

# Eerste Kamer moet wetsvoorstel over hacken door politie opschorten

Hacken verenigt telefoontap, huiszoeking en heimelijke observatie in één digitale variant



**Axel Arnbak**

Zonder specifieke wettelijke bevoegdheid hacken Nederlandse opsporingsdiensten computers in binnen- en buitenland. In ieder geval sinds het Bredolab-incident in 2010. Even lang al probeert het ministerie van Veiligheid en Justitie een wet langs de Staten-Generaal te loodsen die deze inzet van overheidsdwang moet legaliseren. Iedereen vindt dat internet-criminaliteit moet kunnen worden aangepakt en toch stuit de voorgestelde hackbevoegdheid al jaren op stevige kritiek uit alle hoeken van de samenleving.

Tot veler frustratie hielp coalitiepartner PvdA eind 2016, vlak voor de verkiezingen, de VVD als nog aan een meerderheid in de Tweede Kamer voor de hackwet. Nu moet de Eerste Kamer constitutionele chocola maken van de controversiële wet. Juist de senaat, de grondrechtenwaakhond van ons staatsbestel, moet het hoofd koel houden en de hackbevoegdheid pas goedkeuren als het kabinet de talloze onbeantwoorde vragen en aanzienlijke bezwaren wegneemt.

Op het eerste gezicht klinkt het logisch de politie een hackbevoegdheid toe te kennen, vooral gelet op soms geavanceerde en vaak weerzinwekkende vormen van cybercrime. Maar de hack-

bevoegdheid is een ongekend verregaande vorm van overheidsdwang. Hacken verenigt namelijk de telefoontap, huiszoeking, heimelijke observatie, infiltrant en zo'n beetje het hele analoge arsenaal van de politie in één digitale equivalent. Politiek en samenleving debatteren dus scherp over de impact op individuele privacy, collectieve cybersecurity en geopolitieke verhoudingen.

De principiële privacybezwaren zijn evident en het kabinet deed hier en daar al wat water bij de wijn. Toch blijft het universele karakter van de hackwet problematisch voor het parlementaire debat. Want hoe verhoudt de hackwet zich tot haar fysieke evenknieën? En is het, in lijn met de voorstellen van de Tilburgse hoogleraar Bert-Jaap Koops, niet tijd voor een nieuw digitaal huisrecht voor computersystemen en clouds, waarin administratie, brieven en fotoboeken handig bij elkaar staan opgeslagen? Eén hack kan alle digitale kroonjuwelen ineens prijsgeven.

Het Wetboek van Strafvordering heeft zich in twee eeuwen ontwikkeld tot een elegante catalogus, waarbij per dwangmiddel

**Politie heeft met een hackwet belang bij kwetsbare ICT-systemen**

de privacy-schending en waarborgen genuanceerd zijn afgewogen. Voor zulke vragen heeft de Eerste Kamer onvoldoende tijd. Rechters, die de inzet van hacken in individuele gevallen vooraf moeten goedkeuren, klagen terecht dat het aan tijd en budget ontbreekt om die taak te vervullen. De Raad voor de Rechtspraak pleit dan ook voor een nieuw toezichtsorgaan dat de inzet van de hackbevoegdheid naast individueel ook integraal toetst.

De impact van de hackwet op cybersecurity is zowel fascinerend als zorgelijk. De samenleving kan niet zonder veilige ICT, maar de politie heeft met een hackwet belang bij kwetsbare systemen. De Amerikaanse overheid ligt op dit gebied al jaren in de clinch met Apple en WhatsApp, omdat de iPhone en de app de cybersecurity van burgers 'te goed' beschermen. Inmiddels kun je als hacker meer dan \$ 1 mln verdienen door een nog onbekende kwetsbaarheid in het besturingssysteem van de iPhone te ontdekken en te verkopen aan digitale wapenhandelaren. Zij maken vervolgens peperdure hackingtools voor onze politie. Zo stimuleert de hackwet een cultuur van onveiligheid.

De geopolitieke dimensie is nog ingewikkelder. Net als analoge wapenhandelaren leveren digitale collega's hun waar vaak aan onfrisse regimes. Zo publiceerde WikiLeaks al in 2014 dat

ILLUSTRATIE: HEIN DE KORT VOOR HET FINANCIËLE DAGBLAD

de Nederlandse politie dezelfde FinFinsher-spyware heeft ingekocht als kwade regimes in Bahrein, Pakistan en Oeganda. De hackwet verbiedt het inkopen van kwetsbaarheden, maar zegt niets over zakendoen met kwetsieuze wapenhandelaren. Daarnaast bevat de hackwet geen verbod op hacken over de grens. Behalve als een schending van soevereiniteit, zien China, Rusland en Iran de hackwet ook als uitnodiging hier te komen hacken. Activisten en R&D-intensieve bedrijven zijn daar niet bepaald blij mee.

De Eerste Kamer heeft dus nog een stevig debat over de wenselijkheid en de uitvoerbaarheid van de hackwet te voeren. In de Tweede Kamer kon de wet nog overleven dankzij politieke opportuniteit. De Eerste Kamer doet er goed aan de hackwet op te schorten, totdat de essentiële vragen en aanzienlijke bezwaren zijn geadresseerd.



**Axel Arnbak** is advocaat bij De Brauw Blackstone Westbroek en onderzoeker aan het Instituut voor Informatierecht (UvA). Reacties: @axelarnbak. Dit artikel is een verkorte bewerking van een lezing in de Eerste Kamer tijdens de 'Deskundigenbijeenkomst privacy' op 20 juni a.s.