HANDELSOORLOG

Cybersecurity dekmantel voor digitale boterberg

Axel Arnbak

Voor liefhebbers van geopolitiek, technologie en romige boterbabbelaars is het weer volop smullen deze zomer. Onlangs deed de Chinese overheid een aantal Amerikaanse bedrijven in de ban, zoals beveiligingssoftwaregigant Symantec, voor de levering van antivirus aan de overheid. Ook adviseerde ze Chinese banken IBM niet langer te vertrouwen. Vorig jaar al bestempelde het Amerikaanse Congres Chinese telecomgiganten als onveilige leveranciers voor de Amerikaanse overheid en landelijke ICT-infrastructuur. Voor de bühne beroepen beleidsmakers zich aan weerszijden op nationale veiligheid en 'cybersecurity', zoals internetbeveiliging in Amerikaanse beleidskringen heet. Achter de schermen speelt een ordinaire handelsoorlog. Iedereen heeft boter op het hoofd en reële internetbeveiliging is het kind van de rekening.

De nationaliteit van een bedrijf is geen garantie voor internetbeveiliging. De Amerikaanse en Chinese overheid weten donders goed dat informatieknooppunten en -koeriers al eeuwenlang het mikpunt zijn van buitenlandse inlichtingendiensten. Caesar schreef zijn opdrachten aan veldheren al in een door hem ontwikkelde geheimtaal. Door de post van de Franse ambassadeur te onderscheppen, ontdekte stadhouder Willem III in 1684 de steun van Amsterdamse kooplieden voor een Franse invasie.

Vandaag de dag kun je soft- en hardware ook nog eens hacken van een afstandje, zonder dat de informatiekoerier het zelf doorheeft. In maart onthulde The New York Times operatie Shotgiant van de Amerikaanse inlichtingendienst NSA. Blijkbaar infiltreert de NSA het Chinese telecombedrijf Huawei sinds 2007. Eerst om de banden met de Chinese inlichtingendienst te onderzoeken, later om mee te kunnen luisteren met alle communicatie die het Chinese bedrijf wereldwijd verzorgt. Iedereen hackt iedereen.

Stel je internetbeveiliging centraal, dan is het onderliggende probleem dat een kleine groep grote bedrijven de basistechnologie levert van onze communicatienetwerken. De werking van die basistechnologie wordt doorgaans geheimgehouden. Zolang de werking niet transparant is, kun je als afnemer niet weten wat die technologie uitspookt.

Voor het grote publiek is geheime technologie, en de afhankelijkheid daarvan, meestal een verrassing. Neem het Nederlandse mobiele internet. Het precieze getal is onbekend, maar je hoort vaak dat 90% van het verkeer wordt afgehandeld door Huawei-apparatuur, zoals zendmasten en routers. Lekker goedkoop, maar of de spullen en de broncode veilig zijn, laat staan of Chinese of Amerikaanse inlichtingendiensten meeluisteren: niemand die het weet. Gegeven deze afhankelijkheid van Huawei en de Shotgiant-onthulling, komt de wens om KPN vanwege nationale veiligheid te beschermen tegen een overname door América Móvil ietwat onbeholpen over. Aangezien andere kritieke infrastructuren als die van water, elektriciteit en zorg eenzelfde ICT-afhankelijkheid kennen, is het probleem niet beperkt tot telecom.

Caesar schreef zijn opdrachten aan veldheren al in een door hem ontwikkelde geheimtaal

Na al dit protectionistische geboterbabbel, wordt het tijd om volwassen te worden. Neem je internetbeveiliging serieus, verklein dan je afhankelijkheid. Niet via handelsembargo's of 'Europese clouds', maar door effectieve maatregelen. Kies voor open-sourcesoft- en -hardware, of eis volledige inzage in de technologie van leveranciers op straffe van aansprakelijkheid. Heb je hoge beveiligingseisen, stel jezelf dan in staat om het gekochte vlees te keuren, in plaats van ICT-leveranciers te geloven op hun blauwe ogen. En versleutel informatie en communicatie met openbaar gepubliceerde encryptietechnieken. Al helemaal als je gebruikmaakt van andermans netwerken en serverparken.

Slimme ondernemers zullen profiteren van het gat in de markt voor open-sourcesoft- en -hardware. Nederlandse beleidsmakers moeten zich realiseren dat open source voor nationaliteit dient te gaan. OpenSSL, de open encryptietechnologie, draait al jarenlang op een te krap budget. Met een noodfonds voor open internetbeveiliging maakt Nederland een goede beurt en geeft het gestalte aan rationeel beleid te midden van cybergrootmachten: maak het internet niet kwetsbaarder voor aanvallers, maar veiliger voor iedereen. Voor internetbeveiliging zijn transparantie, onafhankelijkheid en redundantie cruciaal. Internetprotectionisme onder het mom van nationale veiligheid en 'cybersecurity' creëert alleen maar digitale boterbergen.

Axel Arnbak is onderzoeker cybersecurity en informatierecht aan het Instituut voor Informatierecht van de UvA en het Berkman Center, Harvard University.