Nederlandse politie koopt spyware van controversiële bedrijven (samenvatting II)

Overheid screent deze bedrijven in het geheel niet

Commerciële spyware bedrijven leveren ook aan repressieve regimes die het inzetten tegen oppositieleden, activisten en journalisten. Volgens de overheid koopt Nederland geen spyware van bedrijven die ook leveren aan dubieuze regimes en vindt er een screening van bedrijven plaats. In de praktijk stelt deze screening echter niets voor. De politie vertrouwt volledig op verklaringen van bedrijven dat zij niet leveren aan dubieuze regimes, maar doet geen eigen onderzoek.

Ook in andere opzichten is screening van leveranciers beperkt. Er vindt geen onderzoek plaatst naar de banden van bedrijven met nationale inlichtingdiensten, en hun belastingbeleid en exportbeleid. Ook vindt geen antecedentenonderzoek plaats naar mogelijke strafrechtelijke vervolging van functionarissen van bedrijven en tussenhandelaren.

De Nederlandse politie maakt de afgelopen jaren steeds vaker gebruik van spyware van commerciële bedrijven om laptops, computers, smartphones en andere gegevensdragers van verdachten binnen te dringen. De cybersurveillance industrie is controversieel, ondermeer vanwege de betrokkenheid van bedrijven bij mensenrechtenschendingen. In de loop der jaren zijn talloze voorbeelden bekend geworden van bedrijven die spyware leveren aan repressieve regimes die het inzetten tegen journalisten, activisten en oppositieleden. Het gaat daarbij ook om spyware van bedrijven die ook aan Nederland hebben geleverd, of waarin de Nederlandse overheid interesse had.

De Nederlandse overheid geeft geen openheid van zaken over van welke bedrijven spyware is aangeschaft. In de loop der jaren is

hierover echter het een en ander bekend geworden. Nederland heeft spyware afgenomen van ondermeer Gamma Group en de Israëlische NSO Group. De FinFisher spyware van Gamma Group is aangeschaft door onder andere het Egypte van Moebarak, Oeganda, Ethiopië, Turkije en Saoedi-Arabië, waar het is ingezet tegen onder andere journalisten, mensenrechtenactivisten en oppositieleden. NSO leverde haar Pegasus spyware aan onder meer Bangladesh, Egypte, Mexico, Marokko, Polen en Saoedi-Arabië.

Screening stelt niets voor

In het regeerakkoord 2017-2021 is vastgelegd dat leveranciers van hacksoftware die wordt ingekocht door opsporingsdiensten niet mogen leveren aan dubieuze regimes. In de praktijk is van een screening echter geen sprake. De politie doet geen eigen onderzoek en vraagt de bedrijven slechts om een verklaring dat zij niet leveren aan dubieuze regimes.

Het is echter niet duidelijk welke landen hiermee worden bedoeld. De Minister van Veiligheid en Justitie verklaarde meest recentelijk in december 2022 in antwoord op Kamervragen respectievelijk dat het ging om 'landen waartegen EU of VN-sancties bestaan' en 'landen die mensenrechtenschendingen begaan'. Volgens de Minister wordt deze toets periodiek herhaald. Uit rapporten van de Inspectie Justitie en Veiligheid blijkt echter dat dit in de praktijk niet gebeurt.

De Inspectie constateert ook dat de screening van leveranciers van spyware slechts bestaat uit het vragen van een verklaringen aan bedrijven dat zij niet leveren aan dubieuze regimes. De Inspectie maakt echter niet duidelijk of ze deze verklaringen ook heeft ingezien, en plaatst geen kritische kanttekeningen bij de gebrekkige screening van de leveranciers.

Cyber surveillance industrie controversieel

De politie vertrouwt dus volledig op de verklaringen van bedrijven dat zij niet leveren aan dubieuze regimes. De screening van bedrijven is ook in andere opzichten beperkt. Veel controversiële aspecten van de cybersurveillance industrie blijven volledig buiten beschouwing.

Commerciële leveranciers van spyware hebben vaak nauwe banden met de nationale inlichtingendiensten in de landen waar zij zijn gevestigd. De belangen van deze buitenlandse inlichtingendiensten komen vanzelfsprekend vaak niet overeen met Nederlandse belangen. Bij de screening van leveranciers van spyware wordt hier geen rekening mee gehouden. Hierdoor, en door de mogelijke aanwezigheid van backdoors in de spyware, is de nationale veiligheid in geding.

Er wordt ook geen onderzoek gedaan naar het belastingbeleid en exportbeleid van de bedrijven, hoewel dit wel op zijn plaats is. De meeste spyware bedrijven hebben namelijk ook vestigingen in belastingparadijzen en maken gebruik van offshore accounts, hetgeen belastingontduiking en mogelijk witwassen faciliteert. De bedrijven exporteren vaak ook via vestigingen in andere landen om exportbeperkingen te omzeilen.

Er vindt evenmin antecedentenonderzoek plaats naar mogelijke strafrechtelijke vervolging van functionarissen van bedrijven en tussenhandelaren. Functionarissen van spyware bedrijven zijn echter veroordeeld voor het betalen van steekpenningen, corruptie en zware georganiseerde criminaliteit of hiermee in verband gebracht.

In het onderzoek ‘Een Politie Black Box, het gebruik van spyware door de Nederlandse politie’ borduurt Buro Jansen & Janssen voort op eerdere onderzoeken van het Buro naar de cybersurveillance industrie en de relatie tussen de Nederlandse politie en leveranciers van spyware. Er is gebruik gemaakt van openbare bronnen, Woo-verzoeken en rapporten van de Inspectie Justitie en Veiligheid dat toezicht houdt op de uitvoering van de hackbevoegdheid door de Nederlandse politie.