te voorzien in een universele achterdeur bij het ontwerpen van diensten of producten. Deze achterdeur zou enkel toegankelijk zijn voor rechtshandhavers.

Dit werd in het verleden al gepoogd, maar werd al snel verlaten[36]. Dit zou vandaag de dag niet anders zijn[37]. Het zou het de hackers enkel gemakkelijker maken om in te breken, nu ze hun pijlen op slechts één deur zouden moeten richten.

---

[35] The Internet Organized Crime Threat Assessment (IOCTA) 2015, p. 67, https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.
[36] Clipper chip (https://en.wikipedia.org/wiki/Clipper_chip).
[37] ABELSON, H., e.a., "Keys under doormats: mandating insecurity by requiring government access to all data and communications", Journal of cybersecurity, 2015, https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

Zeer recent bleek nog dat anti-virus software in hetzelfde bedje ziek is, dat deze software aan veel strengere veiligheidsnormen moet voldoen gelet op de rol die het speelt en de machtigingen die het heeft binnen systemen[38].

Een eventuele oplossing, zij het geenszins zaligmakend, kan bestaan in een medewerkingsverplichting. Hierbij zou de verdachte verplicht kunnen worden om de encryptie-sleutels in zijn of haar bezit te onthullen en zou een weigering strafbaar gesteld worden.

Internationaal werd er vaak opgeworpen voor de rechtbanken dat zulke verplichting strijdig zou zijn met het zwijgrecht, doorgaans werd echter aanvaard dat deze gerechtvaardigd kan zijn in het kader van gerechtelijke vervolging[39].

De Belgische wetgever[40] voorziet deze mogelijkheid in artikel 88quater §1 Sv, zij het dat de rechtspraak daar soms anders over oordeelt[41].

Dergelijk decryptiebevel voor verdachten kan een inbreuk op het nemo-teneturbeginsel uitmaken, maar kan in bepaalde omstandigheden toch gerechtvaardigd zijn. Hierbij zal de rechter in totaliteit moeten kijken naar de aard en mate van uitgeoefende dwang, de aanwezigheid van relevante waarborgen in de procedure, de manier waarop het afgedwongen materiaal wordt gebruikt en het gewicht van het publiek belang[42], om te oordelen of een afgedwongen medewerking een schending oplevert van het nemo-teneturbeginsel.

De tijd lijkt gekomen om deze hypothese te beproeven voor de hoven en rechtbanken en zo de rechtsvinding de kans te geven om tot hedendaagse werkbare oplossingen te komen.

De toename van het gebruik van encryptie gaat daarenboven hand in hand met een stijging in anonimisering. Zelfs de kleinste cybercrimineel doet vandaag de dag beroep op technologieën om zijn IP-adres te verbergen, zij het via *The Onion Router* (TOR) of via andere proxy- of virtual private network (VPN) diensten.

---

[38] https://www.wired.com/2016/06/symantecs-woes-expose-antivirus-software-security-gaps/.
[39] The Internet Organized Crime Threat Assessment (IOCTA) 2015, p. 69, https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.
[40] MvT, *Parl. St.,* Kamer, 1999-2000, nr. 50K0213/001, p. 27, *In re Boucher*, 19 februari 2009, No. 2:06-mj-91, 2009 WL 424718.
[41] Gent, 23 juni 2015, *NjW*, 2016, nr. 336, p. 134; *contra*: CONINGS C., "Ontsleutelplicht van verdachte en verbod op zelfincriminatie", *NjW*, 2016, nr. 336, p. 135; KERKHOFS J., VAN LINTHOUT Ph., *Cybercrime*, Politeia, Brussel, 2013, nr. 346, p. 367.
[42] KOOPS, B.J., Het decryptiebevel en het nemo-teneturbeginsel, 2012, p. 168, http://www.wodc.nl/onderzoeksdatabase/decryptiebevel-kinderpornografie.aspx; CONINGS, C., "Statusupdate: Belgische opsporing - ☹ voelt zich #verward bij het speuren in sociale media", in: X. *Sociale media anno 2015 – Actuele juridische aspecten*, Intersentia, Antwerpen, p. 291 e.v.

Oplossingen ?

1. Sensibiliseren – "Voorkomen is beter dan genezen"

"Home computer systems are insecure because they are administered by untrained users"[43]

In elk beleid dat ontwikkeld wordt omtrent cyberveiligheid en cybercrime dient preventie en sensibilisering van de gebruikers een prominente plaats in te nemen.

Hier is een belangrijke taak weggelegd voor het Centrum voor Cybersecurity België, zowel naar de burgers toe als de bedrijven en de vitale sectoren in dit land.

De thuiscomputer is een belangrijk doelwit geworden van hackers, niet enkel om persoonlijke gegevens te kunnen bemachtiging (bv via phisingfraude), ransomware-aanvallen uit te voeren, maar ook om te infecteren en te kunnen misbruiken in een botnet zonder dat de gebruiker zich nog maar bewust is van dit misbruik. Deze botnets bieden de mogelijkheid om de zogenaamde DDos-aanvallen uit te voeren waarvan zich recent nog verschillende gevallen hebben voorgedaan (downsec legt tax-on-web plat).

Veilig omgaan met ICT begint bij onszelf en elk van ons dient bewust om te gaan met de moderne communicatietechnologie en sociale media.

Te vaak wordt er op vertrouwd dat de systemen wel door de producenten, providers en systeem-beheerders voldoende beveiligd zullen worden, maar zelf wordt er dikwijls op een onverantwoorde manier mee omgegaan.

Het belang van preventie en sensibilisering kan niet genoeg benadrukt worden en op dit vlak zijn er reeds tal van initiatieven ontwikkeld.[44] Het dient echter een permanent en wederkerend aandachtspunt te zijn in elk beleid rond cybersecurity en cybercrime.

2. Internationale samenwerking versterken

Wat de opsporings- en vervolgingsbevoegdheden betreft, heeft de Belgische wetgever met de wet van 28 november 2000 betreffende informaticacriminaliteit een hele reeks vernieuwingen doorgevoerd in het Strafwetboek en in het Wetboek van Strafvordering, in het bijzonder door het invoeren van de mogelijkheid om door middel van een zoeking in een informaticasysteem of in een deel ervan bewijsmateriaal in het buitenland te bekomen (artikel 88ter Sv dat in de nieuw aankomende wetgeving geïncorporeerd zou worden in artikel 39bis Sv).

[43] R. Wash, Michigin State University, "Folk Models of Home Computer Security".
[44] Bij wijze van voorbeeld: http://www.childfocus.be/nl/preventie/clicksafe-veilig-internetten: ontwikkeld door Child Focus; www.safeonweb.be ontwikkeld door CERT.BE.

De voorbereidende werken verduidelijken dat de wetgever op die manier de unilaterale grensoverschrijdende netwerkzoeking onder strikte voorwaarden mogelijk wou maken om het hoofd te kunnen bieden aan het grote risico op verlies van bewijs.

België lijkt hiermee een pragmatische en een realistische benadering te hanteren voor het vergaren van e-evidence.

Ook wat betreft de verplichting die rust op verstrekkers van elektronische communicatiediensten om hun medewerking te verlenen teneinde te kunnen overgaan tot identificaties heeft het Openbaar Ministerie met de vervolging en definitieve veroordeling van Yahoo! inc duidelijkheid uitgelokt.

Dit betekent niet dat alles opgelost is op het vlak van internationale samenwerking en op het vlak van de problematiek van de lokalisatie van opsporingen in een virtuele omgeving, integendeel.

Binnen de Raad van de Europese Unie groeit stilaan het besef, mede onder impuls van de Belgische regering naar aanleiding van de terroristische aanslagen in Brussel van 22 maart 2016, dat er op Europees vlak maatregelen dienen genomen te worden voor de verbetering van de strafrechtspleging in de cyberruimte.

Hierbij lijken onze academici een voortrekkersrol te kunnen spelen door oplossingen aan te reiken omtrent de problematiek van extra-territorialiteit/territorialiteit en van de soevereiniteit die minstens de moeite waard zijn om nader te bekijken.

Zo wordt voorgesteld om de zoeking niet langer te lokaliseren op de plaats waar de data kunnen worden gevonden maar wel op de plaats waar de gebruiker van die data zich bevindt.

Onderzoekshandelingen naar data *in real time* moeten dan worden gelokaliseerd op de plaats waar de onderzochte persoon zich bevindt. Dit is niet noodzakelijk de verdachte. Het is bijvoorbeeld de persoon wiens toetsaanslagen worden geregistreerd, wiens lokalisatie *in real time* wordt geregistreerd of wiens communicatie wordt onderschept.

Dit ligt perfect in lijn met de Europese benadering in de overeenkomst inzake wederzijdse rechtshulp en het Europees Onderzoeksbevel, waar het onderscheppen van communicatie ook wordt gelokaliseerd op de plaats waar de afgetapte persoon zich bevindt. Zoekingen naar data die op een afstand worden opgeslagen en die geen *real time* zoekingen uitmaken, zouden dan worden gelokaliseerd op de plaats waar de onderzochte persoon zijn gewoonlijke verblijfplaats heeft. De opsporingshandeling in bv. een webmailaccount of sociale media account van een persoon met gewoonlijke verblijfplaats in België, maakt dan een puur territoriale, Belgische opsporingsmaatregel uit.

Internationale samenwerking is alsdan niet nodig.

De focus verschuift van de locatie van de gezochte data naar de onderzochte persoon en zijn gewoonlijke verblijfplaats [45].

Verder kan het belangrijk initiatief en de beslissing tot oprichting van een Europees justitieel Cybercrime netwerk binnen Eurojust ook worden geciteerd.

Samenbrengen van expertise en uitwisselen van *best practices*, delen van kennis en ervaring en het bevorderen van de samenwerking tussen de gerechtelijke overheden van de verschillende lidstaten inzake de bestrijding van cybercriminaliteit is, net als op het nationale niveau, hierbij de boodschap.

3. Samenwerking met privé-partners

Zoals reeds eerder benadrukt, is een nauwe samenwerking met de private spelers primordiaal in de bestrijding van de cybercriminaliteit.

Met de *Internet Access Providers* (Telenet, Proximus, Orange, Scarlet, etc.) wordt dagelijks nauw samengewerkt in goede verstandhouding. Hun medewerking is cruciaal voor het gros van de strafonderzoeken. Zij kennen immers doorgaans welke IP-adressen er aan welke abonnee worden toegekend en vormen zo een brug tussen het virtuele en de realiteit.

Er lopen ver gevorderde onderhandelingen om deze samenwerking inzake telefonieonderzoek en internetvorderingen verder te stroomlijnen en om de hieruit voortvloeiende gerechtskosten te drukken.

Bovendien worden zij ook nauw betrokken bij de initiatieven van het CCB om sneller gebruikers te informeren omtrent een eventuele besmetting van hun IT-systemen. Zeer concreet staat er een project in de startblokken waarbij de IAP's aan hun klanten zullen melden wanneer hun IT-systeem tot een botnet behoort met het oog op het herstel van de veiligheid van hun systeem.

De medewerking van de *Internet Service Providers* is eveneens onontbeerlijk. Zij beschikken over de IP-adressen van internauten die gebruik maken van hun diensten, IP-adressen die noodzakelijk zijn om de fysieke personen als gebruiker te identificeren. Het dient benadrukt te worden dat de vestigingsplaats van deze dienstverleners hierbij niet langer doorslaggevend is bij het beoordelen van de samenwerking.

[45] Charlotte Conings, "De lokalisatie van opsporing in een virtuele omgeving", Nullum Crimen, 2014.

Deze trend blijkt ook uit de Europese Verordening 2016/679 van 27 april 2016 waarin een substantiële verruiming van het territoriaal toepassingsgebied voorligt, en waarbij de focus ligt op de *targeting* van datasubjecten in de Europese Unie. De verordening zal daarmee ook van toepassing zijn op de verwerkers van buiten de Europese Unie, die goederen en diensten aan datasubjecten in de EU monitoren[46].

Een zeer concreet voorbeeld van de evolutie in België betreft de *Internet Service Provider* YAHOO. YAHOO had in essentie opgeworpen dat zij als onderneming op Amerikaans grondgebied gevestigd was en dat zij dan ook niet verplicht was de gevorderde gegevens te verstrekken, omdat dit de uitoefening inhoudt van een niet toegelaten uitvoerende jurisdictie buiten het Belgisch grondgebied en het principe van de soevereine gelijkheid van Staten miskent.

Met het YAHOO-arrest van 1 december 2015 heeft het Hof van Cassatie de Belgische rechtshandhaver een sterk wapen in handen gegeven. Het Hof stelde dat een vordering overeenkomstig artikel 46bis Sv gericht kan worden aan elke operator of verstrekker van telecommunicatiediensten die in zijn economische activiteit zich actief richt op en tot Belgische consumenten, ongeacht de plaats waar deze operator of verstrekker zich gevestigd heeft.

Door gebruik te maken van een domeinnaam met extensie ".be", door het gebruik van de lokale taal, door het tonen van reclame gebaseerd op de locatie van de gebruikers van haar diensten en haar bereikbaarheid in België voor die gebruikers via onder meer een klachtenbus of een vraagbaak, heeft de verstrekker zich vrijwillig onderworpen aan de Belgische wetten en is zij territoriaal aanwezig in België. Met dit arrest heeft het Hof van Cassatie paal en perk gesteld aan de schijn van extraterritorialiteit.

Ook de samenwerking met de particulieren mag niet uit het oog verloren worden.

Internationaal zijn de zogenaamde *white hat hackers*, ethische hackers, een belangrijke partner bij het streven naar een betere cyberveiligheid. Zij zoeken zwakheden in systemen van overheden en bedrijven, maar misbruiken deze niet, in tegenstelling tot de *black hat hackers*. Zodra er een eerder onbekende zwakheid (*zero day exploit*) gevonden wordt, geven zij dit door aan het potentiële slachtoffer in alle discretie, opdat deze de kans zou hebben dit gat in hun beveiliging te dichten. Sommige bedrijven bieden hiervoor zelfs geld aan, de zogenaamde bug bounties.

Deze werkwijze zorgt voor een grote dynamiek en uiteindelijk veiligere producten en diensten, zodat eenieder daarbij gebaat is. Vandaag de dag is dergelijk ethisch hacken naar Belgisch recht strafbaar. Hacking is een misdrijf met een algemeen opzet. Er wordt thans door het CCB gewerkt aan een kader om dit ethisch hacken mogelijk te maken. Hierbij moet echter ook onderzocht worden welke personen

[46] Verordening 2016/679, *EU Publ*., L 119/5, Overweging 23; Verordening 2016/679, *EU Publ*., L 119/33, Art. 3.2; VAN DE MEULEBROUCKE, A., "De Algemene Verordening Gegevensbescherming", *R.W.*, 2015-16, p. 1562.

dergelijke ethische aanvallen zouden mogen uitvoeren en aan de aansprakelijkheid voor de schade berokkend aan de systemen tijdens dergelijke zoektochten naar lekken in de beveiliging[47].

Ook de medewerking van de bedrijven is gewenst. In het bijzonder bij de ontwikkeling van nieuwe producten en diensten dient er reeds van bij aanvang terdege rekening gehouden te worden met cyberveiligheid, zeker gelet op de toenemende connectiviteit van de maatschappij.

Elk verbonden product kan immers, zoals reeds vermeld, als zwakste schakel een vector worden voor een mogelijke cyberaanval. Bovendien beschikken de bedrijven vaak over een gedegen kennis en expertise in een snel ontwikkelende sector. Kennis die de rechtshandhaver broodnodig heeft nodig heeft, wil men niet geheel uit het wiel gereden worden door de cybercrimineel.

De bedrijven blijken echter vaak weigerachtig om aangifte te doen van cyberaanvallen, met een groot *dark number* tot gevolg, hetgeen de beeldvorming en effectieve bestrijding van cybercrime bemoeilijkt. Het Openbaar Ministerie is dan ook vragende partij voor meer overleg en knowhow-sharing en wil zich in deze als betrouwbare en discrete partner tonen.

Tot slot ligt er een belangrijke rol weggelegd voor de academische wereld om mee te werken aan een integraal cyberveiligheidsbeleid. Hun ontwikkelingen zijn noodzakelijk om gelijke tred te houden met de cybercrimineel en kunnen helpen om te komen tot nieuwe (contra)strategieën en middelen in de cyberwar die op til staat.

4. Open Source Intelligence – Social Media Intelligence

Open-source intelligence (OSINT) is informatie vergaard uit publiek toegankelijke bronnen, zoals daar zijn pers, social media, blogs, wikipedia's, overheidsrapporten en -databanken, wetenschappelijke publicaties (b.v. efemeriden), kaarten (b.v. GoogleMaps).

Wanneer deze informatie uit sociale media komt, spreekt men over *Social Media Intelligence* (SOCMINT): Facebook, LinkedIn, Flickr, Google+, YouTube, Pinterest, etc. Deze sociale media herbergen een schat aan informatie en zijn bijgevolg zeer interessant voor de rechtshandhaving.

In de Kadernota Integrale Veiligheid 2016-2019 wordt uitdrukkelijk gesteld: "*dat er moet worden ingezet op een beter online detecteren van misdrijven door politiediensten.*

[47] http://www.demorgen.be/binnenland/-organiseer-wedstrijden-om-overheidssites-te-hacken-b3abbc9b/.

Dit veronderstelt in eerste instantie dat het wettelijk kader hiervoor wordt uitgewerkt, en in tweede instantie dat de uitbouw van 'internetpatrouilles' en 'internetrecherche' wordt geoperationaliseerd.

Daartoe moet het wettelijk kader worden aangepast aan de technologische evolutie (bijvoorbeeld voor maatregelen in verband met het volgen van de activiteiten van een persoon op het internet, met inbegrip van de sociale media). Ook moet er een betere regeling komen voor de toegang op afstand, al dan niet heimelijk, tot een informaticasysteem in het kader van het strafrechtelijk onderzoek. Daarbij dienen bepaalde pijnpunten van de bestaande wetgeving te worden opgelost, zonder afbreuk te doen aan het globale evenwicht tussen het juridische kader voor de opsporing en vervolging enerzijds en de bescherming van de persoonlijke levenssfeer en het rechten op de verdediging anderzijds.[48]"

Veel van deze informatie is te vinden op het publieke internet, toegankelijk voor eenieder. Echter, grote delen van het internet zijn semipubliek, afgesloten maar wel toegankelijk na zuiver vormelijke registratie b.v. een CAPTCHA, een identificatie of een betaling (b.v. Facebook profielen zijn enkel zichtbaar voor personen die geregistreerd zijn op Facebook).

Tenslotte zijn er nog delen die privaat zijn (b.v. vriendenpagina, groepsblog, etc.), of zelfs exclusief (b.v. privégedeelte van Facebook) enkel toegankelijk voor een select clubje van personen die beschikken over een persoonlijke login of zelfs enkel voor een enkeling.

Het verschil in toegankelijkheid speelt een grote rol in hoever de politiediensten bij het vergaren van informatie mogen gaan. Ook de manier waarop deze gegevens bemachtigd worden is belangrijk.

Gebeurt dit openlijk of heimelijk, met fictieve identiteit of zelfs geheel onzichtbaar middels spyware (b.v. keyloggers)? De grenzen zijn niet duidelijk.

Bovendien moet, ongeacht de toegankelijkheid, ook gedacht worden aan de redelijke verwachting van privacy van de gebruiker, bij het beoordelen van de voorzienbaarheid en rechtmatigheid van deze toegang. Begrippen als proportionaliteit en subsidiariteit lijken hierbij de sleutelwoorden te zijn. In deze zin zal de Europese verordening 2016/679 een veel hogere eis stellen aan de toestemming van gebruikers van informaticadiensten wanneer hun data gebruikt worden voor andere doeleinden[49]. De vraag is dan hoever die toestemming reikt en of deze ook geldt voor rechtshandhaving.

De tijd lijkt gekomen om de nieuwe grenzen af te tasten, binnen het wettelijke kader, teneinde te ontdekken waar dit kader al dan niet aangepast moet worden.

[48] Kadernota Integrale Veiligheid 2016-2019, p. 11.
[49] Verordening 2016/679, *EU Publ*., L 119/5, overweging 32.

Hierbij mag niet uit het oog verloren worden dat de rechtshandhavers zich ook de nieuwe technologieën meester dienen te maken. Zo benadrukt de Kadernota Integrale Veiligheid 2016-2019 terecht dat "*voor de operationele effectieve uitbouw van internetpatrouilles en internetrecherche, de nodige aandacht moet worden besteed aan de opleiding van deze "online"-agenten. Zij moeten immers in staat zijn om niet alleen een zeer brede waaier van misdrijven op te sporen, maar ook over de nodige competenties beschikken om op een correcte en volledige manier de noodzakelijke vaststellingen te doen zodat deze kunnen gebruikt worden bij de voortzetting van onderzoeken".*[50]

Het huidige wettelijke kader lijkt geen gelijke tred te hebben gehouden met de technologische realiteit en dit zorgt voor onduidelijkheid.

Een zeer concreet voorbeeld hiervan is artikel 26 van de Wet op het Politieambt (WPA). Sommige auteurs menen dat huidig artikel 26 de politiediensten toelaat om niet alleen de publieke bronnen te raadplegen, maar ook de semipublieke ruimte die moeten worden beschouwd als voor het publiek toegankelijke plaatsen[51]. Anderen schijnen de mening toegedaan dat burgers er redelijkerwijze van mogen uitgaan dat hun privacy op dergelijke semipublieke plaatsen beschermd is tegen overheidsingrijpen en dat wanneer de politie zou inloggen met een "burgerprofiel" dit misleidend is en derhalve een inbreuk op hun recht op privacy[52].

De privacycommissie deed de aanbeveling het artikel 26 WPA aan te passen aan de huidige stand van zaken en expliciet te stellen dat de politiediensten ook het publieke en semipublieke internet mogen patrouilleren, onverminderd de bestaande bepalingen van het wetboek van strafvordering inzake de bijzondere opsporingsmethodes en de afluistermaatregelen.

Inderdaad, het kan niet de bedoeling zijn om afbreuk te doen aan de bestaande waarborgen inzake bijzondere opsporingsmethodes. Hierbij valt onder meer te denken aan het systematisch observeren van iemands Facebook-pagina, dan wel onder een geloofwaardige fictieve identiteit in interactie te treden met een verdachte. Dit zijn onderzoeksdaden die perfect onder de bestaande BOM-regelgeving kunnen verricht worden.

Het is dan ook tijd om wetgevend werk te maken van de aanpassing van artikel 26 WPA, teneinde de burger hieromtrent klare wijn te kunnen schenken.

[50] Kadernota Integrale Veiligheid 2016-2019, p. 11.
[51] KERKHOFS, J., VAN LINTHOUT, Ph., *Cybercrime*, Politeia, 2013, p. 211 e.v.
[52] Advies nr. 13/2015, 13 mei 2015, Commissie voor de bescherming van de persoonlijke levenssfeer, p. 6, nr. 20.

Een ander – mogelijks onderbelicht – aspect van sociale media, is de mogelijke meerwaarde die ze kunnen bieden aan rechtshandhaving om de burger te informeren, responsabiliseren en zelfs te betrekken bij het vergaren van bewijsmateriaal. Zo zouden succesverhalen kunnen gedeeld worden, burgers gerustgesteld wanneer er paniek dreigt te ontstaan en mogelijke getuigen opgespoord.

Het spreekt voor zich, gelet op het niet te onderschatten bereik van deze nieuwe technologieën, dat dit echter op uiterst zorgvuldige en doordachte wijze moet gebeuren. Zo gaan verhalen op sociale media soms een eigen leven leiden, wordt zeer snel reactie verwacht en kan dit de gebeurlijke mediastrategieën doorkruisen. Willen we dit oordeelkundig doen, is er dringend nood aan een heus *Social Media* beleid voor de rechtshandhavers met tijd en middelen voor *capacity building*, opleidingen en *best practices*.

5. Aankomende wetgeving

Onze wetgeving inzake databeslag, netwerkzoeking en telefoontap dient dringend aangepast te worden aan de eigen realiteit van het internet. Het College van Procureurs-generaal is reeds lange tijd vragende partij om een actualisering door te voeren van de middelen die de gerechtelijke autoriteiten ter beschikking moeten worden gesteld om bewijzen te kunnen verzamelen in informaticasystemen. Zoals reeds aangehaald bij de beeldvorming wordt meer en meer vastgesteld dat criminelen gebruik maken van de mogelijkheden die de informatie- en communicatietechnologie hen biedt. Politiediensten en magistratuur dienen over dezelfde middelen te beschikken.

In april 2015 richtte de Minister van Justitie een werkgroep op samengesteld uit vertegenwoordigers van het College van Procureurs-generaal, het federaal parket, de onderzoeksrechters, de federale politie, de inlichtingendiensten, douane en accijnzen, het directoraat-generaal wetgeving, en de beleidscel.

Uiteindelijk werd het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties voor advies voorgelegd aan onder meer het College van Procureurs-generaal[53].

Dit wetsontwerp gaat in op de noodzaak om wetgevend het hoofd te bieden aan enkele zeer prangende problemen om in een digitale omgeving onderzoeksmatig te kunnen functioneren.

[53] Doc 54/1966/001.

In de loop van het najaar zal het College van procureurs-generaal zich buigen over eventuele voorstellen die er toe strekken de toepassing van de maatregelen die het voorwerp zijn van het voorontwerp te versoepelen of te optimaliseren in termen van hun bruikbaarheid en inzetbaarheid in de praktijk.

Besluit

Het toenemend belang van cybercrime kan niet overschat worden. De rechtshandhaving dient mee op de kar van de technologie te springen, vlucht vooruit, willen ze niet verweesd achterblijven.

De handen moeten in elkaar geslaan worden over de grenzen heen, met alle partners in de keten, privé en publiek.

De rechtstaat moet mee, moet durven kiezen om de gelijke tred te houden met de technologische ontwikkelingen. Hierbij dient er echter steeds over gewaakt te worden dat binnen het wettelijk kader gebleven wordt, maar niet bang om de grenzen hiervan af te tasten of zelfs, waar nodig, door rechtsvinding te verleggen.

The proof of the pudding is in the eating.

*

* *