Geheim overleg met hackers van de NSA

Computerspionage De Amerikaanse NSA is niet de enige die computersystemen hackt. „*The Dutch*" doen dat ook, zegt de NSA in geheime notulen. „Ze zoeken naar goede manieren om hun data te *minen*."

Door **Steven Derix, Glenn Greenwald** en **Huib Modderkolk**

AMSTERDAM/RIO DE JANEIRO. Op 14 februari 2013 - Valentijnsdag - vergaderen medewerkers van de Amerikaanse afluisterdienst NSA met hun Nederlandse *counterparts*. Het is een bijeenkomst voor specialisten: mannen en vrouwen die zich bezighouden met spionage op internet.

Uit het geheime gespreksverslag dat de NSA zal maken, blijkt niet waar de vergadering plaatsvindt. Maar het document maakt wel duidelijk dat de AIVD en de militaire inlichtingendienst MIVD een zware delegatie hebben afgevaardigd. In totaal zitten er negen Nederlanders tegenover de drie Amerikanen.

De Nederlanders steken van wal. Ze vertellen over de veranderingen in hun organisatie. Ze briefen de Amerikanen over hun onderzoek naar de activiteiten van Chinese hackers in Nederland. De Nederlanders willen graag feedback: wat vinden de NSA-collega's van hun onderzoek?

Even is er een ongemakkelijk moment, als de Amerikanen toegeven „nog geen tijd" te hebben gehad om de rapporten te lezen die de Nederlanders hen hebben gestuurd.

Uit de notulen van de vergadering, die zijn gelekt door voormalig NSA-medewerker Edward Snowden, blijkt dat de Amerikanen niet altijd even geboeid zijn door wat hun Nederlandse collega's vertellen. Maar dat verandert als de Nederlanders uitleggen hoe ze inbreken in de servers van openbare webfora, om daar grote hoeveelheden gegevens te verzamelen. „De discussie over de webfora", schrijft een medewerker van de NSA, „was een stuk interessanter."

Webfora zijn een belangrijke bron van inlichtingen voor de diensten. Vorig jaar publiceerde de AIVD een uitgebreide notitie over jihadistische fora op het 'onzichtbare' web. Meer dan 90 procent van het internet is nog niet in kaart gebracht door de zoekmachines van Google. Maar juist op dit *darknet* bevinden zich de webfora waarop moslimextremisten met elkaar discussiëren.

Volgens de AVID vormen de fora „de kern en de motor van de wereldwijde virtuele jihadistische beweging." En het *darknet* is niet alleen een toevluchtsoord voor de internationale jihad. Ook rechtsradicalen en neo-nazi's weten elkaar te vinden op webfora. Hetzelfde geldt voor voetbalhooligans, en voor gewelddadige dierenactivisten.

Sommige webfora worden gehackt door de AIVD. Medewerkers van de dienst slagen er in toegang te krijgen tot de computerservers waarop de websites draaien, en daar kwaadaardige software te installeren. Met behulp van deze *malware* kan de database van het forum, met daarin de gegevens van alle gebruikers, ongemerkt worden weg gesluisd. De technische term voor zo'n aanval is *Computer Network Exploitation* (CNE). De Nederlandse diensten, zo schrijven de Amerikanen, „verzamelen (...) databases door middel van CNE".

Het hacken van computers mag volgens de wet. Het „binnendringen in een geautomatiseerd werk" is één van de „bijzondere bevoegdheden" die de diensten mogen gebruik om informatie te verzamelen. Maar het is een grote inbreuk op de privacy van een burger. Vooraf moet daarom altijd toestemming van de minister worden gevraagd. En in de aanvraag voor de hack moet de dienst overtuigend aantonen dat het beoogde doelwit (een persoon of organisatie) een ernstige bedreiging vormt voor de 'democratische rechtsorde'.

De afgelopen jaren is CNE steeds belangrijker geworden voor de Nederlandse diensten. Vanaf volgend jaar zullen de AIVD en de MIVD hun krachten op het gebied van computerspionage gaan bundelen in een nieuwe gezamenlijke eenheid, die zal opereren vanaf het AIVD-hoofdkwartier in Zoetermeer. Met de oprichting van deze Joint Sigint Cyber Unit (JSCU) worden de capaciteiten van de beide diensten op het gebied van hacken verder versterkt. De AIVD is alvast op zoek naar personeel voor de functie van 'ICT-specialist Computer Network Exploitation'.

Maar de wet is nog niet toegesneden op cyberspionage. De Wet op de inlichtingen- en veiligheidsdiensten (Wiv) dateert uit 2002. In de memorie van toelichting daarop wordt nog gesproken van „het binnendringen van (stand-alone) pc's". Dat was toen al niet zo'n zinnige opmerking - een computer zonder internetverbinding is lastig te hacken. En anno 2013 surfen mensen niet alleen vanaf hun pc, maar ook met hun smartphone en hun tablet.

Data staan niet meer op de harde schijf, maar hangen ergens in de 'cloud'. Daarmee is het ondoenlijk geworden op een computerhack te beperken tot één computer. Als je bijvoorbeeld de e-mail van één redacteur van *NRC Handelsblad* wil lezen, is het het handigst om het mailverkeer van de hele krant te onderscheppen, en daarna te gaan selecteren.

> Diensten moeten bij een hack vooraf aantonen dat het beoogde doelwit een bedreiging is voor de democratische rechtsorde

Zo gaat het ook bij de webfora. Door de hack krijgt de dienst niet de gegevens van één persoon, maar van alle gebruikers van het forum in handen. Volgens het ministerie van Binnenlandse Zaken past het inbreken in webfora binnen artikel 24 van de wet, waarmee hacken wordt toegestaan. In deze optiek kan een webforum worden beschouwd als een 'organisatie' die een bedreiging vormt voor de rechtsorde, als er aanwijzingen zijn dat er staatsondermijnende activiteiten plaatsvinden.

Deskundigen op het gebied van informatierecht en privacy vinden dit echter te ver gaan. Het vermoeden dat een webforum verdacht publiek trekt, betekent nog niet dat álle bezoekers doelwit mogen worden van de dienst. Volgens hoogleraar Nico van Eijk van de Universiteit van Amsterdam gaat de AIVD met het gebruik van deze hackmethode een grens over. „Ze trekken een sleepnet door internetfora en nemen de data van willekeurige personen mee."

Uit het geheime NSA-document blijkt dat de AIVD maximaal gebruik maakt van de gegevens die ze hebben binnen gehaald. Zo probeert de dienst gebruikers te koppelen aan een IP-adres - het unieke nummer van hun internetaansluiting. De Nederlanders, „proberen betrouwbare IP-adressen te genereren", schrijft de NSA. Net als een telefoonnummer is een IP-adres één van de kenmerken op grond waarvan de AIVD iemand kan aanwijzen. Zo kan de database met gebruiksgegevens nieuwe 'targets' opleveren.

En de AIVD doet nog meer. „Ze onderzoeken of ze data uit de webfora kunnen combineren met gegevens van andere sociale media en proberen goede manieren te vinden om de data die ze al hebben te *minen*."

De AIVD hackt dus een forum, haalt de gegevens van alle gebruikers binnen, en gaat vervolgens kijken of er mogelijke targets kunnen worden geïdentificeerd voor nader onderzoek.

In 2011 publiceerde de toezichthouder op de inlichtingendiensten CTIVD een rapport over ongerichte zoekacties. Dat rapport ging niet over computerhacken, maar over het binnenhalen van radio- en satellietcommunicatie door de MIVD. In het Friese Burum worden grote hoeveelheden satellietcommunicatie opgevangen en opgeslagen. Deze bulkinformatie mag niet zomaar worden doorzocht: daar is toestemming van de minister voor nodig.

Net als bij hacken moet er in de aanvraag een specifiek doelwit worden genoemd, een persoon of een organisatie. De praktijk was echter anders, concludeerde de CTIVD.

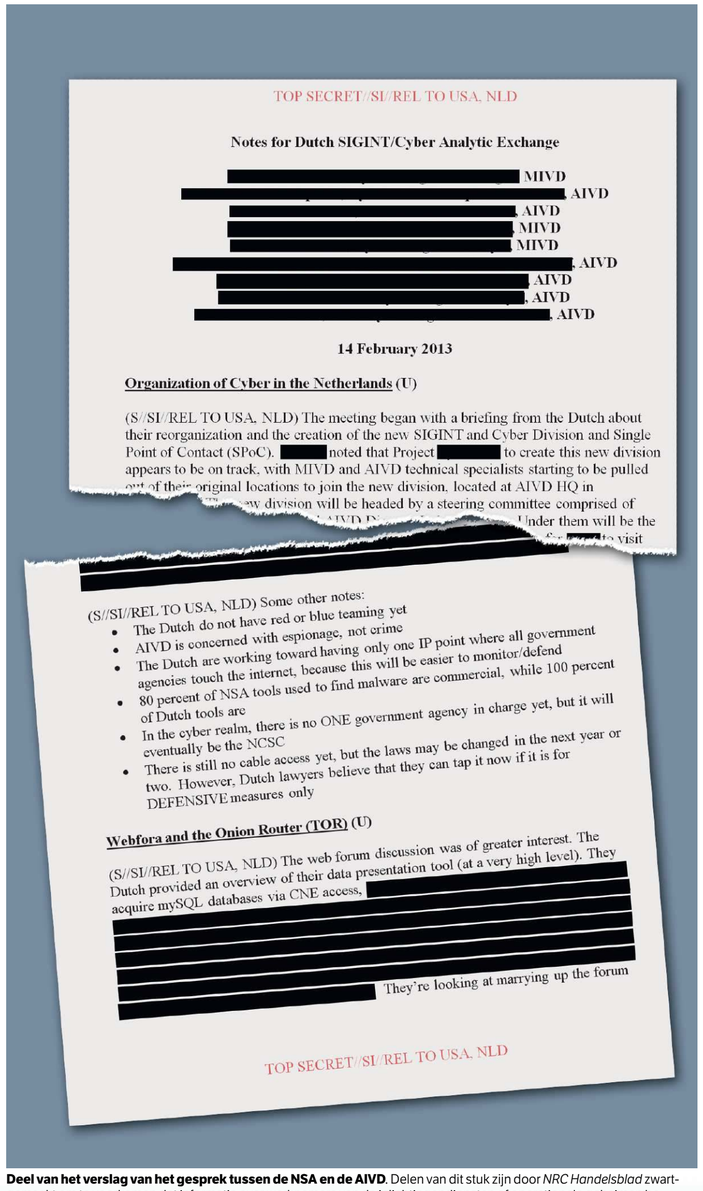
De toezichthouders stelden vast dat de MIVD toestemming kreeg voor het onderzoeken van „breed geformuleerde categorieën van personen en organisaties". Volgens de commissie was dit „niet in overeenstemming met de wet". Inlichtingendiensten mogen dus geen sleepnet uitgooien om verdachten te vinden in de enorme hoeveelheden onderschepte data.

Naar aanleiding van het kritische rapport van de CTIVD zei toenmalig minister van Defensie Hans Hillen (CDA) in het voorjaar van 2012 dat het voor staatsveiligheid nodig kan zijn om „de randen van de wet op te zoeken of zelfs daaroverheen te gaan". Volgens Hillen was het duidelijk dat de techniek de wet heeft ingehaald en dat de Wiv zo snel mogelijk moest worden aangepast.

De afgelopen jaren hebben AIVD en MIVD zich achter de schermen luidkeels beklaagd. De NSA en de Duitse Bundesnachrichtendienst halen op grote schaal e-mails en ander verkeer van het internet. Maar in Nederland is het ongericht aftappen van kabels verboden. Een groot probleem voor de diensten, in een tijdperk waar ruim 90 procent van het dataverkeer over de glasvezelkabel gaat.

Aanstaande maandag zal een commissie onder leiding van de jurist Constant Dessens een rapport presenteren waarin de Wet op de inlichtingen en veiligheidsdiensten wordt geëvalueerd. De algemene verwachting is dat Dessens zal adviseren om de wet te verruimen.

Tijdens hun vergadering met de NSA vertellen de Nederlanders over hun juridische problemen. „Er is nog geen toegang tot de kabel", staat er in het NSA-verslag. „Nederlandse juristen zijn van mening dat hij (de kabel) nu al kan worden getapt, mits het gaat om defensieve maatregelen." Uit de NSA-notulen blijkt niet waar de Nederlanders precies op doelen.



TOP SECRET//SI//REL TO USA, NLD

Notes for Dutch SIGINT/Cyber Analytic Exchange

[redacted] MIVD
[redacted] AIVD
[redacted] AIVD
[redacted] MIVD
[redacted] MIVD
[redacted] AIVD
[redacted] AIVD
[redacted] AIVD
[redacted] AIVD

14 February 2013

Organization of Cyber in the Netherlands (U)

(S//SI//REL TO USA, NLD) The meeting began with a briefing from the Dutch about their reorganization and the creation of the new SIGINT and Cyber Division and Single Point of Contact (SPoC). [redacted] noted that Project [redacted] to create this new division appears to be on track, with MIVD and AIVD technical specialists starting to be pulled out of their original locations to join the new division, located at AIVD HQ in [redacted]. The new division will be headed by a steering committee comprised of [redacted]. Under them will be the [redacted] to visit

(S//SI//REL TO USA, NLD) Some other notes:

- The Dutch do not have red or blue teaming yet
- AIVD is concerned with espionage, not crime
- The Dutch are working toward having only one IP point where all government agencies touch the internet, because this will be easier to monitor/defend
- 80 percent of NSA tools used to find malware are commercial, while 100 percent of Dutch tools are
- In the cyber realm, there is no ONE government agency in charge yet, but it will eventually be the NCSC
- There is still no cable access yet, but the laws may be changed in the next year or two. However, Dutch lawyers believe that they can tap it now if it is for DEFENSIVE measures only

Webfora and the Onion Router (TOR) (U)

(S//SI//REL TO USA, NLD) The web forum discussion was of greater interest. The Dutch provided an overview of their data presentation tool (at a very high level). They acquire mySQL databases via CNE access. [redacted] They're looking at marrying up the forum

TOP SECRET//SI//REL TO USA, NLD

Deel van het verslag van het gesprek tussen de NSA en de AIVD. Delen van dit stuk zijn door *NRC Handelsblad* zwartgemaakt om te voorkomen dat informatie over werknemers van de inlichtingendiensten of operationele geheimen bekend worden. Meer van dit document staat op nrc.nl.

Spanning voor Plasterk stijgt

Achtergrond
Politiek

Zelfs de eigen PvdA van Ronald Plasterk is sceptisch over de werkwijze van de inlichtingendiensten. De roep om parlementair onderzoek zwelt aan.

Door onze redacteur
Tom-Jan Meeus

DEN HAAG. Minister Ronald Plasterk (Binnenlandse Zaken, PvdA) krijgt van de coalitiefracties nog altijd het voordeel van de twijfel. Dat is het goede nieuws voor hem. Evengoed zwelt de kritiek ook in die kringen aan. En dus de twijfel.

De opmerkelijkste reactie komt van de PvdA. Plasterks eigen partij noemt de bevindingen van deze krant over het opereren van de inlichtingendiensten „uitermate zorgelijk", aldus Jeroen Recourt, een oud-rechter.

Recourt betwijfelt of de diensten binnen de wet blijven wanneer ze inbreken in internetfora en vervolgens de gegevens van alle deelnemers verzamelen.

De diensten lijken in zijn ogen een elementair principe te overtreden: ze worden geacht informatie te verzamelen over verdachten; ze mogen geen informatie inwinnen om zo verdachten te vinden. Deze 'sleepnet-methode' is om die reden eerder door toezichthouder CTIVD verworpen.

De werkwijze van de diensten „lijkt me een stap te ver", zegt Recourt daarom, al wil hij de uitleg van Plasterk afwachten voordat hij een definitief oordeel geeft.

Plasterk heeft in reactie op het NSA-schandaal verscheidene malen benadrukt dat de Nederlandse diensten de wet naleven. Hij herhaalde dit deze week in de Kamer.

Plasterk zei bovendien op de hoogte te zijn van alle methoden waarmee de AIVD mogelijke gevaren voor de democratische rechtsorde bestrijdt. „Alles wat bij de AIVD bekend is, daar kunt u vanuit gaan, is dat ook bij mij", zei de minister donderdag in de Kamer.

Maar in de Kamer, ook bij de coalitiefracties, groeit de scepsis over het opereren van de diensten. „Ik maak me er zorgen over", zegt Recourt (PvdA). Ook de woordvoerder van coalitiegenoot VVD, Klaas Dijkhoff, vindt dat Plasterk iets uit te leggen heeft. Hij kan zich voorstellen dat sommige webfora „gericht" worden onderzocht om „bepaalde mensen" te vinden. „Dat doet justitie met kinderporno ook."

Maar ongericht zoeken in de hoop verdachten te vinden is ook voor hem dubieus. „Als de CTIVD de juridische houdbaarheid betwist, is dat iets dat we moeten bespreken", zegt Dijkhoff, een oud-universitair docent recht.

De oppositie is al langer sceptisch over Plasterk in deze zaak. Gerard Schouw (D66), die eerder vergeefs onderzoek vroeg, en Ronald van Raak (SP) roeren zich het meest, gesteund door Voortman (GroenLinks).

Nu groeit ook de scepsis bij partijen als ChristenUnie en CDA. Gert-Jan Segers (ChristenUnie) ziet parallellen met de enquête-Van Traa in de jaren negentig naar de opsporingsmethoden van de recherche. „Enthousiaste onderzoeksmensen die hun boekje te buiten gaan." Ook toen ontbrak de controle. Segers voelt voor eigen parlementair onderzoek. „Dit kan wel eens uitlopen op Van Traa II."

Ronald van Raak (SP) zegt dat de vertrouwensvraag op tafel ligt. „Als dit waar is", zegt hij, „heeft de minister onwaarheid gesproken of hebben de diensten hem niet geïnformeerd. Allebei is onaanvaardbaar."

Gerard Schouw van D66 gaat er na het debat deze week vanuit dat Plasterk bekend was met de nu gebleken opsporingsmethode. Daarmee heeft de minister „een probleem". Het feit dat Plasterk en zijn voorgangers niet handelden na kritiek van de CTIVD op dit type opereren van de diensten, moet de minister worden aangerekend, vindt hij. „Dit opent de deur naar een enquête", zegt hij.

Voor Plasterk zijn de komende dagen cruciaal. Als hij zijn eigen partij of de VVD niet weet te overtuigen van de rechtmatigheid van het werk van de diensten, kan hij de politieke greep op de zaak verliezen. De spanning stijgt, de uitkomst is nog onbekend.