# Reactie op Wetsvoorstel computercriminaliteit III

Matthijs Koot, 29 juni 2013

De hackbevoegdheid is een ingrijpend, zwaar opsporingsmiddel. Bij onze open democratie hoort terughoudendheid bij het toekennen van nieuwe opsporingsbevoegdheden. In de mij bekende informatie, waaronder de MvT, mis ik de onderbouwing voor het toelaten van een nieuwe opsporingsbevoegdheid voor verdenkingen op het brede Artikel 67 Sv. In 2008 was er een zaak waarin verspreiding van illegale navigatiesoftware als "ernstige inbreuk op de rechtsorde" werd gezien en waarbij daardoor telefoontaps waren toegestaan. Mij lijkt evident dat verspreiding van illegale software geen grond kan zijn voor inzet van hackbevoegdheid. Het huidige wetsvoorstel staat dat wél toe. Deskundigen waaronder Ronald Prins en prof. Bart Jacobs stellen dat de hackbevoegdheid vooral wenselijk is voor bestrijding van botnets en aanvallen op vitale infrastructuur. Daar sluit ik me bij aan.

Bij de hackbevoegdheid heb ik nog een reeks andere bedenkingen: hoe wordt het planten van vals bewijs voorkomen? Bij de tapbevoegdheid zijn immers gevallen bekend dat er tapverslagen zijn vervalst/gemanipuleerd --- bijvoorbeeld in de zaak-Baybasin. Verder vraag ik me ook af: gaat buitenland straks ook inbreken in Nederlandse computers en policeware achterlaten? is dat dan ook alleen voor verdenking zware terrorisme/kinderpornodelicten of ook voor copyrightschending, *libel* en godslastering? Hoe herkent Nederland policeware van buitenlandse opsporingsdiensten als zodanig, en wordt voorkomen dat wij interfereren met een lopend onderzoek van een buitenlandse rechtsmacht? Hoe herkennen buitenlandse opsporingsdiensten Nederlandse policeware als zodanig? Wordt de policeware ingekocht (FinFisher?) en zo ja, hoe weet je dan dat die geen achterdeurtjes bevat en bij elke update nog steeds integer is? Wie is verantwoordelijk voor schade/gevolgen als het Trojaanse politiepaard problemen veroorzaakt in een ziekenhuis, elektriciteitscentrale of een spionagegevoelig bedrijf? Antivirusbedrijven claimen niet mee te zullen werken. Gaat de Nederlandse overheid dus de race aan met antivirusbedrijven? (toegegeven: momenteel makkelijk te winnen) En, *last but not least*, zoals BOF zich afvraagt: "Als overheden op de hoogte zijn van het bestaan van kwetsbaarheden in computers, zijn er dan situaties denkbaar waarin zij die kennis geheim moeten houden omwille van de opsporing? Hoe verhoudt dat zich tot de ambitie van de regering om de Nederlandse informatiesamenleving via overheidsorganisaties zoals het Nationaal Cyber Security Centrum (NCSC) te beschermen?"

Dan het decryptiebevel voor verdachten. Uit het TILT-rapport begrijp ik dat nemo tenetur geen absoluut principe is. Wel vraag ik mij af of het nu toelaten van de inbreuk er toe zal leiden dat de wetgevende en rechtsprekende macht meer geneigd zullen zijn die inbreuk uit te breiden naar lichtere verdenkingen dan terrorisme en gewoonte/beroep kinderporno. Dus: kan hier sprake zijn van een glijdende-schaal-effect? En ook: gaat het decryptiebevel, net als de hackbevoegdheid, langs de Centrale Toetsings Commissie?

Over de wijziging t.a.v. NTD: als een "tussenpersoon die communicatiedienst verleent in de doorgifte/opslag van gegevens van anderen" niet voldoet aan een NTD-bevel dan blijft deze strafbaar. Mijn primaire zorg bij deze wijziging is dat het mij de indruk geeft dat dit als drempel tegen klokkenluiden kan werken; niet iedere klokkenluider is immers voldoende technisch/juridisch onderlegd om dit te omzeilen. Mijn twijfel bij deze wijziging: is deze wijziging er vooral om ISP's bang te maken of is het ook echt aannemelijk dat deze daadwerkelijk worden vervolgd?

Mij is duidelijk dat het wetsvoorstel in huidige vorm zonder aanvullende onderbouwing niet acceptabel is.