# De wind van Snowden in de Amerikaanse informatieparaplu

*Axel Arnbak en Joris van Hoboken**

Een positief effect van alle commotie rondom inlichtingenprogramma's als PRISM, Tempora en Dropmire, is dat het publieke debat over transnationale surveillance via '*cloud computing*' naar een hoger niveau is gebracht.[1] In het afgelopen jaar was er al de landelijk media-aandacht rondom mogelijke Amerikaanse toegang tot de gegevens van het biometrische paspoort en het EPD. Minister Schippers kon toen nog wegkomen met haar verbijsterende opmerking op het NOS journaal dat 'Amerikaanse inlichtingendiensten de medische privacy van Nederlandse patiënten zullen respecteren'. Dat de inlichtingendiensten weten welke ministers op kerstavond hun psycholoog bezoeken is ondertussen een realistischer scenario.

Tijdens de recente hoorzitting over PRISM in de Tweede Kamer werd de zaak vanuit andere hoek gebagatelliseerd. Na de bijdrage van de auteurs claimde een Nederlandse vertegenwoordiger van Google dat het op geen enkele wijze betrokken was bij deze programma's van de NSA en dat Google direct noch indirect toegang gaf tot gegevens van klanten aan de overheid. Meerdere Kamerleden vroegen zich hardop af of hij dat daadwerkelijk zelf geloofde en hoe waarschijnlijk het was dat hij zou afweten van dergelijke samenwerking. Kort nadien werden nieuwe documenten openbaar, waaruit zou blijken dat de NSA zelfs apparatuur heeft staan bij Google en andere internetgiganten.[2]

Met de aanhoudende onthullingen over de verwevenheden van internetbedrijven met de '*intelligence community*' in de VS staat de steeds verdere privatisering van surveillance in ieder geval stevig op de politieke agenda. De onthullingen maken duidelijk hoe vergaand het internet is verworden tot instrument in machtspolitieke strijd en nationale veiligheidsagenda's. Het internet, gedomineerd door Amerikaanse bedrijven en de uitwisseling van massaal getapte gegevens uit de cloud, is deel van de '*information umbrella*,' waarvan Libicki in 1998 de waarde al beschreef voor de dominantie van de Verenigde Staten.[3] Het zou goed zijn de al eerder bekritiseerde claim op de internetvrijheidsagenda van de Amerikanen sinds Hillary Clinton in de komende tijd nog eens wat kritischer te bezien.

De onthullingen van klokkenluider Snowden werpen ook nieuw licht op de relatie van transnationale surveillance met een andere beleidsdiscussie, namelijk cybersecurity. De intrigerende relatie tussen de bulk interceptie van internetcommunicatie op het niveau van internationale optische (zee)kabels – zoals het Tempora-programma van de Britse GCHQ – en encryptie is nog nauwelijks besproken. Speculaties rondom het bestaan van bulk surveillance via zeekabels worden meestal getemperd met het argument dat veel van de onderschepte de communicatie vanwege encryptie onbruikbaar zou zijn. Veel commerciële cloud-aanbieders bieden inderdaad middels SSL/TLS-certificaten versleutelde communicatie aan voor allerlei soorten datatransport, zoals HTTPS (browsen) en SMTP (e-mail).

Het zou in het patroon van Snowden's onthullingen passen als een volgend lek licht zou werpen op de mogelijke systematische bevraging van encryptiesleutels, ofwel bij Certificaat Autoriteiten (CA) – denk aan Verisign, Comodo en DigiNotar – ofwel direct bij internetbedrijven.[4] Zo kan de op het eerste oog (middels het slotje in de browser) versleutelde communicatie wel degelijk ontsleuteld worden. De gelekte minimalisatieprocedures door de NSA ingeval van 'toevallige bijvangst' van de communicatie van Amerikanen geven inzicht in de interesses van de NSA.[5] Versleutelde data kan onbeperkt worden opgeslagen voor verdere analyse van de inhoud en allerlei andere doeleinden, zoals het ontdekken van nieuwe kwetsbaarheden in software ('*zero-day exploits*') voor cyberoorlogsvoering. Misschien lezen we dus binnenkort meer hierover in de kranten. Wij zullen ons in elk geval geen illusies maken over de ambities en capaciteiten van inlichtingendiensten, mede in de wetenschap dat Amerikaans recht aan deze scenario's niet in de weg staat.

Het is ondertussen van vitaal belang om te weten of en in hoeverre de encryptiesleutels voor communicatie gedeeld worden met inlichtingendiensten. Niet alleen voor burgers, maar ook voor bedrijven, maatschappelijke organisaties en overheden. Zowel de NSA als de Britse GCHQ nemen immers de ruimte voor politieke en economische surveillance en spionage, naast de bescherming van de nationale veiligheid.

Het is bemoedigend dat een brede Kamermeerderheid de inlichtingendiensten-toezichthouder CTIVD opdraagt de rol van AIVD en MIVD in het besprokene te onderzoeken. En er zijn vergelijkbare ontwikkelingen op Europees niveau en in onze buurlanden. Gezien de complexiteit van de materie zal dit een kwestie worden van de lange adem, maar de grondigheid wordt op de langere termijn doorslaggevend. Het ligt misschien niet voor de hand dat de door Snowden opgestoken wind de Amerikaanse informatieparaplu zal wegblazen, maar het maar laten voortduren van de aan het licht gebrachte massale schending van grondrechten in onze informatiesamenleving is wat ons betreft uitgesloten.

* A.M. Arnbak, L.L.M. en dr. J.V.J. van Hoboken zijn onderzoekers aan het Instituut voor Informatierecht (IViR), Universiteit van Amsterdam.

1 J.V.J. van Hoboken, A.M. Arnbak, and N.A.M. Van Eijk, 'Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad', PLSC 2013.

2 Washington Post, NSA slides explain the PRISM data-collection program, 29 June 2013.

3 M.C. Libicki, 'Information War, Information Peace,' *Journal of International Affairs*, 51/2, maart 1998. Zie ook A. Schmidt, The Unfolding of the Information Umbrella, Netdefences.com, 10 June 2013, http://bit.ly/1cDurQ4.

4 H. Asghari, M.J.G. van Eeten, A.M. Arnbak, and N.A.N.M. van Eijk, 'Security Economics in the HTTPS Value Chain', p. 27 e.v., WEIS 2013, 3 June 2013, http://bit.ly/1aRCsUY.

5 The Guardian, 'Procedures used by NSA to minimize data collection from US persons: Exhibit B – full document', Section 5(2), 20 June 2013, http://bit.ly/11Qj6Hm.