Fox-IT in Rusland

Buro Jansen & Janssen

juni 2021

Fox-IT in Rusland

Observant #77 / juni 2021 Fox-IT in Rusland (pdf)

Onderzoek: Fox-IT in Rusland (pdf)

Fox-IT in Rusland

Het Delftse computer- en beveiligingsbedrijf Fox-IT verkoopt sinds 2010 haar producten in Rusland en is hier na de invoering van de internationale sancties tegen het land in 2014 mee doorgegaan. De Nederlandse overheid is een belangrijke klant van Fox-IT. Het bedrijf verzorgt onder andere de beveiliging van staatsgeheimen.

De Rus Evgeny Gengrinovich speelt een sleutelrol in de handel van Fox-IT met Rusland. Hij werkte in het verleden voor verschillende Russische staatsbedrijven. Vanaf 2011 promoot hij de Fox DataDiode namens het Zwitserse Snitegroup GmbH en het Russische ZAO NPF Simet. Later presenteert hij zich als vertegenwoordiger van Fox-IT en heeft hij een sleutelrol bij het aantrekken van andere tussenhandelaren.

De tussenhandelaren van Fox-IT hebben nauwe banden met Russische staatsbedrijven in de energiesector en de financiële sector, maar ook met het Russische Ministerie van Defensie, defensiebedrijven en de Russische inlichtingendienst FSB. Het Delftse bedrijf heeft in het algemeen weinig zicht op de eindgebruikers aan wie haar producten door tussenhandelaren worden aangeboden en doorverkocht.

Gengrinovich heeft zelf ook banden met defensie en de FSB. Zo deed hij van 2010 tot 2014 certificeringswerk voor de FSTEC (Federal Service for Technical and Export Control) en het Ministerie van Defensie. In september 2017 treedt hij als adviseur in dienst van het Russische informatiebeveiligingsbedrijf Infotecs. In 2018 wordt dit bedrijf op de Amerikaanse sanctielijst geplaatst vanwege haar banden met de Russische inlichtingendienst FSB.

Het NFI en TNO werkten met Fox-IT aan een Surveillance Lab in Saoedi-Arabië tijdens de Arabische Lente

In 2011, op het hoogtepunt van de Arabische Lente, werkte Fox-IT bij de voorbereidingen van een Surveillance Lab in Saoedi-Arabië samen met twee overheidsorganen: het NFI (Nederlands Forensisch Instituut) en TNO (Nederlandse Organisatie voor toegepast natuurwetenschappelijk onderzoek). Medewerkers van die organisaties zaten in de stuurgroep van het Saoedische project met als naam 'Forensic Lab', een landelijk netwerk van telefoon- en internetsurveillance.

Fox-IT en de Nederlandse overheid

Computer- en beveiligingsbedrijf Fox-IT werd in 1999 opgericht. De Nederlandse overheid werd al snel een belangrijke klant van het Delftse bedrijf. Daarnaast speelt Fox-IT een rol in de nationale veiligheid. Zo verzorgt het bedrijf de beveiliging van Nederlandse staatsgeheimen, zoals de notulen van de Ministerraad, en wordt het ingehuurd door onder andere de Nationale Politie en de ministeries van Buitenlandse Zaken, Defensie, en Justitie en Veiligheid.

De relatie tussen de overheid en Fox-IT was onderwerp van discussie in 2014, toen het Delftse bedrijf werd overgenomen door de Britse NCC Group. In de Tweede Kamer en de media werden vragen gesteld over het risico dat Nederlandse staatsgeheimen hiermee in buitenlandse handen kunnen komen. De vragen werden destijds opgeworpen, maar zijn eigenlijk nooit beantwoord. Het is natuurlijk ook de vraag of de Nederlandse overheid niet te afhankelijk is van het Delftse bedrijf.

Verantwoording

Dit onderzoek is gebaseerd op Wob-documenten, open bronnen, interne bedrijfsdocumenten en e-mails met betrekking tot de relatie van Fox-IT met haar partner, het Duitse bedrijf AGT (Advanced German Technology), die Buro Jansen & Janssen heeft ontvangen en documenten uit de Hacking Team hack. Het onderzoek borduurt voort op de onderzoeken 'Fox-IT in het Midden-Oosten' en 'Fox-IT en het Nederlandse exportbeleid voor dual-use goederen' en maakt deel uit van een breder onderzoeksprogramma van Buro Jansen & Janssen naar Westerse bedrijven en overheden en hun rol in de opbouw van de surveillance staat zowel in eigen land als in repressieve regimes zoals Rusland en landen in het Midden-Oosten.

In een e-mail en per brief heeft Buro Jansen & Janssen verschillende vragen gesteld aan Fox-IT (e-mail zit bij de documenten). Fox-IT heeft geen antwoord gegeven.

Fox-IT in het Midden-Oosten (2019)
Fox-IT en het Nederlandse exportbeleid voor dual-use goederen (2020)

Ears and Eyes: List of found surveillance devices

The States, according to their role of repression of individuals and groups doing subversive actions, put in place ways of keeping those individuals and groups under surveillance. It seems that some of this surveillance is done through the hiding of surveillance devices in the spaces we live in.

Maak het werk van Buro Jansen & Janssen mogelijk
Word donateur

Wilt u dat Buro Jansen & Janssen de komende jaren onderzoek blijft doen naar politie, justitie en inlichtingendiensten, overheidsoptreden in het algemeen, bedrijven die meewerken aan repressief overheidsbeleid en/of zelf ook repressief of diep ingrijpen in het leven van burgers in Nederland en Europa steun ons dan.

Word donateur of vraag familie, vrienden en bekenden donateur te worden. Rekening NL43 ASNB 0856 9868 52 of rekening NL56 INGB 0000 6039 04 ten name van Stichting Res Publica, Postbus 11556, 1001 GN Amsterdam.

Fox-IT in Rusland (samenvatting)

Het Delftse computer- en beveiligingsbedrijf Fox-IT verkoopt sinds 2010 haar producten in Rusland en is hier na de invoering van de internationale sancties tegen het land in 2014 mee doorgegaan. De Nederlandse overheid is een belangrijke klant van Fox-IT. Het bedrijf verzorgt onder andere de beveiliging van staatsgeheimen.

De Rus Evgeny Gengrinovich speelt een sleutelrol in de handel van Fox-IT met Rusland. Hij werkte in het verleden voor verschillende Russische staatsbedrijven. Vanaf 2011 promoot hij de Fox DataDiode namens het Zwitserse Snitegroup GmbH en het Russische ZAO NPF Simet. Later presenteert hij zich als vertegenwoordiger van Fox-IT en heeft hij een sleutelrol bij het aantrekken van andere tussenhandelaren.

De tussenhandelaren van Fox-IT hebben nauwe banden met Russische staatsbedrijven in de energiesector en de financiële sector, maar ook met het Russische Ministerie van Defensie, defensiebedrijven en de Russische inlichtingendienst FSB. Het Delftse bedrijf heeft in het algemeen weinig zicht op de eindgebruikers aan wie haar producten door tussenhandelaren worden aangeboden en doorverkocht.

Gengrinovich heeft zelf ook banden met defensie en de FSB. Zo deed hij van 2010 tot 2014 certificeringswerk voor de FSTEC (Federal Service for Technical and Export Control) en het Ministerie van Defensie. In september 2017 treedt hij als adviseur in dienst van het Russische informatiebeveiligingsbedrijf Infotecs. In 2018 wordt dit bedrijf op de Amerikaanse sanctielijst geplaatst vanwege haar banden met de Russische inlichtingendienst FSB.

Na de invoering van de internationale sancties in 2014 gaat Fox-IT door met de verkoop van haar producten in Rusland. De oorlog in Oost-Oekraïne, de annexatie van de Krim, het neerhalen van vlucht MH17 en het instellen van de internationale sancties tegen Rusland hebben geen invloed op de verkoopactiviteiten.

Verkoop in Rusland na de sancties

In 2015 verkrijgt Fox-IT zelfs de Russische certificering voor de Fox DataDiode. Het vergroot daarmee haar toegang tot de Russische markt. De FSTEC, dat verantwoordelijk is voor de Russische certificering van de DataDiode, valt onder het Ministerie van Defensie en werkt samen met de FSB.

Over de FSTEC-certificering en het keuringsbedrijf Echelon, dat ook de DataDiode onderzocht, bestaan al sinds 2013 twijfels. In 2017 beoordeelt het gerenommeerde Amerikaanse cybersecurity bedrijf Symantec het certificeringsproces als onvoldoende onafhankelijk van de Russische Staat en ziet het zelfs af van samenwerking met de FSTEC en Echelon.

In 2015 is de Fox DataDiode door ARinteg, een Moskous bedrijf in informatiebeveiliging, te koop aangeboden aan onder andere Russische banken. Volgens commercieel directeur Dmitry Slobodenyuk van ARInteg heeft het bedrijf de Datadiode na de invoering van de internationale sancties in 2014 in ieder geval verkocht aan een van de grootste banken van Rusland.

Veel Russische banken en hun topmannen zijn op de Amerikaanse en Europese sanctielijsten geplaatst vanwege hun banden met de Russische defensie-industrie. Het betreft veelal klanten van ARinteg, zoals de staatsbank Vnesheconombank VEB en de Alfa Bank, een bank die nauw verweven is met de Russische defensie-industrie.

Fox-IT zelf onderkent tot 2015 te hebben geleverd aan Rusland, ook aan de Russische overheid. Het Delftse bedrijf maakt echter niet bekend aan welke overheidsinstanties het heeft geleverd. Het gaat echter in ieder geval om een levering van de Fox DataDiode aan het staatbedrijf RusHydro. Vanwege de nauwe banden van dit bedrijf met het Kremlin worden verschillende topmannen van RusHydro in 2018 op de Amerikaanse sanctielijst geplaatst.

Exportvergunningen

De Fox DataDiode is een soort eenrichtingsverkeer firewall tussen een publiek en een privaat netwerk waarmee toegang tot vertrouwelijke informatie gereguleerd kan worden. Het behoort sinds 2009 tot de dual-use goederen: goederen met een civiele toepassing, die ook een militaire toepassing kennen, waarvoor een exportvergunning vereist is. Volgens Fox-IT zijn overheidsinstellingen in de hele wereld, waaronder de defensie-industrie, belangrijke potentiële klanten voor de Fox DataDiode.

In 2011 beschikte Fox-IT over een globale exportvergunning specifiek voor de Fox Datadiode, waarmee het kon exporteren naar Rusland. In 2012 en 2013 verkreeg het een exportvergunning voor 'apparatuur voor informatiebeveiliging' waaronder naast de DataDiode ook andere Fox-IT producten zoals Redfox en Skytale kunnen vallen. Tot op heden heeft het Ministerie van Buitenlandse Zaken niet bekend gemaakt of, en hoeveel, exportvergunningen Fox-IT sinds 2013 heeft aangevraagd en gekregen. De export van dual-use goederen zonder exportvergunning naar landen buiten de Europese Unie, waaronder Rusland, is in beginsel strafbaar.

Fox-IT reageert niet op vragen van Buro Jansen & Janssen
Op 7, 13, 19 en 20 mei 2021 heeft Buro Jansen & Janssen Fox-IT om commentaar verzocht op de bevindingen van dit onderzoek. Het Delftse bedrijf heeft tot op heden niet gereageerd. Evgeny Gengrinovich reageert ook niet op vragen van Buro Jansen & Janssen.

Terug naar inhoudsopgave

Fox-IT in Rusland

Het Delftse computer- en beveiligingsbedrijf Fox-IT verkoopt sinds 2010 haar producten in Rusland en is hier na de invoering van de internationale sancties tegen het land mee doorgegaan.

Fox-IT werkt in Rusland samen met verschillende partners die haar producten doorverkopen. Deze tussenhandelaren hebben nauwe banden met Russische staatsbedrijven in de energiesector en de financiële sector, maar ook met het Russische Ministerie van Defensie, defensiebedrijven en de Russische inlichtingendienst FSB. Het Delftse bedrijf heeft weinig zicht op de eindgebruiker en aan wie haar producten door tussenhandelaren worden aangeboden en doorverkocht.

Fox-IT onderkent tot 2015 te hebben geleverd aan Rusland, ook aan de Russische overheid. Ook na de invoering van de internationale sancties in 2014 gaat het Delftse bedrijf echter door met de verkoop van haar producten in Rusland. De oorlog in Oost-Oekraïne, de annexatie van de Krim, het neerhalen van vlucht MH17, het instellen van de internationale sancties tegen Rusland in 2014 en de overname door de Engelse NCC Group hebben geen invloed op de verkoopactiviteiten van Fox-IT in Rusland.

Met het verkrijgen van Russische certificering van de Fox DataDiode in 2015 vergroot het bedrijf zelfs haar toegang tot de Russische markt. Russische certificering maakt het product interessanter voor met name grote (overheids-) bedrijven en op de lucratieve markt van de veiligheidsindustrie (opsporings- en inlichtingenwerk en defensie). In de Verenigde Staten bestaan er grote twijfels over de betrokkenheid van defensie en de inlichtingendienst FSB bij die certificering.

Nederland en Rusland klant van Fox-IT

Computer- en beveiligingsbedrijf Fox-IT werd in 1999 opgericht. De Nederlandse overheid waaronder Defensie, opsporings- en inlichtingendiensten, werd al snel een belangrijke klant van het bedrijf.

Fox-IT verzorgt bijvoorbeeld de beveiliging van Nederlandse staatsgeheimen.

Vanaf 2006 werd Fox-IT steeds meer internationaal actief. Zo schreef het Delftse bedrijf in december 2006 in haar nieuwsbrief dat het "een internationale sales force heeft opgericht waarmee we voornamelijk producten aan law enforcement organisaties zullen aanbieden. Denk hierbij aan de data diode, de tapanalyse software FoxReplay en onze cryptografische producten." Het bedrijf breidde haar internationale sales force in de hierop volgende jaren uit.

Fox-IT is vanaf 2010 actief op de Russische markt. Het Delftse bedrijf richt zich in Rusland met name op de verkoop van de Fox DataDiode. Het product behoort sinds 2009 tot de dual-use goederen: goederen met een civiele toepassing, die ook een militaire toepassing kennen. De Fox DataDiode is een soort eenrichtingsverkeer firewall tussen een publiek en een privaat netwerk waarmee toegang tot vertrouwelijke informatie gereguleerd kan worden.

Volgens Fox-IT is de defensie-industrie een van de potentiële klanten voor de DataDiode. In een persbericht in 2010 schrijft het bedrijf: "Met zijn 1G en 10G Ruggedized DataDiodes richt Fox-IT zich op organisaties die de hoogst mogelijke security nodig hebben en onder extreme omstandigheden werken, zoals defensie, overheidsinstellingen en bedrijven in de nucleaire, energie-, olie- en gasindustrie en in andere kritische infrastructuuromgevingen."

Snitegroup GmbH

Fox-IT begint in 2010 met de verkoop aan Rusland. Het Delftse bedrijf werkt hierbij samen met het Zwitserse bedrijf Snitegroup GmbH en het Russische bedrijf ZAO NPF Simet. De Rus Evgeny Gengrinovich speelt een sleutelrol. Vanaf 2010 promoot hij de Fox DataDiode, later presenteert hij zich als vertegenwoordiger van Fox-IT, en heeft hij een sleutelrol bij het aantrekken van andere tussenhandelaren.

Op 1 februari 2011 ondertekenen Snitegroup GmbH en Fox-IT een Reseller Agreement. Hiermee kan het Zwitserse bedrijf producten en diensten van Fox-It doorverkopen.

In maart 2011 verschijnt Snitegroup als partner van Fox-IT voor Russia and CIS op de website van het Delftse bedrijf. Catherina Beretti heeft het Zwitserse bedrijf een jaar eerder, op 30 maart 2010, samen met de Rus Evgeny Gengrinovich ingeschreven bij het handelsregister in Zürich. Het bedrijf is gevestigd in het Zwitserse Schlieren.

Bij de Zwitserse Kamer van Koophandel staat het bedrijf ingeschreven als een onderneming die zich bezighoudt met de ontwikkeling en de verkoop van software in de CIS-landen (Gemenebest van Onafhankelijke Staten): "Entwicklung und der Vertrieb von Computer-Software insbesondere Im Bereich der GUS-Staaten." De CIS-landen zijn Rusland, Wit-Rusland, Armenië, Kazachstan, Kirgizië, Tadzjikistan, Azerbeidzjan, Moldavië en Oezbekistan.

De Zwitserse mede-eigenaar Beretti schrijft dat zij slechts verantwoordelijk was voor de belastingen en administratie met betrekking tot de inschrijving. Het bedrijf ontwikkelde volgens haar geen enkele activiteiten in Zwitserland en de Europese Unie.

Beretti geeft aan dat Snitegroup producten en diensten van Fox-IT heeft afgenomen en die doorverkocht in de Russische Federatie: "Die Snitegroup hat im Rahmen dieses Reseller Agreements Waren und Dienstleistungen von der Fox-IT eingekauft und diese Waren auch in die Russische Föderation weiterverkauft."

Het Zwitserse bedrijf presenteert zich op haar website als consultancy bedrijf voor bedrijfsontwikkeling, marketing en andere essentiële diensten. Volgens haar website heeft het bedrijf partners in zes landen, waaronder Israël en Rusland. De klanten van Snitegroup zijn

energiebedrijven en financiële instellingen: “Among our customers you can find the market leaders in several industries such as Electric Power, Oil and Gas and finance.”

Evgeny Leonidovich Gengrinovich

De schakel voor de handel van Snitegroup met Rusland is mede-eigenaar en CEO Evgeny Gengrinovich. Hij is zijn gehele carrière werkzaam in de door de staat gecontroleerde energiesector in Rusland.

In de jaren negentig is hij vooral betrokken bij automatisering van de Russische energiedistributiebedrijven. Begin deze eeuw werkt hij niet alleen meer voor de uitvoerders in de energiesector, maar ook voor de Russische toezichthouders voor de regulering van de automatisering van energierekeningen en slimme meters. Vanaf 2006 promoot hij de slimme meters van het Zwitserse bedrijf Landis+Gyr.

In 2010 stapt hij over naar de private sector. Hij voert projecten uit voor staatsinstellingen waar hij in het verleden als ambtenaar actief was. Hij werkt als manager op het gebied van automatisering, informatiebeveiliging, en met name sales. Volgens zijn curriculum vitae van 23 mei 2017 voert hij vanaf 2010 projecten uit voor "MOEK" (Moscow United Electric Grid Company), Russian Railways, FGC UES (Federal Grid Company of Unified Energy System), Transneft, Tyumenenergo, Mosenergo, IDGC (Interregional Grid Company of Siberia) en SIBUR.

Gengrinovich zet niet alleen Snitegroup in Zwitserland op, maar is sinds 2010 ook adjunct-directeur van het Russische bedrijf ZOA NPF Simet.

ZAO NPF Simet

Simet is op 17 mei 2005 opgezet door de gebroeders Denis en Vadum Buryakov. Zij hebben honderden bedrijven op hun naam en zijn door de belastingdienst op een lijst van ‘mass directors’ gezet, individuen die bij

veel bedrijven tegelijk directeur zijn. De belastingdienst verdenkt deze eigenaren van belastingontduiking, maar juridische procedures tegen de Buryakovs zijn niet ingesteld.

Als directrice van Simet staat vermeld Smirnova Lyudmila Petrovna. Volgens de gegevens van de Russische Kamer van Koophandel houdt het bedrijf zich bezig met onderzoek en productie van systeemintegratie en metrologie. Het bedrijf lijkt tot eind 2011 een voornamelijk slapend bestaan te leiden.

Fox-IT noemt op haar website vanaf 2011 Snitegroup als partner, terwijl het adres, telefoonnummer en e-mailadres van ZAO NPF Simet bij Snitegroup staat vermeld als Moscow office van het Zwitserse bedrijf: Proletarsky prospekt 1, 115522 Moscow, Russian Federation, emailadres info@simet.ru. Dit is hetzelfde adres dat Snitegroup op haar website als GmbH op de website als adres van Simet vermeldt.

Volgens mede-eigenaar van Snitegroup Beretti wilde het Zwitserse bedrijf met Simet gaan samenwerken op het gebied van scholing voor het gebruik van Fox-IT producten. “Diese Firma hat alle notwendigen Zertifikate um an Ausschreibungen innerhalb Russlands teilzunehmen. Mit dieser Frima wollte die Snitegroup zusammenarbeiten. Die Snitegroup hat geplant, dass Simet in Zukunft die Schulungen von den Fox-IT Produkten in Russland durchführt.”

Volgens Beretti is het nooit tot een overeenkomst tussen Snitegroup en Simet gekomen. Het is echter duidelijk dat Gengrinovich vanaf 2011 een sleutelrol vervult in de verkoop van producten van Fox-IT in Rusland, waarbij hij zich presenteert als vertegenwoordiger van zowel Snitegroup als Simet (en later ook van Fox-IT zelf).

Gengrinovich, de Fox DataDiode salesman

Vanaf 2010 probeert Evgeny Gengrinovich als directeur van Snitegroup en adjunct-directeur van Simet bij allerlei congressen en bijeenkomsten producten van Fox-IT aan te bieden aan Russische bedrijven. Het gaat met name om de Fox DataDiode: een soort eenrichtingsverkeer firewall tussen een publiek en een privaat netwerk waarmee toegang tot vertrouwelijke informatie gereguleerd kan worden.

Twee maanden na het ondertekenen van de reseller agreement tussen Snitegroup en Fox-IT maakt Gengrinovich op 11 april 2011 een PowerPoint Presentatie (bestandsnaam DiodeRussiaMar). In deze presentatie komen beelden voor van de Fox DataDiode. Ook de door Fox-IT gebruikte Dell-servers komen in beeld. Er wordt verwezen naar de EAL7+ en NAVO-certificaten van het product van Fox-IT.

De vermelding van deze certificaten is van belang om potentiële klanten te interesseren. Daarnaast eisen overheden voor sommige werkzaamheden apparatuur die over bepaalde certificering beschikt. Het beveiligingslabel van de EAL (Evaluation Assurance Level) is een internationaal erkende set van veiligheidsstandaarden die wordt gebruikt door overheden en andere organisaties om de veiligheid van technologieproducten vast te stellen.

Op 20 december 2011 is Gengrinovich een van de sprekers op het derde International Energy Forum “Innovation, Infrastructure, Security". Het forum is georganiseerd door de Doema met steun van het Ministerie van Energie en Rosatom. Rosatom, ook bekend onder de namen Rosatom State Nuclear Energy Corporation, the State Atomic Energy Corporation Rosatom en Rosatom State Corporation is het Russische federaal agentschap voor kernenergie. Het houdt zich niet alleen bezig met kernenergie, maar ook met de Russische kernwapens.

Gengrinovich heeft voor de bijeenkomst drie PowerPoint presentaties voorbereid. Een presentatie (bestandsnaam SIMetTGC3v1.96506043) gaat over een project van Simet met de Zwitserse producent van slimme meters Landis+Gyr bij het door de Russische staat gecontroleerde energiebedrijf Mosenergo, een dochteronderneming van Gazprom.

De tweede presentatie gaat over een specifiek product van Landis+Gyr, Converge (bestandsnaam ConvergeSIMetv1.40459327). De derde presentatie (bestandsnaam SIMetBPL.46929715) gaat over zogenoemde Smart Grids (slimme energienetwerken).

Onder de presentaties staan de contactgegevens van Gengrinovich vermeld als Deputy General Director CJSC NPF Simet. In de tweede en derde presentatie wordt Snitegroup genoemd als partner van Simet, maar Gengrinovich laat onvermeld dat hij voor beide bedrijven werkzaam is.

Volgens de presentaties voor het Forum heeft Simet vele professional engineers in dienst en vestigingen in Moskou, Yaroslavl, Nizhny Novgorod, Novosibirsk en Krasnoyarsk. Ook wordt vermeld dat Simet partners heeft in Zwitserland, Duitsland, Slovenië, Rusland en Israël. In deze landen bevinden zich ook het hoofdkantoor en de partners van Snitegroup.

Een jaar later maakt Gengrinovich een presentatie (bestandsnaam SNITEGroupITSecASUTP) op 6 juni 2012 over de Fox DataDiode. In deze presentatie staan de logo's van Fox-IT en Snitegroup GmbH naast elkaar. Veel teksten komen overeen met de presentatie van 11 april 2011 (bestandsnaam DiodeRussiaMar), waaronder de tekst over de EAL7+ en NAVO-certificaten van het product.

Gengrinovich maakt presentaties over de Fox DataDiode. Daarnaast prijzen Snitegroup en Simet het product ook op hun websites aan. Snitegroup presenteert het product vanaf september 2012 op haar website als "A Preferred Solution For High-Security Real-time Electronic Data Transfer Between Networks."

Ook Simet prijst het product aan op haar website. Het bedrijf vermeldt Fox-IT sinds oktober 2012 als partner op haar website. Bij een foto van de Fox DataDiode staat: "Unidirectional, at the physical layer, connection of network segments."

Simet en de Russische staat

De klanten van Snitegroup en Simet komen grotendeels overeen en zijn Russische staatsbedrijven of door de Russische overheid gecontroleerde bedrijven.

Op de websites van beide bedrijven worden de staatsbedrijven Gazprom en zijn dochteronderneming Mosenergo, Russian Railways, Rosseti en zijn dochteronderneming Moesk en Transneft als klant genoemd. Transneft wordt sinds 2007 geleid door voormalig KGB-officier en oud-collega van Poetin, Nikolay Tokarev. Tokarev werkte in 1996 en 1997 samen met Poetin in de Russische regering onder Jeltsin.

Vanwege hun nauwe banden met het Kremlin zijn meerdere klanten van Simet, en hun topmannen, op internationale sanctielijsten geplaatst. Transneft en Gazprom worden in 2014 op de sanctielijst van de Europese Unie geplaatst vanwege betrokkenheid bij de oorlog in Oost-Oekraïne. In 2018 worden Alexei Miller (Gazprom), Oleg Belozerov (Russian Railways), Oleg Budargin (Rosseti) en Nikolai Tokarev (Transneft) op de Amerikaanse sanctielijst geplaatst.

Het enige private bedrijf waar Simet voor werkt, is het petrochemische bedrijf SIBUR. Het bedrijf is nauw verbonden met het Kremlin. Tot in 2010 was SIBUR eigendom van staatsbedrijven Gazprom en Gazprombank die het bedrijf vervolgens 'verkochten' aan Leonid Mikhelson, Gennady Timchenko en Kirill Shamalov. Timchenko is miljardair en een van de judopartners van Vladimir Poetin. Shamalov behoort ook tot de inner circle van Poetin en werkte bij Gazprom, Gazprombank en Rosoboronexport. Rosoboronexport staat onder directe controle van Poetin en is het agentschap voor import en export van defensiemateriaal. In 2018 worden Shamalov en Timchenko op de Amerikaanse sanctielijst geplaatst.

Naast deze bedrijven in de energiesector heeft Simet ook relaties met het Russische Ministerie van Defensie en de defensie-industrie. Sinds 2011 is het bedrijf verwikkeld in een slepende klachtenprocedure tegen het energiebedrijf van het ministerie van Defensie, Oboronenergo. De klacht van Simet gaat over een aanbesteding voor het ontwerp en de bouw van energietussenstations in de regio Kamchatsky in het Oosten van Rusland. Bij de opdracht gaat het om de bouw van een elektriciteitsstation bij militaire eenheid 62695, het onderdeel van de Russische Pacifische Vloot waar ook nucleaire onderzeeboten zijn gestationeerd.

De banden van Simet met de Russische staat blijken niet alleen uit haar klantenkring, maar ook anderszins. In een bedrijfspresentatie van 24 januari 2013 schrijft het bedrijf dat het over allerlei licenties en certificaten beschikt waaronder de licentie van de Russische geheime dienst, de FSB om te werken met staatsgeheimen: "The FSB license to carry out work related to the use of information constituting a state

secret.” Het werken met staatsgeheimen betekent dat Simet kan werken voor staatsbedrijven, bijvoorbeeld in de Russische veiligheidssector.

Gengrinovich en de Russische staat

Evgeny Gengrinovich heeft een sleutelrol bij de verkoop van de Fox DataDiode in Rusland. De klanten van Snitegroup en Simet zijn grotendeels dezelfde staatsbedrijven waarvoor hij volgens zijn curriculum vitae als ambtenaar heeft gewerkt. Gengrinovich heeft niet alleen goede contacten in de energiesector, maar heeft ook connecties met het Russische Ministerie van Defensie en de defensie-industrie.

In zijn curriculum vitae van 23 mei 2017 vermeldt Gengrinovich van 2010 tot 2014 certificeringswerk te hebben verricht voor de FSTEC en het Ministerie van Defensie: “in 2010-2014, work was carried out on the certification of a number of IT solutions at the FSTEC, as well as for use for the needs of the Ministry of Defense and Gazprom.”

De FSTEC (Federal Service for Technical and Export Control) valt onder het Ministerie van Defensie en is het Russisch agentschap dat verantwoordelijk is voor de beveiliging van staatsgeheimen. Het FSTEC heeft nauwe banden met de Russische inlichtingendienst en zal in 2015 de Russische certificering van de Fox DataDiode verrichten.

Daarnaast geeft Gengrinovich in zijn curriculum vitae aan opdrachten te hebben uitgevoerd voor het Ministerie van Defensie (“for use of the needs of the Ministry of Defence).

Dit werk voor defensie ligt in de lijn met zijn presentaties voor het “Innovation. Infrastructure, Security" forum van 20 december 2011, mede-georganiseerd door het Russische kernenergie-agentschap Rosatom dat ook verantwoordelijk is voor de Russische kernwapens. In de presentaties over de Fox DataDiode besteedt Gengrinovich aandacht aan het gebruik van diodes bij het Internationaal Atoomenergieagentschap (IAEA) met een verhandeling over de monitoring van kernenergiecentrales.

Het IAEA komt opnieuw aan bod in een artikel van 10 maart 2015 over de voordelen van DataDiodes op zijn blog, egengrinovich livejournal. Hij schrijft net als in de presentaties dat de instelling DataDiodes gebruikt: "The International Atomic Energy Agency (IAEA) uses them to monitor the operational situation at nuclear power plants."

In hetzelfde artikel stelt Gengrinovich dat defensie- en energiebedrijven de DataDiode hebben aangeschaft: "The list of implementations of DataDiodes is quite wide: from defense to large energy companies." Gengrinovich noemt geen namen van defensiebedrijven of andere bedrijven waaraan de Fox DataDiode is verkocht. Met een uitzondering: RusHydro.

Fox DataDiode naar PJSC RusHydro

Een van de eerste Russische bedrijven die volgens Gengrinovich de DataDiode in gebruik neemt, is RusHydro. Hij schrijft in het artikel van 10 maart 2015 op zijn blog, evgenovich livejournal: "In Russia, one of the first companies to apply this solution was the holding company RusHydro." In het artikel noemt hij Fox-IT niet bij naam.

In zijn curriculum vitae van 23 mei 2017 verwijst hij naar een project bij RusHydro en zegt hij betrokken te zijn geweest bij de installatie van informatiebeveiliging op computernetwerken: "In 2010-2012, a project was implemented to ensure the information security of the technological segments of local computer networks for hydroelectric power plants belonging to JSC RusHydro (8 stations)." Vanaf 2010 was Gengrinovich actief voor Snitegroup en Simet bij de verkoop van de Fox DataDiode.

Het staatsbedrijf RusHydro is een van de grootste waterkrachtbedrijven in de wereld. In 2004 is het bedrijf ontstaan uit de herinrichting van de Russische energiebedrijven.

RusHydro is nauw verweven met de Russische staat. Dat het Kremlin bepaalt hoe het bedrijf wordt gerund blijkt niet alleen uit de ledenlijst van de raad van bestuur van RusHydro, maar ook uit de wijze waarop leidinggevenden worden benoemd of verwijderd uit de top van het bedrijf.

De raad van bestuur van RusHydro bestaat vooral uit mannen die werkzaam waren of zijn in door de Russische staat gecontroleerde bedrijven in de energiesector zoals Rosatom, Transneft, Inter Rao, Rosseti, Rosneft en de door het Kremlin gecontroleerde financiële wereld zoals VTB Bank en Vnesheconombank VEB.

Op 23 november 2009 wordt Evgeny Dod naar voren geschoven als CEO van RusHydro door toenmalig vicepremier van Rusland en vertrouweling van Poetin, Igor Sechin. Sechin is de olieman van Rusland en wordt door diverse media zoals de Financial Times omschreven als de tweede man van Rusland. Zijn macht dankt hij aan zijn positie als CEO bij het Russische oliebedrijf Rosneft. Ook een andere man uit de directe cirkel van Poetin, Boris Kovalchuk, maakt deel uit van de raad van bestuur van RusHydro.

In 2011 wordt een hoge functionaris van de Russische inlichtingendienst FSB aangesteld in het bestuur van RusHydro. Op 10 april 2011 schrijft The Moscow Times dat Poetin de plaatsvervangend minister van energie, Sergei Shmatko, heeft ontslagen uit het bestuur van het bedrijf. Hij wordt vervangen door Sergei Shishin, senior vicepresident van de Russische staatsbank VTB Bank en tevens generaal bij de FSB (en voorloper KGB) waar hij verantwoordelijk is voor de contra-inlichtingenafdeling. In 2012 steekt Poetin 50 biljoen roebel (ruim een miljard euro) in het bedrijf.

De banden tussen het Kremlin en RusHydro zijn reden waarom topmannen van het bedrijf in 2018, waaronder CEO Nikolay Shulginov, op de Amerikaanse sanctielijst van hoge functionarissen van staatsbedrijven zijn geplaatst.

De export van Fox-IT het zicht op de eindgebruikers

Snitegroup, Simet en Gengrinovich proberen vanaf 2010 Fox-IT producten, met name de Fox Datadiode, in Rusland te verkopen. Deze tussenhandelaren hebben nauwe banden met Russische staatsbedrijven in de energiesector en de financiële sector, maar ook met het Russische Ministerie van Defensie, de defensie-industrie en de Russische inlichtingendienst FSB.

Het is de vraag of het Delftse bedrijf weet aan welke partijen haar producten in Rusland te koop worden aangeboden en doorverkocht. Fox-IT onderkent aan Rusland te hebben geleverd. Toenmalig directeur en medeoprichter Ronald Prins verklaart in een interview met Bits & Chips op 17 november 2015 dat het bedrijf de Fox DataDiode in Rusland heeft verkocht.

MT/Sprout vermeldt in een interview met Prins op 15 april 2014 dat het bedrijf ook aan de Russische overheid heeft geleverd: "Het Delftse bedrijf (verwachte omzet 2013: € 21 mln) biedt online beveiligingsoplossingen aan 's werelds meest bekende instituten. Denk niet alleen aan de NASA, NAVO of de Nederlandse, Russische en Indiase overheid, maar ook aan multinationals als T-Mobile en GlobalSign en koepelorganisaties als de NVB en NOC/NSF."

Uit eerder onderzoek van Buro Jansen & Janssen naar de export van Fox-IT blijkt dat het bedrijf vaak niet weet wie de eindgebruikers van haar producten zijn en voor welke doeleinden deze gebruikt worden.

Die export van dual-use goederen (goederen met een civiele toepassing, die ook een militaire toepassing kunnen hebben, en waartoe ook IT-technologie en software kunnen behoren) naar landen buiten de Europese Unie is vergunningsplichtig. Bedrijven dienen een exportvergunning aan te vragen bij de Afdeling Exportcontrole en Strategische Goederen – deze valt sinds 2013 onder het Ministerie van Buitenlandse Zaken, daarvoor onder het Ministerie van Economische Zaken.

In 2009 verkreeg Fox-IT voor de DataDiode een EAL-6 certificering, waarmee het product in ieder geval vergunningsplichtig werd. In 2010 werd een EAL-7 certificering verkregen. Het beveiligingslabel van de EAL (Evaluation Assurance Level) wordt door Gengrinovich, Snitegroup, Simet en andere tussenhandelaren gebruikt om potentiële Russische klanten in de Fox DataDiode te interesseren.

Uit het onderzoek van Buro Jansen & Janssen 'Fox-IT en het Nederlandse exportbeleid voor dual-use goederen' van januari 2020 blijkt dat Fox-IT in 2011, 2012 en 2013 jaarlijks een globale exportvergunning verkreeg. Hiermee kon het bedrijf exporteren naar landen in de gehele wereld –

met uitzondering van zogenaamde 'moeilijke landen' (zoals Noord-Korea en Iran). Fox-IT kon met deze globale exportvergunningen ook naar Rusland exporteren. De exportvergunning van 2011 was voor de Fox Datadiode, maar in de vergunningen van 2012 en 2013 werd geen specifiek product meer genoemd. Het ging om 'apparatuur voor informatiebeveiliging', waaronder ook andere producten zoals Redfox en Skytale kunnen vallen. Tot op heden heeft het ministerie van Buitenlandse Zaken niet bekend gemaakt of en hoeveel, exportvergunningen Fox-IT sinds 2013 heeft aangevraagd en gekregen.

Het exportbeleid voor dual-use goederen beoogt ongewenst eindgebruik te voorkomen. Het Handboek Strategische Goederen en Diensten stelt: 'Het Nederlands dual-use exportcontrolesysteem is gebaseerd op risicoanalyses. De nadruk ligt bij de controle vooraf. Het gaat er om met behulp van risicoanalyses en, waar nodig, het verkrijgen van extra waarborgen, de risico's van ongewenst gebruik of doorgeleiding naar een onwenselijke bestemming tot een minimum te beperken.' Uit het onderzoek 'Fox-IT en het Nederlandse exportbeleid voor dual-use goederen' blijkt dat er in de praktijk nauwelijks sprake is van een risicoanalyse. Fox-IT verstrekt de Afdeling Exportcontrole nauwelijks informatie over de eindgebruikers van de te exporteren producten.

Uit het onderzoek blijkt dat Fox-IT vaak niet weet wie de eindgebruikers zijn van de producten die onder globale exportvergunning worden geëxporteerd. Wanneer bedrijven een exportvergunning aanvragen voor een product dat cryptografie bevat dienen zij een zogenaamd cryptoformulier in te vullen. Hoewel de DataDiode cryptografie bevat vulde Fox-IT bij het aanvragen van exportvergunningen geen cryptoformulier in waardoor het bedrijf minder informatie hoefde te verschaffen over de eindgebruiker. In het formulier wordt namelijk gevraagd tot welke van de vier categorieën (financiële instelling, overheidsinstelling, bedrijf, particulier) de eindgebruiker behoort.

Ook in het onderzoek van Buro Jansen & Janssen 'Fox-IT in het Midden-Oosten' van april 2019 blijkt dat Fox-IT weinig zicht heeft op de eindgebruikers van haar producten. Het Delftse bedrijf werkte in de regio vanaf 2007 samen met het Duitse bedrijf AGT, Advanced German Technology. In de partnerovereenkomst en reseller agreement met AGT

waren geen voorwaarden opgenomen met betrekking tot welke landen en klanten AGT de producten van Fox-IT kon doorverkopen. Fox-IT had dan ook weinig zicht op waar haar producten terechtkwamen en voor welke doeleinden deze gebruikt werden.

Fox-IT en de Russische tussenhandel

Ook bij de handel in Rusland ontbreekt het zicht op de eindgebruiker. Fox-IT maakt in Rusland gebruik van verschillende partnerbedrijven die haar producten als tussenhandelaar proberen door te verkopen.

Het Delftse bedrijf noemt op haar website vanaf 2011 Snitegroup als partner, en later ook OSIsoft (vanaf 2014) en Axoft (vanaf 2015).

Daarnaast bieden ook andere Russische bedrijven de Fox Datadiode aan, zonder dat zij door Fox-IT als partner of wederverkoper worden opgevoerd. Het gaat onder meer om ARinteg (vanaf 2012), RTSoft (vanaf 2013) en de International IT Distribution Group (vanaf 2011). Het is opvallend dat deze bedrijven door Fox-IT op haar website niet worden genoemd als partner. Het is dan ook de vraag of het Delftse bedrijf weet dat haar producten door deze bedrijven in Rusland te koop worden aangeboden.

De relatie tussen het Zwitserse Snitegroup en het Russische International IT Distribution Group (ITD Group) geeft aan hoe het zicht op de eindgebruiker van door Fox-IT geëxporteerde dual-use goederen wordt ontnomen.

Fox-IT en Snitegroup ondertekenden op 1 februari 2011 een reseller overeenkomst zodat Snitegroup de producten van Fox-IT in Rusland kan verkopen. Vier maanden later in mei 2011 ondertekent Snitegroup een geheimhoudingsverklaring (NDA) met de ITD Group, een Russisch distributiebedrijf van hardware en software. Hiermee kan de ITD Group producten van Fox-IT doorverkopen, zonder dat het Snitegroup hoeft te informeren aan wie het doorverkoopt en voor welke doeleinden het product wordt gebruikt.

Caterina Beretti, de Zwitserse mede-eigenaar van Snitegroup, geeft aan dat na de ondertekening van de NDA meteen handel wordt gedreven met het Russische bedrijf. "Mit der Firma International IT Distribution Group hat die Snitegroup im Mai 2011 ein Non-Disclosure Agreement unterzeichnet. Es wurden auch in 2011 Geschäfte zwischen der International IT Distribution Group und der Snitegroup GmbH abgewickelt." Beretti kan vanwege de geheimhoudingsverklaring geen nadere details geven: „Uber die Art der Geschafte kann ich aufgrund des Non-Disclosure Agreements keine weiteren Auskunfte geben."

Gengrinovich is, net als bij de samenwerking van Snitegroup met Simet, ook de verbindende factor met de ITD Group. ITD Group neemt de inhoud van zijn Snitegroup presentatie van 6 juni 2012 over de Fox DataDiode volledig over, waarbij alleen de contactgegevens van Snitegroup worden vervangen door de website van het bedrijf: iitdgroup.ru.

Op 1 februari 2014 publiceert de ITD Group op haar website een artikel over Fox-IT en de DataDiode, waarin het schrijft: "Fox-IT solutions are already being used by government agencies, defense organizations, law enforcement agencies, life support facilities, banks and large commercial organizations around the world." Het artikel besteedt speciale aandacht aan de DataDiode. "In particular, one of the key solutions offered by the company is Fox DataDiode." Bij het artikel zit een pdf over het product (bestandsnaam Crypto-_Fox_DataDiode_for_protecting_secrets-RU). Het is de vertaling van een pdf die ook te vinden is op de website van de NAVO.

Volgens de ITD Group wordt de Fox DataDiode gebruikt door overheidinstanties en organisaties op het gebied van defensie en law enforcement, maar het specificeert niet of het hierbij op Rusland doelt. Wel vermeldt de ITD Group op haar website dat het Russische overheidsorganisaties en banken onder haar klanten heeft: "Leading Russian banks, state organizations, utility, telecom, insurance and transportation companies entrust their security to our company."

Fox-IT heeft de ITD Group nooit als partner of reseller op haar website genoemd. Het Delftse bedrijf heeft echter wel contacten met het bedrijf. Van 1 tot en met 4 oktober 2013 woont Fox-IT de jaarlijkse VIP

conferentie van ITD Group in Tel Aviv (Israël) bij, “Trends in the Development of Information Security of Modern Business.” De beurs wordt bezocht door verschillende bedrijven: “There will be a great opportunity to try the latest products and ask questions to representatives of vendors - Skybox, PineApp, Intellinx, Checkmarx, WhiteBox, Fox-IT and CyberArk.” Het is niet bekend of Gengrinovich ook op deze beurs aanwezig was, al woont hij deels in Israël.

In juni 2015 stapt Gengrinovich zelfs deels over naar de ITD Group. Hij gaat, naast zijn werk voor Snitegroup, werken als adviseur van de algemeen directeur op het terrein van informatiebeveiliging en de productontwikkeling op dat gebied. In zijn curriculum vitae vermeldt hij: “Since June 2015, he has been working in the company AITIDI Group as Advisor to the General Director responsible for the development of the business in the direction of Protection of critical information infrastructure, as well as the development of the company's product line in this area.”

Over de buitenlandse partners van de ITD Group schrijft Gengrinovich: “The work is carried out in constant interaction with potential Customers, Partners and experts, including foreign ones (Israel, Netherlands, Switzerland, Bulgaria).” Deze landen komen (met uitzondering van Bulgarije) overeen met de internationale connecties van Snitegroup en Simet.

De oorlog in Oost-Oekraïne; verkoop Fox-IT gaat door

In 2014 leiden de annexatie van de Krim, de oorlog in Oost Oekraïne en het neerhalen van de MH17 tot het invoeren van sancties tegen Rusland door de Verenigde Staten en de Europese Unie.

Deze ontwikkelingen hebben geen invloed op de verkoopactiviteiten van Fox-IT in Rusland. Hoewel Ronald Prins in een interview met Bits & Chips van 17 november 2015 zegt dat verkoop van de DataDiode aan Rusland niet meer mag, “we verkochten hem ook aan Rusland – dat mag nu niet meer - …”, spreekt bedrijf zich op haar bedrijfskanalen niet uit over mogelijke consequenties van de internationale sancties voor haar

activiteiten in Rusland, bijvoorbeeld een scherpere controle op de eindgebruikers van de door het bedrijf geëxporteerde producten.

Fox-IT doet evenmin aan herbezinning op de samenwerking met haar Russische partners: Snitegroup, Simet en Gengrinovich gaan door met hun verkoopactiviteiten.

In mei 2014 gaat de website foxitcis.com live. Gengrinovich is eigenaar van het domein en contactpersoon. Het Fox-IT logo staat naast dat van Snitegroup op de voorpagina. De website is gericht op de verkoop van Fox-IT producten in de GOS-landen, waaronder Rusland: "Fox-IT (Netherlands), together with partner SNITEGroup GmbH (Switzerland), present information security products for the CIS countries." Het blijft echter niet bij een website alleen. Gengrinovich gaat zich presenteren als vertegenwoordiger van Fox-IT.

Op 28 mei 2014 houdt Gengrinovich een presentatie tijdens de OSIsoft Regional Conference in het Milan Hotel in Moskou. OSIsoft is een Amerikaans bedrijf in applicatiesoftware, met ook een vestiging in Rusland. De presentatie gaat over technische oplossingen voor informatiebeveiliging (Information security of technological segments of a data transmission network). De Rus wordt door OSIsoftRussia op haar Youtube kanaal gepresenteerd als vertegenwoordiger van het Delftse bedrijf Fox-IT: "Evgeny Gengrinovich, company "Fox-IT"".

In februari en maart 2015 publiceert Gengrinovich twee artikelen in het Journal 'Automation in Industry'. Beide artikelen gaan over DataDiodes en de beveiliging van vitale infrastructuur en openbare netwerken. Het artikel 'Information Security of Critical Infrastructure' omschrijft Gengrinovich als technisch adviseur van Fox-IT: "Technical advisor Fox-IT."

Russische FSTEC-certificering

Voor de handel van Fox-IT met Rusland is certificering van haar producten van belang. Hiermee vergroot het Delftse bedrijf haar kansen op de Russische markt. De Russische certificering maakt het product

interessanter voor met name grote (overheids-) bedrijven. En ook op de lucratieve markt van de veiligheidsindustrie (opsporings- en inlichtingenwerk en defensie).

Het Russische certificeringsproces voor de Fox DataDiode is in 2013 begonnen. In de technische factsheet van 1 november 2013 schrijft Fox-IT bij de Russische Federatie: "ФСТЭК (FSTEC) certification in process."

FSTEC (Federal Service for Technical and Export Control) is het Russisch agentschap dat is belast met contraspionage en de beveiliging van staatsgeheimen. Naar aanleiding van een aantal bepalingen van FSTEC in februari 2013 en maart 2014 (Orders Nr. 17, 21, 31 van respectievelijk 11 en 18 februari 2013 en 13 maart 2014) zijn richtlijnen en controlemechanismen opgesteld voor toelating van buitenlandse apparatuur op de Russische markt.

De oorlog in Oost-Oekraïne, het neerhalen van de MH17 en de internationale sancties vormen voor het Delftse bedrijf geen aanleiding om de certificeringsprocedure stop te zetten. Om potentiële klanten op de hoogte te houden van de vorderingen van de procedure past Fox-IT de technische folder van de DataDiode vanaf 2013 regelmatig aan. Bijvoorbeeld op 17 juni 2014 enkele weken voor het neerhalen van de MH17 en in 2015.

Fox-IT heeft de certificeringsprocedure niet zelf in gang gezet. De procedure is opgestart door ARinteg, het bedrijf dat sinds 1 april 2012 de Fox DataDiode aanbiedt. Van alle Russische tussenhandelaren die producten van Fox-IT aanbieden is ARinteg het enige bedrijf dat in 2013 over een FSTEC-licentie beschikt (sinds 3 februari 2010).

ARinteg heeft de certificeringsprocedure opgestart, maar op de achtergrond speelt Evgeny Gengrinovich een rol. In zijn curriculum vitae schrijft hij dat hij van 2010 tot en met 2014 werk heeft uitgevoerd in het kader van de certificering bij FSTEC: "in 2010-2014, work was carried out on the certification of a number of IT solutions at the FSTEC." De belangrijkste 'IT solutions' waar Gengrinovich zich in die jaren mee bezighoudt is de Fox DataDiode.

De FSTEC-certificering wordt succesvol afgerond. Op 3 november 2015 schrijft ARinteg op haar website: “According to the results of tests on the complex, a certificate of conformity No. 3446 was issued.” Op de website van FSTEC staat bij Fox DataDiode de certificering van 27 augustus 2015 tot en met 27 augustus 2018.

Ter verduidelijking geeft ARinteg aan dat sinds 2013 het gebruik van DataDiodes in Rusland is geregeld door de FSTEC: “Since 2013, the use of unidirectional data transmission systems in the Russian Federation has been regulated by orders of the FSTEC (Orders 17, 21 and 31).” Fox-IT vermeldt de verkregen certificering in de technische folder van de DataDiode.

Op 4 maart 2015 schreef Fox-IT in de technische folder nog dat de DataDiode beschikt over NAVO-certificaten (“NATO up to and including NATO SECRET, Green Scheme”) en Nederlandse certificaten (“The Netherlands up to and including Staatsgeheim GEHEIM, by NL-NCSA/NBV (Nationaal Bureau voor Verbindingsbeveiliging)”). Eind augustus 2015 is daar dus na een tweejarige procedure de Russische certificering aan toegevoegd. Het Delftse bedrijf schrijft over de procedure: “This extended certification scope is a result of the Russian government policy on IT security certifications.”

JSC NPO Echelon; inlichtingendienst operatie?

Handel met Rusland is voor Fox-IT onmogelijk zonder bemoeienis van de Russische inlichtingendienst FSB. De FSTEC, dat verantwoordelijk is voor de certificering, valt onder het Ministerie van Defensie en werkt samen met de FSB. Mede door de toegenomen spanningen tussen Rusland en het Westen krijgt certificering van IT-technologie vanaf 2013 een steeds belangrijker inlichtingencomponent. Rusland wil niet dat buitenlandse apparatuur wordt gebruikt voor spionagedoeleinden, maar wil tegelijkertijd inzicht in de nieuwste buitenlandse technologie verwerven. De Verenigde Staten en de Europese Unie maken vanzelfsprekend eenzelfde afweging.

De FSTEC-certificering is hiermee gepolitiseerd. Volgens verschillende Amerikaanse technologiebedrijven kunnen de Russen tijdens het certificeringsproces kwetsbaarheden in producten ontdekken, die vervolgens bij hackpogingen kunnen worden gebruikt: "Those inspections also provide the Russians an opportunity to find vulnerabilities in the products' source code - instructions that control the basic operations of computer equipment - current and former U.S. officials and security experts said" (Reuters 23 juni 2017).

Waar Amerikaanse bedrijven bezwaren signaleren bij de certificeringsprocedure doet Fox-IT dit niet. Het bedrijf vermeldt in de technische folder wel dat het Russische Ministerie van Defensie betrokken is bij de certificering van de DataDiode: "Russian Federation certificate of the Ministry of Defense of Russia for compliance with Level 2 NDV and RDV control *), by CNII EISU (CNII EISU). Certificate on code review and software testing against Russian Ministry of Defense requirements to undeclared features (level 2) and functional requirements correspondingly." Het Delftse bedrijf heeft, in tegenstelling tot Amerikaanse bedrijven, verder geen kanttekeningen.

Een van de Amerikaanse bedrijven, het gerenommeerde cybersecurity bedrijf Symantec, besloot om niet meer mee te werken aan het verzoek van de Russische overheid om de broncode van haar producten in te zien. Voor Symantec een besluit met gevolgen, want door deze weigering worden producten van het bedrijf niet meer toegelaten op de Russische markt. Symantec zegt in 2017 tegen Reuters dat het een van de laboratoria die de tests doen niet onafhankelijk genoeg vindt van de Russische Staat*:* "Symantec said one of the labs inspecting its products was not independent enough from the Russian government" (Reuters 23 juni 2017).

Symantec doelt op JSC NPO Echelon, een van de Russische bedrijven die de certificering voor de FSTEC uitvoert. Symantec twijfelt aan de onafhankelijkheid van dat bedrijf: "The lab "didn't meet our bar" for independence."

De naam van het bedrijf, Echelon, is een Russische knipoog naar het wereldwijde afluisterprogramma van de Verenigde Staten, het Verenigd Koninkrijk, Canada, Australië en Nieuw-Zeeland (de zogenaamde Five

Eyes) ook genaamd Echelon. Symantec's weigering heeft alles te maken met de centrale rol die de Russische inlichtingendienst FSB speelt bij de certificering. Echelon zou vooral in naam onafhankelijk zijn, maar in werkelijkheid sterk gelieerd zijn aan het Russische leger en de FSB.

De betrokkenheid van de Russische inlichtingendienst is voor Symantec reden om haar producten niet te laten certificeren. Fox-IT heeft dergelijke bezwaren niet en heeft zich nooit uitgelaten over de mogelijke risico's van FSTEC-certificering. Hoewel het bedrijf Echelon ook de DataDiode heeft onderzocht, mogelijk ook op kwetsbaarheden die gebruikt kunnen worden bij hackaanvallen.

Fox-IT laat zich niet uit over dit risico. Het vermeldt in de technische folders: "The scope of the Russian security certifications however also include the software that is provided with the device and runs on the proxy servers."

Het is Fox-IT bekend dat bij het certificeringsproces zowel de hardware als de software uitgebreid wordt doorgelicht: "As a result, these certifications do not only warrant the enforced one-way network connection of the Fox DataDiode hardware, but do also warrant the absence of undeclared features (e.g. backdoors and spyware) in the Fox DataDiode software."

Enigszins cryptisch voegt Fox-IT hier nog aan toe dat de Fox DataDiode software bij niet nader genoemde Russische 'trusted sources' kan worden verkregen en dat Fox-IT een Russische standaardvalidatie kan verzorgen: "The certified Fox DataDiode software can be collected from trusted Russian sources. GOST fingerprints are available upon request."

Het handelsbelang weegt voor het Delftse bedrijf zwaarder dan de risico's van de FSTEC-certificering. De certificering van de DataDiode biedt voor Fox-IT nieuwe kansen op de Russische markt. Dit blijkt uit de verkoopactiviteiten van de Russische tussenhandelaar ARinteg.

ARinteg: Levering aan staatsbanken

Het in Moskou gevestigde bedrijf ARinteg houdt zich bezig met systeemintegratie en informatiebeveiliging. Het biedt de Fox DataDiode

al sinds 2012 aan, hoewel het bedrijf door Fox-IT nooit als partner, distributeur of reseller is genoemd.

ARinteg heeft nauwe banden met de Russische overheid. Dit blijkt niet alleen uit haar rol bij de certificering van de DataDiode, maar ook uit haar klantenkring. Veel van ARinteg's klanten behoren tot de door de Russische staat gecontroleerde financiële wereld, zoals de Russische ontwikkelingsbank Vnesheconombank VEB, Promsvyazbank en dochteronderneming Sviaz-Bank, Bank Trust en Project Finance Bank.

Potentiële interesse in een DataDiode bij haar staatsklanten was er al voor het verkrijgen van de certificering. De Vnesheconombank VEB schreef al in 2013 een tender uit voor een DataDiode. Het is niet bekend of ARinteg het product aan de bank heeft verkocht. Wel heeft ARinteg bij de Vnesheconombank VEB een project uitgevoerd dat duidt op de toepassing van een DataDiode. Het bedrijf vermeldt op haar website: "Implement centralized management of the anti-virus and other malicious code protection system."

Niet alleen de Vnesheconombank VEB heeft interesse in een DataDiode. Na de certificering van de Fox DataDiode in augustus 2015 zegt ARinteg commercieel directeur Dmitry Slobodenyuk in het National Banking Journal van 7 december 2015 dat het voor het bedrijf belangrijk was om eenrichtingsverkeer voor de uitwisseling van informatie in het assortiment te hebben.

Een van de grootste banken van Rusland wil deze namelijk in gebruik nemen. "Also significant for us was the commissioning of a software and hardware complex for one-way information transfer in one of the largest banks in the Russian Federation." Slobodenyuk bedoelt de Fox DataDiode. Hij verwijst namelijk naar de certificering door FSTEC: "We have certified this solution at FSTEC and are piloting it in several large companies."

ARinteg heeft de Fox DataDiode verkocht aan een Russische bank, een van de grootste banken van Rusland, maar het maakt niet bekend om welke bank het gaat. De grootste banken van Rusland zijn in 2014 de staatsbanken Sberbank, VTB Bank en Gazprombank. Daarna volgen nog een dochteronderneming van VTB Bank, VTB24, de Otkritie FC Bank en Alfa Bank.

ARinteg noemt op haar website in 2014 verschillende banken als klant: de staatsbanken Vnesheconombank VEB, Promsvyazbank, Sviaz-Bank, Bank Trust en RPFB Project Finance Bank en de private bank Alfa Bank.

ARinteg's commercieel directeur Dmitry Slobodenyuk specificeert niet aan welke bank en welke bedrijven de Fox DataDiode is geleverd. De kans dat dual-use producten van Fox-IT bij de Russische defensie is terechtgekomen is echter reëel. ARinteg heeft namelijk naast veel klanten in de door de Russische staat gecontroleerde financiële sector, ook klanten in de defensie-industrie.

Een van die klanten is het defensiebedrijf VPK NPO Mashinostroyeniya, dat zich sinds het eind van de Koude Oorlog niet alleen meer op militaire productie richt, maar onder andere raketten voor de Russische marine produceert. Het is een van de eerste bedrijven die door de Amerikaanse overheid na de inval op de Krim op 16 juli 2014 op de sanctielijst is geplaatst.

Russische banken en de defensie-industrie

De nauwe banden tussen de Russische financiële sector en het Kremlin leiden na de Russische bezetting van de Krim in 2014 tot internationale sancties tegen meerdere Russische banken, waaronder een aantal banken die klant is van ARinteg.

De eerste banken die in 2014 op sanctielijsten van de Verenigde Staten en de Europese Unie komen te staan zijn de drie grote staatsbanken Sberbank, VTB bank en Gazprombank. Later dat jaar worden de Vnesheconombank VEB en Alfa Bank, beiden klant van ARinteg, op de sanctielijst geplaatst.

Niet alleen de banken zelf worden op de sanctielijsten geplaatst. In 2018 wordt ook een aantal topmannen van banken op de Amerikaanse sanctielijst geplaatst waaronder Sergey Gorkov van de Vnesheconombank VEB, maar ook de topmannen van Sberbank (German Gref), VTB bank (Andrey Kostin) en Gazprom bank (Andrey Akimov).

Van de banken die klant zijn van ARinteg springt met name de Alfa Bank in het oog. Bij de Alfa Bank heeft Arinteg de antivirusbeveiliging gemoderniseerd. Het vermeldt hierover op haar website bij de projectbeschrijving: "Modernization of the anti-virus protection system to bring it in line with the level of modern threats."

Hoewel Alfa Bank een private bank is, is zij sterk verweven met de door het Kremlin gecontroleerde Russische defensie-industrie. De Russische krant Novayagazeta schrijft hierover: "For years before 2018, Alfa Bank provided substantial loans to subsidiaries of Uralvagonzavod (produces up to 40% of Russian military equipment) and other affiliate entities of the Ministry of Defense and Chemezov's Rostechnology."

Ook heeft de bank directe connecties met de Russische kernenergiesector. Volgens de New York Post. "Alfa Bank provided financing throughout the 2000s to Atomstroyexport, the state-owned Russian nuclear vendor that installed the reactors at Bushehr, Iran."

Naast deze financiële banden met het Russische regime heeft Alfa Bank ook contacten met de Russische inlichtingenwereld, met name de buitenlandse inlichtingendienst SVR. Novayagazeta en The Moscow Times melden: "Alfa bank representatives also have a long track record of cooperation with Mikhail Fradkov, head of SVR in 2007-2016, and Vladislav Surkov, Putin's key advisor on propaganda."

Na de invoering van de sancties is het voor de Alfa Bank, net als voor andere Russische banken die de defensie-industrie financieren, moeilijk om internationale kredieten te verkrijgen. De Alfa Bank zou zich sinds 2017 niet meer met defensie bezighouden. De rol van financier van de Russische defensie-industrie wordt overgenomen door een andere klant van ARinteg: de Promsvyazbank.

Begin 2018 wordt de Promsvyazbank met steun van de Russische overheid opgetuigd om met name de defensiesector te ondersteunen: "Russia's Promsvyazbank (PSB), bailed out by the central bank last

month, will be recapitalised and transferred to the government and will service the defence sector, the finance ministry said on Friday.” (Reuters 19 januari 2018)

Fox-IT in Engelse handen: Verkoop in Rusland gaat door

Op 3 november 2015 verkrijgt ARinteg de Russische certificering voor de Fox DataDiode. Tweeëntwintig dagen later wordt het Delftse bedrijf overgenomen door de Britse NCC Group uit Manchester. In de media wordt de overname gepresenteerd als een mogelijkheid voor Fox-IT om internationaal te groeien.

De internationale sancties tegen Rusland vormen voor het Delftse bedrijf geen reden om haar handel met Rusland te heroverwegen. De certificering van de DataDiode vergroot zelfs de toegang tot de Russische markt en maakt het product interessanter voor met name grote (overheids-) bedrijven en op de lucratieve markt van de veiligheidsindustrie (opsporings- en inlichtingenwerk en defensie).

Fox-IT blijft dan ook actief op de Russische markt. Dit blijkt onder meer uit de LinkedIn-pagina van Joy Meijneke. Zij is van april 2017 als International Inside Sales Representative verantwoordelijk voor de verkoop van de DataDiode en andere producten in Rusland en de samenwerking met Russische partners.

Zij vat haar werkzaamheden alsvolgt samen: “Managing opportunities for Fox-IT's High Assurance products (DataDiode, SINA, SkyTale) in collaboration with field representatives. Responsible for inside sales, renewal business, development and employment of partners, and monitoring (partner and end-user) opportunities in the following countries: the Americas, Russia, Asia, Australia and New Zealand.”

Meijneke geeft aan te hebben samengewerkt met vertegenwoordigers in de regio. Het zal hierbij zijn gegaan om onder andere Snitegroup, waarmee Fox-It al sinds 2011 samenwerkt. Snitegroup blijft partner van Fox-IT tot 2019, wanneer het bedrijf wordt uitgeschreven uit het Zwitserse handelsregister.

Volgens mede-eigenaar Caterina Beretti heeft Snitegroup na het instellen van de sancties tegen Rusland geen producten van Fox-IT meer verkocht: “Nach Inkrafttreten der Sanktionen gegen Russland wurden keine Waren mehr von der Fox-IT nach Russland verkauft.”

Wel zou Snitegroup in Rusland een onderhoudscontract hebben verkocht. Volgens Beretti werden de sanctieregels hiermee niet overtreden, omdat er al een relatie was met de ontvangende partij: “Im September 2014 wurde ein Drei-Jahres-Maintenancevertrag der Fox-IT nach Russland verkauft. Da der Endempfänger der Fox-IT bekannt ist, und ein schriftliches Angebot der Fox-IT vorliegt, geht die Snitegroup davon aus, dass Europäische Sanktionen durch diesen Wartungsvertrag durch die Schweizer Firma Snitegroup nicht verletzt wurden.”

Fox-IT werkt na 2014 in Rusland echter niet meer alleen samen met Snitegroup. Het Delftse bedrijf breidt haar Russische netwerk van partnerbedrijven en tussenhandelaren na de invoering van de internationale sancties uit.

In 2014 gaat Fox-IT een samenwerking aan met OSIsoft, een Amerikaans bedrijf in applicatiesoftware, met ook een vestiging in Rusland. OSIsoft wordt technology partner van Fox-IT.

Vanaf oktober 2015 wordt Axoft partner, distribiteur en reseller van Fox-IT in Rusland. De banden tussen beide bedrijven bestonden al langer: al in november 2014 verscheen een artikel over de Fox DataDiode in het bedrijfsmagazine Axoft Times. Het bedrijf zal tot juni 2017 als partner op de website van Fox-IT vermeld blijven.

Het in Moskou gevestigde softwarebedrijf is volgens haar website “the leading IT service distributor in Russia and CIS”. Axoft is distributeur van meer dan 50 fabrikanten. Axoft heeft een opvallende band met NPO Echelon, het bedrijf dat de FSTEC-certificering van de DataDiode uitvoerde en nauwe banden onderhoudt met de Russische inlichtingendienst FSB. Sinds 2015 is Axoft de enige distributeur van producten van Echelon in Rusland en de andere GOS-landen, en biedt ook technische bijstand en aanvullende diensten.

Naast de door Fox-IT op haar website genoemde partners blijven ook andere bedrijven de DataDiode in Rusland aanbieden, zonder dat zij door het Delftse bedrijf als partner genoemd worden. Het gaat hierbij ondermeer om RTSoft, ITD Group en ARinteg.

De ITD Group houdt zich sinds 2011 bezig met de verkoop van de DataDiode in Rusland. De klanten van ITD Group zijn volgens de website van het bedrijf staatsorganisaties en banken: "Leading Russian banks, state organizations, utility, telecom, insurance and transportation companies entrust their security to our company."

ARinteg, het bedrijf dat de FSTEC-certificering van de DataDiode verzorgde, heeft met name veel klanten in de financiële sector, maar ook in de defensie-industrie. Het heeft de Fox DataDiode in ieder geval in 2015 aan een of meerdere Russische banken verkocht.

De verkoopinspanningen van Fox-IT en haar tussenhandelaren blijken succes te hebben. Volgens journalist Andrey Biryukov is de Fox Datadiode op grote schaal verkocht in Rusland. Biryukov schrijft in het januari/februari 2018 nummer van het technologiemagazine 'System Administrator' (samag.ru): "Another foreigner who was widely used in Russian enterprises in the past is Fox DataDiode from the Dutch company Fox IT."

Levering in 2019

Met de Russische certificering van de DataDiode in 2015 heeft Fox-IT haar kansen op de Russische markt vergroot. Tegelijkertijd heeft de Fox DataDiode echter ook een NAVO-certificering. De vraag is of dat NAVO–certificaat vanwege de toegenomen spanningen tussen Rusland en het Westen de verkoop in Rusland niet gaat tegenwerken.

Andrey Biryukov vat dit in zijn artikel in System Administrator in 2018 alsvolgt samen: "The fact is that although this solution has a valid FSTEC certificate, however, Fox DataDiode also has a NATO Secret certificate."

Volgens Biryukov zou Fox-IT de DataDiode in 2018 niet meer leveren in Rusland: “And besides, at present, the company has presented a ban on the supply of this solution in Russia.”

Het is echter onduidelijk waar hij dit op baseert. Fox-IT heeft in haar bedrijfskanalen nooit aangekondigd te stoppen met de export naar Rusland. Snitegroup en Simet worden nog tot 2019 als partners op de website van het Delftse bedrijf genoemd.

En Fox-IT producten vinden ook na 2018 nog hun weg naar Rusland. Dit wordt duidelijk bij een levering van de DataDiode in 2019.

Op 25 maart 2019 arriveert er een pakket in Sint-Petersburg. Het is geïmporteerd door het bedrijf Voortman Stil Mashineri, de Russische vestiging van het Nederlandse Voortman Steel Machinery – een producent van staalbewerkingsmachines. De administratieve afhandeling van de transactie is gedaan door EMG (Emerging Markets Group), een Russisch servicebedrijf dat voor Westerse bedrijven werkt.

Volgens de Russische douane is een Amerikaanse server product Dell geëxporteerd: “The Fox DataDiode Ruggedized 1G” van het bedrijf Fox-IT, Olof Palmestraat 6, 2616 LM Delft, Nederland.” Fox-IT gebruikt Dell servers en bouwt die om tot DataDiodes.

Voortman heeft de DataDiode begin 2019 van Fox-IT gekocht en deze aan haar zusterbedrijf in Rusland opgestuurd. De Russische douane vermeldt: “The Fox DataDiode Ruggedized 1G is categorized under Export Control Classification Number (ECCN) 5A003 of the list of dual-use goods and technologies of the Wassenaar Arrangement (WA-LIST) 5A003b.” Ook wordt vermeld dat het Delftse bedrijf over relevante exportvergunningen beschikt: “Fox-IT holds the necessary export licenses to be able to internationally provide the Fox DataDiode Ruggedized 1G to a very wide range of customers.”

Het blijkt betrekkelijk eenvoudig om een Fox DataDiode naar Rusland te exporteren zonder tussenkomst van tussenhandelaren. Hoewel het hier om een dochteronderneming van Voortman gaan, is het product zonder problemen door de douaneformaliteiten gekomen.

Opvallend is de passage over de exportvergunning in de Russische douanepapieren. Hierin wordt verwezen naar een exportvergunning voor de levering, maar de tekst die gebruikt wordt, “Fox-IT holds the necessary export licenses to be able to internationally provide the Fox DataDiode Ruggedized 1G to a very wide range of customers,” is identiek aan de tekst uit de technische folder van de Fox DataDiode van maart 2015. Export van dual-use goederen, zoals de DataDiode, naar Rusland is vergunningsplichtig. De douanepapieren bevatten echter geen specifieke verwijzing naar een exportvergunning die door het Ministerie van Buitenlandse Zaken is afgegeven.

Ook staat in de Russische douanepapieren vermeld dat het om een server van de Amerikaanse firma Dell gaat, als onderdeel van de Fox DataDiode. De Amerikaanse sancties tegen Rusland (en andere landen waarvoor exportrestricties gelden) zijn strikter dan de Europese. Ze gelden ook voor Amerikaanse onderdelen die niet-Amerikaanse firma’s, zoals Fox-IT, gebruiken in hun product.

Fox-IT, Gengrinovich en de Russische inlichtingendiensten

Handel met Rusland is voor Fox-IT onmogelijk zonder betrokkenheid van de Russische inlichtingendienst FSB. Veel van haar tussenhandelaren en potentiële klanten alsmede de FSTEC, dat de certificering van de DataDiode verzorgt, hebben banden met de Russische staat en/of de inlichtingendienst.

De rol van de Russische inlichtingendienst wordt zichtbaar in de persoon van Evgeny Gengrinovich. Hij speelt een belangrijke rol bij de handel van Fox-IT met Rusland. Vanaf 2011 promoot hij de Fox DataDiode namens het Zwitserse Snitegroup en het Russische Simet, later presenteert hij zich als vertegenwoordiger van Fox-IT en heeft hij een sleutelrol bij het aantrekken van andere tussenhandelaren in ieder geval de Russische ITD Group.

Het is de vraag in hoeverre het Delftse bedrijf zich heeft verdiept in de positie van haar tussenhandelaar. Gengrinovich heeft niet alleen goede connecties met Russische staatsbedrijven, maar ook met de Russische

inlichtingendienst FSB. Zijn bedrijf Simet had een licentie om te werken met staatsgeheimen en hij deed certificeringswerk voor de FSTEC en het Ministerie van Defensie.

In september 2017 worden zijn connecties met de Russische inlichtingendienst (wederom) duidelijk. Gengrinovich stapt over naar een bedrijf dat nauw verbonden is met de FSB. Hij verlaat de ITD Group en wordt adviseur van de algemeen directeur van Infotecs.

Infotecs (Information Technologies and Communication Systems) is een private onderneming die nauw verbonden is met de Russische inlichtingendienst FSB. Infotecs en haar dochteronderneming Advanced Monitoring, de onderzoekstak van het bedrijf, zijn actief op het terrein van informatiebeveiliging.

Infotecs is echter niet alleen een informatiebeveiliger. Het maakt ook deel uit van de TK 26: de Technical Committee for Standardization "Cryptographic Information Security", van de FSB. Het andere bedrijf dat zitting heeft in deze commissie is Kvant Scientific Research Institute. Kvant ontwikkelt afluister- en surveillancetechnologie voor de Russische inlichtingendiensten en staat sinds augustus 2010 onder directe controle van de FSB. Voormalig directeur van Kvant, Georgy Babakin, werkte vijftien jaar voor de FSB.

Infotecs, Advanced Monitoring en Kvant kwamen in 2015 in het nieuws naar aanleiding van de Hacking Team documenten. Deze gehackte documenten geven inzicht in de verkoop en klanten van het Italiaans bedrijf Hacking Team dat software verkoopt aan politie en veiligheidsdiensten, waarmee versleuteld digitaal dataverkeer kan worden ontcijferd en afgeluisterd.

Uit deze documenten bleek dat Hacking Team haar digitale wapens via Infotecs, Advanced Monitoring en Kvant verkocht aan de FSB. Tussen 2012 en 2014 betaalde de FSB het Italiaanse bedrijf via Kvant en Infotecs 450.000 euro voor het digitale wapen Remote Control System. De directeur van Advanced Monitoring Aleksey Kachalin die in contact stond met Hacking Team verhuisde in 2017 naar de grootse staatsbank van Rusland, Sberbank.

In 2018 kondigde de Verenigde Staten sancties af tegen Infotecs en Kvant. De bedrijven worden ervan beschuldigd de Russische inlichtingendiensten in staat te stellen digitale aanvallen uit te voeren in de Verenigde Staten. De Europese Unie heeft de sancties tegen Infotecs en Kvant nog niet overgenomen.

De Amerikaanse sancties tegen Infotecs werpen een vreemd licht op de handel van Fox-IT met Rusland. In 2018 is het bedrijf waarvan Gengrinovich directeur was (Snitegroup) nog altijd partner van Fox-IT, maar wordt zijn werkgever (Infotecs) op de Amerikaanse sanctielijst geplaatst vanwege banden met de Russische inlichtingendienst.

Dit is symbolisch voor de ambivalente houding van het Delftse bedrijf ten opzichte van de Russische inlichtingdienst. Handel met Rusland is voor Fox-IT onmogelijk zonder betrokkenheid van de Russische inlichtingendienst FSB. Maar tegelijkertijd waarschuwt het bedrijf regelmatig voor de bedreiging die de FSB vormt voor de Nederlandse nationale veiligheid.

Waarom handelt Fox-IT met Rusland?

Fox-IT heeft goede connecties met de Nederlandse overheid en de Nederlandse inlichtingendienst AIVD. Nederlandse defensie, opsporings- en inlichtingendiensten vormen een belangrijke klant en het Delftse bedrijf verzorgt de beveiliging van Nederlandse staatsgeheimen. Het Delftse bedrijf lobbyde zelfs openlijk voor de invoering van de Wet op de Inlichtingen- en Veiligheidsdiensten (WIV 2017) tijdens het referendum in 2018.

Fox-IT waarschuwt net als de AIVD al vele jaren voor Russische hackers, al dan niet in relatie tot de Russische staat of de georganiseerde criminaliteit. In 2005 is medeoprichter en voormalig directeur Ronald Prins te gast bij TROS-radio en Computable om te praten over de banden tussen hackers en de Russische maffia. In het achtste nummer van haar nieuwsbrief Fox Nieuws, gebruikt het bedrijf Russische hackers zelfs als een reden om zichzelf aan te prijzen: “Fox-IT kan hier vanzelfsprekend bij van dienst zijn.”

In 2008 schuift Prins regelmatig aan bij de media bij gesprekken over de Russische en Chinese spionageactiviteiten in Nederland. Of de spionage vanuit Rusland door de staat worden uitgevoerd is volgens Prins niet zomaar vast te stellen, maar de staat is blijkbaar volgens Prins wel een van de mogelijke actoren.

Begin 2012 schrijft het Delftse bedrijf over de Russische inlichtingendienst FSB. Op 20 maart 2012 publiceert Fox-IT een artikel op haar website over de arrestatie van acht hackers door de FSB. "Russian authorities have arrested eight men accused of creating and distributing the Carberp banking Trojan in Russia and the Netherlands." Fox-IT schrijft dat het bedrijf als eerste het gebruik van malware door deze groep had geconstateerd.

In 2015 wordt de relatie tussen de Russische inlichtingendienst met Russische hackers nogmaals bevestigd. Samen met de Amerikaanse FBI en het bedrijf Crowdstrike presenteert Fox-IT tijdens de Black Hat conferentie in Las Vegas een onderzoek naar de malware GameOver Zeus dat een product zou zijn van de groeiende samenwerking tussen de Russische inlichtingendienst en cybercriminelen.

De waarschuwingen voor de Russische inlichtingendienst vallen moeilijk te rijmen met de verkoopactiviteiten van het bedrijf in Rusland. Zeker daar met de Russische certificering van de Fox DataDiode kwetsbaarheden van het product in handen kunnen vallen van de Russische inlichtingendiensten en gebruikt kunnen worden voor hackaanvallen. Voor het Amerikaanse bedrijf Symantec vormt dit risico aanleiding om niet aan de certificering van haar producten mee te werken. Fox-IT heeft dergelijke bezwaren echter niet.

Fox-IT gaat door met de verkoop in Rusland, ook na de invoering van de internationale sancties in 2014. Terwijl het bedrijf vaak geen zicht heeft op de eindgebruiker van de naar Rusland geëxporteerde producten en niet weet aan wie haar producten worden doorverkocht en voor welke doeleinden deze worden gebruikt. Het risico op ongewenst eindgebruik is aanzienlijk, aangezien Fox-IT verkoopt via tussenhandelaren die nauwe banden hebben met Russische staatsbedrijven, ook met het ministerie van Defensie, defensiebedrijven en de Russische inlichtingendienst FSB.

Ook de mensenrechtensituatie in Rusland vormt voor Fox-IT geen reden tot herbezinning op de verkoop in Rusland. Toen Fox-IT zich in 2010 op de Russische markt begaf was er al sprake van repressie van politieke oppositie, mensenrechtenactivisten en journalisten. Dit werd in 2006 bijvoorbeeld al duidelijk met de moord op de journalist Anna Politkovskaya en de kritische voormalige medewerker van de inlichtingendienst Alexander Litvinenko in Londen en in 2009 de advocaat Sergei Magnitsky die in een Russische cel overleed aan zijn verwondingen door overheidsfunctionarissen.

De mensenrechtensituatie is in de loop der jaren verslechterd, ook ten aanzien van de internetvrijheid. Vanaf 2014 staat Rusland op de lijst van Enemies of the Internet van Reporters without Borders, een overzicht van landen die die internetvrijheid ernstig beperken, bijvoorbeeld door internettoegang te blokkeren of internetverkeer te monitoren. Van 2010 tot en met 2013 was het land al door Reporters without Borders in het voorportaal van de lijst gezet onder andere in verband met wetgeving waarbij individuen op een internet zwarte lijst werden geplaatst (Internet blacklist law). De lijsten waren onderdeel van maatregelen om de protesten tegen het regime van 2011 tot en met 2013 de kop in te drukken.

De keuze van Fox-IT om zich, ondanks de verslechterende mensenrechtensituatie, op de Russische markt te begeven en in Rusland actief te blijven, staat echter niet op zichzelf. Het Delftse bedrijf raakte al eerder in opspraak vanwege het Midden-Oosten. Tijdens de Arabische lente rond 2011 probeerde het bedrijf haar producten te verkopen aan overheidsinstanties en inlichtingendiensten in landen met een dubieuze reputatie op het gebied van de mensenrechten zoals Syrië, Egypte, Saoedi-Arabië en de Verenigde Arabische Emiraten.

Nader onderzoek naar Fox-IT noodzakelijk

Medeoprichter en toenmalig directeur Ronald Prins onderkent in 2015 dat Fox-IT de DataDiode naar Rusland heeft geëxporteerd, ook naar de Russische overheid. “Die diode is best wel een succesnummer, die gaat

de hele wereld rond. We verkochten hem ook aan Rusland – dat mag nu niet meer – en aan India en Amerika. Allemaal buiten Europa; daar dwingt de overheid dit soort oplossingen ook wel af voor kritieke infrastructuur," zegt hij op 17 november 2015 in een interview met Bits & Chips.

Prins impliceert in 2015 dat Fox-IT de DataDiode na de invoering van de internationale sancties niet meer in Rusland heeft verkocht. Uit dit onderzoek van Buro Jansen & Janssen blijkt echter dat Fox-IT na de invoering van de internationale sancties in 2014 doorging met de verkoop in Rusland. Het bedrijf breidde haar netwerk van tussenhandelaren uit. Met de certificering van de Datadiode vergrootte het bedrijf haar toegang tot de Russische markt, met name overheidsbedrijven en de markt van de veiligheidsindustrie.

Het Nederlandse exportbeleid voor dual-use goederen beoogt ongewenst eindgebruik te voorkomen. Van bedrijven wordt verwacht dat zij informatie verschaffen over de eindgebruiker van geëxporteerde producten. De afgelopen jaren is de controle op ongewenst eindgebruik strenger geworden. Het Openbaar Ministerie stelt vaker vervolging in tegen bedrijven die de regels niet naleven en onvoldoende nagaan naar welke eindgebruikers hun producten worden geëxporteerd en voor welke doeleinden deze worden ingezet.

Het risico op ongewenst eindgebruik is reëel. Fox-IT werkt in Rusland samen met verschillende partners die haar producten doorverkopen, maar het bedrijf heeft weinig zicht op de eindgebruiker en aan wie haar producten door tussenhandelaren worden aangeboden en doorverkocht. Deze tussenhandelaren hebben nauwe banden met Russische staatsbedrijven in de energiesector en de financiële sector, maar ook met het Russische Ministerie van Defensie, defensiebedrijven en de Russische inlichtingendienst FSB.

Van 2011 t/m 2013 verkreeg Fox-IT jaarlijks een globale exportvergunning, waarmee het ook naar Rusland kon exporteren. Het is niet bekend of Fox-IT na 2013 een globale exportvergunning, of een specifieke vergunning voor Rusland, heeft aangevraagd of verkregen. Het Ministerie van Buitenlandse Zaken heeft naar aanleiding van diverse WOB-verzoeken van Buro Jansen en Janssen geen

documenten openbaar gemaakt. De export van dual-use goederen zoals de Fox DataDiode zonder exportvergunning naar landen buiten de Europese Unie, waaronder Rusland, is in beginsel strafbaar.

Na de invoering van de Europese sancties tegen Rusland in 2014 blijft export van dual-use goederen zoals de Fox DataDiode naar Rusland met een exportvergunning mogelijk. Export naar militaire eindgebruikers is echter verboden. Hieronder vallen niet alleen het Ministerie van Defensie en het leger, maar ook inlichtingendiensten, het Ministerie van Binnenlandse Zaken en andere organisaties die belast zijn met de binnenlandse veiligheid, politie en wetshandhaving. Met de in 2015 verkregen Russische certificering werd de Fox DataDiode juist interessanter voor dergelijke organisaties.

De Fox DataDiode is in 2015 in ieder geval geleverd aan Russische banken. Veel Russische banken zijn op de Amerikaanse en Europese sanctielijsten geplaatst vanwege hun banden met de Russische defensie-industrie.

Nader onderzoek naar mogelijk strafbaar handelen van Fox-IT in Rusland is dan ook op zijn plaats.

Fox-IT reageert niet op vragen van Buro Jansen & Janssen
Op 7, 13, 19 en 20 mei 2021 heeft Buro Jansen & Janssen Fox-IT om commentaar verzocht op de bevindingen van dit onderzoek. Het Delftse bedrijf heeft tot op heden niet gereageerd. Evgeny Gengrinovich reageert ook niet op vragen van Buro Jansen & Janssen.

Terug naar inhoudsopgave

Fox-IT in Russia (summary)

The Delft-based computer and security company Fox-IT has been selling its products to Russia since 2010 and has continued doing so after the implementation of international sanctions against the country in 2014. The Dutch government is a major client of Fox-IT's. Among other things, the company safeguards the security of state secrets.

One of the key players in Fox-IT's trade with Russia is the Russian Evgeny Gengrinovich, who used to work for different Russian state companies. Since 2011 he promotes the Fox DataDiode on behalf of the Swiss Snitegroup GmbH and the Russian ZAO NPF Simet. Later on he presents himself as Fox-IT representative and plays a key role in the recruitment of other intermediaries.

Fox-IT intermediaries have close ties to Russian state companies in the energy and financial sectors, but also to the Russian Ministry of Defence, defence contractors and Russian intelligence agency FSB. The Delft-based company in general has little insight into the end users, to whom its products are offered and re-sold by intermediaries.

Gengrinovich himself also has ties to Defence and the FSB. From 2010 to 2014 he provided certification work for the FSTEC (Federal Service for Technical and Export Control) and the Ministry of Defence. In September 2017 he became an advisor for the Russian information security company Infotecs. This company was placed on the American sanctions list due to its ties to the Russian intelligence agency FSB in 2018.

After the implementation of international sanctions in 2014 Fox-IT continued selling its products to Russia. The war in Eastern Ukraine, the annexation of Crimea, the downing of flight MH17 and the implementation of the international sanctions haven't affected its sales.

Russian sales after the sanctions

In 2015 Fox-IT even acquires the Russian certification for the Fox DataDiode, which increases their access to the Russian market. The FSTEC, responsible for the Russian certification of the DataDiode, resorts under the Ministry of Defence and works closely with the FSB.

About FSTEC certification and the certification company Echelon, which also investigated the DataDiode, doubts have been raised since 2013. Renowned American cybersecurity firm Symantec judged the certification process to be insufficiently independent from the Russian state in 2017 and has even stopped cooperating with FSTEC and Echelon.

In 2015 the Fox DataDiode was offered up for sale by ARinteg, a Moscow-based company in information security, among others to Russian banks. According to its commercial director, Dmitry Slobodenyuk, ARingteg sold the DataDiode after the implementation of the international sanctions in 2014 at least to one of the biggest banks of Russia.

Many Russian banks and their figure heads have been put on the American and European sanctions lists, due to their ties to the Russian military industry. Among them many clients of ARinteg, like state bank Vnesheconombank VEB and Alfa Bank, which has close ties to the Russian military industry.

Fox-IT itself acknowledges to have sold to Russia, including to the Russian government, up to 2015. The Delft-based company hasn't revealed, however, which government institutions it has supplied. We do know it involves at least one delivery of the Fox DataDiode to the Russian state company RusHydro. Due to this company's close ties to the Kremlin several of RusHydro's leading figures were added to the American sanctions list in 2018.

Export licences

The Fox DataDiode is a kind of one-way traffic firewall between a public and a private network, which enables the regulation of access to confidential information. Since 2009 it's classed as dual-use goods: goods with a civilian application as well as a military use, which require an export licence. According to Fox-IT, government institutions all over the world, including the military industry, are major potential clients for the Fox DataDiode.

In 2011 Fox-IT possessed a global export licence specifically for the Fox DataDiode, which allowed it to export to Russia. In 2012 and 2013 it obtained an export licence for 'information security equipment', which could, apart from the DataDiode, also include other Fox-IT products, such as Redfox and Skytale. To this day the Foreign Office has failed to disclose if Fox-IT has requested and obtained any export licences, and if so how many, since 2013. Exporting dual use goods without an export licence to countries outside the European Union, including Russia, is in principle illegal.

Fox-IT has not responded to questions asked by Buro Jansen & Janssen.

Buro Jansen & Janssen has requested Fox-IT to comment on the findings of this investigation on May 7th, 13th, 19th and 20th, 2021. Up till now the Delft-based company hasn't responded. Evgeny Gengrinovich also does not respond to questions from Buro Jansen & Janssen.

Back to table of contents

Het NFI en TNO werkten met Fox-IT aan een Surveillance Lab in Saoedi-Arabië tijdens de Arabische Lente

In 2011, op het hoogtepunt van de Arabische Lente, werkte Fox-IT bij de voorbereidingen van een Surveillance Lab in Saoedi-Arabië samen met twee overheidsorganen: het NFI (Nederlands Forensisch Instituut) en TNO (Nederlandse Organisatie voor toegepast natuurwetenschappelijk onderzoek). Medewerkers van die organisaties zaten in de stuurgroep van het Saoedische project met als naam 'Forensic Lab', een landelijk netwerk van telefoon- en internetsurveillance.

Dit blijkt uit documenten die door het NFI en TNO openbaar zijn gemaakt in antwoord op Wob-verzoeken van Buro Jansen & Janssen en uit een grote hoeveelheid interne bedrijfsdocumenten over de relatie van Fox-IT met haar partner, het Duitse bedrijf AGT.

Tien jaar geleden is 2011 het jaar van de Arabische Lente met grote protesten tegen dictators in landen zoals Egypte, Libië, Syrië, Jemen en Bahrein. Ook in Saoedi-Arabië vinden sinds december 2010 protesten tegen het regime plaats.

Tegen deze achtergrond besluit Fox-IT deel te nemen aan het opzetten van een landelijk netwerk van telefoon- en internetsurveillance in Saoedi-Arabië. Hoewel het project in interne correspondentie wordt aangeduid als Forensic(s) Lab is deze naam misleidend. Uit interne documenten blijkt duidelijk dat het project beoogt een landelijk netwerk van telefoon- en internetsurveillance op te zetten.

Het project valt onder het Saoedische Ministerie van Binnenlandse Zaken. Projectleiders zijn het Duitse bedrijf AGT (Advanced German Technology) en het Saoedische bedrijf TCC (Technology Control Company). Fox-IT neemt deel aan drie meerdaagse

voorbereidingsbijeenkomsten over het project: twee in de Saoedische hoofdstad Riyad op 20-22 juni 2011 en 23-29 juli 2011 en een bijeenkomst op 5-7 september 2011 in het Ritz hotel in Berlijn.

Arabische Lente

De timing is opmerkelijk. Begin 2011 worden in de Tweede Kamer vragen gesteld over de export door Nederlandse computer- en beveiligingsbedrijven naar het Midden-Oosten. In antwoord op de Kamervragen laat de minister van Economische Zaken weten in gesprek te gaan met de technologiebedrijven waaronder Fox-IT om hen te wijzen op "mogelijk misbruik van filtertechnologie voor antidemocratische en repressieve doeleinden."
Naar aanleiding van het gesprek volgt er op 19 april 2011 een nieuwsbericht: "Tijdens het gesprek gaven de bedrijven aan nu al zeer kritisch om te gaan met levering van hun producten aan landen waar de mensenrechtensituatie te wensen overlaat."

Toenmalig directeur Ronald Prins zegt in augustus 2011 aan Vrij Nederland dat het Delftse bedrijf kritisch is: "Fox-IT is er om de maatschappij veiliger te maken en niet om machthebbers te beschermen tegen hun eigen volk. Het is wel gebeurd dat landen waar een hoop commotie is opeens aan de lijn hangen en onze spullen willen kopen. En dan ben ik heel duidelijk: dat doen we dus niet."

De uitspraken van Prins vallen echter moeilijk te rijmen met de handel van het bedrijf met het Midden-Oosten. Fox-IT was van 2006 tot 2012 zeer actief op de markt van de surveillance-industrie in het Midden-Oosten. De Golfregio was een belangrijke afzetmarkt voor het Delftse bedrijf. Fox-IT gaf besloten workshops, onder meer in Syrië, Egypte en de Verenigde Arabische Emiraten, waarin het haar producten probeerde te verkopen aan overheidsinstanties, militairen en inlichtingendiensten. Het bedrijf richtte zich in de regio met name op de verkoop van de FoxReplay en Data Diode. De FoxReplay is vanaf 2006 op de markt en behelst interceptie-apparatuur om het internetverkeer al dan niet real time te analyseren.

De uitspraken van Prins staan ook haaks op de betrokkenheid van Fox-IT bij het Surveillance Lab in Saoedi-Arabië in 2011. Sinds december 2010 vinden daar protesten plaats tegen het regime. Het land staat al sinds 2006 op de lijst van 'Enemies of the Internet' van Reporters without Borders. In 2011 introduceert de Saoedische regering nieuwe wetgeving voor het gebruik van het internet die ernstige beperkingen van de vrijheid van meningsuiting met zich meebrengt. Zo worden alle online kranten en bloggers verplicht om een speciale licentie bij het Ministerie van Informatie aan te vragen. Bloggers en mensenrechtenactivisten worden gemonitord op sociale media en riskeren vervolging.

Dit vormt voor Fox-IT echter geen bezwaar om deel te nemen aan een project voor het opzetten van een landelijk netwerk van telefoon- en internetsurveillance.

NFI en TNO in stuurgroep

Ook de betrokkenheid van onderdelen van de Nederlandse overheid, TNO en NFI, bij het Saoedische project staat in schril contrast met de inhoud van het nieuwsbericht van het Ministerie van Economische Zaken van 11 april 2011: "Bedrijven die internetbeveiliging exporteren gaan zich samen met de overheid inspannen om misbruik van deze technologieën tegen te gaan. Zowel de bedrijven als de overheid onderschrijven het belang van internetvrijheid en onderkennen de gevaren van mogelijk misbruik van beveiligingstechnologieën."

TNO en NFI zijn bestuursorganen, maar werken niet exclusief voor de overheid, zij hebben ook private opdrachtgevers. Het NFI is het meest bekend door haar onderzoek naar DNA en sporen op plaatsen delict. TNO doet onderzoek op allerlei terreinen zoals energietransitie, milieu en circulaire economie maar ook defensie en veiligheid.

De keuze van Fox-IT om het NFI en TNO bij het project te betrekken is niet verwonderlijk. Het Delftse bedrijf heeft nauwe banden met beide organisaties. Het gaat deels om personele banden: verschillende werknemers van Fox-IT komen van het NFI en TNO en vice versa.

Ook werken de organisaties geregeld samen. Zo werkte Fox-IT met het NFI samen bij de ontmanteling van het Bredolab botnet in 2010. En werkten Fox-IT en TNO samen bij de ontwikkeling van een systeem om digitale spionage sneller te detecteren en de ontwikkeling van het Internet Recherche Onderzoek Netwerk (iRN) van de politie.

Tijdens de eerste voorbereidingsbijeenkomst van het Surveillance Lab op 16 juni 2011 in Riyad, geeft Fox-IT een power point presentatie met een voorstel voor de opzet en inrichting van het Saoedische Lab. Het bedrijf refereert in haar presentatie aan het NFI met onder meer een foto van het NFI-hoofdkantoor.

In de presentatie stipt Fox-IT tevens de gezamenlijke 'forensische' geschiedenis met AGT, het Duitse bedrijf dat een van de projectleiders is, aan. In de presentatie worden de ontwikkeling van een netwerk van tussenhandelaren in 2007 en een gezamenlijke training in Egypte in 2008 genoemd.

Vanaf het begin van de handel in het Midden-Oosten werkt Fox-IT al samen met AGT. Het in 2002 opgerichte bedrijf heeft naast Berlijn vestigingen in Dubai (Verenigde Arabische Emiraten), Syrië, Egypte en Saoedi-Arabië. Als tussenhandelaar houdt het zich met name bezig met de verkoop van Europese technologie in het Midden-Oosten.

Gezien het portfolio van het Duitse bedrijf is de betrokkenheid van TNO en het NFI bij het project opmerkelijk te noemen. AGT heeft klanten in landen met repressieve regimes, waaronder overheidsinstanties. De klantenkring van AGT is bekend bij de Nederlanders. De namen zijn namelijk gewoon terug te vinden op de website van het bedrijf, omdat AGT in de beginjaren redelijk open is over haar contacten en projecten in het Midden-Oosten.

Tijdens de tweede voorbereidingsbijeenkomst in juli 2011 in Riyad wordt het NFI door AGT genoemd als een van de leden van de stuurgroep van het project. AGT vermeldt in haar PowerPoint Presentatie op pagina 24: "Steering committee from TCC, MOI (het Saoedische Ministerie van Binnenlandse Zaken), founder of AD (Het Amerikaanse bedrijf

AccessData), CEO Guidance's (het Amerikaanse bedrijf Guidance Solutions), former Interpol Deputy, founder of the NFI, FBI Lab, former BKA Audio Forensic Lab (Bunder Kriminal Amt)".

AGT maakt in de presentatie niet duidelijk wie er wordt bedoeld met 'founder of the NFI'. Uit de via de WOB openbaar gemaakte documenten wordt echter duidelijk dat Zeno Gerardts betrokken is bij het project. Hij wordt door AGT genoemd als lid van de stuurgroep. Geradts is sinds 1992 in diverse functies werkzaam bij het NFI, onder andere als senior forensics scientist.

Ook het TNO wordt door AGT genoemd als lid van de stuurgroep. Het gaat om Arie van Tol, sinds juni 2011 Programme Manager Law Enforcement bij TNO. Hij wordt uitgenodigd voor de tweede voorbereidingsbijeenkomst in Riyad in juli.

Tijdens de voorbereidingen van deze bijeenkomst schrijft AGT in een email aan mede-projectleider TCC: "As I confirmed to you, this the passports from the 09 team member, one expert from TNO did not send his copy, but the number of the passports, (…)" Het bericht volgt op een vraag van TCC naar ondertekende NDA's geheimhoudingsovereenkomsten) en teaming agreements van de partners.

Op 13 juli 2011 mailt AGT dat alle partners een NDA hebben ontvangen en vraagt een update over de visa van de deelnemers. "This is to inform you that all the partners received the NDA Agreement, you will receive the agreements signed by the end of this week or early next week at the latest." De visumaanvragen verlopen stroef: "as part of the preparation for the upcoming meeting next week in the kingdom of Saudi Arabia, I would kindly ask you which is the status of the visa of the participants."

Op 17 juli 2011 verstuurt AGT de uitnodigingsbrieven voor de bijeenkomst. "Please find attached the copy of the invitation letter for you and Mr. Adrianus Cornelis van Tol. I will also attach the Commercial Registration of the Sponsor Company". Arie van Tol staat op de ledenlijst van de stuurgroep van het project (het 'KSA TEAM July 23 - 28, 2011').

In het Excel document 'Checklist2' van 18 juli 2011 is TNO op plaats 33 toegevoegd: "33, TNO, Adrianus Cornelis Van Tol."

Offerte van de Nederlandse holmes (NFI)

Het NFI wordt door Fox-IT betrokken bij het project vanwege haar kennis over 'Digitale Technologie & Biometrie (DTB).' Fox-IT werkt samen met de afdeling DTB die onder andere werkt aan 'Beeldbewerking & Biometrie', 'Spraak en audio,' en 'Vingersporen.' De website van de afdeling DTB heeft als domeinnaam holmes.nl.

Het NFI neemt een deel van het project voor haar rekening. Op 11 augustus mailt het NFI aan Fox-IT: "Naar aanleiding van de bespreking van gisteren heb ik bijgaande brief verwoord zoals we verder kunnen doen aan consultancy, training education etc in Saudi Arabie." Het NFI kondigt aan een offerte op te stellen.

Enkele dagen later (14 augustus) laat het NFI weten dat het maken van de offerte meer tijd in beslag zal nemen omdat de juridische afdeling er nog naar moet kijken. NFI tekent al wel een LOI (Letter of Intent). Op 15 augustus 2011 mailt een medewerker van Fox-IT aan de Divisie Digitale en Biometrie Sporen (DBS) van NFI: "Ik heb er nog een keer bij AGT op aangedrongen dat de letter of
intent wordt getekend en dat jullie met die partij contact willen hebben. Ik ga verder wel aan de slag met de informatie die we nu van jullie hebben ontvangen." Fox-IT stuurt de LOI op 19 augustus door aan AGT: "Ik heb LOI die je me hebt gestuurd aan AGT gestuurd."

Cognitech

Fox-IT betrekt ook het Amerikaanse Cognitech bij het Saoedische project. Dit bedrijf levert forensische software op het terrein van visuele dataverzameling en analyse van zowel actuele analoge en digitale informatie.

Het bedrijf schrijft op haar website dat het bij de software om "Real-Time forensic video processing, capturing, and forensic encoding software", "forensic video and image enhancement", "capturing analog and digital data media and sources" en "bio-metric and scene measurements" gaat. Een van de slogans van het bedrijf is "detect, verify and authenticate."

Cognitech bevestigt op 17 augustus haar interesse in het project. Het stuurt Fox-IT, het NFI en TNO een bericht met als onderwerp 'Cognitech in resellers Saudi Arabia region'. Hier schetst het haar visie op het Lab: "The image and video forensics lab will be 10 persons in 5 years from now. I was thinking of 2 licences and a training for 6 persons." Twee dagen later mailt Fox-IT het NFI: "Inmiddels ben ik zo ver dat ze een offerte gaan maken en Fox mag gaan resellen ;-) (smile)."

Surveillance policing van TNO

Uit de via de WOB openbaar gemaakte documenten wordt niet duidelijk welke rol het TNO heeft in de voorbereidingen van het project. TNO maakt geen documenten openbaar over haar betrokkenheid bij het project. Op 9 juli 2019 laat het weten dat er "geen e-mailverkeer van TNO met het Duitse bedrijf AGT en met het bedrijf TCC uit Saudi-Arabië is aangetroffen."

De betrokkenheid van Arie van Tol geeft echter een indruk van de expertise die TNO inbrengt. Als Programme Manager Law Enforcement is van Tol verantwoordelijk voor onderzoek op het terrein van de overlap tussen inlichtingenwerk en opsporingsdiensten zoals sensing (informatie gestuurd politiewerk), predictive policing (voorspellend politiewerk) en prescriptive policing (voorspellend effectief politiewerk gericht op interventies).

Deze onderzoeksterreinen passen in het Surveillance Lab. Zeker in een repressief regime zoals Saoedi-Arabië waar opsporing bovenal te maken heeft met het opsporen van oppositionele of afwijkende meningen en

gedragingen. Hierbij gaat het niet meer alleen om opsporing, maar om inlichtingenwerk.

NFI trekt zich terug

In september 2011 trekt het NFI zich plots terug uit het project. Het meldt op 13 september aan Fox-IT: "helaas moeten we afhaken". De reden wordt door het NFI niet openbaar gemaakt. De passages zijn in de via de Wob openbaar gemaakte documenten onleesbaar gemaakt. Een NFI-medewerker lijkt nader onderzoek te hebben gedaan naar de achtergrond en impact van het project, maar de inhoud van zijn bevindingen wordt niet openbaar gemaakt.

Fox-IT heeft zelf geen onderzoek naar het Saudische project gedaan en heeft niet onderzocht of het Lab kan bijdragen aan repressie en mensenrechtenschendingen. Het Delftse bedrijf mailt dezelfde dag: "Bedankt dat jullie dit zo zorgvuldig hebben uitgezocht. Voor fox betekent dat wij ons ondanks onze investeringen en bezoeken en offertes terugtrekken uit het project."

Op 29 september 2011 mailt Fox-IT het NFI dat AGT op de hoogte is gesteld van het besluit van het NFI: "Ik heb AGT geïnformeerd over jullie besluit en de consequentie daarvan voor Fox." De consequentie voor Fox-IT is dat het zich ook terugtrekt, maar het Delftse bedrijf doet dat dus niet uit zichzelf.

Fox-IT en het NFI worden door AGT nog wel uitgenodigd voor de inauguratie van de stuurgroep op 15-16 november 2011 in Riyad. Hans Henseler (Fox-IT) en Zeno Geradts van het NFI (Senior Forensic Scientist Digital Technology and Biometrics) worden in de uitnodiging vermeld als leden van de stuurgroep, maar er zijn geen aanwijzingen dat zij de inauguratie hebben bezocht.

Na een oproep van AGT om snel te reageren in verband met het maken van hotelboekingen: "Accommodation is being arranged and therefore I would request that you confirm your attendance at the earliest

opportunity", stuurt een AGT-medewerker een bericht vanaf zijn Iphone: "Fox and NFI are out."

TNO geeft geen openheid

TNO heeft in antwoord op het Wob-verzoek van Buro Jansen & Janssen geen documenten openbaar gemaakt over haar betrokkenheid bij het Saoedische project. Een jurist van TNO schrijft op 24 juni 2019: "Van … heb ik begrepen dat dit project (forensic lab) nimmer in samenwerking met TNO is uitgevoerd – althans heeft TNO hier niet in geparticipeerd - omdat er bezwaren rondom het project bestonden, o.a. van ethische aard."

TNO schrijft niet te hebben geparticipeerd in het project, maar de beantwoording van het Wob-verzoek laat veel vragen onbeantwoord. Het maakt niet duidelijk of het zelf onderzoek heeft gedaan naar het project en haar mogelijke bijdrage aan repressie en mensenrechtenschendingen. Evenmin wordt duidelijk hoe het kan dat TNO betrokken raakte bij de voorbereidingen van het project en welke afwegingen hierin zijn gemaakt. TNO-medewerker Arie van Tol was immers betrokken bij de voorbereidingen van het project, nam deel aan de voorbereidingsbijeenkomst in juli in Riyad en werd genoemd als lid van de stuurgroep.

Gaan Fox-IT en de overheid kritisch om met mensenrechten?

Tijdens de Arabische Lente heeft de minister van Economische Zaken een gesprek met Nederlandse bedrijven die actief zijn in het Midden-Oosten. In een verslag van het gesprek stelt het ministerie op 19 april 2011 dat "de bedrijven al zeer kritisch om gaan met levering van hun producten aan landen waar de mensenrechtensituatie te wensen overlaat."

Het surveillance lab in Saoedi-Arabië laat zien dat dit voor Fox-IT niet het geval is. Het Delftse bedrijf Fox-IT heeft zelf geen onderzoek gedaan

naar de mogelijke bijdrage van het project aan repressie en mensenrechtenschendingen. Fox-IT trekt zich pas terug uit het project naar aanleiding van de bij het NFI gerezen bezwaren.

Ook de handelwijze van de overheidsorganen NFI en TNO staat in schril contrast met het nieuwsbericht van het Ministerie van Economische Zaken van 11 april 2011, dat stelt: "Bedrijven die internetbeveiliging exporteren gaan zich samen met de overheid inspannen om misbruik van deze technologieën tegen te gaan."

Het NFI en TNO nemen echter zonder voorafgaand onderzoek deel aan de voorbereidingen van het Saoedische Surveillance Lab. Dit is opmerkelijk, zeker gezien de politieke discussie die op dat moment gaande is over de export van technologie aan repressieve regimes.

Hierbij is het opvallend dat de betrokkenen van Fox-IT, NFI en TNO tevens actief zijn in het Nederlandse onderwijs. Hans Henseler is in 2011 - naast zijn werk voor Fox-IT - ook aangesteld aan de Hogeschool Leiden als lector Digital Forensics & E-discovery en aan de Hogeschool van Amsterdam als lector E-discovery. Zeno Geradts is in 2011 - naast zijn werk voor het NFI - ook verbonden aan de Universiteit van Amsterdam als Forensic Data Scientist. Arie van Tol is niet actief in het onderwijs, maar zijn TNO-afdeling is verbonden aan ondermeer de Universiteit van Amsterdam en de TU Delft.

De betrokkenheid van Fox-IT, het NFI en TNO aan het Saoedische Surveillance Lab is een schoolvoorbeeld van het uit de weggaan van de discussie over de Nederlandse steun aan repressieve regimes en de mogelijke bijdrage van Nederlandse instellingen aan repressie en mensenrechtenschendingen.

Terug naar inhoudsopgave

Fox-IT en de overheid

Computer- en beveiligingsbedrijf Fox-IT werd in 1999 opgericht. De Nederlandse overheid werd al snel een belangrijke klant van het Delftse bedrijf. Daarnaast speelt Fox-IT een rol in de nationale veiligheid. Zo verzorgt het bedrijf de beveiliging van Nederlandse staatsgeheimen, zoals de notulen van de Ministerraad, en wordt het ingehuurd door onder andere de Nationale Politie en de ministeries van Buitenlandse Zaken, Defensie, en Justitie en Veiligheid.

De relatie tussen de overheid en Fox-IT was onderwerp van discussie in 2014, toen het Delftse bedrijf werd overgenomen door de Britse NCC Group. In de Tweede Kamer en de media werden vragen gesteld over het risico dat Nederlandse staatsgeheimen hiermee in buitenlandse handen kunnen komen. De vragen werden destijds opgeworpen, maar zijn eigenlijk nooit beantwoord. Het is natuurlijk ook de vraag of de Nederlandse overheid niet te afhankelijk is van het Delftse bedrijf.

Buro Jansen & Janssen heeft de afgelopen jaren via de Wet Openbaarheid van Bestuur informatie boven tafel proberen te krijgen over de relatie tussen de Nederlandse overheid en Fox-IT. Dit is niet eenvoudig door lange procedures, een gebrek aan transparantie van overheidszijde en zelfs een actieve rol van Fox-IT om informatie geheim te houden. Zo adviseert Fox-IT het Ministerie van Economische Zaken bepaalde informatie niet openbaar te maken omdat dit *"de belangen van De Staat, klanten, partners, relaties en medewerkers Van Fox-IT en Fox-IT zelf onevenredig zal of kan schaden."* Het Ministerie neemt de suggesties van Fox-IT over.

Buro Jansen en Janssen brengt in dit onderzoek de relatie tussen de Nederlandse overheid en Fox-IT in kaart. De relatie is innig. Er zijn personele banden en korte lijnen tussen de overheid en het bedrijf. Fox-IT wordt voor uiteenlopende opdrachten ingehuurd. Niet alleen voor onderhoud en beveiliging van de digitale infrastructuur van ministeries en andere overheidsinstanties, maar het bedrijf speelt ook een belangrijke rol in de nationale veiligheid.

Het is ook opvallend dat Fox-IT een uitzonderingspositie heeft weten te bemachtigen. Het neemt niet alleen aan actieve rol in de beantwoording van Wob-verzoeken en welke informatie door de overheid over het bedrijf openbaar wordt gemaakt. Ook heeft het bedrijf een uitzonderingspositie bedongen ten aanzien van de bedrijfsaansprakelijkheid in de Algemene Rijksvoorwaarden bij de aanbesteding van overheidsopdrachten.

Nette mensen, ex-justitie

De nauwe banden tussen Fox-IT en de Nederlandse overheid kunnen niet los worden gezien van de personele banden. De twee oprichters van het bedrijf, Ronald Prins en Menno van der Marel, kennen elkaar van het gerechtelijk laboratorium van het Ministerie van Justitie, de voorloper van het NFI (Nederlands Forensisch Instituut), waar zij beiden in de jaren 90 werken.

Ook Hans Henseler, afdelingshoofd computeronderzoek bij het gerechtelijk laboratorium en in de jaren 90 baas van Prins en van der Marel, treedt jaren later (in 2010) toe tot Fox-IT. Als directeur van Fox-IT profileert Prins zich tot cybersecurity expert van Nederland. Niet alleen de overheid gaat bij Prins te rade. Ook in de media mag hij regelmatig bij talkshows en actualiteitenprogramma's aanschuiven.

De banden tussen de overheid en het bedrijf betreffen niet alleen het NFI, maar ook de AIVD (Algemene Inlichtingen en Veiligheidsdienst). Prins werkt in 1998-1999 ook nog korte tijd bij de BVD (Binnenlandse Veiligheidsdienst), de voorloper van de AIVD. Na de verkoop van Fox-IT aan de Britse NCC Group in 2014 blijft Prins aanvankelijk nog aan als directeur, maar in 2018 keert hij terug naar de overheid. Hij wordt benoemd tot lid van de TIB (Toetsingscommissie Inzet Bevoegdheden), de commissie die toezicht houdt op de Nederlandse inlichtingendiensten.

De huidige directeur van Fox-IT, Inge Bryan, die begin 2021 in dienst trad van Fox-IT, heeft ook een verleden bij de AIVD. Vervolgens wordt zij verantwoordelijk voor Team High Tech Crime (THTC) van de Nationale Politie en vanaf 2018 cybersecurity-directeur van Deloitte Risk Advisory Nederland.

Deloitte is net als Fox-IT actief bij de beveiliging van de vitale infrastructuur, waaronder die van de overheid. Beide bedrijven kennen elkaar ook als partners van The Hague Security Delta, een samenwerkingsverband op het gebied van IT- en databeveiliging. Ronald Prins was een van de initiatiefnemers en penningmeester, Inge Bryan nam deel aan de adviesraad van het netwerk.

In een interview in MTsprout van 15 april 2014 zegt Prins dat de overheid de belangrijkste klant is van het Delftse bedrijf. Veertig procent van de omzet van het bedrijf zou van de overheid afkomstig zijn. Twee factoren hebben volgens hem geholpen bij het smeden van de relatie tussen Fox-IT en de overheid. Ten eerste natuurlijk de personele banden met het NFI. Ook na 1999 vertrekken medewerkers van het NFI regelmatig naar het Delftse bedrijf, en omgekeerd.

Prins verwijst daarnaast naar de overname van Philips Crypto in 2003, het onderdeel van Philips dat zich bezighield met de ontwikkeling van cryptografische producten. *"Daardoor hadden we ineens de mensen en de technologie in huis om staatsgeheimen te beschermen,"* aldus Prins.

Volgens Prins had het bedrijf geen concurrentie te duchten van andere bedrijven. *"Als je naar de concurrentie in het high end segment kijkt, hebben we daar in Nederland nog altijd niet van te duchten,"* zegt Prins. Fox-IT kreeg zelfs een voorkeursbehandeling door de overheid door de afwezigheid van aanbestedingsprocedures.

"Met aanbestedingsprocedures hebben we vrijwel niet te maken, de overheid komt direct naar ons toe. Nog steeds. Dat komt omdat het erg lastig is in Nederland een tweede Fox-IT op te starten. Probeer maar eens hackers te vinden die de strijd met ons aankunnen. De beste die je in Europa kan vinden, hebben we al in huis," volgens de toenmalig directeur Prins in 2014.

De goede relatie van Fox-IT met de overheid wordt niet alleen door Prins zelf gememoreerd. Ton Fintelman, beveiligingsautoriteit (BVA) bij het Ministerie van Justitie en Alfons Lammerts van Bueren, senior-beleidsmedewerker bij de Dienst Justitiële Inrichtingen vatten de verhouding tussen de overheid en het bedrijf in de Fox-IT nieuwsbrief van mei 2006 als volgt samen: *"Fox-IT wordt gezien als betrouwbare en kundige partner onder het motto 'nette mensen, ex-justitie'."* Fintelman geeft tevens aan *"blij te zijn dat Fox-IT in 2003 de unieke cryptotechnologie van Philips overnam."*

De innige relatie met de Nederlandse overheid en de kennis van Philips Crypto hebben voor het Delftse bedrijf deuren geopend. Niet alleen bij de overheid, maar ook bij bedrijven zoals T-Mobile en koepelorganisaties zoals de NVB (Nederlandse Vereniging van Banken). In het MTsprout-interview zegt Prins dat Fox-IT van alles levert van "*beveiligd bellen, bestrijding van computervirussen, het detecteren van hacks, authenticatie, het traceren van kinderporno, tot de versleuteling van staatsgeheimen."*

De goede relatie met de Nederlandse overheid zal ook hebben geholpen bij de internationale groei van het bedrijf. Vanaf 2006 wordt Fox-IT steeds meer internationaal actief. Het richt zich met name op Europa, het Midden-Oosten, Rusland en India.

Fox-IT huisleverancier overheid

Fox-IT wordt voor de meest uiteenlopende opdrachten door de Nederlandse overheid ingehuurd. Het gaat onder meer om onderhoud en beveiliging van de digitale infrastructuur van ministeries.

Zo blijkt uit via de Wob openbaar gemaakte documenten dat Fox-IT door het Ministerie van Economische Zaken in de periode 2008-2013 voor uiteenlopende zaken wordt gevraagd. In oktober 2008 wordt het bedrijf gevraagd om een offerte uit te brengen voor "*het testen van software en hardware voor de veiling van frequentieruimte 2,6 GHz."* Onduidelijk is of er ook andere bedrijven worden benaderd. Fox-IT krijgt de opdracht.

In februari 2010 verkrijgt het bedrijf een opdracht van het Agentschap Telecom, onderdeel van het Ministerie, en in juni dat jaar traint het Delftse bedrijf medewerkers in het 'rechercheren op het Internet.' De opdracht is onderhands aanbesteed. Uit de Wob-documenten wordt niet duidelijk waarom het Ministerie niet kiest voor openbare aanbesteding.

Ook in de hierop volgende jaren wordt Fox-IT door het Ministerie van Economische Zaken voor verschillende opdrachten ingehuurd. In maart 2011 voor een security audit, in augustus en november 2011 voor projecten rond een ´Audit veilingwebsite 2012´, en in het najaar van 2012 voor het ´project ER – Torenvalk´ en een training voor medewerkers.

Op 5 april 2013 ondertekenen het Ministerie van Economische Zaken en Fox-IT een opdrachtbevestiging voor niet nader gespecificeerde ´diensten, aanvullende diensten, nader onderzoek en overige diensten´. In dezelfde maand volgt een verzoek om een offerte voor een pentest (een test om de kwetsbaarheid van computersystemen te onderzoeken) en in mei en juni 2013 volgen opdrachten voor het project: 'FoxCERT - Blue Lagoon'. FoxCERT is de afdeling van het bedrijf dat zich bezighoudt met beveiligingsincidenten, 'Emergency Response & Investigations Service.'

De lijst is niet volledig. Net als andere overheidsinstanties heeft het Ministerie niet alle documenten openbaar gemaakt, zoals blijkt uit de inventarislijst die bij de beantwoording van de Wob is bijgevoegd.

Fox-IT wordt door het Ministerie van Economische Zaken vooral ingehuurd voor werkzaamheden rond het onderhoud van de digitale structuur van het ministerie. Dit is ook bij andere ministeries en overheidsinstanties het geval. De samenwerking gaat in veel gevallen echter verder.

In de loop der jaren is Fox-IT een steeds belangrijker rol gaan spelen in de nationale veiligheid en werkt hierin samen met verschillende overheidsinstantie. Ton Fintelman van het Ministerie van Justitie spreekt in mei 2006 al over de samenwerking tussen Justitie en Fox-IT die zover gaat dat het ministerie "zelfs recherchewerk aan Fox-IT uitbesteedt."

De samenwerking tussen de overheid en het Delftse bedrijf inzake nationale veiligheid wordt niet alleen duidelijk bij het Ministerie van Justitie, maar ook in ontwikkeling van de relatie tussen het Delftse bedrijf en de Nationale Politie.

Externe Politie-eenheid

Fox-IT werkt al sinds het begin van deze eeuw samen met de Nederlandse politie. Het is duidelijk dat de banden met het NFI een belangrijke rol hebben gespeeld bij het ontstaan van deze relatie. Toenmalig directeur Ronald Prins zegt hierover in april 2014 in MTsprout: *"Wat ook meehielp, is dat we door ons werk voor het Nederlands Forensisch Instituut al warme contacten met de politie onderhielden. Daarvoor hebben we in onze startersjaren onder meer geholpen bij het forensisch onderzoek naar Etienne Urka. Ook hebben we een aantal keren de laptops van politieteams beveiligd."*

De samenwerking met de politie begon bescheiden in september 2001 met de aanwezigheid van Fox-IT op de Politievak, een vakbeurs voor politie en beveiliging. In de jaren hierna raakt het bedrijf betrokken bij vertrouwelijke politie-informatie, interceptie en uiteindelijk recherchewerk. In 2003 ontvangt Fox-IT Group een POB (Particulier Onderzoeksbureau) nummer van het Ministerie van Justitie: POB 824. Particuliere beveiligingsorganisaties of recherchebureaus moeten hier een vergunning voor aanvragen.

In juni 2004 schrijft het bedrijf in haar nieuwsbrief 'Fox-IT Nieuws' over het bedrijfsonderdeel Forensic IT: *"Het forensische bedrijfsonderdeel van Fox-IT is dus uitgegroeid tot een volledige particuliere recherchetak, waarbij de digitale sporen altijd bijzondere aandacht blijven verdienen, maar de traditionele recherchetaken mogen niet over het hoofd worden gezien."*

In september 2005 bereikt de relatie tussen Fox-IT en de politie een ander niveau. Het Delftse bedrijft levert een systeem waarmee politie informatie landelijk veilig kan worden ontsloten. *"Fox-IT heeft de betreffende politieregisters van alle politieregio's, de nationale recherche en de bijzondere opsporingsdiensten hiervoor met elkaar verbonden,"* aldus Fox-IT in haar nieuwsbrief van december 2005.

Volgens Fox-IT werden *"aan deze koppeling zeer hoge veiligheidseisen gesteld aangezien het hierbij om zeer vertrouwelijke informatie gaat, die onder meer is aangeleverd door politie-informanten."*

Na het beveiligen van door politie-informanten aangeleverde informatie is het voor het bedrijf een kleine stap naar het zelf-verzamelen van informatie. Die stap zet Fox-IT in 2010. *"The Dutch police have recently purchased FoxReplay Analyst"*, schrijft het bedrijf in november 2010 in haar nieuwsbrief. FoxReplay is interceptie-apparatuur om het internetverkeer al dan niet '*real time'* te analyseren. Volgens het bedrijf heeft de politie de software al in gebruik en worden agenten getraind in het gebruik hiervan.

Toenmalig directeur Ronald Prins zegt op 15 april 2014 in het interview in MTsprout: *"Verder is de keuze om afluistersoftware te ontwikkelen een hele goede geweest. Op een dag klopte een kennis bij me op de deur met dat idee, en toen zijn we het gewoon gaan doen. Dat heeft ons veel omzet opgeleverd."*

Na de aanschaf van FoxReplay door de Nederlandse politie in 2010 neemt Fox-IT in hetzelfde jaar deel aan het oprollen van het zogenaamde Bredolab netwerk. Vanuit dit netwerk van computerservers in Nederland zouden miljoenen computers in de hele wereld geïnfecteerd worden met malware.

Fox-IT sluit samen met de THTC (Team High Tech Crime) van de landelijke politie, het NFI, Govcert (het computer ondersteuningsnetwerk van de Nederlandse overheid), het openbaar ministerie en hostingprovider Leaseweb 143 computerservers van het internet af. Volgens berichtgeving in de media speelde Fox-IT een belangrijke rol in de operatie.

Het succes van deze samenwerking wordt door sommige onderzoekers overigens betwijfeld. Michel van Eeten, hoogleraar bestuurskunde aan de faculteit Techniek, Bestuur & Management van de TU Delft zegt op 2 november 2010 in Computable dat *"het Bredolab-netwerk nooit is opgerold."*

Volgens de wetenschapper werden weliswaar *"op maandag 25 oktober de servers uitgeschakeld waarop de commando- en controlesoftware van dit botnet draaide,"* maar volgens de hoogleraar bleven *"de bots in het netwerk gewoon in de lucht."* Van Eeten stelt zelfs dat *"de KLPD het aantal machines dat door het botnet is geïnfecteerd met een factor tien overdrijft."*

Succesvol of niet, Fox-IT heeft zijn positie in het recherchewerk verstevigd. Een jaar later, in 2011, leidt het bedrijf een onderzoek naar een hack bij het bedrijf DigiNotar. DigiNotar geeft digitale certificaten uit die echtheid garanties moeten bieden. Klanten van DigiNotar zijn, naast de Belastingdienst, ook bedrijven als Google en Microsoft.

Fox-IT wordt door DigiNotar ingehuurd om het onderzoek naar de hack uit te voeren. Het is opvallend dat DigiNotar kiest voor het inhuren van de private onderneming Fox-IT. DigiNotar wendt zich niet tot de politie (THTC) of het NCSC (Nationaal Cyber Security Centrum), dat onder de NCTV (Nationaal Coördinator Terrorisme en Veiligheid) valt, en in Nederland als nationale emergency reponse dienst fungeert.

B.V. Staatsgeheimen: Fox Crypto B.V.

De overname van een deel van Philips Crypto in 2003 is een belangrijke stap in de ontwikkeling van Fox-IT. Het opent deuren bij de Nederlandse overheid, met name rond zaken betreffende de nationale veiligheid. Het Delftse bedrijf kondigt dit bij de overname eigenlijk zelf al aan.

In haar persbericht van 6 november 2003 met de kop *"Fox-IT levert door overname nu ook staatsgeheim beveiliging,"* zegt het bedrijf zich ook op de markt van de *"bescherming van staatsgeheimen"* te begeven en producten voor *"het beveiligen van de opslag en communicatie van staatsgeheimen"* te ontwikkelen.

Hiermee wordt de afhankelijkheid van de Nederlandse overheid van Fox-IT groter. Volgens het bedrijf zelf zijn *"met name de Ministeries van Defensie en Buitenlandse Zaken gebruikers van dit soort geavanceerde cryptografische oplossingen."*

Het gaat bijvoorbeeld om de beveiliging van de notulen van de Ministerraad en - in samenwerking met het Zweedse bedrijf Sectra - de beveiliging van telefoons van leden van het kabinet en hoge ambtenaren.

De samenwerking met Sectra is niet los te zien van de overname van Philips Crypto. Voor die overname sluit het Delftse bedrijf in 2003 een overeenkomst met de Zweden. In de vijfde Fox-IT nieuwsbrief van oktober 2003 schrijft het bedrijf: *"Fox-IT heeft een unieke overeenkomst gesloten met het Zweedse bedrijf Sectra. Dit bedrijf is als enige op de wereld in staat gebleken om een gsm te ontwikkelen die door de NATO is goedgekeurd tot op het niveau van NATO Secret."*

In het artikel maakt Fox-IT ook duidelijk op welke wijze zij commercieel belang hebben bij deze overeenkomst: *"De nieuwste ontwikkeling van Sectra is een losse bluetooth crypto module. Via dit kleine kastje en een normale mobiele telefoon die bluetooth ondersteunt, kunt u gesprekken voeren die door niemand af te luisteren zijn."* Fox-IT gaat de bluetooth crypto module aanbieden.

Het bedrijf brengt het werk met betrekking tot staatsgeheimen onder in een zelfstandige onderneming: Fox Crypto B.V. Dit bedrijf blijft honderd procent eigendom van Fox-IT.

Een paar jaar later, eind 2007, gaat Fox-IT samen met Sectra beveiligde telefoons leveren aan leden van het kabinet en hoge ambtenaren. De website electrospaces.net meldt hierover: *"The partnership between Fox-IT for the management and Sectra as the supplier of the hardware was established in 2007 by the VECOM (Veilige Communicatie) contract. Under this contract all Dutch cabinet members and high-level officials of their departments are provided with secure phones."*

Een analyse van een foto van de telefoons van premier Rutte uit 2012 door dezelfde website duidt op het gebruik van een Sectra Tiger XS Office. In 2003 adverteerde Fox-IT na de overeenkomst met Sectra al met de Tiger XS op haar website. Bijna tien jaar later gebruikt de Nederlandse premier de telefoon uit de Fox-IT advertentie nog altijd.

Hacktests voor Buitenlandse Zaken

In 2003 leveren de overname van Philips Crypto en de overeenkomst met Sectra Fox-IT een unieke positie op ten opzichte van de Nederlandse overheid, met name rond kwesties van nationale veiligheid. Fox-IT noemde in haar persbericht bij de overname van Fox Crypto in 2003 al dat *"met name de Ministeries van Defensie en Buitenlandse Zaken gebruikers zijn van dit soort geavanceerde cryptografische oplossingen."*

In de loop der jaren wordt het Delftse bedrijf regelmatig ingehuurd door het Ministerie van Buitenlandse Zaken. Zo gaat het bedrijf onder andere smartphone hack tests voor het Ministerie uitvoeren. Op 5 maart 2009 aanvaardt Fox-IT de 'Opdracht Hack test Iphone'. Het ministerie vraagt Fox-IT: *"Voor deze Iphone dient een hack test uitgevoerd te worden. De hacktest zal zich met name concentreren op de DME (Dynamic Mobile Exchange)."* In juni 2010 verzoekt Buitenlandse Zaken om een *"hertest DME Iphone."*

Een jaar later, eind 2011, is de BlackBerry aan de beurt. "Op dit moment heeft de gebruiker daarbij weinig vrijheden om van de functionaliteiten van het BlackBerry toestel gebruik te maken. Het Ministerie is voornemens om hier verandering in aan te gaan brengen door gebruik te maken van BlackBerry Balance; Balance maakt een scheiding tussen 'privé' en 'zakelijk' mogelijk op een BlackBerry toestel. Dit betekent meer concreet dat op een BlackBerry toestel een 'container" met BZ-Outlookinformatie komt te staan", schrijft een ambtenaar van het Ministerie.

Het werk voor het Ministerie van Buitenlandse Zaken bestrijkt echter meer dan alleen de beveiliging van de communicatie. Fox-IT wordt door het Ministerie ook regelmatig ingehuurd voor opdrachten met betrekking tot de gehele digitale infrastructuur, zoals versleuteling, beveiliging, onderzoek aan systemen en datarecovery.

Op 8 september 2010 wordt het ondersteuningscontract van het Ministerie met Fox-IT gewijzigd van *"het 'oude' supportcontract naar het strippenkaart contract"*, zo blijkt uit openbaar gemaakte documenten. Onderdelen van de contract wijziging zijn onder andere "*de 'Support Fox Fort File Encryptor (FFFE)' en 'Support Fox Random Card (FRC)' die worden gewijzigd in telefonische ondersteuning voor … problemen. Daarnaast valt de reparatie en het herladen van de kaarten onder het strippenkaart contract net als de data retrieval van defecte harde schijven en de ondersteuning bij de jaarlijkse sleutelwisseling."*

Naast versleutelingswerk vraagt het Ministerie Fox-IT in 2011 om onderzoek te doen naar ´Remote Toegang Diensten´. Het Ministerie wil de beveiliging van de 'Citrix Access Gateway´ onderzocht hebben. In 2012 vraagt Buitenlandse Zaken om de beveiliging van alle internettoegang te onderzoeken: *"De standaard IT-diensten bestaan uit de volgende generieke diensten: E-mail, kantoorautomatiseringspakket, intranet, internet op de Werkplek, opslagcapaciteit op netwerk, overige standaard applicaties, printfaciliteiten, backup en recovery van opgeslagen gegevens."*

De relatie tussen het Ministerie van Buitenlandse Zaken en Fox-IT is dusdanig dat het Ministerie zich ook voor de aanschaf van middelen en workshops tot het Delftse bedrijf wendt. In 2013 kan het NBV (Nationaal Bureau voor Verbindingsbeveiliging) van de AIVD, dat de Rijksoverheid ondersteunt bij de beveiliging van bijzondere informatie, zoals staatsgeheimen, geen Fort Fox File Encryptor (FFFE) Cards leveren. Het ministerie besluit in alle haast 150 FFFE Cards direct bij Fox-IT te kopen.

Ditzelfde herhaalt zich bij contraspionage en informatiebeveiliging. In hetzelfde jaar wordt Fox-IT ook ingehuurd voor het doorlichten van het Ministerie met betrekking tot spionageweerbaarheid, `Assessment Spionageweerbaarheid´ en het geven van een workshop informatiebeveiliging.

Geheim en confidentieel werk voor Defensie

Naast het Ministerie van Buitenlandse Zaken noemt Fox-IT in haar persbericht van 2003 ook het Ministerie van Defensie als potentiele gebruiker van haar cryptografische producten. Ook dit Ministerie huurt het Delftse bedrijf sinds 2006 in voor verschillende opdrachten. Defensie geeft echter geen openheid over het type werkzaamheden. In de documenten is veel onleesbaar gemaakt, sommige informatie is als geheim geclassificeerd en sommige informatie als confidentieel.

Wel wordt uit de Wob documenten duidelijk dat Fox-IT veel te maken heeft met de MIVD (Militaire Inlichtingen- en Veiligheidsdienst). In verband met de verantwoordelijkheid voor de beveiliging van Nederlandse staatsgeheimen moet Fox-IT allerlei aanvullende maatregelen nemen, zoals verhoogde screening, extra beveiliging en incidentrapportages aan de MIVD.

Zo is het Hoofd Afdeling Contra-inlichtingen en Veiligheid van de MIVD verantwoordelijk voor de screening en benoeming van beveiligingsfunctionarissen bij Fox-IT en Fox Crypto B.V. Er is geregeld contact tussen de directeur van het Delftse bedrijf en de MIVD, zoals bijvoorbeeld in juli 2007: *"Naar ik heb begrepen heeft op 18 juli 2007 tussen jou, … een gesprek plaatsgevonden om de overdracht te bespreken en … te introduceren. Tijdens dit gesprek is geen bezwaar gerezen vanuit alle partijen ten aanzien van de vervulling van de functie van (sub)beveiligingsfunctionaris door …"*

Naast deze screening meldt Fox-IT incidenten over pogingen tot inbraak, het afgaan van het alarm bij het Bureau Industrieveiligheid van de MIVD en indicaties van verdachte activiteiten. Zo meldt Fox-IT op 15 januari en 17 mei 2006 pogingen tot inbraak. Op zondag 24 september 2006 een *"melding door het alarmsysteem van de businessunit Fox Crypto."* Drie dagen later meldt een Fox-IT medewerker dat hij een man van middelbare leeftijd foto's heeft zien maken van het pand van Fox-IT.

Onderdeel van de nationale veiligheidsstructuur

Fox-IT heeft zich vanaf 2003 ontwikkeld als onmisbaar onderdeel van de nationale veiligheid. Dit blijkt niet alleen uit haar werk voor de politie en de Ministeries van Buitenlandse Zaken en Defensie, maar ook uit haar intensieve relatie met de NCTV (Nationaal Coördinator Terrorisme en Veiligheid), onderdeel van het Ministerie van Justitie en Veiligheid.

Fox-IT wordt door de NCTV onder meer ingehuurd voor onderhoud en beveiliging van de digitale infrastructuur, zoals hardware, opslagcapaciteit, backups, webruimte, migratie en trainingen, met de bijbehorende servicecontracten.

In 2009 is er sprake van 'de levering (en installatie) van de goederen/diensten zoals vermeld op bijgevoegde bestellijst.' Ook in 2009 verzorgt Fox-IT diverse trainingen voor NCTV-medewerkers. In april 2012 gaat het om de huur van hardware voor ´CC-NCTV Voorstel Traffic Assesment´. In de zomer van 2012 huurt de terrorismecoördinator Fox-IT in voor de ´levering van de goederen en diensten … ten behoeve van de backup- en uitwijklocatie van de NCTV´. En eind 2012 voor ´twee splinternieuwe … voor FTP en SMTP´ en ´analyse omvang apparatuur aan internet´.

De NCTV huurt het Delftse bedrijf niet alleen in voor onderhoud van de digitale infrastructuur, maar werkt ook met Fox-IT samen bij internationale oefeningen en beveiliging van internationale evenementen.

In maart 2013 wordt het bedrijf gevraagd voor de levering van programmatuur aan het NCSC (Nationaal Cyber Security Centrum), een onderdeel van de NCTV. De apparatuur wordt gebruikt tijdens de wereldwijde oefening Cyber Storm IV. De oefening is onderdeel van de Cyber Storm oefeningen van het Amerikaanse Department of Homeland Security, waarbij de weerbaarheid van overheden tegen aanvallen op het internet worden getest.

Een jaar later wordt Fox-IT door de NCTV zelfs gevraagd om voor de NSS 2014 (Nucleair Security Summit) 'een extra cyber-weerbaarheid-inventarisatie uit te voeren'. Tijdens de NSS 2014 op 24 en 25 maart 2014 zijn grote delen van Den Haag en omgeving niet toegankelijk voor het publiek door het verblijf van vele regeringsleiders waaronder de Amerikaanse president. Vrijheid van meningsuiting en het recht op manifestatie is in die periode verregaand ingeperkt. Ook wordt het Delftse bedrijf gevraagd om 'een spoedonderzoek op de netwerkdata van de online accreditatie omgeving van de NSS' uit te voeren.

Ook het Ministerie van Buitenlandse Zaken roept tijden de NSS 2014 de hulp van Fox-IT in voor de opdracht 'NSS red teaming.' Het bedrijf wordt gevraagd de weerbaarheid van het ministerie te testen tegen fysieke en digitale dreigingen, zowel van binnenuit als van buitenaf. Op 17 februari 2014 wil Fox-IT voor deze opdracht *"de beschikking krijgen over een aantal accounts voor de website."*

Tevens geeft het Delftse bedrijf aan dat ze *"vanaf vanavond ook BZ medewerkers gericht aanvallen. … We willen graag aanstaande vrijdag bij jullie intern testen. Enerzijds vanaf een systeem van een reguliere BZ medewerker (geen IT beheerder), anderzijds vanaf een zelf meegebracht systeem wat we aan jullie netwerk koppelen."* De oefening duurt tot in maart. Op 14 maart 2014 meldt Fox-IT *dat "de relevante logging op onze C&C server helaas is gecrashed. We hebben deze week wel een remote uninstall gedaan, dus de machine zou opgeschoond moeten zijn."* Wat de gecrashte server betekent

voor het resultaat en de kwaliteit van het werk van Fox-IT is door het Ministerie van Buitenlandse Zaken niet openbaar gemaakt.

Soort standaardafwijking Rijksvoorwaarden voor Fox-IT

De opdracht aan Fox-IT voor de NSS 2014 bevat een opvallende passage. In het plan van aanpak schrijft de NCTV over het werk dat het Delftse bedrijf: *"Hoewel Fox-IT leidend is bij het uitvoeren van de werkzaamheden, bestaat de mogelijk voor externen van de overheid, betrokken te worden bij de aanpak en eventueel uitvoering van de werkzaamheden."*

Fox-IT heeft dus een leidende rol bij de opdracht. Dit is op zichzelf al opmerkelijk. Het gaat echter verder. Het Delftse bedrijf bedingt speciale voorwaarden bij het verkrijgen van overheidsopdrachten.

De overheid hanteert bij het uitbesteden van opdrachten aan externe bedrijven de Algemene Rijksvoorwaarden voor het verstrekken van opdrachten (ARVODI). Deze voorwaarden worden periodiek gewijzigd in 2008, 2011 en 2014. Uit openbaar gemaakte documenten wordt duidelijk dat Fox-IT regelmatig een uitzonderingspositie bedingt op de Rijksvoorwaarden. Dit is bijvoorbeeld het geval bij een offerte van Fox-IT Crypto (datum niet openbaar gemaakt) voor een opdracht bij de politie.

Hiervoor zijn in beginsel de Rijksvoorwaarden ARIV 2008 en ARVODI 2008 van toepassing. Fox-IT bedingt echter een aansprakelijkheidsbeperking. Het bedrijf levert de Dienst Operationele Ondersteuning (Meldpunt Cybercrime) een dienst, mogelijk een VPN-applicatie, maar wil niet aansprakelijk gesteld worden voor de geleverde dienst.

Het is op zich al opmerkelijk dat het bedrijf geen aansprakelijkheid accepteert voor de door het bedrijf geleverde dienst, maar daar blijft het niet bij. Fox-IT wijst de Rijksvoorwaarden af en hanteert in de offerte haar eigen voorwaarden. Het Delftse bedrijf schrijft de politie: *"Algemene voorwaarden van het KLPD (Korps Landelijke*

Politiediensten red.), alsmede andere in de branche van het KLPD gebruikelijke voorwaarden, zijn niet van toepassing en worden door Fox-IT uitdrukkelijk van de hand gewezen, tenzij Fox-IT deze geheel of gedeeltelijk uitdrukkelijk schriftelijk heeft aanvaard. Een dergelijke aanvaarding kan niet worden afgeleid uit het onweersproken blijven van een mededeling van het KLPD dat deze de ICT Officevoorwaarden niet aanvaardt en zijn eigen voorwaarden van toepassing verklaart" (datum niet openbaar gemaakt).

Deze opstelling van Fox-IT is geen uitzondering. Het bedrijft stelt zich bij meer opdrachten voor de politie op een vergelijkbare wijze op. Bij een andere goedgekeurde offerte (datum niet openbaar gemaakt) wijst het bedrijf ook elke verantwoordelijkheid van de hand. *"Fox-IT aanvaardt geen aansprakelijkheid ten aanzien van eventuele schade die direct of indirect voortvloeien uit de werkzaamheden die Fox Crypto BV uitvoert in opdracht van de opdrachtgever."*

Het Delftse bedrijf bedingt niet alleen bij de politie een aparte positie. Ook bij opdrachten voor de NCTV heeft Fox-IT bij de onderhandelingen voor opdrachten in 2014 *"een soort standaardafwijking van ARVODI"* weten te bedingen aldus een ambtenaar in een e-mail van 15 mei 2014.

Op 11 juni 2014 schrijft een ambtenaar van de NCTV een mail met het onderwerp ARVOD 2014: *"Zou je dit met … kunnen kortsluiten? Hij geeft aan dat we normaal gesproken akkoord gaan met de voorwaarden van Fox-IT."* Al eerder, in e-mail van Fox-IT 19 september 2012, had Fox-IT aangegeven bij de *"aansprakelijkheid en intellectueel eigendom een paar kanttekeningen plaatsen."* Het Ministerie van Justitie en Veiligheid heeft niet openbaar gemaakt welke kanttekeningen het bedrijf hier precies heeft.

Korte lijnen met overheid en kabinet

Fox-IT heeft een speciale positie bij de overheid. Dit blijkt niet alleen uit haar uitzonderingspositie bij de Rijksvoorwaarden, maar ook uit de korte lijnen met ambtenaren, ambassades, het kabinet en

vakministers. Tijdens eerder onderzoek van Buro Jansen & Janssen naar Fox-IT kwam dit slechts zijdelings aan bod.

Zo vertelt Matthijs van der Wel, toenmalig Manager Business Development EMEA (Europe, Middle East and Africa) tijdens een zakenreis in 2007 in Dubai aan de Duitse zakenpartner AGT van Fox-IT dat hij *"an urgent meeting with the Dutch government"* heeft. Eerst moet hij daarvoor terug naar Nederland, later besluit hij te blijven en het overleg telefonisch te voeren. Wat de verkoopmanager van Fox-IT in het Midden-Oosten moet bespreken met het Nederlandse kabinet is niet openbaar gemaakt. Het is vreemd dat van der Wel deze informatie deelt met een twijfelachtige handelspartner als AGT.

In het buitenland vindt Fox-IT een gewillig oor bij de Nederlandse ambassades. Wanneer het bedrijf in 2007 voor verkoopactiviteiten in het Midden-Oosten besloten workshops geeft aan overheidsinstanties, militairen en inlichtingendiensten in onder meer Egypte, Syrië, Saoedi-Arabië en de Verenigde Arabische Emiraten, heeft Fox-IT afspraken met de Nederlandse ambassades in onder andere Saoedi-Arabië en Syrië. In Syrië een lunchafspraak een dag voor een workshop aan vertegenwoordigers van de Syrische overheid en inlichtingendiensten.

Het Delftse bedrijf trekt zelfs in 2011 samen op met twee Nederlandse overheidsinstanties, het NFI en TNO (Nederlandse Organisatie voor Toegepast natuurwetenschappelijk Onderzoek) bij de voorbereidingen van een Surveillance Lab in Saoedi-Arabië. Het Surveillance Lab behelst het opzetten van een landelijk netwerk van telefoon- en internetsurveillance onder verantwoordelijkheid van het Saoedische Ministerie van Binnenlandse Zaken.

In het MTsprout interview van april 2014 geeft voormalig Fox-IT directeur nog een ander voorbeeld van een korte lijn met de top van de Nederlandse overheid. Hij suggereert de toenmalige Minister van Defensie Jeanine Hennis-Plaschaert te hebben gepolst voor investeringen in de cyber security branche, waartoe ook zijn eigen bedrijf Fox-IT behoort. Prins zegt in het interview dat de minister *"op dezelfde lijn lijkt te zitten als wij"* (Fox-IT).

Als voorbeeld van die lijn noemt Prins het in die periode opgerichte The Hague Security Delta (HSD). Volgens Prins *"kan dat uitgroeien tot een soort van Silicon Valley."* In de loop der jaren worden in de media echter vraagtekens gezet bij het succes van HSD. Het initiatief zou veel subsidie hebben ontvangen, maar niet veel hebben opgeleverd. Ook in de Haagse gemeenteraad zijn vragen gesteld over The Hague Security Delta.

De overheid doet wat Fox-IT wil bij de Wob

Fox-IT heeft een speciale positie bij de overheid. Door de personele banden en de verscheidenheid aan opdrachten waarvoor het Delftse bedrijf wordt ingehuurd zijn er korte lijnen. Opvallend bij die innige relatie tussen Fox-IT en de overheid is de actieve betrokkenheid van het bedrijf bij de beantwoording van Wob-verzoeken door bestuursorganen.

Buro Jansen & Janssen heeft in de loop der jaren veel Wob-verzoeken bij de overheid ingediend over haar relatie met Fox-IT. De overheid maakt in antwoord op die Wob-verzoeken enige documenten openbaar, maar veel documenten worden niet openbaar gemaakt en veel informatie is onleesbaar gemaakt. Dit is op zichzelf eerder regel dan uitzondering bij de beantwoording van Wob-verzoeken, maar bij Wob-verzoeken over Fox-IT is nog iets anders aan de hand. Het bedrijf heeft een actieve rol in de beantwoording van de Wob-verzoeken en zorgt er hiermee voor dat er nog minder informatie openbaar wordt gemaakt.

Bij verzoeken op grond van de Wet Openbaarheid van Bestuur kunnen derden in gelegenheid worden gesteld om een zienswijze te geven over de documenten die de overheid openbaar maakt. Fox-IT geeft niet alleen een zienswijze, maar bemoeit zich actief met de beantwoording en voegt zich in juridische procedures.

Naar aanleiding van de Wob-verzoeken zoekt toenmalig directeur Ronald Prins in 2014 direct contact met Jansen & Janssen. Het Delftse bedrijf is geïnformeerd over de ingediende WOB-verzoeken.

Het is op zich gebruikelijk dat bedrijven een zienswijze mogen indienen. Het is echter zeer opmerkelijk dat de overheid voor de zienswijze-fase Fox-IT informeert over de identiteit van de indiener van de Wob-verzoeken, omdat de privacy van indieners door de overheid conform Artikel 8 van de Wet Bescherming Persoonsgegevens beschermd dient te worden.

Na deze benadering heeft Buro Jansen & Janssen bij diverse Ministeries een Wob-verzoek ingediend over de wijze waarop de Wob-verzoeken over Fox-IT zijn afgehandeld. Het Ministerie van Economische Zaken maakt hierop documenten openbaar waaruit blijkt dat het bedrijf aanzienlijke invloed heeft bij de beantwoording van het bij het Ministerie ingediende Wob-verzoek over Fox-IT en welke informatie door het Ministerie wel en niet openbaar wordt gemaakt.

Fox-IT schrijft op 15 juli 2014: *"Fox-IT stelt dat het overleggen van bepaalde documenten of onderdelen daarvan de belangen van De Staat, klanten, partners, relaties en medewerkers van Fox-IT en Fox-IT zelf onevenredig zal of kan schaden."*

Vervolgens bekijkt Fox-IT zelf de stukken en schrijft het Ministerie voor welke informatie niet openbaar gemaakt mag worden: *"In de bijgevoegde documenten zelf is met een markeerstift aangegeven welke onderdelen van de betreffende documenten wat Fox-IT B.V: betreft niet geopenbaard kunnen worden. Deze onderdelen dienen dan ook deugdelijk te worden verwijderd of onherkenbaar te worden gemaakt."*

In een begeleidende brief bij de door Fox-IT met markeerstift bewerkte documenten concludeert het bedrijf tevreden: *"Fox-IT heeft overigens ook begrepen dat op de documenten op de genoemde wijze zullen worden aangepast?"*

Fox-IT heeft niet alleen een actieve rol tijdens de primaire en bezwaarfase van Wob-verzoeken, maar ook tijdens de beroepsfase. Zo wordt Fox-IT in 2017 door de rechtbank toegelaten als belanghebbende bij de behandeling van een in 2014 ingediend Wob-verzoek van Buro Jansen & Janssen bij de Nationale Politie. Het bedrijf mag als derde partij, naast de politie, optreden als verweerder.

De gang van zaken rond het Wob-verzoek is opmerkelijk. In 2014 vraagt Buro Jansen & Janssen openbaarmaking van alle documenten over de relatie van de politie met Fox-IT. Zoals gewoonlijk wil de politie zo min mogelijk openbaar maken. Fox-IT deelt dat standpunt.

Uiteindelijk worden er in maart 2018 na de beroepsfase enkele stukken openbaar gemaakt. In deze documenten is zelfs een deel van het briefhoofd van een van de documenten onleesbaar gemaakt. Boven een opdracht van ´Hardware support … Equipment March 2013 – June 2013´ staat ´Fox …, a Wholly-Owned Subsidiary of NetScout Systems, Inc.´

Na Fox moet Replay staan, Fox-IT verkoopt op 26 september 2011 FoxReplay aan het Amerikaanse bedrijf Netscout dat lange tijd nog als FoxReplay door Netscout wordt aangeboden. In de General Terms van de overeenkomst tussen landelijke eenheid van de politie en Netscout komt de naam van het Amerikaanse bedrijf niet voor, maar wordt er gesproken over FoxReplay al is Replay dan wel zwartgemaakt.

In 2010 schreef Fox-IT nog trots in haar nieuwsbrief: *"The Dutch police have recently purchased FoxReplay Analyst."* Tien jaar later wil het bedrijf voorkomen dat haar naam gekoppeld wordt aan de afluister software.

Beantwoording van Kamervragen door Fox-IT

Fox-IT heeft dus veel invloed op welke informatie over het bedrijf door de Nederlandse overheid naar buiten wordt gebracht. Dit blijkt niet alleen uit de beantwoording van de Wob-verzoeken, maar bleek ook al eerder bij de beantwoording van Kamervragen in oktober 2011.

Op 17 oktober 2011 stelt Tweede Kamerlid El-Fassed Kamervragen over de export van internetfilters en aftaptechnologie door Nederlandse bedrijven aan de Minister van Economische Zaken. Uit openbaar gemaakte documenten blijkt dat Fox-IT de ministeriële antwoorden dicteert.

Op 27 oktober vindt er, naar aanleiding van de Kamervragen, een gesprek tussen het Ministerie en een aantal bedrijven, waaronder Fox-IT, plaats. Het Ministerie legt de concept-antwoorden op 21 november 2011 aan Fox-IT voor: *"Ik wil u vragen om te bevestigen dat u akkoord kunt gaan met de vermelding van uw antwoorden zoals verwoord in antwoord 3. Ik heb de vrijheid genomen hier en daar een klein beetje te redigeren, maar heb getracht uw antwoorden zoveel mogelijk intact te laten."* Fox-IT is tevreden dat het ministerie haar tekst heeft overgenomen en antwoordt met een smiley: *"Geen bezwaar. Voor zover dat bericht niet al binnen was gekomen."*

Fox-IT krijgt zijn zin. In de Kamerbrief van 18 januari 2012 worden de bedrijven die bij het gesprek aanwezig waren geciteerd. In de Kamerbrief wordt zeer summier naar Fox-IT verwezen in een zin, welke integraal afkomstig is uit de e-mail van het bedrijf aan het Ministerie van 26 oktober: *"Fox IT is niet langer actief op het gebied van Lawful Interception. Alle activiteiten op dit gebied zijn overgenomen door het Amerikaanse bedrijf NetScout."*

Onevenwichtige relatie Fox-IT en overheid?

De verhouding tussen de Nederlandse overheid en het betrekkelijke kleine bedrijf Fox-IT is opmerkelijk te noemen. In de loop van een decennium hebben voormalig medewerkers van politie, justitie en inlichtingendiensten een bedrijf opgezet dat op allerlei niveaus voor de overheid werkt.

Fox-IT werkt samen met ministeries en andere overheidsinstanties bij een verscheidenheid van opdrachten. Zo werkt het samen bij opsporingsonderzoeken, bij het uitzetten van servers die voor criminele doeleinden worden gebruikt, beveiligt het staatsgeheimen, verzorgt het versleutelde communicatie, voert hacktests uit, wordt het ingehuurd voor de aanschaf van apparatuur, verzorgd het workshops, helpt het mee bij oefeningen van NAVO-partners, en is het betrokken bij de accreditatie van een internationale cyber conferentie waar de President van de Verenigde Staten aanwezig is.

De lijst aan overheidsopdrachten is zonder meer indrukwekkend. Het is echter ook een lijst die vragen oproept.

Het is ten eerste de vraag of de Nederlandse overheid te afhankelijk is van Fox-IT. Een vraag die na de overname in 2014 door de Britse NCC Group nog een andere dimensie heeft gekregen. Het is namelijk niet alleen de vraag hoe veilig Nederlandse staatsgeheimen zijn bij een bedrijf dat in buitenlandse handen is gekomen, maar het gaat ook om de veiligheid van allerlei andere door Fox-IT verzorgde diensten zoals versleutelde communicatie en hacktests.

De tweede vraag heeft betrekking op de onderhandelingspositie van Fox-IT bij het aannemen van opdrachten van de overheid.
Het bedrijf heeft een innige relatie met de overheid, waarbij Fox-IT opdrachten krijgt zonder aanbesteding, een speciale positie heeft bedongen bij de Rijksvoorwaarden, een grote rol heeft bij de openbaarmaking van documenten en bij de beantwoording van Kamervragen.

Vloeit deze onderhandelingspositie en de daarbij gepaard gaande mogelijkheid om eisen te stellen voort uit de afhankelijkheidspositie van de overheid, de omvang en verscheidenheid van de opdrachten die het bedrijf uitvoert, de korte lijnen en personele banden met de overheid, oftewel de innige relatie tussen opdrachtgever en opdrachtnemer. Of werken er gewoon goede onderhandelaars bij het Delftse bedrijf?

De derde vraag draait om controle en toezicht op Fox-IT door de overheid. Deze vraag vloeit voort uit zowel de afhankelijkheid als de onderhandelingspositie. Is de Nederlandse overheid namelijk wel in staat om een bedrijf als Fox-IT te controleren bij de opdrachten die het voor de overheid uitvoert, maar ook bij het verstrekken van vergunningen die het bedrijf nodig heeft.

Over een van die vergunningen, exportvergunningen, gaat het onderzoek ‘Fox-IT en het Nederlandse exportbeleid voor dual-use goederen’ van Buro Jansen & Janssen van februari 2020. Dit onderzoek toont aan dat er in de praktijk geen sprake was van risicoanalyse om ongewenst eindgebruik te voorkomen, omdat de Afdeling Exportcontrole meer prioriteit gaf aan het faciliteren van de export van het Delftse bedrijf. Fox-IT verstrekt de Afdeling Exportcontrole nauwelijks informatie over de eindgebruikers van de te exporteren producten en overheid vraagt het bedrijf nauwelijks om informatie.

De relatie tussen de Nederlandse overheid en Fox-IT is dus in meerdere opzichten onevenwichtig. Dit klemt te meer daar zowel de overheid als Fox-IT, onder meer bij de beantwoording van WOB-verzoeken, de indruk wekken iets verborgen te willen houden.

Terug naar inhoudsopgave

Documenten bij het onderzoek naar Fox-IT

Hieronder vindt u een selectie van de gebruikte documenten. Voor het onderzoek is veel meer informatie verzameld.

Dit onderzoek is gebaseerd op Wob-documenten, open bronnen, interne bedrijfsdocumenten en e-mails met betrekking tot de relatie van Fox-IT met haar partner, het Duitse bedrijf AGT (Advanced German Technology), die Buro Jansen & Janssen heeft ontvangen en documenten uit de Hacking Team hack. Het onderzoek borduurt voort op de onderzoeken 'Fox-IT in het Midden-Oosten' en 'Fox-IT en het Nederlandse exportbeleid voor dual-use goederen' en maakt deel uit van een breder onderzoeksprogramma van Buro Jansen & Janssen naar Westerse bedrijven en overheden en hun rol in de opbouw van de surveillance staat zowel in eigen land als in repressieve regimes zoals Rusland en landen in het Midden-Oosten.

In een e-mail en per brief heeft Buro Jansen & Janssen verschillende vragen gesteld aan Fox-IT (e-mail zit bij de documenten). Fox-IT heeft geen antwoord gegeven.

- Fox-IT in Rusland (samenvatting)
- Fox-IT in Rusland (onderzoek)

- Het NFI en TNO werkten met Fox-IT aan een Surveillance Lab in Saoedi-Arabië tijdens de Arabische Lente

- Fox-IT en de Nederlandse overheid

- Gehele Onderzoek: Fox-IT in Rusland (pdf)

- Vragen aan Fox-IT gesteld op 7, 13, 19 en 20 mei 2021

Fox-IT en het Nederlandse exportbeleid voor dual-use goederen, onderzoek in 2020

- Documenten bij het onderzoek Fox-IT en het Nederlandse exportbeleid voor dual-use goederen
- Vragen van Buro Jansen & Janssen aan Fox-IT
- Antwoord van Fox-IT op vragen van Buro Jansen & Janssen
- Fox-IT exporteerde zonder exportvergunning naar het Midden-Oosten (samenvatting)
- Fox-IT en het Nederlandse exportbeleid voor dual-use goederen (onderzoek)
- Documenten Fox-IT en het Nederlandse exportbeleid voor dual-use goederen (documenten)
- Fox-IT exporteerde zonder exportvergunning naar het Midden-Oosten (pdf)
- Fox-IT en het Nederlandse exportbeleid voor dual-use goederen (pdf)
- Documenten Fox-IT en het Nederlandse exportbeleid voor dual-use goederen (pdf)
- Het gehele onderzoek Fox-IT en het Nederlandse exportbeleid voor dual-use goederen (pdf)

Fox-IT in het Midden-Oosten, onderzoek in 2019

- Documenten bij het onderzoek Fox-IT in het Midden-Oosten
- Vragen van Buro Jansen & Janssen aan Fox-IT
- Antwoord van Fox-IT op vragen van Buro Jansen & Janssen
- AIVD-toezichthouder deed zaken met Moebarak en Assad (samenvatting)
- Fox-IT in het Midden-Oosten
- Documenten bij het onderzoek Fox-IT in het Midden-Oosten
- AIVD-toezichthouder deed zaken met Moebarak en Assad (samenvatting) (pdf)
- Fox-IT in het Midden-Oosten (pdf)
- Documenten bij het onderzoek Fox-IT in het Midden-Oosten (pdf)
- Het onderzoek Fox-IT in het Midden-Oosten (pdf)

Snitegroup GmbH

- https://handelsregister.help.ch/gmbh.cfm?nr=CH-020.4.042.282-7&name=SNITEGROUP-GmbH
- https://swiss-data-history.com/company_detail.aspx/CH02040422827--SNITEGROUP-GmbH--Schlieren-8952-82DE
- https://www.shabex.ch/en/co/exc/snitegroup_gmbh_CH-020.4.042.282-7.htm
- Обзоругроз.DataDiode.pdf
- ИнформационнаябезопасностьтехнологическихсегментовIP-сети(СКАДА,АСУТПипрочее).pdf
- SNITEGroupITSecASUTP.57049341.pdf
- SNITEGrpoupsensor.17844346.pdf
- HandelsregisterauszugSNITEGROUP.pdf
- DiodeRussiaMar.94593518.pdf
- archive-publication-4049271.pdf
- Accesslayerandotherpresentationspartnerofsnitegroup.pdf

Simet

- http://www.tbnenergo.ru/NEWS/2012-05-29/ https://prezi.com/ouvaedugpq5m/presentation/%20(Evgeny%20Gengrinovich%20Updated%2024%20January%202013)
- измерениеобучениеит-архитектурапребиллингSNITEGROUPGmbHИнструментыпереходаотобычныхсетейкинтеллектуальным(SmartGrid).pdf
- Комплексзащитысистемавтоматизацииизданий«ЩИТ».pdf
- SNITEGroupProductOverview18.86497893.pdf
- SimetMetrolPO.49732261.pdf
- SimetBuildingdefence.18640404.pdf
- SIMetBPL.46929715.pdf
- ConvergeSIMetv1.40459327.pdf
- ChlenyOtrOtdZHKHjune2014.pdf
- SIMetTGC3v1.96506043.pdf
- измерениеобучениеит-архитектурапребиллингАИИСКУЭОАО«Мосэнерго»(ТГК-3).pdf

Foxitcis.com

- КомпанияFox.pdf
- Domainfoxitcis.pdf

IITD

- ОбзоругрозDataDiode.pdf

OSIsoft

- https://www.youtube.com/watch?v=1r5mrDLDMik

ARinteg

- Vanaf1april2012foxoparintegwebsite.pdf
- ProjectsARintegBanksandfinancialorganizations.pdf
- BankenpartnersvanArinteg.pdf
- arintegfstec.pdf
- arintegceretificaatfoxdatadiode.pdf
- 344627fstecdatadiode.pdf
- https://issuu.com/nbj_magazine/docs/the_best_up/48КомпанияARintegзавершилапроцесссертификациипрограммноаппаратногокомплексаFoxDataDiode.pdf

Axoft

- TheAxoftTimes4PublishedonNov52014.pdf

Evgeny Gengrinovich

- https://soc-forum-2015.ib-bank.ru/files/files/06_genrigovich.pdf
- https://docplayer.ru/51878740-Kiberataki-odna-iz-prichin-avariy-na-proizvodstve.html
- https://avtprom.ru/gengrinovich-el
- https://egengrinovich.livejournal.com/
- httpitemru08oratoraspID22.pdf
- https://il.linkedin.com/in/evgeny-gengrinovich-49351924
- https://professionali.ru/~evgenij-gengrinovich/
- http://nts-ees.ru/zasedanie-sekcii-avtomatizirovannyy-uchet-elektroenergii-i-upravlenie-elektropotrebleniem
- https://www.superjob.ru/resume/generalnyj-direktor-24740388.html
- https://www.superjob.ru/resume/generalnyj-direktor-24740388.html
- https://it-wall.com/member/19
- https://www.deloros.ru/FILEB/members.pdf
- https://rosbankmc.ru/poisk_inn/7709751352.html
- http://energyexpert.ru/content/view/1019/
- http://old.cskp.ru/recs/10370/?print
- Fox-IT Russia Timeline

Fox DataDiode

- FoxDataDiodeSecurityTargetEAL7(v2.04).pdf
- FoxDataDiodeEAL71GbpsFox.pdf
- FoxDataDiode_en.pdf
- EN-Fox-IT-Datadiode_Ruggedized-1G 2019.pdf
- document(9)factsheet20142015.pdf
- document(10)folder2013205.pdf
- informationsecuritysolutionsforics-150311111939-conversion-gate01.pdf
- Принцип-включения-Fox-DataDiode.png

Documenten met betrekking tot Surveillance Lab in Saoedi-Arabië

- AGT Forensic Lab. KSA REVISED
- Mailksameetingpowerpointagtfoxit
- mailuitnodigingksatcc
- mailvisumforksa
- KSA_contact_Details_Team
- Agreements Status Table
- Ach_4Seasons_Checklist
- 4Seasons_Checklist-1
- 4Seasons_Checklist
- Checklist
- Checklist (2)
- Checklist2A
- Checklist_Contact_Details
- Checklist_NDA_Details
- Contact_Details
- Fox-IT AGT Technology vision on Forensic Lab
- 20110620 Fox-IT AGT Technology Fox-IT Forensic Team
- Mailbijeenkomstinberlijnfl
- Attendees_Checklist
- List of Attendees
- List of Guests in Ritz
- 08292011_List of Guests in Ritz
- Copy of 20110822_ACH_ Berlin Step III Attendees_Checklist

(in het Arabisch Ministerie van Buitenlandse Zaken document met namen)

Documenten met betrekking tot AGT en een controversiële partner

- CA_Fox iT
- FoxIT_NDA_2011_signed
- Corporate Profile Fox IT-AGT June 2011
- mailsonthendaagreement2011
- mailanasonthendaagreement2011
- mailsignednda

Fox Files

- Fox-IT_Fox_Nieuws_1(NL)
- Fox-IT_Fox_Nieuws_2(NL)
- Fox-IT_Fox_Nieuws_3(NL)
- Fox-IT_Fox_Nieuws_4(NL)
- Fox-IT_Fox_Nieuws_5(NL)
- Fox-IT_Fox_Nieuws_6(NL)
- Fox-IT_Fox_Nieuws_7(NL)
- Fox-IT_Fox_Nieuws_8(NL)
- Fox-IT_Fox_Nieuws_9(NL)
- Fox-IT_Fox_Nieuws_10(NL)
- Fox-IT_Fox_Nieuws_11(NL)
- foxfiles_november_2010_GB
- Fox files maart 2011 Nederland
- FOX files september 2011 Nederlands
- foxfiles_nov_2011_nl
- FoxFiles_march_2012_EN
- Fox-Files-aug-2012-NL
- fox-files-november-2012-eng
- fox-files-march-2013-gb

Philips USFA/Crypto

- Connectie Philips, Philips USFA/Crypto en Fox-IT

Verkregen stukken tot nu toe ook van andere wob verzoeken

- Ministerie van Veiligheid en Justitie en Fox- IT

- Ministerie van Defensie en Fox-IT

- Ministerie van Buitenlandse Zaken en Fox-IT
- Buza besluit van juni 2013 plus deel I en II 576.pdf
- Wob documenten Deel I (definitief)
- Wob documenten deel II
- Wob documenten deel 2 andere versie
- Wob documenten deel 2 andere versie
- Wob documenten geheel andere versie
- Wob documenten geheel andere versie
- Meta Wob documenten (slecht kopie geleverd door het ministerie)

- politie en Fox IT
- politie en Fox-IT stukken na bezwaar beroep
- politie en Fox-IT stukken na bezwaar beroep 2
- politie en Fox-IT stukken na bezwaar beroep 3
- politie en Fox-IT stukken na bezwaar beroep extra

- Ministerie Economische Zaken en Fox-IT
- Ministerie Economische Zaken en Fox-IT 2

- agentschap telecom en Fox-IT
- 7-deel-ii-definitief.pdf
- 13499.pdf
- 576.pdf

overname Fox-IT door NCC-Group

- Wob+besluit+13+januari+2017+Fox-It.pdf
- Bijlagen+bij+Wob-besluit+13+januari+2017.pdf
- Deelbesluit+1+Wob-verzoek+over+de+overname+van+Fox-IT.pdf
- Bijlage+2+bij+deelbesluit+1+wob-verzoek+Fox-IT.pdf

Nationale veiligheid

- brief-wob-publicatie-informatie_tcm31-30325.pdf
- bijlage-2-nr-11047826-betr-besluit-op-wob-verzoek.pdf
- Wob+besluit+7+september+2018+.pdf

gerelateerd aan Diginotar

- besluit-wob-verzoek-totstandkoming-onderzoeksrapport-2011-fox-it-naar-diginotar.pdf
- wob-besluit-met-bijlagen-juridisch-kader-overname-diginotar.pdf
- wob-verzoek-diginotar-beverwijk-deelbesluit-2.pdf
- wob-verzoek-betreffende-diginotar.pdf

Terug naar inhoudsopgave

The Ears and the Eyes (and the GPS trackers)

The States, according to their role of repression of individuals and groups doing subversive actions, put in place ways of keeping those individuals and groups under surveillance. It seems that some of this surveillance is done through the hiding of surveillance devices in the spaces we live in.

These devices take different forms : microphones, cameras, geolocation devices. Targeted spaces can be all the spaces we go through : buildings, vehicles, public space. These practices are sometimes legal, authorized by a judge for example, and sometimes not, done illegally by intelligence agencies.

So…

We noticed the lack of informations available around us concerning this kind of surveillance. What is the real use of these devices by intelligence agencies? Which kind of devices are used? In which contexts? How efficiently? What can we do to oppose this kind of surveillance?

We want to gather informations about this subject. We want to focus on surveillance carried out by intelligence agencies and political police against individuals or groups doing subversive actions. Also, we limit ourselves to the study of physical surveillance devices hidden in the spaces inhabited by the suveilled individuals and groups (so we won't talk about other kind of surveillance such as shadowing, phone-tapping and Internet surveillance).

What you will find on this website

Regularly, hidden surveillance devices are found in squats, activist spaces, vehicles, homes, or outside during public events. Sometimes these findings are made public on the Internet. We try to follow the news, and we publish these discoveries on the articles section of our website. We also publish an overview of surveillance devices and a list of found surveillance devices, which contains around fifty examples of found devices since 2007, mostly in Italy but also in other countries.

When cops decide to spy on us using surveillance devices, they need to get the devices from somewhere. It seems that they often buy these devices from private companies. The companies that manufacture and market surveillance-related products and services to law enforcement agencies, governments, and armed forces, form what we call the surveillance industry. We publish a few resources about this industry, including a list of companies that sell physical surveillance devices designed to be hidden in spaces to law enforcement agencies.

Update of the list of devices: 11 cases added (may 2021)

As part of our research work on the use of hidden physical surveillance devices by law enforcement and intelligence agencies, we publish a list of found surveillance devices.

In this update, 11 cases from 1988 to 2013 have been added to the list. Also, we now include a "methodology" section, which explains how the list is constructed. Documentation was added on:

- A tracking device found under a car in Berlin (Germany) in july 1988
- GPS trackers found under three cars in Boulder (United States) in july 2003
- A surveillance device found in a car in Rovereto (Italy) in november 2004
- A surveillance device found in a car in Bologna (Italy) in march 2005
- A GPS tracker found under a car in Bad Oldesloe (Germany) in march 2007
- A GPS tracker found in a car in Berlin (Germany) in may 2007
- A GPS tracker found under the car of Marius Mason in Cincinnati (United States) in february 2008. About a month after the device was found, Marius Mason was arrested and later sentenced to 22 years in prison for arson attacks (more information available at supportmariusmason.org).
- A GPS tracker found under a car in Levin (New Zealand) in april 2010
- A tracking device found under a car in Lübeck (Germany) in april 2013
- A GPS tracker found under a car in Leipzig (Germany) in may 2013
- A GPS tracker found under a car in Stuttgart (Germany) in june 2013

Contact us

If you have questions or comments, or if you wish to contribute to the website, you can contact us, desoreillesetdesyeux@riseup.net

List of found surveillance devices - updated in april 2021

Terug naar inhoudsopgave

Maak het werk van Buro Jansen & Janssen mogelijk

Word donateur

Wilt u dat Buro Jansen & Janssen de komende jaren onderzoek blijft doen naar politie, justitie en inlichtingendiensten, overheidsoptreden in het algemeen, bedrijven die meewerken aan repressief overheidsbeleid en/of zelf ook repressief of diep ingrijpen in het leven van burgers in Nederland en Europa steun ons dan.

Word donateur of vraag familie, vrienden en bekenden donateur te worden. Rekening NL43 ASNB 0856 9868 52 of rekening NL56 INGB 0000 6039 04 ten name van Stichting Res Publica, Postbus 11556, 1001 GN Amsterdam.

Stichting Res Publica is aangemerkt als ANBI (Algemeen Nut Beogende Instellingen) instelling. Dit betekent voor mensen die ons willen steunen het volgende:

– Als een instelling door de Belastingdienst is aangewezen als een ANBI, kan een donateur giften van de inkomsten- of vennootschapsbelasting aftrekken (uiteraard binnen de daarvoor geldende regels).

De werkvelden worden onderverdeeld in grondrechten, directe actie en vrije meningsuiting, radicale transparantie en fundamentele kritiek.

Grondrechten

- Centraal staan bij Buro Jansen & Janssen grondrechten in de breedste zin van het woord

Onderzoek van Buro Jansen & Janssen richt zich op politie, inlichtingendiensten, justitie, migratie en de overheid in het algemeen vooral in Nederland, een beetje Europa, maar de laatste jaren meer en meer ook buiten Europa zoals het Midden-Oosten en Centraal-Amerika. Onderwerpen in Nederland zijn in het kader van beperking van grondrechten; geweldsgebruik (onder andere politiewapen, pepperspray, stroomstootwapen, aanhoudingseenheden, mobiele eenheid), profilering/discriminatie (onder andere etnisch profileren, ochtendgloren, mobiel banditisme), overheid in de publieke ruimte (onder andere preventief fouilleren, identificatieplicht, gebiedsverboden), opsporingsmiddelen in het algemeen, digitale opsporingsmiddelen (onder andere politie spyware/malware, Social Media surveillance), inlichtingen operaties en privacy (inlichtingendiensten) en nog veel meer. Over veel zaken zijn in de afgelopen jaren diverse publicaties verschenen.

Directe actie en vrije meningsuiting

- Wij blijven op de achtergrond radicaal activisme steunen

Deels door publicaties zoals recentelijk de arrestantenhandleiding, een totaal vernieuwde update van het oude Tips tegen Tralies waarvan nu een tweede druk komt, maar ook door mensen te ondersteunen bij benaderingen, onderzoek naar mogelijke informanten, steun bij klachten, beschikbaar stellen van de digitale infrastructuur voor publicaties als de kraakhandleiding en andere wijzen. Alle publicaties en informatie zijn op de websites van Buro Jansen & Janssen te vinden.

Radicale transparantie

- Wij ondersteuning onderzoek en verbeteren van informatiepositie van individuen en groepen

Naast informatieverzoeken voor het eigen onderzoek ondersteunt Buro Jansen & Janssen individuen en groepen bij hun onderzoek en het verbeteren van hun informatiepositie en kennis. Het gaat hierbij om milieubeleid, drugsbeleid, sociale zekerheid, vrouwenrechten en andere terreinen. Al geruime tijd worden openbaarheid punt nl alle openbaar gemaakte documenten door Buro Jansen & Janssen online gezet. Ook door anderen verkregen Wob documenten worden daar nu aan toegevoegd. Rond de inlichtingendiensten is het nationaal veiligheidsarchief opgezet dat langzaam wordt uitgebouwd.

Fundamentele kritiek

- Impliciet heeft Buro Jansen & Janssen al sinds de jaren tachtig kritiek geuit op beleid en praktijk. Actieve lobby doet het Buro niet, maar het onderzoek, de artikelen en de documenten worden door veel mensen gebruikt. De laatste jaren wordt in artikelen van Buro Jansen & Janssen wel explicieter fundamentele kritiek geuit als onderdeel van een onderzoek. Voorbeelden zijn het magazine over de WIV2017, de observant over Social Media Surveillance in Nederland, een reeks artikelen en onderzoek naar de relatie tussen de wetenschap en de politie, over het duurzaamheidsbeleid van Nederlandse overheid en het gebruik van spyware/malware door de Nederlandse overheid en de bedrijven die die digitale wapens ontwikkelen.

Terug naar inhoudsopgave