Cybercrime Tweede Kamer praat vandaag over voorstel om politie de mogelijkheid te geven in computers in te breken

Het cybercrimebeleid dreigt te mislukken als de politie mag inbreken op computers en goedwillende hackers van zich vervreemdt, stelt de Nijmeegse hoogleraar Bart Jacobs. „Kinderporno wordt, net als terrorisme, gebruikt om absurde regels te introduceren."

Kinderporno als excuus voor een spionerende politie

Door onze redacteur
MARC HIJINK

NIJMEGEN. Tien jaar geleden waren de aanslagen op de Twin Towers en de metro in Londen de aanleiding om de vrijheden van burgers fors in te perken. Nu is de strijd tegen digitale kinderpornonetwerken en cybercrime de drijfveer voor een nieuwe golf van maatregelen die de politie meer macht moeten geven.

Vanmiddag discussieert de Tweede Kamer over het voorstel van minister Opstelten (Veiligheid en Justitie, VVD) om agenten in staat te stellen afluistersoftware – 'spyware' – te plaatsen op pc's, smartphones en verdachte webservers. Deze nieuwe bevoegdheden moeten de politie de mogelijkheid geven sneller in te grijpen, bijvoorbeeld als er vanuit een Oekraïense server een aanval op een Nederlandse bank wordt uitgevoerd. Of als er op een server in Korea kinderporno van Nederlandse makelij wordt aangetroffen. Officieel mag de Nederlandse politie alleen op het eigen grondgebied opereren, waardoor de opsporingsdiensten met lede ogen aanzien hoe buitenlandse cybercriminelen Nederlandse slachtoffers maken.

Systemen hacken, Bart Jacobs weet er alles van: zijn studenten kraakten onder meer de OV-chipkaart. „Maar ik leer studenten dat ze binnen de grens moeten blijven. Als we eens met één teen de wet moeten overtreden, doen we dat zonder er zelf beter van te worden en met een nadrukkelijk maatschappelijk belang."

Terwijl hij zijn studenten de mores van het hacken inpepert, maakt de hoogleraar zich ernstige zorgen over het plan voor *policeware*. Jacobs is lid van de door Opstelten opgerichte Cyber Security Raad en waarschuwt dat de politie zich bedient van de middelen die ze moet bestrijden: „De minister beweegt zich als een olifant in de porseleinkast. Het cybersecuritybeleid dreigt te mislukken."

Wat is uw belangrijkste zorg over de extra bevoegdheden voor de politie?

„Als je software installeert op een pc neem je iemands identiteit over. Je kunt hem vervolgens niet nog ergens van beschuldigen. Iedere crimineel zal tegen de rechter zeggen: dat heeft de politie er zelf neergezet. Bij huiszoekingen gaat altijd een rechter-commissaris mee. Die moet er op letten dat de politie niet zelf de cocaïne neerlegt. Maar hoe doe je zoiets digitaal? Hoe controleer je dat, hoe leg je dat vast in een veilig document dat ook door de advocaat van de beschuldigde geaccepteerd wordt?"

Expert in computerbeveiliging

Bart Jacobs, 49 jaar, is hoogleraar bij het Institute for Computing and Information Sciences van de Radboud Universiteit Nijmegen. Hij studeerde wiskunde en filosofie en was onder meer adviseur bij de commissie-Korthals Altes die in 2007 de onveilige stemmachines onderzocht. Jacobs' studenten ontdekten hoe makkelijk het was de ov-chipkaart te kraken. Hij werd als adviseur geraadpleegd tijdens de Diginotar-affaire en zit sinds 2011 in de Nationale Raad voor Cybersecurity. Hij is officier in de Orde van Oranje-Nassau.

Moet de overheid niet de mogelijkheid hebben om terug te slaan?

„We moeten geen doetjes zijn. Stel dat een Nederlandse bank digitaal wordt aangevallen vanuit het buitenland. Banken stappen nu naar een beveiligingsbedrijf toe en vragen: schop jij die server eens om. Of ze huren een buitenlands bedrijf in. Zo belanden we het grijze circuit en dat is niet goed.

De politie mag wat mij betreft wel servers verstoren. Wat ik bloedlink vind is om dit te combineren met opsporing. Om zo'n computer om te schoppen, moet je toch hacken en uiteindelijk de schijf wissen. Je moet ook sniffersoftware installeren om wachtwoorden te achterhalen. Bij burgers gaat dit te ver. Zodra ik jouw pc of smartphone beheers kan ik alles installeren wat ik wil, kan ik alles lezen, namens jou mailtjes versturen, chats opzetten, mailtjes toevoegen..."

Houdt de rechter-commissaris dat niet in de gaten?

„Het is technisch moeilijk en onpraktisch: er is geen enkele rechter-commissaris in Nederland te vinden die hier enig benul van heeft. Je vraagt om problemen als de overheid zich permitteert om de identiteit van de eigen burgers over te nemen zonder dat daar een geloofwaardige waarborg tegenover staat."

Ontbreekt het de overheid dan nog aan kennis op ICT-gebied?

„Dat wordt iets te makkelijk geroepen. Mijn ervaring is dat de kennis er wel zit, maar dat er op hogere niveaus niet naar geluisterd wordt. Bij het Team High Tech Crime, de inlichtingendiensten en het Nationaal Cyber Security Centrum zitten toch echt mensen die weten wat ze doen.

„Bij de Diginotar-affaire verliep de aanpak redelijk goed. [De dienstverlening van de overheid dreigde in 2011 platgelegd te worden door valse digitale certificaten van dit bedrijf.] Een van de redenen hiervoor was, dat de ministers direct zeiden: we weten hier niets van. Ze waren eindelijk een keer bereid te luisteren naar wat er in de hiërarchie tegen hen gezegd werd. De verantwoordelijke topambtenaar was een informaticus. Dat scheelt."

Veel van de voorgestelde bevoegdheden dienen voor zware gevallen, bijvoorbeeld om kinderporno op geanonimiseerde servers te verwijderen.

„Kinderporno op internet wordt zwaar overschat. Het dreigt zo'n onderwerp te worden als drugs waren in het verleden. Daar ging ontzettend veel geld en capaciteit naar toe, terwijl het dweilen met de kraan open was.

„Als je iets kunt doen aan de productie van kinderporno, moet je keihard ingrijpen. Daar zitten de grootste klootzakken. En als de politie ergens een computer in beslag neemt, moeten ze er altijd naar zoeken. Maar hoe vaak kom je nou al surfend die troep tegen? Nooit! Het zit zo diep, versleuteld, in het internet."

U bedoelt dat de distributie via internet geen maatschappelijk bedreiging is?

„Kinderporno dreigt als argument misbruikt te worden om absurde bevoegdheden te introduceren. Net zoals 10 jaar geleden terrorisme te pas en te onpas gebruikt werd om absurde bevoegdheden te introduceren. Het is bloedlink zoiets hardop te zeggen..."

Maar dat doet u nu wel.

„Ik weet het. Je krijgt snel emotionele reacties over je heen. En ja, ik heb ook kinderen en ik zou ook over de rooie gaan als er met hen iets gebeurt. Maar je moet de zaken in perspectief zien. Ik begrijp van de politie dat ze de meldingen bij het Meldpunt Kinderporno niet eens aan kunnen, qua capaciteit. Regel dat eerst."

Jacobs pauzeert. Even afstand. Hij was twee jaar geleden, zo benadrukt hij, „werkelijk aangenaam verrast" door Opsteltens aanpak van cyber security: een strategie, een adviesraad met externe experts en zelfs in het huidige regeerakkoord gaat er meer geld naar de bestrijding van cybercrime. Maar volgens Jacobs ligt de nadruk nu te veel op grote partijen die de veiligheid van infrastructuur moeten waarborgen. Het contact met de Nederlandse hackersgemeenschap is niet goed opgebouwd, terwijl *white hat hackers* – krakers met goede bedoelingen – volgens de hoogleraar onmisbaar zijn in de bestrijding van cybercrime.

Toen het Dorifel-virus dit najaar enkele gemeentehuizen platlegde, was de informatievoorziening van de overheid mede afhankelijk van hackers die op eigen initiatief op onderzoek uitgingen. „Hackers zijn de voelsprieten, zij hebben kennis van het systeem", zegt Jacobs. Hij is boos over de arrestatie van de hacker van het Groene Hart Ziekenhuis in Leiden; die bewees dat patiëntengegevens onveilig waren maar werd aangehouden.

Jacobs: „Als je de afgelopen weken bekijkt, dreigt het cybersecuritybeleid te mislukken omdat de minister als een olifant in de porseleinkast opereert met dit wetsvoorstel. Er heerst nu de reflex dat de knuppel eroverheen moet, terwijl je juist moet meeveren, meeleven met de wereld van de hackers."

Kunnen overheid en hackercultuur wel samenwerken?

„Met deze voorstellen voor extra bevoegdheden voor politie krijg je het contact met de hackers zeker niet. Probeer in overheidsorganisaties die sfeer te handhaven van paardenstaarten en jonge honden. Mijn angst is dat het kapotgebureaucratiseerd wordt, dat de goede mensen weglopen. En zorg voor een regeling met white hat hackers. Als ze een lek vinden zouden ze het moeten kunnen melden bij het Nationaal Cyber Security Centrum. Geef ze bevestiging: als het lek door iemand anders naar buiten gebracht wordt, verklaren wij dat *jij* als eerste het lek gevonden hebt. Het gaat om prioriteit, respect. Pas je aan die cultuur aan."

Hackers moeten worden beloond, niet bestraft?

„Als zelfs KPN [dat begin dit jaar door een ernstig datalek getroffen werden] nu een beloning uitreikt aan hackers die een lek vinden, kan de overheid dat ook doen. Nederlandse bedrijven moeten het melden als ze beveiligingproblemen hebben gehad. Maar de eerste de beste amateurpsycholoog zal je zeggen dat organisaties veel moeite hebben over hun eigen gedrag te rapporteren. Het levert meer op als buitenstaanders, hackers, ook zwakheden kunnen melden. Dat is veel efficiënter."

U adviseerde tijdens de Diginotar-affaire, maar is de Cyber Security Raad niet geraadpleegd bij deze voorstellen?

Voor alle duidelijkheid: mijn kritiek is persoonlijk, niet als lid van de raad. We hebben een adviesrol op de lange termijn en we hoeven niet over ieder individueel wetsvoorstel te discussiëren, tenzij daar expliciet om gevraagd wordt. Handig vind ik het niet. Ik heb mijn bezwaren wel genoemd, in een bijeenkomst in Den Haag, net nadat de brief gepubliceerd was. Maar er viel alleen een ongemakkelijke stilte."

Bart Jacobs naast een Duitse Enigma-machine uit de Tweede Wereldoorlog. Het apparaat werd gebruikt om gecodeerde berichten te versturen en werd gehackt door de Britten.
Foto Anoek Bleumer

Ronald Prins: slechte marketing van justitie

Ronald Prins is directeur van Fox-IT, het Nederlandse bedrijf dat vaak door de overheid wordt ingeschakeld bij cyberbedreigingen. Hij pleit al jaren voor meer bevoegdheden voor opsporingsambtenaren, maar is niet blij met manier waarop de voorstellen gepresenteerd worden. Prins stelt vraagtekens bij de „marketing van justitie" en heeft de indruk dat het door een klein clubje mensen in elkaar geschroefd is in het departement, zonder te informeren bij externe experts.

De Delftse hoogleraar **Michel van Eeten** is lid van de Cyber Security Raad en heeft moeite met het voorstel. „Rechters zullen blind moeten varen op bewijs, omdat geknoei met spyware achteraf nauwelijks is vast te stellen." Hij heeft morele bezwaren: „We laten onze democratische waarden los als we op eigen houtje met spyware buiten Nederland gaan opereren. Dat zijn dezelfde middelen die China gebruikt." Van Eeten waarschuwt dat het platleggen van servers gevaren met zich meebrengt. „Je loopt het risico dat er ook 400 andere websites uit de lucht gehaald worden die op diezelfde server staan. Of dat de criminele server op een gehackte machine van een bank of ziekenhuis staat."

Volgens **Bert Jaap Koops**, hoogleraar regulering technologie aan de Universiteit van Tilburg, heeft een rechter-commissaris niet voldoende verstand van zaken om te kunnen beoordelen of plaatsen van spyware gerechtvaardigd is. „Het risico bestaat dat het net als bij de telefoontaps een soort stempelmachine wordt." Hij pleit voor onafhankelijke toetsing, door een soort ombudsman. Koops vindt het „vrij naïef" van de makers van het voorstel om eerst een bevoegdheid voor te stellen en pas later te kijken hoe de techniek precies in de praktijk gebruikt kan worden.

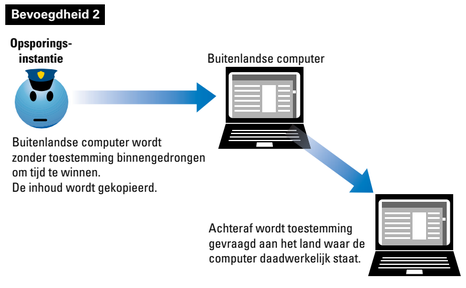
Cybercriminelen laten zich lastig vangen, daarom wil de politie extra bevoegdheden

Bevoegdheid 1

Spyware luistert af via smartphone en pc

Opsporingsinstanties willen kunnen inbreken op een computer of telefoon en daar spyware (verborgen software) plaatsen. Zo kun je toetsaanslagen opslaan om wachtwoorden te achterhalen. Ook kun je de ingebouwde microfoon en camera op afstand gebruiken om mee te luisteren met WhatsApp of Skype. Spyware mag niet herkend worden door antivirussoftware. Maar het risico bestaat dat die toch ontdekt wordt en vervolgens misbruikt. Dat gebeurde onder meer in Duitsland.

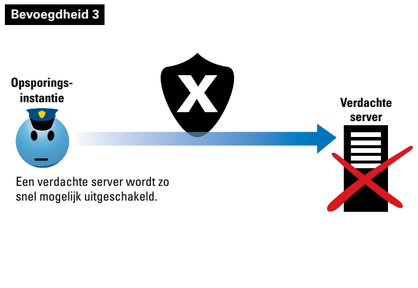
Bevoegdheid 2



Servers manipuleren, ook over de grens

Opsporingsinstanties willen inzage krijgen in computers waarvan niet vaststaat of ze binnen de Nederlandse landsgrenzen staan. Politieagenten mogen alleen in het buitenland opereren met toestemming van de betreffende staat, maar dat werkt niet snel genoeg om cybercriminelen te pakken – die verhuist snel naar een andere server. Het voorstel is om gegevens van zo'n computer te kopiëren en bewaren en naderhand te bepalen of er een rechtshulpverzoek nodig was geweest.

Bevoegdheid 3



Ontoegankelijk maken van gegevens

Als de politie op een verdachte server bijvoorbeeld kinderporno vindt, dan moet die activiteit worden afgesloten voor de buitenwereld. Ook als niet duidelijk is waar de computer staat en wie de beheerder is – dat is het geval bij anonieme servers in het versleutelde TOR-netwerk – moeten ernstige strafbare feiten meteen gestopt kunnen worden. De vraag is of er ook zo snel wordt ingegrepen als vanaf zo'n server bijvoorbeeld illegale kopieën van Hollywoodfilms de wereld rondgestuurd worden.

Bevoegdheid 4

Heling van creditcard-gegevens strafbaar

De strafbaarstelling van het helen van (digitale) gegevens. Handel in creditcardgegevens of persoonsgegevens uit gekraakte databases (mailaccounts, Facebook, webwinkels) is een belangrijke bron van inkomsten voor cybercriminelen. Het is nog niet strafbaar om websites te runnen waar die gegevens verhandeld worden. De politie kan pas ingrijpen als er daadwerkelijk misbruik van die gegevens gemaakt wordt, bijvoorbeeld door een onterechte aankoop.