# Veiligheid versus privacy: een valse tegenstelling

Maakt een nee-stem tegen de Wet inlichtingen- en veiligheidsdiensten (Wiv) de samenleving onveiliger? Voorstanders van de nieuwe wet zeggen zonder voorbehoud "ja". Maar wij, cybersecurityonderzoekers, computerwetenschappers en security professionals, plaatsen bij die stelligheid vraagtekens.

Het publieke debat over de nieuwe Wiv vinden wij te simpel geframed: veiligheid versus privacy. Ben je voor veiligheid dan stem je "ja"; vind je privacy van groter belang, dan stem je "nee". Dat de nieuwe wet zelf veiligheidsrisico's creëert past niet in dit frame, maar dit is helaas toch waar. Deze risico's moeten worden meegenomen in het debat en vertaald naar juiste afwegingen in de wet.

Het eerste veiligheidsprobleem wordt gevormd door de uitgebreide hackbevoegdheid die de diensten toestaat om via onbekende kwetsbaarheden binnen te dringen op apparatuur en in netwerken. Deze kwetsbaarheden hoeven zij niet te melden bij de producenten en ontwikkelaars van de apparatuur of software. Door dit stilhouden blijft niet alleen het spionagedoelwit kwetsbaar maar ook talloze burgers in binnen- en buitenland. De kans is reëel dat anderen van diezelfde kwetsbaarheid gebruik maken voor andere doeleinden. Cybercriminelen en minder frisse inlichtingendiensten zullen ofwel zelf de kwetsbaarheid vinden ofwel de databank van de diensten hacken om deze informatie te stelen. De meerdaagse cyberaanval op de containerterminal in de Rotterdamse haven van afgelopen zomer wordt in verband gebracht met informatie over kwetsbaarheden die eerder bij de Amerikaanse dienst NSA is buitgemaakt. Het niet melden van kwetsbaarheden is een gevaar dat ernstige economische schade veroorzaakt en moeilijk te verenigen is met de veiligheidstaak van de diensten. Het gebruik van kwetsbaarheden in apparaten en software door de overheid kan ook nieuwe kwetsbaarheden veroorzaken. In Duitsland heeft men dit ondervonden met de Bundestrojaner: opsporingssoftware die de Duitse overheid in het geniep plaatste op computers van verdachten, maar waarvan de controle gemakkelijk door derden was over te nemen. Dit veiligheidsrisico wordt versterkt door een nieuwe bevoegdheid in de Wiv. De wet staat de diensten toe om de apparaten van derden te hacken die zelf geen doelwit van de diensten zijn. Het gaat dan om apparaten die met een doelwit in verbinding staan, bijvoorbeeld de netwerkapparatuur die door een systeembeheerder wordt onderhouden. Personen met een sleutelrol binnen de IT, zoals systeembeheerders, worden door de toevoeging van overheidssoftware nog kwetsbaarder voor aanvallen van buitenaf.

Het tweede veiligheidsprobleem houdt verband met de bulkinterceptie, het fenomeen waaraan de nieuwe wet zijn bijnaam dankt: de sleepwet. Om het dataverkeer in bulk van de kabel op te pikken worden tappunten in het netwerk aangebracht. Binnen de cybersecurity is ieder tappunt een extra kwetsbaarheid. Hoe weten we zeker dat hackers niet ook van die taps gebruik maken? Bovendien kleven aan de opslag van de in bulk verworven data zwaarwegende veiligheidsrisico's, want die bergen data zijn ook voor andere spionnen en cybercriminelen een goudmijn. Met welke mate van zekerheid kunnen de Nederlandse diensten het niet lekken van deze data garanderen? De dreiging van datalekken wordt groter nu de opgeslagen bulkinformatie (ook zonder dat ernaar gekeken is) gedeeld mag worden met buitenlandse diensten. Dit gaat Nederland naar alle waarschijnlijkheid doen met o.a. de Britten en de Amerikanen. Beide landen hebben echter een rijke geschiedenis van datalekken bij de overheid. Data delen met deze landen is dus niet zonder veiligheidsrisico voor Nederland.

Daarnaast wordt steeds meer communicatie effectief versleuteld en metadata wordt gemaskeerd, zeker door criminelen en (potentiële) terroristen. Hierdoor vult het sleepnet zich al snel met data van willekeurige burgers. Dit geeft overheden met een sleepnet de prikkel om beveiligingstechnieken zoals end-to-end versleuteling en VPN's te verbieden. We zien dit momenteel in China gebeuren. Deze technieken zijn echter broodnodig voor een veilig internet en het verbieden hiervan levert een groot beveiligingsrisico op voor burgers en de maatschappij.

Het derde veiligheidsrisico zit in het verlies van controle op het gebruik van de gedeelde bulkinformatie door buitenlandse diensten. Opgeslagen bulkinformatie, inclusief bijvangst, mag (ook zonder ernaar gekeken te hebben) gedeeld worden met buitenlandse diensten. Misbruik van gunsten door bevriende diensten is in de wereld van spionnen niet ongewoon. Zo verleende de Duitse dienst BND nietsvermoedend toegang aan de Amerikaanse dienst NSA tot haar databases in de strijd tegen het terrorisme. Later bleek dat die toegang werd misbruikt door de Amerikanen voor industriële spionage tegen Duitsland. De nieuwe toetsingscommissie (de TIB) noch de toezichthouder (CTIVD) kan controleren wat er buiten de landsgrenzen met onze gedeelde data gebeurt. Dit veiligheidsrisico verdient een plaats in het debat.

Tot zover een aantal veiligheidsgevaren van de nieuwe wet. Er zijn ook sterke aanwijzingen dat nut en noodzaak van het sleepnet in de strijd tegen terrorisme door de voorstanders worden overdreven. Er is geen bewijs dat ongerichte bulkverzameling en de geautomatiseerde (meta)analyse daarvan het meest geschikte middel is. Niet alleen biedt het geen uitkomst om de zogenaamde "lone wolves" eruit te vissen. Ook blijkt achteraf vaak dat aanslagplegers al bekend waren bij de geheime diensten. Met traditionele en gerichte tapbevoegdheden - waarover de Nederlandse geheime diensten reeds beschikken - zouden zij hen in het vizier moeten kunnen krijgen.

Uit onderzoek uitgevoerd door de New America Foundation naar de effectiviteit van bulkinterceptie bij meer dan 200 strafrechtelijke onderzoeken naar terrorismeverdachten in de Verenigde Staten bleek dan ook dat traditionele onderzoeksmethoden veelal de initiële drijfveer waren, denk aan het gebruik van informanten, tips van lokale gemeenschappen en gerichte surveillanceoperaties. Zelfs het Anderson review report roept scepsis op over de noodzaak van dit zeer ingrijpende middel in de strijd tegen terrorisme. Voorstanders van de wet citeren dit onderzoek omdat het het nut van bulkinterceptie door de Britse inlichtingendiensten aan zou tonen. Van de vijf onderzochte contraterrorisme-casussen - die de diensten zelf hadden aangedragen als succesvoorbeelden - bleek dat het sleepnet vooral toegepast werd in gevallen waarbij de uiteindelijke verdachten al deel uitmaakten van een bestaand terrorismenetwerk of contact hadden met doelwitten, waardoor gericht tappen hetzelfde resultaat zou hebben gehad. De noodzaak van bulkinterceptie is dus op z'n minst discutabel.

In de zoektocht naar veiligheid creëert de Nederlandse wetgever de bovenstaande veiligheidsrisico's. Deze moeten worden meegenomen in het debat dat helaas een stuk gecompliceerder is dan domweg privacy versus veiligheid. Was het maar zo simpel.

## De eerste ondertekenaars

Dr. Greg Alpar
Open Universiteit & Radboud Universiteit

Jaya Baloo

KPN

Erwin Bleumink
SURF

Prof.dr.ir. Herbert Bos
Vrije Universiteit Amsterdam

Stoffel Bos

Prorail

Dr. Fabian van den Broek
Open University

Prof. dr. Marko van Eekelen
Open Universiteit & Radboud Universiteit

Sacha van Geffen
Directeur Greenhost

Simon Hania

TomTom

Dr. Jaap-Henk Hoepman
Radboud Universiteit Nijmegen

Dr. Andreas Hülsing
Technische Universiteit Eindhoven

dr. Slinger Jansen
Universiteit Utrecht

Dr. Ir. Hugo Jonker
Open Universiteit

LLM Merel Koning
Radboud Universiteit Nijmegen

Prof. dr. Bert-Jaap Koops
Tilburg University

dr.ing. Matthijs Koot
Secura B.V. & Universiteit Amsterdam

prof. dr. Eleni Kosta
Tilburg University

Prof. Dr. Tanja Lange
Technische Universiteit Eindhoven

Michiel Leenaars
Director of Strategy NLnet Foundation

Rachel Marbus

KPN

Dr. Veelasha Moonsamy
Universiteit Utrecht

Adriana Nugter

Wireless Development Partners

Dr. Andreas Peter
Universiteit Twente

dr. Jean Popma
Radboud Universiteit Nijmegen

Prof. Dr. Aiko Pras
Universiteit Twente

Dr.ir. Rick van Rein
OpenFortress B.V.

Dr. Melanie R. Rieback
Radically Open Security B.V.

dr. ir. Roland van Rijswijk-Deij
Universiteit Twente

Dr. Christian Schaffner
Universiteit van Amsterdam

Dr. Peter Schwabe
Radboud Universiteit Nijmegen

Dr. Boris Skoric
Technische Universiteit Eindhoven

Prof. dr. Jan M. Smits
Technische Universiteit Eindhoven

Rogier Spoor
Honeypot programm, TCC

dr. Marco Spruit
Universiteit Utrecht

Dr. Erik Tews
Universiteit Twente

ing. Hans Van de Looy RCX
UNICORN Security

dr. Benne de Weger
Technische Universiteit Eindhoven

Dr. Philip R. Zimmermann
TU Delft Cybersecurity Group