Policeware

Bart Jacobs[1]

Minister Opstelten heeft vergaande plannen geopenbaard om computercriminaliteit te bestrijden. Maar is het wel zo verstandig om de politie precies die bevoegdheden te geven die zij probeert te bestrijden? Door het plaatsen van zogenoemde *policeware* op computers wordt totale controle over deze computers verkregen. Feitelijk is daarmee sprake van een vorm van identiteitsdiefstal door de opsporingsinstanties. Bovendien is het maar de vraag of het probleem dat bestreden moet worden zo wordt opgelost. De grootste bedreigingen komen op dit moment van criminele hackers die vanuit het (verre) buitenland opereren. Daadwerkelijke vervolging van deze hackers is geen erg realistisch traject. Het heeft dan ook weinig zin daarvoor zulke ingrijpende, risicovolle opsporingsbevoegdheden te introduceren.

Op 15 oktober 2012 stuurde minister Opstelten (Veiligheid en Justitie) een brief naar de Tweede Kamer waarin hij nieuwe bevoegdheden voorstelt ten behoeve van opsporing en vervolging. De minister wil het voor de politie mogelijk maken om zelf te hacken en eigen software, hier afgekort tot *policeware*, heimelijk op een computer van een verdachte te plaatsen. De volgende vier punten komen letterlijk uit de brief van de minister.

- Het op afstand binnendringen van geautomatiseerde werken (=computers) en het plaatsen van technische hulpmiddelen (waaronder software) ten behoeve van de opsporing van ernstige vormen van cybercrime.
- Het op afstand doorzoeken van gegevens die vanuit een geautomatiseerd werk (computer) toegankelijk zijn, ongeacht de locatie van het geautomatiseerde werk waarop die gegevens zijn opgeslagen en met inachtneming van de afspraken en regels over de internationale rechtshulp.
- Het op afstand ontoegankelijk maken van gegevens die vanuit een geautomatiseerd werk (computer) toegankelijk zijn, ongeacht de locatie van het geautomatiseerde werk waarop die gegevens zijn opgeslagen en met inachtneming van de afspraken en regels over de internationale rechtshulp.
- De strafbaarstelling van het helen van (digitale) gegevens.

Hieronder zal nader worden ingegaan op de eerste drie punten: binnendringen, doorzoeken, en ontoegankelijk maken. Het perspectief zal niet juridisch van aard zijn, maar wordt ingegeven door de computerpraktijk. In wat door de minister wordt voorgesteld zijn twee aspecten opvallend en controversieel: de niet-locatie-gebondenheid en de ingrijpendheid van het plaatsen van *policeware*. De nadruk ligt hier vooral op dat laatste aspect.

Cybercrime

Cybercrime omvat strafbare handelingen waarbij computers een essentiële rol spelen, als middel of doel van handeling. De ontwikkeling van cybercrime laat zich duidelijk illustreren aan de hand van de ontwikkelingen in de bancaire sector. Zo is het aantal fysieke bankovervallen de laatste jaren spectaculair gedaald, maar daartegenover staat een even spectaculaire stijging van de digitale aanvallen op het geldverkeer. Het gaat dan vooral om het plunderen van bankrekeningen via het op onrechtmatige wijze bemachtigen en kopiëren van betaalkaartgegevens (skimmen van bankpassen) of het besmetten met kwaadaardige software *(malicious sofware*, gewoonlijk afgekort tot *malware*) van computers die gebruikt worden voor internetbankieren. De schade beloopt tientallen miljoenen euro's per jaar.

Deze verschuiving is begrijpelijk vanuit het perspectief van de crimineel: bij het betreden van een bankfiliaal met een afgezaagd geweer hoort een ander risicoprofiel dan bij het binnendringen van de pc van een internetbankierende burger, zeker als die digitale roof vanuit Oost-Europa of West-Afrika uitgevoerd of geregisseerd kan worden. Voor criminelen zijn dit soort aanvallen routine werkzaamheden geworden, waarbij ze gebruikmaken van zogenoemde *botnets*: netwerken van met *malware* geïnfecteerde computers die op afstand, vanuit *command en control servers*, aangestuurd worden. Er wordt geschat dat rond de 10-20% van alle pc's in Nederland onderdeel uitmaakt van een of ander botnet. Dat is zeer verontrustend. Indien je pc in zo'n botnet zit, kunnen alle (privé- of zakelijke) gegevens ervan afgehaald worden, bijvoorbeeld voor identiteitsfraude of spionage, en kan de pc voor allerlei andere niet bedoelde taken ingezet worden, bijvoorbeeld het versturen van spam of het uitvoeren van een (DDOS) aanval op andere computers.

De hiervoor beschreven verschuiving van fysieke naar digitale (computer)criminaliteit geldt niet alleen voor de bancaire sector. Ook in meer algemene zin geldt: *the bad guys have gone digital*. Het is deze vorm van cri-

Auteur

1. Prof. dr. B.P.F. Jacobs is als hoogleraar verbonden aan het Institute for Computing and Information Sciences van de Radboud Universiteit Nijmegen.

minaliteit die de minister met de door hem voorgestelde maatregelen wil bestrijden. Maar is het nodig om de politie voor dat doel precies die bevoegdheden te geven die zij probeert te bestrijden?

Het binnendringen van de computer van een ander is immers een strafbare handeling (volgens Sr. 138a), die aangeduid wordt als 'computervredebreuk'. Om juist die handeling toe te staan aan de politie is zeer verstrekkend en brengt aanzienlijke risico's met zich mee. Bovendien is het zeer de vraag of het probleem dat dit middel moet bestrijden daarmee daadwerkelijk wordt opgelost.

Computervredebreuk is een aanslag op het vrije individu

Een impliciet kenmerk van strafvorderlijke bevoegdheden gericht op gegevensverzameling is dat de politie doorgaans een passieve rol aanneemt. Een actieve rol, zoals bij infiltratie, draagt grote risico's met zich, niet alleen in fysieke zin, maar ook omdat daarbij het gevaar bestaat van beïnvloeding of manipulatie door de politie: de wetgever heeft daarom een uitdrukkelijk uitlokkingsverbod in geval van infiltratie in de wet opgenomen. Zeker in de digitale wereld zijn de bevoegdheden tot nu toe passief van aard. Bijvoorbeeld, bij een telefoon- of internettap krijgt de provider opdracht al het verkeer van de verdachte te selecteren en via een speciale verbinding aan de politie door te geven. De politie heeft daarbij geen invloed op de inhoud en het verloop van dat verkeer.

Een fundamenteel punt is dat bij computervredebreuk door de politie het onderscheid tussen passief en actief optreden verloren gaat: je kunt niet op een computer binnendringen en vervolgens alleen 'lezen', zonder ook te 'schrijven'. Alleen al het plaatsen van *policeware* door de politie op mijn computer is een actieve handeling waarbij in het geheugen van mijn computer geschreven wordt en de toestand ervan actief veranderd wordt. Voor het installeren van software op mijn computer zijn zogenoemde *admin* of *root* gebruikersrechten nodig, waarbij sprake is van totale controle over mijn computer. In kringen van hackers wordt bij het bereiken van zulke privileges dan ook, met enig bravoure, gesproken in termen van: *I own you*. Inderdaad is op dat moment werkelijk alles mogelijk: lezen, schrijven, toevoegen, weglaten. Dit heeft verstrekkende gevolgen. Het (sociale) leven van de moderne mens speelt zich in aanzienlijke mate af in de digitale wereld: pc's, mobiele telefoons en tablets zitten vol met persoonlijke gegevens (contacten, email / SMS / chat verkeer, locatiegegevens, webhistorie, wachtwoorden enz.). Als gevolg daarvan is er bij het bereiken van *root/admin*-status feitelijk sprake van het overnemen van iemands identiteit. Het plaatsen van *policeware* omvat dus niet alleen computervredebreuk maar ook identiteitsfraude: het onderscheid tussen het handelen van verdachte en politie gaat verloren. Het voornemen van de overheid om in haar repressieve rol burgers te willen *ownen* is diep verontrustend. Dit is een aanslag op het autonome, vrije individu. Je kunt niet eerst iemands identiteit overnemen en hem vervolgens beschuldigen.

In Duitsland is het gebruik van *policeware* eerder onderwerp van discussie geweest. Daar is het *Bundesverfassungsgericht* gevraagd zich over deze materie te buigen. Dit hoogste Duitse rechtscollege heeft het grijze, ongereguleerde gebied van computervredebreuk en identiteitsfraude door de politie benaderd vanuit de bestaande wetgeving en daarbij een nieuw recht geëxpliciteerd, namelijk een recht op confidentialiteit en integriteit van eigen computersystemen:[2]

> *Das allgemeine Persönlichkeitsrecht (...) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.*

Overigens is dit recht niet absoluut: onder specifieke omstandigheden zijn inbreuken gerechtvaardigd. Maar het genoemde recht is een stevig uitgangspunt. Deze Duitse les is in Nederland niet gevolgd.

Policeware stuit op praktische bezwaren

Naast deze fundamentele bezwaren tegen justitiële computerinfiltratie zijn er praktische problemen.

1) Bij een huiszoeking dient in beginsel een rechter-commissaris (RC) aanwezig te zijn om op het ordentelijk verloop ervan toe te zien. Hoewel het wellicht ongebruikelijk is om dit te benadrukken, draagt de aanwezigheid van de RC eraan bij dat de politie zich bij de doorzoeking beperkt tot een passieve rol, en niet actief zelf zaken toevoegt of wijzigt. In de plannen van de minister is een vergelijkbare rol van de RC voorzien bij het plaatsen en gebruik van *policeware*. In de digitale wereld gaat het er echter volstrekt anders aan toe: op afstand geplaatste software opereert autonoom, en kan op ieder moment haar gedrag aanpassen, nieuwe software downloaden en nieuwe functionaliteit toevoegen. Een RC zou vooraf inzage in de broncode van *policeware* kunnen krijgen maar moet die dan in detail bekijken en begrijpen, en er ook vertrouwen in hebben dat juist deze broncode (en geen andere) bij infiltratie gebruikt wordt. Beter zou het zijn indien de *policeware* voorzien is van *secure logging* functionaliteit, waarmee iedere actie die de software uitvoert eenduidig en onveranderlijk geregistreerd wordt. Daarmee zou zelfs de verdediging ervan overtuigd moeten kunnen worden dat de door de *policeware* verrichtte handelingen binnen de strafvorderlijke kaders blijven. Het is echter volstrekt onduidelijk hoe dergelijke *secure logging* gerealiseerd moet worden.
2) Juist omdat met *policeware* iemands identiteit volledig overgenomen kan worden valt het te verwachten dat iedere verdachte die aan dit nieuwe opsporingsmiddel

Het plaatsen van *policeware* omvat niet alleen computervredebreuk maar ook identiteitsfraude: het onderscheid tussen het handelen van verdachte en politie gaat verloren

© Images.com/Corbis

is blootgesteld zal beweren dat eventuele belastende informatie door de politie zelf gecreëerd en op de computer geplaatst is. In het licht van het voorgaande punt is onduidelijk hoe de politie zich hier effectief tegen zal kunnen verdedigen. Het middel kan erger blijken te zijn dan de kwaal: een voorbeeld van de uiterst complexe discussie die dit kan opleveren is de zaak-*Baybasin* waarover nu een herzieningsverzoek wordt behandeld. Het is daarmee ook in het belang van justitie dat *policeware* voor opsporing slechts ingezet wordt met de eerder genoemde *secure logging*.

3) Het plaatsen van *malware* of *policeware* op een specifieke computer is een tijdrovende operatie die veel kennis en kunde vereist. Makkelijker en efficiënter is het om dergelijke software grootschalig te gaan verspreiden, via systematische exploitatie van kwetsbaarheden in (consumenten)software. Dit is de strategie die digitale criminelen (en offensieve inlichtingendiensten) volgen, via phishing emails en websites met besmette inhoud, om posities op te bouwen in de computersystemen van de tegenstander. Is dit de strategie die ook de Nederlandse politie zal gaan volgen bij het verspreiden van *policeware*, mogelijk zelfs via eigen botnets? Gezien de bestaande efficiëntie- en prestatiedruk en gezien de lage drempel die de minister voor ogen staat – er wordt gesproken van misdrijven waar minstens vier jaar op staat – ligt dat wel in de lijn van de verwachtingen. Daarbij zal de overheid, via de politie, er dus belang bij hebben dat kwetsbaarheden in software niet gepubliceerd en gerepareerd worden maar juist

Noten

2. BVerfG, 1 BvR 370/07 van 27 feb. 2008, zie www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.

geheim en exploiteerbaar blijven. Dit staat op gespannen voet met het algemeen belang van een betrouwbare digitale infrastructuur.

4) Het beheersen van eenmaal uitgezette *policeware* is een uitdaging op zich. Dit leert de ervaring in Duitsland. In oktober 2010 publiceerde de hackersvereniging *Chaos Computer Club* (CCC) een eigen analyse[3] van software die door Duitse autoriteiten gebruikt werd om Skype gesprekken te volgen, screenshots te maken, of wachtwoorden voor privécommunicatie te achterhalen. De CCC wees op verschillende zwakheden in deze *policeware*, die weer door anderen misbruikt konden worden. Ook op de beruchte *Stuxnet malware*, die door de Verenigde Staten samen met Israel ontwikkeld is om het Iraanse atoomprogramma te saboteren, is door onvoorziene omstandigheden de controle verloren.[4] Deze sabotage software is vervolgens publiekelijk geanalyseerd en heeft aanleiding gegeven tot een nieuwe generatie van kwaadaardige digitale aanvallen.

Een interessante en ongemakkelijke situatie doet zich voor wanneer antivirussoftware *policeware* aantreft op de computer/tablet/smartphone van een burger

5) Als burgers worden wij door de overheid en door bedrijven (met name banken) regelmatig gewaarschuwd onze computers goed te beveiligen en actuele antivirussoftware te gebruiken. Een interessante en ongemakkelijke situatie doet zich voor wanneer dergelijke antivirussoftware *policeware* aantreft op de computer/tablet/smart phone van een burger. Zal de overheid van antivirusbedrijven verwachten (of eisen) dat ze dergelijke *policeware* juist niet detecteren, vermelden en verwijderen en daarmee hun klanten kwetsbaar laten? Of kan de *policeware* gewoon verwijderd worden, en wordt dit gezien als bedrijfsrisico voor de politie?
6) Verschillende partijen hebben hun zinnen gezet op het meekijken en beïnvloeden van de privégegevens op de computerapparatuur van de moderne, digitaal opererende burger, via commerciële *adware*, criminele *malware* en justitiële *policeware*. De idee van een autonoom, vrij opererend individu brokkelt hiermee af: deze apparatuur wordt steeds minder geschikt voor eigen, onbespiede, authentieke uitingen. Het enige technische hulpmiddel waarvan de exclusieve individuele controle vooralsnog niet systematisch ondermijnd wordt is de chipkaart. Het is daarmee de beste bergplaats voor persoonlijke (cryptografische) sleutels ten behoeve van digitale handtekeningen en voor toegang tot versleuteld materiaal dat elders opgeslagen ligt.

Het inzetten van computervredebreuk als opsporingsmiddel kent dus grote fundamentele en praktische problemen. De voornemens uit de *policeware* brief van de minister dienen dan ook geen vervolg te krijgen.

Alternatief: computervredebreuk enkel als verstoringsmiddel

De grootste bedreigingen komen op dit moment van criminele hackers die vanuit het (verre) buitenland opereren. Tegen dergelijke activiteiten moet snelle, effectieve actie ondernomen kunnen worden. Op dit moment zijn het eigenlijk alleen private partijen die hier iets tegen willen of kunnen doen. Het voornemen van de minister om ook de politie daarbij een rol te geven verdient steun. Daadwerkelijke vervolging van deze hackers is echter geen erg realistisch traject, omdat, als deze lieden al gelokaliseerd en geïdentificeerd kunnen worden, uitlevering problematisch is. Het heeft dan ook weinig zin daarvoor zulke ingrijpende, risicovolle opsporingsbevoegdheden te introduceren. Veel realistischer is het om in deze situatie *hacken om te verstoren* als nieuwe bevoegdheid voor de politie te introduceren (dat wil zeggen om de voorstellen in de brief van de minister hiertoe te beperken). Zo'n verstoringsbevoegdheid heeft veel beperktere doelen en toepassingen, en sluit goed aan bij de bestaande praktijk, zoals nu uitgevoerd door private partijen. De verstoringsbevoegdheid zou reactief ingezet moeten worden, in (acute) situaties waarin sprake is van aanvallen op personen of infrastructuur in Nederland. De verstoringsactiviteiten van de politie zouden zich moeten richten op de ICT-infrastructuur van de aanvallers en computervredebreuk kunnen omvatten. Wanneer bij die inzet geen sprake is van een opsporingsdoel, zal de onvermijdelijke manipulatie van gegevens op de computer van de agressor bij computervredebreuk door de politie niet kunnen leiden tot beschuldigingen dat strafbare feiten door de politie zelf gecreëerd zijn.

Het voorstel van de minister om de politie in haar handelen niet te beperken wanneer geografische informatie ontbreekt is nuttig en verdedigbaar bij een bevoegdheid die tot verstoring beperkt blijft (en geen opsporing omvat). Bij de operationele inzet van de bevoegdheid dient men zich bewust te zijn van het risico op een tegenactie die computers en gegevens van Nederlanders in gevaar brengt. Zo'n verstoringsbevoegdheid wordt daarom bij voorkeur binnen een internationaal kader georganiseerd. Daarbij moet inzet van de bevoegdheid alleen toegestaan zijn als reactie op externe, acuut bedreigende agressie, en nadrukkelijk niet op de mogelijk onwelgevallige inhoud van (buitenlandse) websites. De vrijheid en rijkdom die het internet ons biedt verdient voortdurende bescherming. •

3. Zie de website: www.ccc.de/de/updates/2011/staatstrojaner.

4. Voor meer informatie, zie: D.E. Sanger, *Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power.* Random House, New York, 2012.