PUBLIC BRIEFING / MAART 2017

Bestrijding cyber crime vraagt om breed meersporenbeleid, inclusief digitale kwaliteit

Klassieke digitale misdaad is letterlijk aan de orde van seconde. *Phishing*, virus en Trojaans paard, virtuele kinderpornografie, *ransomware*, DDoS-aanval, piraterij van intellectuele eigendom en wat dies meer zij. Verder zijn elektronische spionage en cyberterrorisme tegenwoordig in zwang. Het openbaar ministerie verwacht dat in 2021 de helft van de misdaad computer-gerelateerd is. Wij constateren nog een trendbreuk. Met digitale oorlogsvoering, zowel verdedigend als aanvallend, betreedt computercriminaliteit het militaire domein. 'De vijand komt uit het stopcontact', luidt de pakkende oneliner. Één inmiddels notoir juridisch probleem betreft de waarschijnlijk blijvende spanning tussen privacy en maatschappelijk veiligheid. Daarnaast doemt een nieuw probleem van geheel andere aard op. De bewust scherp gescheiden maatschappelijke domeinen van de burgerlijke en de militaire overheid vervagen, en mogelijk daarmee ook deze rechtssystematieke waterscheiding.

Mr. V.A. de Pous[1]

Een praktijkgeval

Uit de digitale inbraak bij het U.S. Office of Personnel Management (OPM) in Washington DC, die in juni 2015 bekend werd gemaakt, kunnen we belangrijke lessen trekken (https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach). De hack is massaal en ronduit ingrijpend: persoonsgegevens van 21,5 miljoen Amerikanen zijn gelekt in de vorm van antecedenten, sociale-zekerheidsnummers en zelfs vingerafdrukken. Een buitenlandse inlichtingen- of veiligheidsdienst wordt verdacht. Deze partij heeft zich gedurende tenminste anderhalf jaar op onrechtmatige wijze toegang verschaft en persoonsgegevens heeft gekopieerd. Volgens Director of National Security James Clapper is China de *leading suspect*. De betrokkenen — degenen wiens persoonsgegevens worden verwerkt — zijn divers van aard. Het gaat om werknemers, ex-personeel, gepensioneerden en freelancers van de federale overheid. Ook familieleden van hen zijn getroffen. Voor de goede orde: het OPM voert 90% van het antecedentenonderzoek voor ongeveer 100 federale overheidsorganisaties uit. Van FBI tot het ministerie van Landbouw. De inbraak wordt nadrukkelijk beoordeeld als 'passive intelligence collection', hetgeen van oudsher tot de reguliere spionagepraktijk van inlichtingendiensten behoort.

[1] Victor de Pous is bestuurslid van de Stichting Cloud Community Europe Nederland en zelfstandig bedrijfsjurist voor digitale technologie sinds 1983.

De gekozen terminologie is van groot belang voor de toepasselijkheid van het oorlogsrecht. Van een 'cyber attack' of 'act of war' zou in deze casus geen sprake zijn.

Gevolgen

Ten behoeve van de betrokkenen bood de federale overheid anti-fraudebescherming aan. Hun financiële status werd door een externe partij voortdurende gecontroleerd, waarvoor de regering de rekening betaalde. Vooralsnog gaat het om een bedrag van 330 miljoen dollar. Iedere betrokkene ontving een gratis abonnement op CSID Protector Plus voor de periode van 18 maanden. Het pakket van maatregelen bevatte onder meer het recht op een identiteitsdiefstalverzekering met een verzekerde som van USD 1.000.000 en toegang tot een identiteitheersteldienst door CSID tot 12 juli 2016.

Deze aanpak kreeg echter in zoverre kritiek, omdat het Witte Huis de gevolgen voor de nationale veiligheid kennelijk niet woog. De gelekte persoonsgegevens kunnen immers op allerlei manieren door een vreemde mogendheid worden gebruikt, zoals voor spionage-doeleinden. Sommigen voeren aan dat de impact van de OPM-hack 40 jaar lang merkbaar zal zijn.[2] Voor de directeur van de National Security Agency NSA en hoofd van het U.S. Cyber Command Mike Rodgers staat het overigens buiten kijf dat er meer omvangrijke inbraken in federale overheidsorganisaties à la OPM zullen plaatsvinden.[3]

Burgerlijk en militair

Tijdens de Warschau-top op 8 en 9 juli 2016 nam de NAVO het besluit een digitale aanval op één lidstaat te beschouwen *als oorlogsdaad* en vervolgens als een klassiek militair conflict een aanval op *alle* lidstaten van de Atlantische bondgenootschap te bestempelen.[4] Het belangrijkste criterium is, wat het Nederlandse kabinet betreft, 'langdurige ontwrichting' van een samenleving.[5] Daarover zal het laatste woord nog niet gezegd zijn.

Maatschappelijke ontwrichting in relatie tot het gebruik van ICT toont zich ook anderszins, namelijk juridisch. De wetgever bracht in de loop der jaren diverse rechtssystematische scheidingen aan. Denk aan de tweedeling tussen consument en degene die handelt uit hoofde van een beroep of bedrijf, die civiel-, fiscaal-, bestuurs- en strafrechtelijk doorwerkt. Daarnaast normeert het mededingingsrecht eerlijke concurrentie in iedere sector; gereguleerd of niet. Met beiden worstelt bijvoorbeeld de deeleconomie fundamenteel.

Een en ander mag dan problemen veroorzaken; de genoemde juridische scheidslijnen zijn telkens aangebracht *binnen de burgerlijke overheid*. Wat we nu waarnemen heeft betrekking op de vermenging van burgerlijke met de *militaire overheid*. Met name ontwikkelingen in Washington DC geven blijk dat, in de relatie tot ICT, de scheiding tussen de civiele en militaire overheid vervaagt. Zo zet de Amerikaanse federale overheid gekwalificeerde burgers — IT professionals — in ten behoeve van de opbouw van het omvangrijke U.S. Cyber Command. Het gaat om een digitale strijdkracht van in totaal 6200 man sterk, die nu

[2] http://fedscoop.com/opm-losses-a-40-year-problem-for-intelligence-communit .

[3] http://www.wsj.com/articles/nsa-chief-expects-more-cyberattacks-like-opm-hack-1436985600

[4] http://www.nato.int/cps/en/natohq/official_texts_133177.htm

[5] http://nos.nl/artikel/2116481-de-vijand-komt-uit-het-stopcontact.html?npo_cc=na&npo_rnd=891707612&npo_cc_skip_wall=1

op stoom komt.[6] Verder voert het Department of Defense sinds kort het antecedenten-onderzoek ten behoeve van de gehele federale overheid (civiel en militair) uit en dus heeft overgenomen het gekraakte U.S. Office of Personnel Management.

Onomkeerbare ontwikkelingen

Terug in de tijd. Tijdens de werkzaamheden van de Commissie Computercriminaliteit in 1986 werd er gediscussieerd over de strafbaarstelling van computervredebreuk (*hacking)*. Nemen we wel of niet het doorbreken van beveiliging in de delictsomschrijving op? (Toen wel, later is dat vereiste teruggedraaid.) Dertig jaar later staan strafrecht en strafvordering met het wetsvoorstel Computercriminaliteit III voor de derde grote uitbouw.[7] Dat is hard nodig. Computercriminaliteit veranderde van een schaarse exotische misdaadcategorie, beoefend door uiterst gekwalificeerde professionals, in een alledaagse vorm van digitale criminaliteit, waarvoor de middelen op Internet worden gekocht of zelfs op afroep als dienst afgenomen. Grootschaligheid *en* laagdrempeligheid troef. Een kind kan de was doen. Sterker nog, met computercriminaliteit gaat het dusdanig goed dat het openbaar ministerie binnen afzienbare tijd een trendbreuk verwacht. 'Over vijf jaar heeft vijftig procent van onze criminaliteit te maken met computers', aldus procureur-generaal Gerrit van der Burg.[8]

Computercriminaliteit III

Met het wetsontwerp bestrijding cybercrime (Computercriminaliteit III), dat op 22 december 2015 bij de Tweede Kamer is ingediend, wil de regering opsporing en vervolging van computercriminaliteit versterken wegens technologische ontwikkelingen op Internet en het gebruik van computers voor communicatie en de verwerking en opslag van gegevens.[9] Ook moeten burgers beter worden beschermd tegen bijvoorbeeld 'grooming' — kort gezegd: kinderlokken via Internet — of de verspreiding van kinderpornografie en tegen ernstige criminaliteit waarbij computers worden gebruikt.

Tevens worden de formele bevoegdheden verbreed. Zo mogen politie en justitie straks heimelijk en op afstand (online) onderzoek doen in computers. Dat kan een personal computer zijn, een mobiele telefoon of een server. Dit wordt in de volksmond soms 'terug-hacken' genoemd. In het wetsvoorstel wordt het ontoegankelijk maken of kopiëren van gegevens toegestaan bij een zeer ernstig misdrijf, waarop in beginsel een gevangenisstraf staat van acht jaar of meer. Denk aan mensenhandel of deelname aan een terroristische organisatie. In beginsel, want in een *beperkt aantal gevallen* kan dat ook bij misdrijven met een vrijheidsstraf lager dan acht jaar, wanneer er sprake is van een duidelijk maatschappelijk belang om een einde te maken aan de strafbare situatie, zoals *grooming*, kinderpornografie of een DDoS-aanval.

---

[6] Zes jaar geleden startte het Amerikaanse ministerie van Defensie het US Cyber Command. Deze speciale eenheid voert desgewenst digitale aanvallen op tegenstander uit en zorgt voor de beveiliging van militaire netwerken.

[7] https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/23/wetsvoorstel-computercriminaliteit-iii

[8] Nieuwsuur, 15 juni 2016. http://nos.nl/nieuwsuur/artikel/2111280-over-vijf-jaar-helft-misdaad-door-cybercriminelen.html?npo_cc=na&npo_rnd=232703334&npo_cc_skip_wall=1

[9] Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III). https://www.eerstekamer.nl/wetsvoorstel/34372_computercriminaliteit_III

Dat terughacken blijft, ondanks de interventie van de Raad van State ter zake strengere privacyvoorwaarden, een *omstreden bevoegdheid*, in het bijzonder wanneer de informatie-systemen zich in het buitenland bevinden. Op 20 december 2016 nam de Tweede Kamer Computercriminaliteit III aan.

Conclusies

Digitale technologie verandert de wereld telkens onomkeerbaar en blijft dat waarschijnlijk doen; zowel positief als negatief bezien. Dat laat het recht niet beroerd. De *strafrechtelijke* strijd tegen allerlei vormen van misbruik in relatie tot ICT toont tegelijkertijd de beperking van het recht aan. De praktijk laat zien dat materiële en formele strafrechtregels computer-criminaliteit geen halt toeroepen.

Een meersporenbeleid is vereist, inclusief voldoende budget, mankracht en expertise van politie, justitie en veiligheidsdiensten, inclusief het leger. Andere maatregelen vinden we in de kwaliteitsverbetering van digitale producten en diensten en de juridische borging daarvan in wet- en regelgeving, terwijl ICT-gebruikers niet aan een gedragsverandering kunnen ontkomen om bewuster en zorgvuldiger te handelen. Geconsolideerd beschouwd, gaat om de versterking van onze digitale weerbaarheid en veiligheid.

Tenslotte creëert de vervaging tussen de burgerlijke en militaire overheid een nieuwe juridische spanning; naast het bekende spanningsveld tussen de bescherming van de persoonlijke levenssfeer enerzijds en de maatschappelijke veiligheid anderzijds. Over beiden moet Nederland als rechtstaat niet lichtvaardig denken.

Analyses

- Bij voorkoming, opsporing en vervolging van ernstige criminaliteit, zoals terrorisme en georganiseerde misdaad, worstelen overheidsinstanties met anonimiteit op Internet en encryptie. We zien in toenemende mate autonome wetgevers — per land (verschillend) — verregaande bevoegdheden voor politie en justitie en veiligheidsdiensten inzetten. De Nederlandse regering wil in ieder geval het gebruik van encryptietechnieken *niet* verbieden en de digitale sector *geen* verplichting op te leggen achterdeuren in beveiligde producten of diensten in te bouwen. Daarentegen pleiten Duitsland en Frankrijk wel voor encryptiewetgeving om berichten van bijvoorbeeld Whatsapp en Telegram te kunnen ontsluiten. Dat pleidooi is ondertussen bij het openbaar ministerie en de AIVD in goede aarde gevallen. Zelfs binnen Nederland sluiten de rijen zich dus niet.
- Er is weliswaar veel veranderd sinds de politie medio jaren tachtig via zegge en schrijve drie pilot-teams computercriminaliteit de strijd met deze nieuwe misdaadvormen aanging, maar evenals de privacytoezichthouder eerder hijst de politie nu de financiële stormbal. Door een budgettekort — in dit geval is er zelfs sprake van bezuinigingen — komt de digitale opsporing in gevaar. De wetgever behoort echter vanzelfsprekend rekening te houden met de kosten voor de adequate uitvoering van nieuwe regels;

zeker wanneer deze een groot maatschappelijk doel beogen zoals de versterking van onze digitale veiligheid.

- Het besluit van de NAVO om een digitale aanval op één lidstaat te beschouwen als oorlogsdaad en als aanval op alle lidstaten, vraagt allereerst om een zorgvuldige classificatie. Welke digitale handelingen van een vreemde mogendheid zijn onder welke omstandigheden aan te merken als oorlogsdaad? Geen sinecure. Volgens de Nederlandse regering vormt 'langdurige ontwrichting' van de samenleving het belangrijkste criterium. Dat moet nauwgezet worden uitgewerkt. Neem de aanval met de geavanceerde *stuxnet worm* van 2010 in ogenschouw. Hoogwaardige elektronische technologie wordt door een of meerdere landen (naar verluidt de VS en Israel) ingezet op het verstoren van kritische infrastructuur (een kerncentrale) in een andere soevereine staat (Iran). Beschouwt Den Haag dit als een oorlogsdaad?