‘Je weet maar nooit’
Na privacy en de onschuld, is nu ook de veiligheid dood

De Nederlandse overheid propageert geheimzinnigheid rond digitale wapens en 'zero-days', een zorgelijke ontwikkeling die als een boemerang de Nederlandse economie en veiligheidsdiensten zal treffen. Want als de laatste decennia iets hebben duidelijk gemaakt, is dat overheden de digitale revolutie niet in de hand hebben.

Elke zomer is het raak. De politie breekt in bij burgers en laat 'witte voetjes' achter indien blijkt dat de woningen niet goed zijn afgesloten. De actie vond in 2015 plaats in Wassenaar, dit jaar, 2016, in Leiden en Noordwijk. De politie zegt dat het goed bedoeld is, want mensen moeten opletten. Sluit deuren en ramen voor het gevaar, de inbrekers. Of deze acties zin hebben, effectief zijn, mensen eerder de stuipen op het lijf jagen dan een gevoel van veiligheid geven, het is onduidelijk. De politie wil dienstverlenend zijn en breekt daarom in om aan te tonen dat mensen hun veiligheid niet op orde hebben.

De 'witte voetjes' acties hebben veel weg van de voorlichting eind vorige eeuw over beter hang- en sluitwerk, ze gaan alleen een stap verder. Gebrekkige regelgeving zorgde er destijds voor dat inbrekers hang- en sluitwerk tegenkwamen dat al open gingen als je er maar naar keek. De overheid had verzuimd strengere regelgeving in te voeren waarmee uitsluitend deugdelijk sluitwerk op de markt toe wordt gelaten. De politie werd voorlichter van beter hang- en sluitwerk. Inbrekers oppakken was onbegonnen werk, bewoners moesten voortaan voor hun eigen veiligheid gaan zorgen.

Handhaving digitale kwetsbaarheid

De situatie van destijds in relatie tot fysieke beveiliging herhaalt zich nu in de digitale wereld. De overheid verzuimt duidelijke regelgeving in te voeren en te handhaven aan de hand waarvan de veiligheid van burgers serieus wordt genomen. Daarentegen propageert zij maatregelen en werkt nauw samen met bedrijven die de veiligheid van het internet ondermijnen. Het is niet zozeer dat de politie achter de feiten aanloopt bij cybercriminaliteit. Politie, OM en het Ministerie van Veiligheid en

Justitie propageren geen serieuze veiligheid van het internetgebruik, zij houden de digitale kwetsbaarheid in stand.

Argument hiervoor is dat boeven en terroristen moeten worden gevangen. Die zouden via beveiligde netwerken communiceren over hun snode plannen. Of het afluisteren van die informatie uiteindelijk een belangrijke bijdrage levert aan de veiligheid in Nederland is allang geen vraag meer. De overheid wil zo zicht houden op de kwaadwillenden. Dat het beleid daarmee onveiligheid stimuleert lijkt geen punt. Lapwerk als het 'witte voetjes' programma moet de burger gerust stellen.

De analogie met het slechte hang- en sluitwerk uit de vorige eeuw gaat nog verder. De overheid wil namelijk te allen tijde zicht houden op de boefjes. Wie dat zijn is allang geen vraag meer. Om schurken en terroristen te vangen moet er namelijk soms ingebroken worden via het internet. Zodra woningen en bedrijfspanden onneembare vestingen zijn geworden, kost het opsporings- en inlichtingendiensten ook meer tijd om de percelen binnen te komen om verborgen camera’s op te hangen, afluisterapparatuur en andere technische middelen te installeren. Dat slechte sloten iedereen treft, is niet van belang. Politie- en inlichtingendiensten willen zicht houden op de inwoners van dit land.

Fysiek inbreken in woningen is echter een stuk arbeidsintensiever dan digitaal inbreken op smartphones. Voor criminelen en politie zou het onbegonnen werk zijn om miljoenen deuren open te breken en de ruimten te scannen op waardevolle goederen of interessante informatie om mensen af te persen. Digitaal is dat allemaal minder arbeidsintensief. Vanachter het bureau in Driebergen of Katwijk kan zo in korte tijd een schat aan informatie worden verzameld uit slecht beveiligde communicatie of opslag van digitale hulpmiddelen.

Dood van de veiligheid

De dood van de veiligheid is de derde stap in de ontmanteling van de rechtsstaat en volgt daarmee privacy en onschuld. In maart 2008 publiceerde Buro Jansen & Janssen (J&J) het artikel ‘Niet de privacy maar (...) de onschuld is dood’. In de eerste alinea werd verwezen naar de ranking van Nederland op de privacyladder van Privacy International:

'In het jaarrapport van de NGO Privacy International wordt Nederland afgeschilderd als een staat waar het met de privacy slecht is gesteld.

Nederland staat onderaan hun ranglijst van privacy schendende staten. De plaats op de lijst is een gevolg van de stortvloed van genomen maatregelen die het niet zo nauw nemen met de bescherming van persoonlijke levenssfeer van Nederlandse burgers. Politici en opsporings- en inlichtingendienstambtenaren zeggen dat het inleveren van onze privacy de prijs is die wij voor een veilige samenleving moeten betalen. Maar is dat wel zo?'

Eind jaren '80, begin jaren '90 veranderde het denken over criminaliteit. Eenduidige oorzaken van die verandering zijn niet direct aan te wijzen. Vaak wordt verwezen naar de val van de Muur, de opkomst van criminele organisaties uit het Oosten en migratie. De drugssmokkel was toentertijd echter niet in handen van Oost-Europese criminele organisaties en in de jaren '70 en '80 vond er ook georganiseerde criminaliteit plaats. Wel nam de migratie toe door meer en goedkopere vliegroutes en, mede als gevolg daarvan, ruimere mogelijkheden om conflicten te ontvluchten.

De Sovjet-Unie viel uiteen en de tweedeling in goed en kwaad uit de tijd van de Koude Oorlog was ten einde. Het veiligheidsapparaat leek in een soort vacuüm beland zonder een duidelijk ‘vijandbeeld’. De aanpak van de georganiseerde criminaliteit ontspoorde in de eerste helft van de jaren '90, maar die criminaliteit staat niet voor een bepaalde groep in de samenleving. De georganiseerde criminaliteit is complexer en laat juist de verwevenheid tussen de boven- en onderwereld zien, maar ook tussen criminelen en rechtshandhavers. Opsporings- en inlichtingendiensten gingen zich in die jaren explicieter richten op bepaalde bevolkingsgroepen.

In een periode van enkele jaren werd een nieuw vijandsbeeld gecreëerd en nieuwe potentiële bedreigingen voor de rechtsstaat aangewezen. Allereerst waren daar de vluchtelingen die in de jaren '80 naar Europa waren gekomen en organisaties die die vluchtelingen ondersteunden. Ook illegalen maakten deel uit van de vermeende dreiging van migranten. Daarnaast waren er de dak- en thuislozen en drugsgebruikers en tot slot krakers en actievoerders.

Opschorting van het onschuld-adagium

In de jaren '90 liet J&J zien dat voor die groepen in de samenleving de privacy al dood was. Zeker voor vluchtelingen en illegale migranten die probeerden te overleven was privacy volledig uit het zicht verdwenen.

Een reeks wetten maakte tevens een eind aan de solidariteit onder de bevolking: invoering van de Wet op de Identificatieplicht op het werk, Koppelingswet, toepassing van het Sociaal-Fiscaal nummer (SoFi, thans Burger Service Nummer geheten) als controlemiddel, nieuwe controlediensten als het Mobiel Toezicht Vreemdelingen (MTV). In de brochure *Administratieve Apartheid* van het Autonoom Centrum werd die tweedeling in de samenleving onderbouwd.

Naast de privacy werd in de jaren '90 ook langzaamaan het onschuld-adagium voor bepaalde bevolkingsgroepen in de rechtsstaat opgeschort. Tijdens de Eurotop in Amsterdam in juni 1997 gingen 50.000 mensen de straat op om te protesteren tegen de Europese Unie. Ook werden tijdens die Europese top honderden demonstranten preventief opgepakt en enkele dagen vastgezet. Zowel rechters als de Ombudsman veroordeelden deze preventieve hechtenis, maar politiek, politie en justitie oordeelden dat zij in de toekomst op dezelfde wijze zouden handelen.

Protest tegen de Europese Unie, zeker op straat, is steeds spaarzamer geworden. De overheid zet vaker grove middelen in als noodverordeningen en noodbevelen, een soort noodtoestand die politie en justitie verregaande bevoegdheden geeft. Het is steeds ‘normaler’ geworden dat mensen die protesteren preventief worden gearresteerd.

Niet alleen demonstranten worden geconfronteerd met het einde van het onschuld-adagium in de loop van de jaren '90, ook vluchtelingen en illegalen. Zij moeten aantonen dat zij ‘echte’ vluchtelingen zijn en kunnen preventief, maanden soms jaren, worden opgesloten, alleen omdat zij zonder geldige papieren in Nederland verblijven.

Andere groepen die in de loop der jaren hun privacy en hun recht op onschuld verloren zijn de dak- en thuislozen en drugsgebruikers. In de schaduw van de bestrijding van de georganiseerde criminaliteit en de doorgeschoten opsporingsmethoden (commissie Van Traa) werd gewerkt aan een kaartenbak van daklozen en drugsgebruikers. Die ontwikkeling is in de 21ste eeuw mede dankzij voortschrijdende digitale technieken verder uitgekristalliseerd.

De intensieve samenwerking tussen hulpverleningsorganisaties, opsporingsdiensten en gemeenten met de toenemende automatisering zorgde voor een digitaal overzicht van daklozen en drugsgebruikers. Controle in binnensteden verscherpte eind jaren '90 en het begin van

deze eeuw. Onder de noemer openbare orde werden ‘bekende’ gebruikers en daklozen gecontroleerd. Blijkt iemand ‘gebruikers benodigdheden’ op zak te hebben dan kan een gebiedsverbod worden opgelegd.

In de loop der jaren is de termijn en omvang van die verboden in diverse gemeenten toegenomen. Gebiedsverboden lijken veel op de stadionverboden die bij de bestrijding van supportersgeweld wordt gebruikt. Voetbalsupporters zijn ook een groep die in de afgelopen drie decennia hun privacy en onschuld hebben moeten inleveren.

Je was erbij dus je bent erbij

Gebiedsverboden, stadionverboden en noodverordeningen worden gebruikt als openbare orde maatregelen om demonstraties, manifestaties, uitingen van vrijheid van meningsuiting en andere grondwettelijke rechten op te schorten. Uitgangspunt bij deze maatregelen is niet meer het onschuld-adagium, maar het principe dat iedereen schuldig is tenzij hij of zij het tegendeel kan bewijzen.

De strafmaatregel wordt niet opgelegd voor de eigenlijke overtreding, maar een mogelijke overtreding die eventueel zal worden begaan. In het strafrecht doet daarnaast ook de groepsveroordeling zijn intrede. Het principe 'je was erbij dus je bent erbij', zonder dat de individuele bijdrage aan een strafbaar feit door de overheid hoeft te worden aangetoond.

Daar waar in het eerste decennium na de val van de Muur ‘randgroepen’ gericht werden aangepakt, verschoof de aandacht na de eeuwwisseling naar een groter segment van de bevolking. De invoering van de uitgebreide Identificatieplicht (WUID) (eigenlijk gewoon een plicht voor iedereen om zich te legitimeren), preventief fouilleren, grote gecombineerde verkeerscontroles en andere maatregelen richten zich op de gehele bevolking vanwege het principe 'je was erbij dus je bent erbij'.

Van de identificatieplicht kan nog worden gezegd dat het alleen mensen treft die in overtreding zijn of een strafbaar feit begaan, maar in werkelijkheid is daarvan geen sprake. Wie onwetend met een kapot achterlicht rondfietst, kan worden aangehouden en beboet. Indien er geen legitimatiebewijs kan worden getoond, volgt in sommige gevallen de politiecel. De overheid treedt steeds meer op vanuit een onredelijk

repressieve opstelling, de burger is strafbaar.

Bij een grote verkeerscontrole wordt de automobilist gedwongen om een gevaarlijke parkeerplaats op te rijden waar allerlei opsporingsdiensten op hem wachten. Vervolgens worden hem alle gegevens ontfutseld en wordt hij door een wasstraat geleid op zoek naar strafbare feiten en overtredingen. Elke vondst van een vergrijp wordt breeduit gemeten in de media. Meestal gaan die verkeerscontroles gepaard met preventief fouilleren.

De burger moet ook betast worden door de overheid, want iedereen die zich op die parkeerplaats, of het centrum van een stad of achterstandsbuurt begeeft, is potentieel een wapendrager. Los van het stigmatiserende karakter van preventief fouilleren - alleen bepaalde wijken worden aangewezen op basis van discutabele cijfers en analyses – betekent de maatregel ook dat wie weigert nog verder van huis is. De publieke ruimte is niet van de argeloze burger, nee, de overheid is daarin heer en meester.

WUID levert dubbele boetes op

Onderzoek van Buro Jansen & Janssen naar de werking van de Wet op de Uitgebreide Identificatieplicht (WUID) toont aan dat veel mensen dubbel beboet worden. Dit zijn vaak dezelfde dak- en thuislozen en drugsgebruikers die al bekend zijn bij de overheid, maar die toch hard moeten worden aangepakt. Dubbele boetes voor het door rood licht oversteken op een zebrapad of ergens staan waar een politieagent van vindt dat dat niet mag.

De WUID is ook een extra controlemiddel om te jagen op vluchtelingen, illegalen, bewoners van Nederland die geen standaard witte huid hebben. Een groot deel van de boetes voor overtreding van de identificatieplicht wordt al jaren opgelegd zonder daadwerkelijke overtreding of vergrijp. Etnisch profileren is in die zin geen nieuwe maatregel, maar vloeit voort uit bovenstaande maatregelen waarbij de overheid bepaalt wat er gebeurt in de openbare ruimte.

Hebben al die maatregelen een veiliger samenleving opgeleverd? Volgens de politiestatistieken daalt de criminaliteit al jaren, maar in hoeverre die cijfers waarheidsgetrouw zijn blijft onduidelijk. De aangiftebereidheid onder bewoners van Nederland is laag, rond de 27

procent. Dit verschilt wel enigszins per regio en per delict, maar het lage percentage geeft wel aan hoeveel vertrouwen er is in politie en justitie.

Naast de geringe aangiftebereidheid is de oplossingsgraad van strafbare feiten door politie en justitie al jaren bedroevend laag. Nu blijkt zelfs dat er getwijfeld wordt aan het lage aantal moorden. OM iets te doen nemen bedrijven en burgers zelf actie. Fysieke beveiliging van huizen en winkels blijken de afgelopen dertig jaar meer effect te hebben gehad, dan enig optreden van de politie of maatregelen van de overheid.

Onderzoek van J&J naar grote verkeerscontroles maakt duidelijk dat woninginbraken in de dorpen rondom die operaties niet zijn afgenomen. De overheid communiceert nog wel met veel bombarie de vangst bij dergelijke grote controles, opgezet om insluipers met inbrekerssetjes te vangen, maar in de evaluaties gaat het vooral om de ‘leuke’ samenwerking tussen allerlei opsporingsgroepen in Nederland.

'Je weet maar nooit' argumenten

Redenen voor invoering van wetgeving die zowel de privacy als de onschuld inperken, blijken fluïde en verschuiven regelmatig. Politieke verschillen zijn er niet echt als het gaat om het veiligheidsbeleid. De invoering van de identificatieplicht werd door D66-bewindslieden gepromoot vanuit het oogpunt van terrorismebestrijding. Toen de wet eenmaal in de maak was en besproken werd in het parlement kwam dat facet niet meer ter sprake. Een rechter van PvdA-huize vond de wet noodzakelijk om hangjongeren aan te pakken. Daarbij ging het niet om jongeren die een strafbaar feit of overtreding hadden begaan, maar om bestrijding van het onschuld-adagium. Het ‘je weet maar nooit’ argument voor invoering van veel repressieve wetgeving.

Dat ‘je weet maar nooit’ argument is ook een van de argumenten geweest voor het invoeren van preventief fouilleren. De bevoegdheden worden opgerekt, want de overheid moet genoeg instrumenten hebben om op te kunnen optreden. Onderzoek van J&J toonde aan dat preventief fouilleren vaak ineffectief is en soms zelfs contraproductief. Er zijn indicaties dat geweldscriminaliteit toeneemt in die gebieden die door de overheid worden aangewezen als onveilig, als risicogebieden. De overheid bestempelt een buurt als veiligheidsrisicogebied en burgers gaan deze straten mijden. Anderen die zich er wel in begeven bewapenen zich, want ‘je weet maar nooit.’

Niet alleen in de openbare ruimte wil de overheid burgers disciplineren. Zowel in de fysieke als in de digitale wereld rukt zij op. Werkplicht, voorschriften over kleding en uiterlijk voor mensen met een uitkering, druk op dak- en thuislozen en drugsgebruikers om aan allerlei programma's deel te nemen, inkomens gestuurde huisvesting, controle van bewoning door woningbouwverenigingen samen met bestuur en politie, etc. Langzaam wordt er een arsenaal aan maatregelen uitgerold om ook direct in het leven van burgers in te kunnen grijpen.

Bij dat arsenaal hoort ook het 'toezicht' door de overheid op het internet, sociale media en webfora. Deels laat de techniek dit toe, maar er ontbreekt tevens duidelijke wetgeving omtrent bevoegdheden van politiefunctionarissen op het internet en is patrouilleren, het verzamelen van persoonsgegevens en het opstellen van profielen op en met behulp van sociale media zeer eenvoudig. Mensen zijn zich vaak niet bewust van wat zij allemaal aan informatie en sporen op het internet achterlaten en met wie zij die informatie delen. Dit gebeurt meestal op sociale media, maar ook op andere plaatsen op het internet.

Smartphone als alter ego voor de burger

Fysieke en digitale werkelijkheid convergeren steeds vaker. Door plaatsbepaling, toegenomen kennis van bedrijven over interesses, wensen, verlangens, voorkeuren (zowel seksueel, politiek of anderszins) van burgers; sociale media spelen daarbij een belangrijke rol. Gerichte reclames, aanbiedingen bij het passeren van winkels en horecagelegenheden; het is onderdeel geworden van de interactie tussen de fysieke en digitale werkelijkheid.

Het algemene gebruik van de smartphone maakt in combinatie met de plaatsbepaling het allemaal veel gemakkelijker om te profileren en gericht individuen te benaderen. Berichten, foto's, contacten, cv's, identiteitsgegevens en bankgegevens komen allemaal voort vanuit een digitaal apparaat. De smartphone is vandaag de dag dé keuzebepaler voor films, eten, restaurants, boeken, relaties maar ook voor huishoudelijke doeleinden, zoals aansluitingen voor gas, licht en water, betalingen, bankzaken, contact met de overheid, identiteit, reizen, boardingpas voor vliegreizen, etc.

De smartphone heeft zich als digitale en fysieke alter ego van burgers

ontwikkeld. Het verbindt beide werelden en is sterk geïndividualiseerd, al is dat aan het apparaat zelf nog niet af te lezen. Niet alleen bedrijven azen op dat alter ego. Naast commerciële interesses zijn vooral de overheid en opsporings- en inlichtingendiensten geïnteresseerd in al die gegevens en sporen die burgers achterlaten.

Het begon met invoering van de Wet bewaarplicht van telecommunicatiegegevens in 2009, Nederlandse wetgeving gebaseerd op een Europese richtlijn. De bewaarplicht (dataretentie) werd ingevoerd onder druk van aanslagen in de Verenigde Staten, Spanje en het Verenigd Koninkrijk. Bedrijven worden door de bewaarplicht voorgeschreven communicatiegegevens voor een bepaalde tijd bewaren. Het gaat vooral om gegevens als wanneer en met wie er wordt gecommuniceerd en de metadata van een bericht. De inhoud werd buiten beschouwing gelaten in verband met het briefgeheim en 'privacy' issues.

De bewaarplicht raakt iedereen en niet alleen specifieke verdachten van strafbare feiten. Of de maatregelen terrorisme-aanslagen voorkomen, de samenleving veiliger maken... het antwoord blijft uit. De effectiviteit is nooit onderzocht. Dat is ook onmogelijk bij zo'n algemene weg. De argumentatie voor invoering was 'je weet maar nooit' en nieuwe repressieve maatregelen staan alweer op de rol.

IP-tap

Op het internet waren tot aan de invoering van de bewaarplicht nog geen specifieke maatregelen getroffen ten aanzien van bepaalde groepen. Sommige webfora en nieuwspagina's van radicaal-linkse en extreem-rechtse groepen werden al wel in de gaten gehouden, maar van specifieke *targeting* van groepen zoals in de fysieke wereld bleek nog geen sprake.

De internettap (IP-tap) werd wel uitgebreid zoals de telefoontap. Niet meer alleen de verdachten werden gericht afgeluisterd, ook familie, vrienden, kennissen. Dit was voortgekomen uit de ontspoorde opsporingsmethoden in de jaren '80/'90 en de commissie Van Traa. De Bijzondere Opsporingsbevoegdheden formaliseerden echter die methoden en in de nieuwe eeuw werden zij aan de gewone strafvordering toegevoegd.

Toch is de IP-tap niet te vergelijken met databanken van vluchtelingen, illegalen, activisten, dak- en thuislozen en andere randgroepen. Aan de andere kant heeft de bewaarplicht echter wel de poorten opengezet om verder binnen te dringen in het digitale leven van burgers, en daarmee ook in het fysieke leven.

De laatste jaren monitort de overheid steeds meer sociale media. Daarbij gaat het niet langer alleen om wie met wie communiceert en wanneer, nee, het gaat steeds vaker om de inhoud en om facetten zoals plaatsbepaling. De schroom wat betreft persoonsgegevens, privécommunicatie; het lijkt allemaal niet meer relevant. De politie volgt berichten op Twitter die niet per se voor publieke doeleinden zijn bedoeld, Facebook berichten die niet exclusief aan vrienden zijn gericht. De overheid wil op FB ook 'bevriend' raken met burgers zodat zij zicht kan houden op de communicatie binnen afgesloten groepen.

Bij politiepatrouilles in de fysieke werkelijkheid kan aan de hand van gegevens van de GBA (Gemeentelijke Basisadministratie) en de RDW (Rijksdienst voor het Wegverkeer) worden gecheckt wie welk huis bewoont en wat voor auto hij bezit. Met de identificatieplicht en preventief fouilleren kunnen opsporingsdiensten al grote stappen vooruit maken in het binnendringen van de persoonlijke levenssfeer. U moet zich legitimeren en aantonen dat u geen gevaarlijke wapendrager bent.

Patrouilleren in de digitale wereld, op sociale media, onthult echter allerlei persoonlijke opvattingen waaronder politieke meningen, met wie die worden gedeeld en wanneer, en wie het met die meningen eens is. Het algemene gebruik van de smartphone als digitaal hulpmiddel om ons op het internet of sociale media te begeven, maakt het ook mogelijk plaatsbepaling en andere gegevens aan die dataset toe te voegen.

Nog een bredere toegang gewenst

De overheid wil desondanks nog bredere toegang. Dat uit zich bijvoorbeeld in het pleidooi tegen encryptie van opsporings- en inlichtingendiensten. Het zou het werk van die diensten bemoeilijken en de veiligheid in gevaar brengen. Afscherming, privacy en anonimiteit zijn volgens de overheid schuilplaatsen van het kwaad. De veiligheidsdiensten moeten toegang hebben, want 'je weet maar nooit'.

De overheid gaat echter nog een stap verder. Zij wil graag inbreken op

digitale hulpmiddelen van de slechteriken. Nu is dat te vergelijken met een gerichte telefoon- of internettap, de verdachte is het doel. Voor dat gericht inbreken is het echter noodzakelijk dat besturingssystemen van smartphones, tablets, laptops, etc. veiligheidslekken hebben, anders kan er niet worden ingebroken. Die veiligheidslekken worden regelmatig ontdekt, de zogenoemde *zero-days*, beveiligingslekken die net bekend zijn (nul dagen) en door bedrijven die software hebben ontwikkeld nog niet zijn gedicht.

Die *zero-days* en de digitale wapens om in te breken kopen Nederlandse opsporings- en inlichtingendiensten van individuen en bedrijven of via bedrijven zoals Hacking Team en Gamma Group. De beveiligingslekken gelden echter niet alleen voor de smartphone van een verdachte, maar voor iedereen met een vergelijkbare telefoon of hetzelfde besturingssysteem. Opsporings- en inlichtingendiensten willen die lekken onder de pet houden, want dan zijn ze vaker te misbruiken om in te breken. *Die zero-days* zijn echter niet exclusief voor de Nederlandse politie. Meestal zijn veel meer partijen op de hoogte van dezelfde lekken. Dat zijn overheden, opsporings- en inlichtingendiensten, maar ook bedrijven en criminele organisaties. De Nederlandse overheid ontwikkelt zelf niet de digitale wapens en ontdekt ook niet zelf de *zero-days*.

Nederlandse diensten lopen dus constant achter de feiten aan en laten burgers bewust rondlopen met onveilige smartphones, laptops en tablets. Het zou echter essentieel zijn voor de opsporing, hoewel dat argument niet met feiten wordt onderbouwd. Wat wel duidelijk is en door feiten wordt gestaafd, is dat bedrijven als Hacking Team en Gamma Group het niet zo nauw nemen met burger- en mensenrechten. Zij verkopen hun waar aan repressieve regimes als Soedan, Ethiopië, Egypte, Rusland en lijken er geen bezwaar tegen te hebben dat hun wapens worden ingezet tegen oppositiegroepen en journalisten.

Aan die bedrijven kleven weer allerlei andere bezwaren zoals het gebrek aan duidelijkheid over de rol van investeerders en de relaties die deze bedrijven hebben met bepaalde overheden, militaire eenheden, inlichtingendiensten en investeerders. Ook is de geschiedenis van de technologie waar hun digitale wapens op gebaseerd is niet te controleren en kunnen overheden, diensten en bedrijven daar een rol in hebben gespeeld bijvoorbeeld door de aanwezigheid van *backdoors* die de veiligheid van verdachten, en dus van de gehele bevolking, in gevaar kan brengen. En tot slot is er zelfs sprake van onduidelijke bedrijfsstructuren en twijfels over de economische integriteit door het gebruik van BV’s in

belastingparadijzen als Cyprus, Libanon, Panama en de Britse Maagdeneilanden.

Wit voetje halen

In de zomer breekt de politie fysiek in om een 'wit voetje' bij de burger te halen. Als dienstverlener wil ze waarschuwen voor het kwaad. Het gehele jaar laat diezelfde politie de deuren van smartphones en andere digitale middelen wagenwijd open staan. Die veiligheidslekken moeten gebruikt kunnen worden voor de enkele keer dat de diensten inbreken bij een verdachte, want 'je weet maar nooit'. Hoewel fysieke goederen nog steeds gewild zijn bij inbrekers, zijn digitale goederen veel meer waard. De smartphone, het alter ego van veel burgers, omvat veel gegevens en sporen, data die voor een cybercrimineel interessanter en waardevoller zijn dan de nieuwste gekromde UHDTV.

Hoe makkelijk het is om digitaal in te kunnen breken, laat de constante stroom hack-incidenten ons zien. In de zomer van 2016 werd bijvoorbeeld een Duitse hacker gearresteerd die wist in te breken op de computers van 150 Duitse schoolmeiden. Hij bespiedde hen via hun webcam en slaagde erin via het chatprogramma ICQ binnen te dringen. Met behulp van een trojan, een programma waarmee je een computer infecteert en op afstand kan besturen, kon hij zo de webcam overnemen. De hack werd niet ontdekt door de politie maar door een man die lesgeeft over databeveiliging op middelbare scholen. Het voorbeeld laat zien dat databescherming essentieel is en eigenlijk een grondwettelijk recht moet zijn.

De Nederlandse overheid propageert echter geen databescherming en veilige communicatie. Zij wil op de hoogte gehouden worden van datalekken, maar wat dat bijdraagt aan een grotere veiligheid op het internet is onduidelijk. Opsporings- en inlichtingendiensten willen geen encryptie, willen inbreken op digitale hulpmiddelen van burgers en *zero-days* onder de pet houden. Meerdere datalekken zullen het gevolg zullen daarvan zijn en minder digitale veiligheid. Voeg dit bij een lage aangiftebereidheid en een zeer lage oplossingsgraad van politie en justitie, en zie daar de onveilige samenleving die zich verder ontwikkelt.

Strenge regelgeving ten aanzien van software en hardware die op de markt komen is essentieel, zeker nu veel apparatuur bijna standaard aan het internet is gekoppeld. Controle ten aanzien van het updaten van die

software en hardware in het licht van de snelle ontwikkelingen. Een verbod op de handel in *zero-days,* met zware straffen als die niet wordt gemeld, en een verbod op het maken van digitale wapens.

Boemerang

De kans dat de Nederlandse overheid deze stappen zal gaan zetten, is nihil. Zij propageert geheimzinnigheid rond digitale wapens en *zero-days,* een zorgelijke ontwikkeling die als een boemerang de Nederlandse economie en veiligheidsdiensten zal treffen. Want als de laatste decennia iets hebben duidelijk gemaakt, is dat overheden de digitale revolutie niet in de hand hebben.

Na de privacy en het onschuld-adagium is nu ook de veiligheid geofferd. Langzaamaan wordt de rechtsstaat ontmanteld. De argumenten daarvoor zijn veelal niet gebaseerd op feiten. Terrorismebestrijding, criminaliteitsbestrijding, openbare orde; de eventueel controleerbare argumenten voor de invoering van maatregelen zijn naar de achtergrond verschoven. Noodzakelijk onderzoek of die maatregelen wel het juiste effect hebben gesorteerd, wordt vermeden of uitgevoerd op een manier waardoor opsporings- en inlichtingendiensten altijd in het gelijk worden gesteld zonder feitelijke onderbouwing. Wat overblijft is het enge argument dat de overheid en de diensten keer op keer herhalen: ‘je weet maar nooit’.

‘Je weet maar nooit’; Na privacy en de onschuld, is nu ook de veiligheid dood (pdf)