Nederland als internetdokter tussen cybergrootmachten

Faciliteer een veilige en vrije IT-infrastructuur passend bij onze structurele culturele, economische en politieke belangen

Axel Arnbak

Al jaren roepen privacy- en beveiligingsexperts dat internetbeveiliging en digitale grondrechten goed ziek zijn. Maar zonder de onthullingen van klokkenluider Edward Snowden en de samenwerking met journalisten als Glenn Greenwald zou de wereld nog steeds in een staat van collectieve verdoving verkeren. Sinds juni 2013 is eindelijk een wereldwijde diagnose gestart dankzij de continue stroom aan onthullingen over afluisteroperaties door westerse inlichtingendiensten. Volgens Greenwalds nieuwe boek *No Place to Hide* zijn we pas op de helft. Hoe ziek is de patiënt en kan een klein land als Nederland hem genezen, te midden van cybergrootmachten als de VS, het Verenigd Koninkrijk, Rusland en China? En heeft Nederland daar belang bij?

Westerse inlichtingendiensten hebben decennialang onder het mom van nationale veiligheid onopgemerkt iedere uithoek van het internet gesaboteerd en afgeluisterd. Er al veel gezegd over Prism, het innige huwelijk tussen de Amerikaanse inlichtingendienst NSA en grote Amerikaanse technologiebedrijven. Minder bekend zijn programma's als Incenser, Shelltrumpet en Fairview; sleepnetoperaties die triljarden 'data records' binnenslepen op kritieke internetknooppunten. Daarnaast zijn routers, standaard internetprotocollen en zelfs games als Angrybirds gehackt om mee te luisteren, met alles en iedereen. De afluister- en hacklust van inlichtingendiensten manifesteert zich als het krachtigste virus voor internet.

Waarom alles afluisteren? Vorige week onthulde Greenwald honderden nieuwe operaties en de nieuwe strategie van de NSA: 'sniff it all, analyse it all, know it all'. Zeer recentelijk hebben meerdere toezichtsrapporten in de VS bevestigd dat massale, ongerichte surveillance niet helpt. Ouderwets maatwerk wel, zoals direct reageren op tips over de Nigeriaanse 'onderbroekenterrorist' van zijn eigen vader, of van de Russische diensten over Tsarnaev en de Boston Marathon. 'Know it all' gaat daarentegen om politieke spionage en bedrijfsspionage. Politieke toppen, oliemaatschappijen en veel meer — vrijwel al uw informatie, omdat het kan.

Minister Ronald Plasterk praat met een deelnemer van een 'hackathon', een bijeenkomst van software- en websiteontwikkelaars. FOTO: ANP

Is de patiënt terminaal ziek of zijn er nog behandelingen mogelijk? En wat is nu de rol van een klein land als Nederland? Serieuze bedrijven en overheden vertrouwen belangrijke gegevens niet meer toe aan internetcommunicatie, laat staan aan cloudopslag.

De afluister- en hacklust van inlichtingendiensten manifesteert zich als het krachtigste virus

Die vertrouwenscrisis is ernstig en corrumpeert alle voordelen die het internet biedt. Toch biedt ze kansen voor Nederland. Nu zelfs in democratische landen het internet in een staat van totale surveillance verkeert, hunkert de wereld naar een robuuste, veilige en vrije IT-infrastructuur.

Nederland heeft alles in huis om zich internationaal te onderscheiden als een betrouwbare 'haven': een geografische ligging als internetknooppunt voor hoge breedbandsnelheden, vestiging van internationale internetinstituties, een gigantische hosting- en app-industrie, mondiaal leiderschap op belangrijke dossiers als netneutraliteit en 'responsible disclosure', een vroeg begonnen cybersecuritycentrum, sterke wetenschappelijke en maatschappelijke instituties, een bloeiende internetcultuur en een relatief stabiel politiek en juridisch vestigingsklimaat.

Maar de politieke daden blijven vooralsnog achter. Het is verontrustend dat er geluiden opgaan Nederlandse diensten, net als de NSA in Amerika, de bevoegdheid te geven ongericht alle internetverkeer te monitoren. Het is tijd voor originelere, effectievere behandelmethoden van de patiënt, die zich distantiëren van de ziekteoorzaak. Nederland moet eindelijk werk maken van meldplichten voor beveiligingslekken. Stevige zorgplichten zijn nodig voor de veiligheid van hard- en software, vooral wanneer er sprake is van aanzienlijke marktpenetratie. Bedrijven als Microsoft en Cisco hebben een door wetgevers vrijwel ongestoord miljardenimperium kunnen opbouwen en werken nauw samen met de NSA. Nederlandse consumenten, bedrijven en overheden moeten als volstrekt afhankelijke afnemers internetbeveiliging en privacy terugverlangen. Steviger inzetten op encryptieverplichtingen voor internetserviceproviders vormt een effectief medicijn tegen sleepnetsurveillance. Daarnaast kan de overheid middelen vrij maken voor onafhankelijk beveiligingsonderzoek van vrije, open software — zoals OpenSSL dat met Heartbleed onlangs wereldnieuws was. Daarmee kan Nederland internationaal leiderschap en visie tonen.

Al eeuwen kent Nederland een relatief vrije informatiecultuur en vertrouwt de rest van de wereld informatie aan ons toe. Het is tijd die eeuwenoude combinatie van idealisme maar vooral ook pragmatisme te vertalen naar de 21ste eeuw. Er zal zich geen betere aanleiding voordoen dan de onthullingen van Snowden.

Waar we nu nog de diagnose aan het stellen zijn, zal de Eerste Kamer over een aantal maanden de zieke patiënt behandelen — bijvoorbeeld bij de herziening van de Wet op de inlichtingen- en veiligheidsdiensten 2002. Staat deze 'chambre de réflection' toe de patiënt met nog meer surveillance- en hackbevoegdheden zieker te maken? Er is een alternatief dat beter aansluit bij structurele culturele, economische en politieke belangen van Nederland: garandeer een robuuste, veilige en vrije IT-infrastructuur; maak van Nederland de internetdokter tussen cybergrootmachten.

Axel Arnbak is onderzoeker cybersecurity en informatierecht, Universiteit van Amsterdam en research fellow, Berkman Center, Harvard University. Dit artikel is een verkorte bewerking van een lezing in de Eerste Kamer tijdens de expertbijeenkomst 'Cyberintelligence en publiek belang' op 6 mei jl.