VASTech Cyberupt

Buro Jansen & Janssen

Observant #79, juni 2022

Inhoudsopgave Observant #79 / juni 2022

VASTech / Cyberupt

Gehele Observant #79 / juni 2022 VASTech / Cyberupt (pdf)

De Nederlandse overheid faciliteerde de vestiging van het Zuid-Afrikaanse bedrijf VASTech in Nederland. VASTech leverde surveillance apparatuur aan onder meer het Zimbabwe van Mugabe, het Libië van al-Qadhafi, het Egypte van Moebarak, Syrië en in 2021 een monitoring centrum aan Saoedi-Arabië.

Het Zuid-Afrikaanse bedrijf VASTech richt zich op de productie van programmatuur en software voor het opnemen van communicatie voor zowel de publieke als de commerciële markt. Oprichter Frans Dreyer was voorheen werkzaam bij het Zuid-Afrikaanse ICT-bedrijf Spescom Limited. VASTech trad in eerste instantie op als reseller van de producten van dit bedrijf en ontwikkelde deze verder door tot het VASTech Zebra systeem. De naam Zebra wordt niet meer gebruikt door het bedrijf en is vervangen door Portevia, Strata en Galaxia. Naast deze surveillance apparatuur heeft VASTech ook analyse tools ontwikkeld zoals Badger, een social media monitoring tool.

De onthullingen in 2011 over de levering aan Libië leidde, noch in Zuid-Afrika noch elders, tot nader onderzoek of vervolging vanwege mogelijke betrokkenheid bij mensenrechtenschendingen. VASTech bleef leveren aan repressieve regimes. Vanaf 2018 werkte het aan een monitoring centrum voor Saoedi-Arabië, dat in 2021 werd opgeleverd. Ook verkocht het bedrijf apparatuur aan onder meer Mexico, Pakistan en Georgië.

Het bedenkelijke trackrecord van VASTech op het gebied van leveringen aan repressieve regimes en de afwezigheid van beleid van het bedrijf op de mogelijke impact van haar leveranties op de mensenrechten vormden geen belemmering voor Nederlandse overheid om het bedrijf te ondersteunen bij de vestiging in Nederland. Het bedrijf werd met alle egards ontvangen en langs diverse bestuursorganen geleid.

Naast het onderzoek naar de Nederlandse dochter Cyberupt van het Zuid-Afrikaanse bedrijf VASTech is ook uitgebreid onderzoek gedaan naar VASTech in het algemeen. Het resultaat daarvan is een profiel van het bedrijf.

Export naar repressieve regimes komt niet alleen terug bij surveillance, spyware apparatuur en digitale wapens, ook in het algemeen bij wapenhandel en de steun aan de militaire opbouw van die regimes. In deze Observant ook een collectie artikelen die op nieuwsblog zijn te vinden over de steun aan het Russische leger door Europese en Amerikaanse bedrijven. Oorlog als het ultieme verdienmodel.

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 NL56 INGB 0000 6039 04 ten name van Stichting Res Publica, Postbus 11556, 1001 GN Amsterdam.

Nederlandse overheid rolt rode loper uit voor Zuid-Afrikaans surveillance bedrijf dat levert aan repressieve regimes (samenvatting)

De Nederlandse overheid faciliteerde de vestiging van het Zuid-Afrikaanse bedrijf VASTech in Nederland. VASTech leverde surveillance apparatuur aan onder meer het Zimbabwe van Mugabe, het Libië van al-Qadhafi, het Egypte van Moebarak, Syrië en in 2021 een monitoring centrum aan Saoedi-Arabië.

Het Zuid-Afrikaanse bedrijf VASTech richt zich op de productie van programmatuur en software voor het opnemen van communicatie voor zowel de publieke als de commerciële markt. Oprichter Frans Dreyer was voorheen werkzaam bij het Zuid-Afrikaanse ICT-bedrijf Spescom Limited. VASTech trad in eerste instantie op als reseller van de producten van dit bedrijf en ontwikkelde deze verder door tot het VASTech Zebra systeem. De naam Zebra wordt niet meer gebruikt door het bedrijf en is vervangen door Portevia, Strata en Galaxia. Naast deze surveillance apparatuur heeft VASTech ook analyse tools ontwikkeld zoals Badger, een social media monitoring tool.

Na de oprichting in 1999 werd VASTech internationaal actief en groeide uit tot een speler op de internationale surveillance markt. In 2011 raakte VASTech in opspraak na onthullingen over de levering van surveillance apparatuur aan het Libië van al-Qadhafi. Libië werd voorzien van een monitoringcentrum voor het internationale communicatieverkeer. Het bedrijf leverde daarnaast surveillance apparatuur aan onder meer het Zimbabwe van Mugabe en het Egypte van Moebarak.

Sinds 2002 leverde VASTech aan Syrië en het was in Syrië het enige bedrijf dat in 2008 een voorstel kon indienen voor ‘monitoring equipment for international exchange’. In 2008 werd het Ministerie van Binnenlandse Zaken van de Verenigde Arabische Emiraten voorzien van een ‘mass monitoring system’.

De onthullingen in 2011 over de levering aan Libië leidde, noch in Zuid-Afrika noch elders, tot nader onderzoek of vervolging vanwege mogelijke betrokkenheid bij mensenrechtenschendingen. VASTech bleef leveren aan repressieve regimes. Vanaf 2018 werkte het aan een monitoring centrum voor Saoedi-Arabië, dat in 2021 werd opgeleverd. Ook verkocht het bedrijf apparatuur aan onder meer Mexico, Pakistan en Georgië.

Het Zuid-Afrikaanse bedrijf beweerde bij monde van CEO William Barnard dat VASTech apparatuur alleen wordt gebruikt voor opsporingsdoeleinden ter voorkoming van criminele activiteiten zoals witwassen, drugs- en mensen smokkel. Brochures van het bedrijf spreken echter over apparatuur voor inlichtingendiensten en bulkinterceptie, en niet over specifieke operaties gericht op individuele verdachten.

VASTech in Nederland

VASTech richtte in 2017 een Nederlandse vestiging op, Cyberupt. Daarnaast heeft VASTech ook dochterondernemingen in Oman, de Verenigde Arabische Emiraten en Zwitserland.

Het bedenkelijke trackrecord van VASTech op het gebied van leveringen aan repressieve regimes en de afwezigheid van beleid van het bedrijf op de mogelijke impact van haar leveranties op de mensenrechten vormden geen belemmering voor Nederlandse overheid om het bedrijf te ondersteunen bij de vestiging in Nederland. Het bedrijf werd met alle egards ontvangen en langs diverse bestuursorganen geleid.

Zo organiseerde het Ministerie van Economische Zaken en Klimaat en de ontwikkelingsmaatschappijen van de provincie Noord-Brabant en Zuid-Holland in 2016 een tweedaags programma voor VASTech. Een delegatie van het bedrijf sprak met het Ministerie van Buitenlandse Zaken, het Ministerie van Economische Zaken en Klimaat, het Innovation Quarter en de Brabantse Ontwikkelings Maatschappij (BOM Foreign Investments).

In 2017 registreert VASTech een dochteronderneming in Amsterdam: Cyberupt BV. Cyberupt wordt in 2019 lid van de Hague Security Delta, een samenwerkingsverband op het gebied van IT- en databeveiliging, en het open innovation platform Amsterdam Smart City. Cyberupt probeert in Nederland tevens aansluiting te vinden in de academische wereld. Het bezocht onder andere de Eindhoven University of Technology, de Technische Universiteit Delft en de Haagsche Hogeschool. Professor David van Leeuwen van de Radboud Universiteit Nijmegen werkt al sinds 2006 samen met een medewerker van VASTech/Cyberupt, Niko Brummer.

Het onderzoek van Buro Jansen & Janssen naar VASTech en Cyberupt is gebaseerd op openbare bronnen, interne bedrijfsdocumenten en e-mails die Buro Jansen & Janssen in 2017 heeft ontvangen over de relatie van het Nederlandse bedrijf Fox-IT met het Duitse bedrijf AGT, de door Wikileaks openbaar gemaakte Hacking Team files en diverse Wob/Woo verzoeken.

Naar inhoudsopgave Observant #79

Nederlandse overheid rolt rode loper uit voor Zuid-Afrikaans surveillance bedrijf dat levert aan repressieve regimes

De Nederlandse overheid faciliteerde de vestiging van het Zuid-Afrikaanse bedrijf VASTech in Nederland. VASTech leverde surveillance apparatuur aan onder meer het Zimbabwe van Mugabe, het Libië van al-Qadhafi, het Egypte van Moebarak, Syrië en in 2021 een monitoring centrum aan Saoedi-Arabië. Het bedenkelijke trackrecord van VASTech op het gebied van leveringen aan repressieve regimes en de afwezigheid van beleid van het bedrijf op de mogelijke impact van haar leveranties op de mensenrechten vormden geen belemmering voor Nederlandse overheid om het bedrijf te ondersteunen bij de vestiging in Nederland. VASTech werd met alle egards ontvangen en langs diverse instanties geleid.

Zo organiseerde het Ministerie van Economische Zaken en Klimaat en de ontwikkelingsmaatschappijen van de provincie Noord-Brabant en Zuid-Holland in 2016 een tweedaags programma voor VASTech. Een delegatie van het bedrijf sprak met het Ministerie van Buitenlandse Zaken, het Ministerie van Economische Zaken, het Innovation Quarter, de Brabantse Ontwikkelings Maatschappij (BOM Foreign Investments) en andere bestuursorganen.

In 2017 registreert VASTech een dochteronderneming in Amsterdam: Cyberupt BV. Cyberupt wordt in 2019 lid van de Hague Security Delta, een samenwerkingsverband op het gebied van IT- en databeveiliging, en van het open innovation platform Amsterdam Smart City.

VASTech/Cyberupt zoekt ook contacten in de universitaire wereld. De VASTech delegatie bezoekt in 2016 de Eindhoven University of Technology, de Technische Universiteit Delft en de Haagsche Hogeschool. Professor David van Leeuwen van de Nijmeegse Radboud Universiteit werkt al sinds 2006 samen met een medewerker van VASTech/Cyberupt, Niko Brummer.

Dit onderzoek van Buro Jansen & Janssen is gebaseerd op openbare bronnen, interne bedrijfsdocumenten en e-mails die Buro Jansen & Janssen in 2017 heeft ontvangen over de relatie van het Nederlandse bedrijf Fox-IT met het Duitse bedrijf AGT, de door Wikileaks openbaar gemaakte Hacking Team files en diverse Wob/Woo verzoeken.

Cyberupt

VASTech werd in 1999 in Stellenbosch opgericht door Frans Dreyer, die daarvoor werkte bij het Zuid-Afrikaanse ICT-bedrijf Spescom Limited. VASTech richt zich op de productie van programmatuur en software voor het opnemen van communicatie voor zowel de publieke als de commerciële markt. Het bouwt hierbij voort op oude producten van Spescom DataVoice, de ontwikkelingsafdeling van Spescom Limited, waarvan VASTech deels de rechten kocht.

Het bedrijf werd internationaal actief en werd een speler op de internationale surveillance markt. Het opzetten van Cyberupt past in de mondiale ambities van VASTech. Het Zuid-Afrikaanse bedrijf heeft in de loop der jaren diverse vestigingen opgezet om de handel met bepaalde regio's te bevorderen. In 2008 opende het een kantoor in Dubai (VASTech ME FZE), in 2011 in Oman (VASTech LLC) en in 2013 VASTech AG in Zwitserland.

In 2016 beginnen de voorbereidingen voor het opzetten van Cyberupt. Op 1 april 2016 worden verschillende domeinen (cyberupt.com/.org/.info/.net) vastgelegd door Divan Dreyer. De website komt echter nooit van de grond. Wel wordt de bv een jaar later op 31 maart 2017, ingeschreven in Amsterdam, met een vestigingsadres in Amstelveen en een kantoor in Breukelen.

Cyberupt BV is in handen van Delm Invest (PTY) LTD, een bedrijf van Divan Dreyer. Bestuurders van de bv zijn, naast Dreyer (ook bestuurder bij VASTech SA en Seartech), Willem Johannes Barnard (ook bestuurder bij het Zwitserse VASTech AG) en Marthinus Casper (Marius) Ackerman. Ackerman werkte, net als VASTech oprichter Frans Dreyer, voor Spescom DataFusion en van 2003 tot 2017 bij VASTech in Zuid-Afrika als technical director en contract specialist. Vanaf juli 2017 is hij technical director van Cyberupt.

Niet alleen Ackerman heeft een verleden bij VASTech en Spescom. Cyberupt neemt ook andere mensen in dienst met eenzelfde achtergrond. Charl Johannes van der Merwe treedt in juli 2017 in dienst bij Cyberupt en houdt zich volgens zijn LinkedIn-pagina bezig met business development. Hij treedt in mei 2018 tevens toe tot het bestuur van Cyberupt. Hij is afkomstig van Spescom DataVoice en stapte in 2010 over naar VASTech, waar hij tot 2014 verantwoordelijk was voor product management, sales en marketing. Martin Booyens werkt vanaf april 2016 als software engineer en developer voor Cyberupt. Ook hij werkte in het verleden voor Spescom en VASTech.

Het opzetten van Cyberupt BV valt samen met het uitbreiden van de verkoopactiviteiten van VASTech binnen de Europese Unie. In januari 2016 huurt VASTech de diensten in van Nils Reinders. Reinders is werkzaam voor het Israëlische Dignia Systems, een bedrijf gespecialiseerd in beveiligings- en defensieoplossingen.

Reinders richt zich vooral op de lobby in Brussel bij diplomatieke vertegenwoordigers van EU-landen en militaire attachés van Afrikaanse en Zuidoost Aziatische landen. Naast zijn werk voor Dignia Systems is hij ook contactpersoon voor de Amerikaanse defensiebedrijven Northrop Grunman en General Dynamics Ordnance and Tactital Systems. Reinders omschrijft zich op zijn LinkedIn-pagina als "main contact person for National Security Solutions and interception systems of Vastech (SA) in 2016."

VASTech bezoekt Nederland

Op 30 en 31 augustus 2016 bezoekt een delegatie van twee medewerkers van VASTech Nederland. Voor het Zuid-Afrikaanse bedrijf is een programma georganiseerd door de Netherlands Foreign Investment Agency (NFIA) en de provinciale ontwikkelingsmaatschappijen Innovation Quarter en de Brabantse Ontwikkelings Maatschappij (BOM Foreign Investments). In het Innovation Quarter werkt het Ministerie van Economische Zaken en Klimaat samen met de provincie Zuid-Holland en enkele gemeenten en onderwijsinstellingen uit die provincie.

De NFIA ondersteunt buitenlandse bedrijven die activiteiten in Nederland willen opzetten en valt onder de verantwoordelijkheid van het Ministerie van Economische Zaken en Klimaat. De NFIA geeft uitleg over de wet- en regelgeving in Nederland en is verantwoordelijk voor de internationale promotie van Nederland als vestigingslocatie voor bedrijven. De NFIA heeft ook een kantoor in Zuid-Afrika.

De NFIA ondersteunt buitenlandse bedrijven, maar houdt zich niet bezig met de achtergrond van de betreffende bedrijven. De NFIA werkt voor bedrijven in alle sectoren, de dienstverlening is gratis. Ondersteuning wordt alleen onthouden wanneer "de Nederlandse wet contacten met bedrijven met bepaalde activiteiten niet toestaat." De NFIA "ondersteunt dus geen brievenbusmaatschappijen of andere papieren constructies".

Volgens haar taakomschrijving moet de NFIA zich verdiept hebben in de achtergrond en klantenkring van VASTech en het bedrijf hierover hebben bevraagd. Uit de openbaar gemaakte communicatie blijkt dit niet. Levering van surveillance apparatuur aan repressieve regimes vormt geen beletsel voor ondersteuning van bedrijven die zich in Nederland willen vestigen.

Het programma van VASTech begint op dinsdag 30 augustus met een gesprek om 9.30 uur op het Ministerie van Economische Zaken en Klimaat met medewerkers van de NFIA en Innovation Quarter.

Gesprek op Buitenlandse Zaken – mogelijke export via Nederland?

Na het gesprek op Economische Zaken geven de twee VASTech delegatieleden dezelfde dag van 10.30 tot 11.30 uur een presentatie aan twee ambtenaren van het Ministerie van Buitenlandse Zaken (Directie Veiligheidsbeleid en de Directie Internationale Marktordening en Handelspolitiek), een ambtenaar van de NFIA en een ambtenaar van Innovation Quarter.

De delegatieleden geven aan mede geïnteresseerd te zijn in vestiging in Nederland, omdat dit mogelijkheden biedt om via Nederland te exporteren. Tijdens de presentatie geeft VASTech geeft een overzicht van haar producten. De ambtenaar schrijft dat VASTech: "systemen levert voor massive data capture & storage (ordegroot 10-14 Gbite/sec). Soms ook wel aangeduid als illegal interception. 'Onderzoekers' kunnen met of zonder gerechtelijk bevel zoeken in de data." Volgens het gespreksverslag is "software het voornaamste product" van het Zuid-Afrikaanse bedrijf. "Hardware meestal off-the-shelf ongecontroleerd op enkele gateways (encryptie) na."

Tijdens het gesprek komt de Wassenaar Arrangement (WA) ter sprake. WA is een akkoord over de beperking van de export van conventionele wapens en dual-use-technologieën: goederen met een civiele toepassing, die ook een militaire toepassing kunnen hebben, en waartoe ook IT-technologie en software kunnen behoren.

"Key: software systeem moet international scrutiny kunnen doorstaan. Is nu niet WA gecontroleerd, ook al gebruiken klanten wel voor militaire doeleinden. Alleen aan legale overheden in landen in Europa, Z-Amerika en Azië met goede reputatie, zonder sancties, embargo's, etc. Nu: ontwikkeling van software systemen voor militair eindgebruik, die vanwege encryptie gecontroleerd zijn," staat in het gespreksverslag.

Het is opmerkelijk dat in het gespreksverslag wordt vermeld dat VASTech alleen levert aan 'landen met een goede reputatie'. De twee aanwezige ambtenaren van Buitenlandse Zaken houden zich bezig met internationaal maatschappelijk verantwoord ondernemen en non-proliferatie, ontwapening, wapenbeheersing en exportcontrole beleid. In hun functie worden zij geacht een kritische houding te hebben ten opzichte van de landen waaraan geleverd wordt.

Uit het gesprekverslag blijkt hier niets van. De VASTech medewerkers worden niet kritisch bevraagd over de landen waaraan het bedrijf levert en mogelijke leveringen aan repressieve regimes. Hier is aanleiding toe. De onthullingen over de leverantie van surveillance apparatuur aan Libië hebben in 2011 de nodige media-aandacht getrokken en het bedrijf raakte kortstondig in opspraak.

De ambtenaar van het Ministerie van Buitenlandse Zaken schrijft dat Nederland binnen de Europese Unie pleitbezorger is van exportcontroles in verband met mogelijke mensenrechtenschendingen: "Gevoelig in publieke debat. DU (Dual Use red.) verordening wordt herzien, met sterke MR (mensenrechten red.) component inclusief cyber surveillance technologie. … Binnen WA maar ook binnen EU is NL relatief scherp op MR consequenties van exporten. Kortom: mogelijk/onmogelijk afhankelijk van eindbestemming en -gebruik."

De ambtenaar suggereert dat de Nederlandse overheid 'scherp' is bij het verstrekken van exportvergunningen voor dual-use goederen en het risico op mogelijk ongewenst eindgebruik laat meewegen. Hiervan blijkt dus niets tijdens het gesprek met de VASTech delegatie. Ook voorafgaande aan het bezoek van de VASTech delegatie zijn geen schriftelijke vragen gesteld over de leveringen aan repressieve regimes en het MVO-beleid van het bedrijf.

Het gebrek aan een scherpe en kritische houding blijkt ook uit het onderzoek van Buro Jansen & Janssen 'Fox-IT en het Nederlandse exportbeleid voor dual-use goederen' van februari 2020. Export van dual-use goederen naar landen buiten de Europese Unie is vergunningsplichtig. Bedrijven dienen een exportvergunning aan te vragen bij de Afdeling Exportcontrole en Strategische Goederen. Het exportbeleid voor dual-use goederen vereist een risicoanalyse om ongewenst eindgebruik te voorkomen. Fox-IT verstrekte de Afdeling Exportcontrole nauwelijks informatie over de eindgebruikers van de te exporteren producten. De Afdeling vroeg het bedrijf nauwelijks om informatie, die noodzakelijk is voor het maken van een risicoanalyse om ongewenst eindgebruik te voorkomen.

Bestuursorganen in de rij

Na de gesprekken op Economische Zaken en Buitenlandse Zaken volgen er in de middag bezoeken aan de Hague Security Delta, de TU Delft en de Haagsche Hogeschool. Dit blijkt uit een mail van een medewerker van de NFIA aan het Ministerie van Buitenlandse Zaken: "Voor jullie informatie we zullen op 30 augustus ook de Hague Security Delta, TU Delft, Haagsche Hogeschool bezoeken en spreken met een recruiter en tax advisor."

Een gedetailleerd middagprogramma is niet openbaar gemaakt, hoewel er voor de VASTech delegatie tot 17.30 uur een programma is georganiseerd. Ook een groot deel van het programma van woensdag 31 augustus 2016 is weggelakt, behalve een afspraak op de High Tech Campus van de Eindhoven University of Technology.

Na het tweedaagse bezoek aan overheidsinstanties en universiteiten reist de VASTech delegatie door naar Ierland: “Vastech maakt een tour door NL en Ierland ter verkenning mogelijkheden,” zo schrijft een ambtenaar in een interne email.

De Nederlandse overheid biedt dus geen volledige openheid over welke instellingen door de VASTech delegatie bezocht zijn. Het is echter aannemelijk dat de VASTech delegatie, naast in de openbaar gemaakte documenten genoemde ministeries, provinciale investeringsorganen en onderwijsinstellingen, ook andere bestuursorganen heeft bezocht.

De VASTech delegatie heeft in ieder geval contact gehad met het Nederlands Forensisch Instituut (NFI). Het NFI meldt vier maanden na een door Buro Jansen & Janssen ingediend Wob/Woo verzoek dat er documenten over VASTech en/of Cyberupt bij het NFI aanwezig zijn, maar heeft deze nog niet openbaar gemaakt Gezien de hechte samenwerking van het NFI met de politie en inlichtingendiensten zullen ook deze organen interesse in het Zuid-Afrikaanse bedrijf hebben. Buro Jansen & Janssen heeft verschillende WOB verzoeken ingediend bij de Nationale Politie en de inlichtingendiensten, maar de behandeling hiervan duurt jaren.

Hoewel de ministers van Binnenlandse Zaken en Koninkrijksrelaties en Defensie recentelijk in antwoorden op Kamervragen stellen dat bulkinterceptie technisch niet mogelijk is in Nederland, wil dit niet zeggen dat opsporings- en inlichtingendiensten deze mogelijkheden niet aftasten. Bijvoorbeeld door apparatuur van bedrijven die surveillance apparatuur aan andere overheden leveren uit te proberen.

Cyberupt gebruikt naam VASTech niet

Tijdens het gesprek met ambtenaren van Economische Zaken en Buitenlandse Zaken maakt de VASTech delegatie duidelijk dat het een “permanente startup wil beginnen in NL vanwege transparante regulering en nabijheid technische universiteiten.”

De transparante regulering verwijst naar het exportbeleid voor dual-use goederen en de mogelijkheid om via een Nederlandse dochteronderneming te exporteren. In het gespreksverslag wordt dit gekoppeld aan vertragingen in de Zuid-Afrikaanse wetgeving: "Z-Afrika loopt achter met implementatie WA regels met als risico dat contracten Vastech worden ingehaald door (vertraagde) implementatie." De nabijheid van technische universiteiten biedt voor VASTech mogelijkheden tot samenwerking in de Nederlandse universitaire wereld.

Een half jaar na het bezoek van de VASTech delegatie wordt Cyberupt BV ingeschreven bij de Kamer van Koophandel. Hoewel de delegatieleden zich tijdens het bezoek aan Nederland in augustus 2016 presenteren als vertegenwoordigers van VASTech, profileert Cyberupt zich in de hierop volgende jaren publiekelijk nooit als dochteronderneming van het Zuid-Afrikaanse bedrijf. De naam VASTech wordt ook nooit in haar externe uitingen genoemd. Dit is waarschijnlijk een bewuste keuze van het bedrijf. Men realiseert zich dat VASTech mogelijk voor sommigen een besmette naam is.

Voor de Nederlandse overheid vormen de onthullingen over de leveringen van surveillance apparatuur aan Libië weliswaar geen bezwaar om het bedrijf te faciliteren bij de vestiging in Nederland. Het is echter niet denkbeeldig dat de associatie met VASTech publiekelijk bekend zal worden en voor negatieve publiciteit kan zorgen.

Cyberupt sluit zich in 2018 aan bij de Hague Security Delta. Ook hier verzwijgt het bedrijf haar banden met VASTech.

Hague Security Delta

The Hague Security Delta is een samenwerkingsverband op het gebied van IT- en databeveiliging. Ronald Prins, voormalig directeur van Fox-IT, was een van de initiatiefnemers en penningmeester van de HSD. De huidige directeur van Fox-IT, Inge Bryan, heeft zitting in de adviesraad van het netwerk.

In de loop der jaren worden in de media vraagtekens gezet bij het succes van HSD. Het initiatief zou veel subsidie hebben ontvangen, maar niet veel hebben opgeleverd, zo blijkt uit onderzoek van *De Correspondent* en *Follow the Money.*

Cyberupt probeert lid te worden van de HSD en slaagt hierin. In augustus 2016 brengt de VASTech delegatie al een bezoek aan de HSD. Namens Cyberupt neemt Charl van de Merwe op 4 oktober 2018 deel aan 'matchmaking event' in het kader van de Cyber Security Week van de HSD.

\Van der Merwe is zeer te spreken over de 'matchmaking,' zo maakt hij duidelijk op de website van Enterprise Europe Network. Hij weet de HSD te overtuigen van de kwaliteiten van Cyberupt, want op 20 mei 2019 wordt het bedrijf verwelkomd als partner van het netwerk. "On Monday 20 May 2019 organisations aXite, Navaio, Tata Consultancy Services, Checkpoint Software Technologies, TIIN Capital, uCrowds, Cyberupt, Profit4SF were officially welcomed to the HSD community during the weekly HSD Campus lunch," zo meldt de HSD in een persbericht.

De timing is opmerkelijk. Tijdens de toetreding tot de HSD werkt VASTech aan een monitoring centrum in Saoedi-Arabië. Op 2 oktober 2018 wordt journalist Jamal Khashoggi vermoord door Saoediërs die een directe link hebben met de belangrijkste kroonprins van het land Mohammed bin Salman. Daarnaast zijn er al jaren grote zorgen over ernstige beperkingen van de vrijheid van meningsuiting, de behandeling van gevangenen en het rechtssysteem. VASTech werkt sinds 2018 aan de opdracht. Het centrum zal in 2021 opgeleverd worden.

De HSD lijkt geen voorwaarden te hebben voor bedrijven om lid te worden van het netwerk. Ook bedrijven die surveillance apparatuur leveren aan repressieve regimes, zoals VASTech, blijken lid te kunnen worden. De HSD maakt in haar berichtgeving over de toetreding van Cyberupt tot het netwerk geen melding van de associatie van het bedrijf met VASTech.

The Hague Security Delta verwelkomt het bedrijf: “Cyberupt develops solutions for optimum decision making and domain awareness” en “Cyberupt develops technology and products which enables data driven decision-making.” Het schrijft ook dat de ‘Cyberupt's machine intelligence solutions’ verkoopt die data uit verschillende digitale en fysieke bronnen bij elkaar brengen. De beschrijvingen komen overeen met de surveillance apparatuur en data-analyse tools van VASTech.

Niet alleen in Den Haag, maar ook in Amsterdam sluit Cyberupt zich aan bij een initiatief: Amsterdam Smart City. Amsterdam Smart City maakt deel uit van the Amsterdam Economic Board, een samenwerkingsverband van bedrijfsleven, kennisinstellingen en overheden. In de Board zitten verschillende gemeenten, ministeries en provincies, de Universiteit van Amsterdam, de Waag en bedrijven zoals Tata Steel Nederland, Shell en Philips, Shell, Philips.

Op Europees niveau presenteert het bedrijf zich op onder andere de Interspeech conferentie 2019 van 15 tot en met 19 september in Graz, Oostenrijk en op de CIPRE-conferentie en expositie (Critical Infrastructure Protection & Resilience Europe) van 14 tot 16 oktober 2019 in Milaan, Italië. Directeur Charl van der Merwe houdt op CIPRE een lezing over artificiële intelligentie: “Rethink AI: Insight in threat behaviour through Machine Intelligence and Information Fusion.

Radboud Universiteit, professor David van Leeuwen

Cyberupt schrijft op de website van de Cyber Security & Cloud Expo, die in september 2022 in de Amsterdamse RAI plaatsvindt, dat het bedrijf data wetenschappers in dienst heeft die gespecialiseerd zijn in de omgang met omvangrijke datasets: “Our engineer and data scientists have skills in the management and mining of massive data sets, machine learning, probabilistic modelling and fusion as well as design, development and deployment of very large distributed systems.” Cyberupt doelt hier waarschijnlijk op de datawetenschappers die in Zuid-Afrika in dienst zijn van VASTech.

Medewerkers van VASTech werken regelmatig samen met academici. Cyberupt zoekt in Nederland ook aansluiting in de universitaire wereld. In 2016 maakte de VASTech delegatie al kenbaar interesse te hebben in Nederland als vestigingsland vanwege de nabijheid van technische universiteiten. De delegatie bezocht de TU Delft, de Eindhoven University of Technology en de Haagsche hogeschool.

De interesse is niet verwonderlijk en het past in de strategie van het Zuid-Afrikaanse bedrijf. Ook in Stellenbosch, waar het hoofdkantoor van VASTech gevestigd is, werkt VASTech nauw samen met de universiteit.

Niko Brummer is een van de wetenschappers die een rol spelen bij de contacten met de universitaire wereld. In 2010 promoveerde hij aan de University of Stellenbosch. Hij werkte net als VASTech oprichter Frans Dreyer voor het Zuid-Afrikaanse ICT-bedrijf Spescom Limited. Brummer werkte bij Spescom DataFusion. Sinds 2009 is hij werkzaam voor het Spaanse Agnitio S.L. Het bedrijf is bekend van haar spraakherkenning software en naar eigen zeggen marktleider in forensische vocale biometrie. Het levert aan politiediensten in meer dan 35 landen in Europa, Azië en Amerika. In 2016 is Agnitio overgenomen door Nuance Communications, nu onderdeel van Microsoft.

In 2019 werkt Brummer mee aan het artikel ‘Large-Scale Speaker Diarization of Radio Broadcast Archives’. Het artikel is geschreven door verschillende mensen, waaronder twee medewerkers van de Radboud Universiteit van Nijmegen: Professor David van Leeuwen, bijzonder hoogleraar Machine learning on human-generated data, Henk van den Heuvel van het Centre for Language and Speech Technology van de Radboud Universiteit. Brummer ondertekent het artikel als ‘Niko Brummer, Cyberupt BV South Africa’. Ook op het programma van de Interspeech 2019 conferentie, waar een paneldiscussie plaatsvindt naar aanleiding van het artikel, wordt Brummer vermeld als medewerker van Cyberupt.

Van de Heuvel en Van Leeuwen willen geen nadere informatie of toelichting geven over hun relatie met Brummer en Cyberupt. Bij navraag door Buro Jansen & Janssen schrijft Henk van den Heuvel: "Ik heb geen enkel contact met Niko Brummer of Cyberrupt (spelling van de Heuvel) gehad. Het contact met Niko Brummer liep via David van Leeuwen."

Van Leeuwen beantwoordt vragen van Buro Jansen & Janssen zeer summier en schrijft alleen dat hij niets weet over Cyberupt: "Ik weet verder niets van Cyberupt." Buro Jansen & Janssen vroeg Van Leeuwen ook naar zijn relatie met Niko Brummer. Hij beantwoordt deze vraag echter niet.

De reactie van professor Van Leeuwen is opmerkelijk, omdat hij sinds 2006 regelmatig samen met Brummer artikelen heeft gepubliceerd. De eerste artikelen, "On calibration of language recognition scores' en 'Channel-dependent GMM and Multi-class Logistic Regression' werden geschreven voor de Odyssey 2006 conferentie in de Verenigde Staten. Er volgen meer artikelen in onder andere 2007, 2013, 2014 en 2015. Ook schrijven Brummer en Van Leeuwen samen artikelen of hoofdstukken in boeken zoals 'An Introduction to Application-Independent Evaluation of Speaker Recognition Systems' voor het boek 'Speaker Classification I: Fundamentals, Features, and Methods' in 2007.

Ook werken Van Leeuwen en Brummer samen bij de Interspeech conferenties in 2013, 2015 en bij de eerdergenoemde conferentie van 2019. Zo schrijven zij in 2013 de paper 'The distribution of calibrated likelihood-ratios in speaker recognition' en in 2015 met enkele andere auteurs het artikel 'The RedDots data collection for speaker recognition'.

De verklaringen van professor van Leeuwen over zijn banden met Cyberupt en Niko Brummer zijn dan ook weinig geloofwaardig. Hij lijkt te willen verdoezelen dat hij al jaren samenwerkt met Brummer. Zijn houding lijkt hiermee op de handelwijze van Cyberupt, dat haar relatie met VASTech niet publiekelijk bekend maakt.

Niko Brummer en het 'surveillance and interception eco-system'

Niko Brummer presenteert zich sinds enkele jaren als medewerker van Cyberupt, maar is werkzaam voor het Spaanse bedrijf Agnitio. Dit Spaanse bedrijf verklaart in haar externe communicatie dat het apparatuur aan politie en opsporingsdiensten levert. Dit is hetzelfde verweer van VASTech wanneer het wordt geconfronteerd met bewijzen van leveringen aan repressieve regimes.

Agnitio opereert in dezelfde kringen als VASTech. Het heeft een kantoor in Stellenbosch, Zuid-Afrika vlakbij het kantoor van VASTech. Ook neemt het bedrijf sinds 2008 vaak deel aan ISS World conferenties. ISS World (Intelligence Support Systems) is een handelsbeurs voor afluister- en surveillance-apparatuur, waar bedrijven en medewerkers van legers, politie en inlichtingendiensten uit verschillende landen aanwezig zijn. Agnitio bezoekt niet alleen beurzen in Europe en de Verenigde Staten, maar, maar in 2009, 2010 en 2015 ook in Dubai, in 2011 in Brasilia, in 2008 en 2009 in Singapore, en 2015 in Kuala Lumpur.

VASTech is ook bijna altijd op deze beurzen aanwezig, net zoals andere controversiële bedrijven, zoals bijvoorbeeld het Italiaanse Hacking Team. Het in 2003 opgerichte computerbedrijf Hacking Team heeft een bedenkelijke reputatie, onder meer vanwege het leveren van digitale wapens aan autoritaire regeringen die ze hebben ingezet tegen oppositieleden, journalisten en mensenrechtenactivisten.

Bedrijven in de surveillance industrie zijn vaak nauw met elkaar verweven en medewerkers van de bedrijven stappen regelmatig over naar een ander bedrijf. Zo blijkt uit de door Wikileaks openbaar gemaakte bedrijfsdocumenten van Hacking Team dat medewerkers van VASTech, Hacking Team en Agnitio van bedrijf wisselen.

Een nieuwe medewerker van Hacking Team, Philippe Vinci, mailt in april 2015: "I have decided to move from AGNITiO and join a new adventure in Hacking Team. You may have heard about Hacking Team, as we are in the same surveillance and interception eco-system." Twee maanden later meldt Fabrizio Diantina aan Vinci dat hij VASTech na dertien jaar VASTech verruilt voor Agnitio. Diantina verwijst hierbij in zijn mail naar een bezoek van VASTech medewerkers aan Hacking Team bedoeld om de samenwerking op het terrein van marketing en sales te vergroten: "… explore together how Vastech can help us with your local customers."

Niko Brummer maakt dus onderdeel uit van dit 'surveillance and interception eco-system' van bedrijven die regelmatig surveillance apparatuur leveren aan repressieve regimes. Het is verontrustend dat wetenschappers een dergelijke rol vervullen, dat VASTech ook in Nederland aansluiting probeert te zoeken in de academische wereld, dat Cyberupt is ontvangen door enkele onderwijsinstanties en dat professor David van Leeuwen niet transparant is over zijn relaties met VASTech, Cyberupt en Brummer.

Mensenrechtenschendingen en leveringen aan repressieve regimes geen bezwaar

Vanaf augustus 2016 opereert Cyberupt als dochteronderneming van VASTech in Nederland. Cyberupt BV wordt op 14 september 2020 uitgeschreven uit het handelsregister, maar het bedrijf is nog altijd actief in Nederland. Dit blijkt uit de aanmelding voor deelname aan de Cyber Security & Cloud Expo in September 2022 in Amsterdam.

Het is onduidelijk welke activiteiten Cyberupt in Nederland precies heeft ondernomen en of VASTech via Nederland naar andere landen heeft geëxporteerd. Het is echter wel duidelijk dat het Ministerie van Economische Zaken en Klimaat de vestiging van het bedrijf in Nederland faciliteerde, zonder zich in de achtergrond van het bedrijf te verdiepen. Ook het Ministerie van Buitenlandse Zaken, het NFI en verschillende onderwijsinstellingen hadden contact met VASTech.

David van Leeuwen van de Radboud Universiteit Nijmegen werkt zelfs al jaren samen met een vertegenwoordiger van Cyberupt.
Het bedenkelijke trackrecord van VASTech op het gebied van leveringen aan repressieve regimes en de afwezigheid van beleid van het bedrijf op de mogelijke impact van haar leveranties op de mensenrechten vormde voor geen van deze bestuursorganen een belemmering om in gesprek te gaan met het Zuid-Afrikaanse bedrijf.

Naar inhoudsopgave Observant #79

Zuid-Afrikaans surveillance bedrijf VASTech leverancier van repressieve regimes

Het Zuid Afrikaanse VASTech raakte in 2011 in opspraak na onthullingen over de levering van surveillance apparatuur aan het Libië van al-Qadhafi. Het leidde niet tot nader onderzoek of vervolging vanwege mogelijke betrokkenheid bij mensenrechtenschendingen.

Dit was niet de eerste keer dat VASTech surveillance apparatuur verkocht aan een repressief regime. Het bedrijf leverde aan het Zimbabwe van Mugabe en het Egypte van Moebarak. VASTech was sinds 2002 actief in Syrië en was in 2008 het enige bedrijf dat een voorstel kon indienen voor 'monitoring equipment for international exchange'. In 2008 werd het Ministerie van Binnenlandse Zaken van de Verenigde Arabische Emiraten voorzien van een 'mass monitoring system'.

Het Zuid-Afrikaanse bedrijf bleef na de onthullingen over Libië leveren aan repressieve regimes. Vanaf 2018 werkte het aan een monitoring centrum voor Saoedi-Arabië, dat in 2021 werd opgeleverd. Ook verkocht het bedrijf apparatuur aan onder meer Mexico, Pakistan en Georgië.

Het Zuid-Afrikaanse bedrijf beweerde bij monde van CEO William Barnard dat VASTech apparatuur alleen wordt gebruikt voor opsporingsdoeleinden ter voorkoming van criminele activiteiten zoals witwassen, drugs- en mensen smokkel. Brochures van het bedrijf spreken echter over apparatuur voor inlichtingendiensten en bulkinterceptie, en niet over specifieke operaties gericht op individuele verdachten.

VASTech is mondiaal actief, maar houdt geen rekening met de mogelijke impact van haar leveranties op de mensenrechten. Het Zuid-Afrikaanse bedrijf had korte tijd een Nederlandse vestiging, Cyberupt, naast haar dochterondernemingen in Oman, de Verenigde Arabische Emiraten en Zwitserland.

Dit onderzoek van Buro Jansen & Janssen is gebaseerd op openbare bronnen, interne bedrijfsdocumenten en e-mails die Buro Jansen & Janssen in 2017 heeft ontvangen over de relatie van het Nederlandse bedrijf Fox-IT met het Duitse bedrijf AGT, de door Wikileaks openbaar gemaakte Hacking Team files en diverse Wob verzoeken.

Onthullingen over VASTech in Libië

VASTech kwam in 2011 in opspraak na onthullingen over de levering van surveillance apparatuur aan het Libië van al-Qadhafi. Op 30 augustus 2011 publiceerde *Wall Street Journal* het artikel 'Firms Aided Libyan Spies'. De journalisten bezochten een kantoor van de inlichtingendienst van wijlen dictator al-Qadhafi en troffen er apparatuur van VASTech aan. Hiermee werd per maand 30 tot 40 miljoen minuten aan vast en mobiel communicatieverkeer verzameld van de Libische burgers die met het buitenland communiceerden. Het land kende destijds nog geen zes miljoen inwoners.

De onthullingen leidden niet tot nader onderzoek en mogelijke strafrechtelijke vervolging van het bedrijf vanwege betrokkenheid bij mensenrechtenschendingen. De Zuid-Afrikaanse overheid is, net als veel Europese landen, niet bereid om onderzoek te doen naar de activiteiten van haar surveillance-industrie. Hoewel tijdens de Arabische Lente van 2011 steeds meer bekend werd over de betrokkenheid van Westerse bedrijven bij de opbouw van de surveillancestaat in verschillende landen in het Midden-Oosten en hierover in verschillende nationale parlementen en het Europees Parlement vragen over werden gesteld.

VASTech produceert apparatuur voor het opnemen van communicatie voor zowel de publieke als de commerciële markt zoals telecomproviders. Het bedrijf stelt dat het haar apparatuur verkoopt aan overheden voor het verzamelen van inlichtingen ter voorkoming van criminele activiteiten zoals witwassen, drugs- en mensen smokkel.

Na de onthullingen in 2011 over de levering aan Libië verschaft VASTech nog nauwelijks informatie over haar verkoopactiviteiten en klantenkring. In antwoord op vragen over de levering zegt CEO Willem Barnard op 28 februari 2012 in Cape Times dat VASTech geen controle uitoefent op mogelijk misbruik van haar apparatuur bijvoorbeeld door de inzet tegen de oppositie of de onderdrukking van burger- en mensenrechten: "Barnard said it was like selling a pistol to a police force and not knowing whether it would be used in a lethal manner."

Barnard voegt hieraan toe dat VASTech geen enkele verantwoordelijkheid draagt voor mogelijke schendingen van mensenrechten: "We only know that governments have the ability to make sure that the systems are applied within the laws of their countries and have a responsibility to their citizens." said Barnard."

De uitspraken van Barnard zijn symptomatisch voor het bedrijf. Haar apparatuur is niet alleen bedoeld voor specifieke opsporingsoperaties, maar ook bedoeld voor surveillance en sociale media monitoring. VASTech leverde niet alleen aan Libië. Maar ook aan andere landen met een bedenkelijke reputatie op het gebied van de mensenrechten, zoals Oeganda (Datalink integrates French military surveillance systems sold to Riyadh, Intelligence Online 30 november 2021), Syrië, Verenigde Arabische Emiraten, Egypte, Zimbabwe en Saoedi-Arabië.

Van Spescom Monitor Centre Solution naar VASTech Zebra

VASTech wordt in 1999 in Stellenbosch opgericht door Frans Dreyer. Dreyer werkte tot 1999 bij het Zuid-Afrikaanse ICT-bedrijf Spescom Limited. Spescom had een eigen ontwikkelafdeling: Spescom DataVoice. Dreyer vertelt in april 2006 aan *iWeek* magazine dat VASTech begon als startup bij de Innovation Hub, een programma van

de Zuid-Afrikaanse overheid. Het bedrijf uit Stellenbosch richt zich op de productie van programmatuur en software voor het opnemen van communicatie voor zowel de publieke als de commerciële markt. Het bouwt hierbij voort op oude producten van Spescom DataVoice zoals Libra, Libra Mobile en Nexus, waarvan VASTech deels de rechten koopt.

In een bedrijfsprofiel van februari 2008 schrijft VASTech: "Our experience in interception and monitoring spans 20 years as VASTech was born out of DataVoice who manufactured interception and monitoring equipment since 1987 and laid the foundation for the development of our latest platform, codenamed ZEBRA." VASTech treedt dus in eerste instantie op als reseller van Spescom DataVoice en ontwikkelt tegelijkertijd een product verder door tot het VASTech Zebra systeem.

Door het overnemen van de producten en de klanten van Spescom verkrijgt VASTech erkenning: "Although VASTech started in 1999, we have a proud track record going back to 1987 due to VASTech buying the monitor centre line of business including products and customer base and employing former staff from a well known manufacturer of monitor centres and digital voice recorders… The products that preceded the ZEBRA range belongs to VASTech and are still running in many places around the globe. Our previous generation product for interception and monitoring, are collectively referred to as the VASTech Monitor Centre Solution," aldus VASTech in 2008.

Deze erkenning leidt weer tot de verwerving van grotere klanten. Zo wordt VASTech in 2002 toeleverancier van het Duitse Siemens via een contract ter waarde van 2.4 miljoen Rand (toentertijd 240.000 euro). In het bedrijfsprofiel van 2008 schrijft VASTech: "We sell our products into the EMEA, Pacific Rim and Far East markets through a two tier marketing approach. Tier one is for OEM (original equipment manufacturer red.) and alliance partners such as Nokia Siemens Networks GmbH & Co. KG and Spectronic Denmark A/S."

Het tweede deel van de strategie bestaat uit het opzetten van regionale dochterondernemingen zoals VASTech ME FZE in Dubai en de samenwerking met tussenhandelaren zoals het Duitse bedrijf AGT. ”Tier two is serviced by a combination of in-country resellers and regional subsidiaries to ensure closer proximity to our customer base for after sales service and support. In this case our proposal is submitted by VASTech ME,” staat in het bedrijfsprofiel.

Het is niet bekend tot wanneer VASTech met Siemens heeft samengewerkt. De monitoring divisie ‘Siemens Intelligence Solutions’ wordt in 2009 door de joint venture Nokia Siemens Networks (NSN) verkocht aan de investeringsmaatschappij Perusa Partners Fund 1 LP en gaat verder als Trovicor. De verkoop van NSN vindt plaats op het moment dat NSN wordt beschuldigd van de levering van surveillance systemen aan Iran.

VASTech is niet alleen in Europa succesvol. Ook in de Verenigde Staten wordt het in dezelfde periode ingehuurd door het technologiebedrijf Cisco. “For example, our engineers have been involved in the development and installation (in the USA) of the first Cisco AVVID Voice over Internet Protocol (VoIP) recording platforms, whilst others worked under contract for some of the largest telecommunication companies in the world on recording technologies,” aldus VASTech in het bedrijfsprofiel van 2008.

Naast de commerciële markt, zoals telecomproviders, verkoopt VASTech haar producten ook aan overheden. Met het Zebra monitoring system (en de Monitoring Centre Solution van Spescom) kan een grote hoeveelheid data, telefoon, internet en andere communicatie, worden opgenomen en ‘gefilterd.’ VASTech spreekt in 2006 van een opname en indexeer capaciteit van 100.000 afzonderlijke gesprekken op elk moment, met een totale capaciteit van 400 miljoen eenheden. Het Zebra systeem is bedoeld voor surveillance, niet voor specifieke operaties van opsporingsdiensten.

Volgens Dreyer behoort het Zebra systeem tot de 'derde generatie opname technologie'. Het maakt geen gebruik van tapes of audio kaarten voor de omzet van de data, maar de communicatie wordt vol–automatisch opgenomen en omgezet in een standaardformaat. Het systeem is volgens de toenmalige CEO ook zeer compact. Met drie computerserver kasten kunnen in 2006 30.000 afzonderlijke communicatiekanalen worden gemonitord.

Dreyer omschrijft het Zebra systeem in het interview met *iWeek* in 2006 als een 'intelligence-gathering platform,' een inlichtingen verzamelend systeem. Ook zegt hij dat het Zebra systeem het beste van de wereld kan zijn en dat VASTech het op allerlei shows heeft gepresenteerd: "We believe this could be the best technology of its kind in the world. We've exhibited our product at shows around the world, and our competitors have nothing like it."

Als internationaal distributeur van Spescom DataVoice had VASTech vanaf het begin al contacten in Afrika, het Midden-Oosten, Azië en Europa. Dreyer verklaart in 2006 dat het bedrijf het Zebra systeem heeft verkocht aan overheden in Afrika, het Midden-Oosten en Azië. In de beginjaren is bedrijf nog tamelijk open over haar klantenkring. Zo verklaarde Dreyer in het interview in *iWeek* magazine dat het bedrijf haar apparatuur heeft verkocht aan Zimbabwe en Maleisië.

Servicing the less-developed world with surveillance

Volgens Dreyer bedraagt de omzet van VASTech in 2006 30 miljoen Rand (ongeveer 4 miljoen euro in 2006). Het blijkt dat de verkoop aan private partijen het meest winstgevend is. De groei van het bedrijf komt vooral door de verkoop aan overheden.

VASTech sluit in 2005 een driejarig contract af met de Zuid-Afrikaanse overheid voor het gebruik van het monitoringsysteem. Het bedrijf verkoopt de Zuid-Afrikaanse overheid een voorloper van het Zebra systeem dat volgens Dreyer in 2006 bijna klaar is voor een internationale marketingcampagne. "Within the next three to six months, it will produce a demonstration model with which it will begin its marketing effort to launch network-based recording services in earnest," tekent *iWeek* op.

Het testen van het systeem beperkt zich niet alleen tot in Zuid-Afrika. Ook het Zimbabwe van dictator Mugabe is een klant van VASTech. Human Rights Watch en Amnesty International schrijven in dat jaar over grove mensenrechtenschendingen in dat land zoals aanvallen op de media, de oppositie en burgers, willekeurige arrestaties, martelingen en de slechte behandeling van gedetineerden. Een jaar eerder, in 2005, werden tijdens de zgn. Operatie Murambatsvina tienduizenden mensen uit huis gezet en hun huizen verwoest.

In het interview met *iWeek* wordt Dreyer niet gevraagd naar de ethische aspecten van de verkoop van apparatuur en software die voor surveillance gebruikt kunnen worden aan repressieve regimes. Zimbabwe is zelfs volgens Dreyer de grootste klant van DataVoice producten in Afrika, maar de CEO van VASTech laat daarbij in het midden of ook het Zebra systeem aan het land is verkocht. "It`s interesting to note that its biggest customer for DataVoice products in Africa is Zimbabwe, while Malaysia accounts for most of its revenue outside of the continent," schrijft *iWeek.*

Zuid-Afrika en Zimbabwe zijn in de beginjaren de voornaamste klanten van VASTech. Buiten het Afrikaanse continent is Maleisië een grote klant. Ook dit land staat bekend om haar zorgelijke mensenrechtensituatie. Amnesty International rapporteert in 2006 onder andere over detentie zonder proces, beperkingen in de vrijheid van godsdienst en de zeer slechte behandeling van arbeidsmigranten, illegalen en vluchtelingen.

VASTech richt zich in de beginjaren niet zozeer op het Westen, maar vooral op het minder ontwikkelde deel van de wereld. Zoals Dreyer het *iWeek* noemt: "We focus on servicing the less-developed world." Dreyer is openhartig: "We have no competitors locally, but face competition from about thirty companies internationally."

VASTech groeit daardoor binnen enkele jaren uit tot een speler op de internationale surveillance markt. Het Zuid-Afrikaanse bedrijf heeft in 2008 vijftig medewerkers in dienst. "VASTech employs 50 people of whom at least 40 are engineering and technical staff," is in het bedrijfsprofiel van februari 2008 te lezen. In de hieropvolgende jaren groeit het personeelsbestand van VASTech wel iets, maar zal nooit boven de honderd werknemers stijgen.

De competitie waar Dreyer over spreekt is echter betrekkelijk. VASTech concurreert niet alleen met andere bedrijven, maar trekt tegelijkertijd vaak samen op met deze overwegend Europese bedrijven om haar producten te verkopen. Dit zal bijvoorbeeld blijken bij de verkoopactiviteiten van het bedrijf in het Midden-Oosten.

Zuid-Afrikaanse overheidssubsidie voor VASTech

Steun van Zuid-Afrikaanse overheid was belangrijk voor de ontwikkeling van VASTech. Volgens het tijdschrift *Surveillance Insider* werd VASTech begin deze eeuw niet alleen internationaal opgemerkt, maar ook door de eigen regering: "The company's technology eventually caught the eye not only [of] potential customers, but also the government of South Africa." Volgens *Surveillance Insider* volgde de Zuid-Afrikaanse regering het Amerikaanse voorbeeld en begon het VASTech te subsidiëren: "In a foreshadowing of CIA funding would [that] later kick-start Palantir, the government of South Africa began pouring funds into further VASTech development."

Overheidssteun kwam er in allerlei vormen. Zo huurde VASTech vanaf februari 2005 kantoorruimte op de Scientia campus van de Council for Scientific and Industrial Research (CSIR), een overheidsinstantie. In 2006 werd VASTech opgenomen in het innovatieprogramma van de Zuid-Afrikaanse provincie Gauteng. Via het 'Innovation Hub "incubation" programme for new businesses' verkrijgt VASTech juridische dienstverlening, zakelijk advies en ondersteuning bij de huur van kantoorruimte en marketing. In 2007 en 2008 ontvangt VASTech 1.3 miljoen Rand (130.000 euro) subsidie van het Ministerie van Handel en Industrie voor de verdere ontwikkeling van het Zebra systeem. In 2010 volgt een nieuwe subsidie in het kader van het Support Program for Industrial Innovation (SPII) van 2.69 miljoen Rand (269.000 euro) voor het VASTech 'project Next'.

Naast faciliteiten, diensten en subsidie tekenen VASTech en de Zuid-Afrikaanse overheid in 2005 ook een driejarig contract voor het leveren van een 'recording solution', zoals Frans Dreyer in 2006 aan *iWeek* magazine vertelt. Het magazine omschrijft VASTech als het succesverhaal van de hig-tech incubatie programma en noemt het 'the biggest success story of the maxum incubator'.

ISS-World beurzen instrumenteel voor internationale groei

Vanaf 2006 wordt VASTech steeds meer internationaal actief. Onderdeel van de internationale strategie is deelname aan internationale beurzen, waar het Zuid-Afrikaanse bedrijf haar producten onder de aandacht probeert te brengen. Het bedrijf is sponsor van de eerste ISS World beurs, die in december 2006 in Washington wordt gehouden. In februari 2007 geven technisch directeur Marius Ackerman en directeur Andre Scholtz de eerste presentatie van het Zebra systeem op een ISS World beurs in Dubai, Verenigde Arabische Emiraten. Het bedrijf zal hierna jaarlijks op de beurs in Dubai aanwezig zijn.

ISS-World (Intelligence Support Systems) is een handelsbeurs voor afluister- en surveillance-apparatuur. Op de beurzen in Dubai zijn - naast bedrijven - medewerkers van legers, politie en inlichtingendiensten uit verschillende landen in het Midden-Oosten aanwezig. Ook het Nederlandse IT-beveiligingsbedrijf Fox-IT, dat onder andere verantwoordelijk is voor de beveiliging van Nederlandse staatsgeheimen, is regelmatig aanwezig op deze beurzen.

Het Midden-Oosten is een speerpunt voor VASTech. Het bedrijf presenteert zich vanaf 2008 ook jaarlijks op de Milipol beurzen, georganiseerd door het Ministerie Binnenlandse Zaken van Qatar. De beurs van 2008 wordt door de organisatoren aangeprezen als beurs over 'internal state security' (binnenlandse staatsveiligheid).

Daarnaast zet het Zuid-Afrikaanse bedrijf dochterondernemingen in de regio op om contacten met potentiële klanten in het Midden-Oosten te vergemakkelijken. Op 10 september 2008 wordt VASTech ME FZE in Dubai geregistreerd en op 28 mei 2011 VASTech LLC in Oman.

Publiekelijk heeft VASTech zich nooit uitgelaten over aan welke landen in het Midden-Oosten het haar Zebra systeem heeft geleverd. Uit interne bedrijfsdocumenten en e-mails die Buro Jansen & Janssen in 2017 heeft ontvangen over de relatie van het Nederlandse bedrijf Fox-IT met het Duitse bedrijf AGT blijkt echter dat VASTech in 2007 surveillance apparatuur aan de Verenigde Arabische Emiraten heeft geleverd.

Mass monitoring system voor Abu Dhabi

Het Ministerie van Binnenlandse Zaken van de Verenigde Arabische Emiraten is in 2007 bezig met de voorbereidingen voor een surveillance systeem. In november 2007 wordt er door het Ministerie een tender uitgeschreven voor een 'mass monitoring system': 'MMS Monitoring System (MMS) General Specifications Nov 2007'.

VASTech reageert op de tender. Het werkt hierbij samen met het Duitse bedrijf Advanced German Technology (AGT) van de Syrisch Duitse broers Anas en Aghiath Chbib. AGT ontwikkelde zich vanaf haar oprichting in 2002 tot een belangrijke tussenhandelaar voor Europese technologiebedrijven en heeft klanten in Egypte, Syrië, Saoedi-Arabië en de Verenigde Arabische Emiraten. In deze landen heeft AGT ook eigen vestigingen. Ook het Nederlandse bedrijf Fox-IT maakte gebruik van de diensten van AGT.

Het Zuid-Afrikaanse bedrijf ontwikkelt een nauwe band met AGT. Op 1 juli 2007 sluit de AGT afdeling in Dubai, AGT FZ LLC, met VASTech CEO Frans Dreyer zelfs een arbeidsovereenkomst. Voor "a basic salary of 20.000 Dirhams per month all inclusive" gaat Dreyer werken bij AGT FZ LLC, aldus punt 2.1.1 van het contract. VASTech zal op 10 september 2008 zelf een officiële vestiging in Dubai openen, VASTech ME FZE.

AGT speelt een belangrijke rol bij de totstandkoming van de deal. Het helpt VASTech met het leggen van de nodige contacten. Dreyer en VASTech Sales Executive Deon Wolfswinkel spreken tijdens de Milipol beurs in Parijs in oktober 2007 met Anas Chbib van AGT over een mogelijke demonstratie aan ambtenaren van het Ministerie van Binnenlandse Zaken van Abu Dhabi in november 2007.

Begin november 2007 is de demonstratie van VASTech apparatuur gepland. "For this venue it is important that it is on the ground floor ideally with a window onto a small garden as we have to put up a satellite antenna which we will connect to the equipment we will be demonstrating. It was for this reason that I suggested to Anas something like the Dubai Marina or the golf club he belongs to," schrijft Wolfswinkel aan AGT op 6 november 2007.

VASTech stuurt vijf mannen naar Dubai voor de presentatie: Deon Wolfswinkel, satelliet expert Japie Coetzer en systeembeheerder Andre Vorster uit Zuid-Afrika en twee Oekraïense technici, Oleksandr Kovtoniuk en Igor Zvarych. Op 7 februari 2008 stuurt VASTech haar voorstel naar het Ministerie. Volgens directeur Andre Scholtz is het Zebra systeem van VASTech uitermate geschikt voor het Ministerie. "We are particularly excited about your requirement as our Zebra system was designed and developed with the specific aim to fulfill very large and ultra-high capacity requirements such as yours," zo mailt hij het Ministerie.

Volgens Scholtz kan het VASTech product per 24 uur 22,6 miljoen verbindingen opnemen met een totale opslagcapaciteit van 9 Petabytes of 9.000 Terabytes. In een VASTech profiel van 8 februari 2008 beschrijft het bedrijf het deze surveillance bij het kopje 'Intelligence Value' in het hoofdstuk 'Acquisition Criteria': "Zebra Feature that plays a role; Intelligence Value accepts intercepts from all types of networks, Satellite, fixed line and mobile in one system. Provides intelligence services a unified view of all the different forms of communication that can lead to the discovery of new links and relationships."

Het Zebra systeem kan dus communicatie van satelliet, vaste en mobiele bronnen afluisteren. De totale communicatie opslag geeft volgens het Zuid-Afrikaanse bedrijf een uniek beeld en kan tot de ontdekking van nieuwe connecties en relaties leiden: "the discovery of new links and relationships." Dit unieke beeld komt volgens VASTech ook tot stand omdat het Zebra systeem naast de eigenlijke communicatie ook de metadata over die communicatie, bijvoorbeeld de locatie van personen, verzamelt. "The metadata or intercept related information (IRI) is stored in an industry standard database (MS SQL). ZEBRA automatically collates intercepts from different sites or systems in a data warehouse for further processing by intelligence extraction tools." Met software voert het systeem ook datamining uit op de afgeluisterde gegevens.

VASTech beweert in haar communicatie na de ontdekking van het surveillance systeem in Libië in 2011 dat het Zebra systeem alleen bedoeld is voor specifieke operaties in het kader van criminaliteitsbestrijding. Uit de documenten die VASTech instuurt voor de opdracht in de Verenigde Arabische Emiraten blijkt echter dat het systeem eigenlijk gebouwd is voor inlichtingendiensten: "Drawing from our many years of experience and today's soft switch technologies, VASTech proudly presents its new-generation monitor centre architecture for intelligence agencies."

Uit de openbaar geworden documenten over de deal blijkt op geen enkele wijze dat het Zuid-Afrikaanse bedrijf rekening houdt met mensenrechten aspecten. Verenigde Arabische Emiraten kent ernstige beperkingen op het gebied van de vrijheid van meningsuiting en vergadering en zeer beperkte mogelijkheden om oppositie te voeren.

VASTech haalt de opdracht voor een surveillance systeem in Abu Dhabi binnen. Frans Dreyer zal er later aan refereren wanneer het bedrijf meedingt op een tender van de Syrian Telecom Establishment (STE). Hij schrijft op 4 juni 2009 in een brief aan STE dat VASTech projecten heeft lopen in Noord-Afrika, het Midden-Oosten en Syrië: "I state that the consortium has 3 similar projects running, 1 in North Africa, 1 in the Middle East, and 1 in Syria (since 2002)."

Met het Noord-Afrikaanse surveillance project doelt Dreyer op het project dat in 2011 ontdekt is in Libië. Het project in het Midden-Oosten is het 'MMS system' (mass monitoring system) voor het Ministerie van Binnenlandse Zaken in Abu Dhabi bestaande uit "the VASTech Zebra architecture and operationally proven Zebra Capture Units (ZCU)".

VASTech Zebra voor Libische surveillance

Tegelijk met de levering van het monitoringsysteem aan de Verenigde Arabische Emiraten is het Zuid-Afrikaanse bedrijf ook in Libië actief. Ook hierbij werkt VASTech samen het Duitse bedrijf AGT, dat al sinds 2005 in dat land actief is. Van 18 tot en met 21 mei 2008 bezoeken

Deon Wolfswinkel van VASTech en Paul Joyce van het Britse Komcept Solutions Ltd. in Libië. Komcept Solutions Ltd. is gespecialiseerd in telecommunicatie, surveillance en digitale audio en video.

Het bezoek van mei 2008 wordt al snel gevolgd door een nieuw bezoek in de zomer van 2008 voor een demonstratie van de producten van VASTech en Komcept Solutions in Tripoli. Aghiath Chbib (AGT) wil zelfs een week na het bezoek in mei al terug, maar de Britten stribbelen tegen: "I cannot see the 1st June happening; we will have the same rushed problems we did with the last two trips."

Na de bezoeken begint VASTech met de bouw van een monitoring centrum voor het internationale communicatieverkeer van het land. Eerst wordt in 2009 het Eagle systeem van het Franse Amesys geïnstalleerd. Dit systeem richt zich op de monitoring van de binnenlandse communicatie. In januari en februari 2010 wordt het project 'VASTech (pty) GPTC Data Center 2010' door het Libische bedrijf Smart System Solutions uitgevoerd. GPTC (General Posts and Telecommunications Company) is het staatsbedrijf dat verantwoordelijk is voor alle post en telecommunicatiediensten in het land.

Het Zebra monitoring systeem van VASTech is in 2010 operationeel. De eersten die voelen wat internet surveillance in Libië betekent zijn leden van de oppositie en activisten die al dan niet anoniem kritiek uiten op het regime. In het *Wired* artikel 'Jamming Tripoli Inside Moammar Gadhafis Secret Surveillance Network' van 18 mei 2012 komen enkele mensen aan het woord die verhalen over wat de gevolgen waren van die surveillance.

Een vrouw vertelt dat haar communicatie (e-mail, skype etc.) was onderschept en door het regime op de staatstelevisie was vertoond. Ook online werden privécommunicatie en beelden openbaar gemaakt. Zij belandde in de gevangenis net als een jonge tandarts die na terugkomst in Libië werd geconfronteerd met zijn communicatie en anonieme berichten op internetfora. Hij werd dagenlang verhoord, maar na maanden vrijgelaten omdat zijn familie contacten onderhield met de familie van al-Qadhafi.

VASTech succesvol in het Midden-Oosten

Op 12 mei 2010 verongelukt Afriqiyah Airways vlucht 771 Johannesburg in Tripoli. 103 van de 104 inzittenden overlijden. Onder de inzittenden bevinden zich ook VASTech CEO Frans Dreyer en algemeen directeur Anton Matthee. Bij het ongeluk in Tripoli komen ook zeventig Nederlanders om het leven.

Het overlijden van Dreyer en Matthee is een schok voor het bedrijf. De zaken gaan echter door. Het Midden-Oosten blijft een belangrijke afzetmarkt voor het bedrijf. De leverantie aan Libië lijkt belangrijk te zijn geweest voor de positionering van het bedrijf in de regio.

Volgens het artikel 'Inside Africas increasingly lucrative surveillance market' van 11 februari 2020 van de website *Jeune Afrique* was het doel van de reis van Dreyer en Matthee niet zozeer om de te verifiëren of het Libische regime tevreden was met de monitoring door Zebra, maar om een nieuwe klant, het Algerijnse regime, te werven.

VASTech benut haar levering aan Libië ook anderszins. In oktober 2010 bezoeken Information Technology Manager Corne Grobler en Peter Habertheuer namens VASTech Milipol Qatar. Zij hebben speciale gasten. Grobler vraagt AGT voor vier Libische 'officials' (Youssef E Elkaial, Abdulbaset O Abdualla Akhmaj, Ahmed el fituri (Ahmed Salem M Elfituri) visa voor Qatar te regelen. Het zou gaan om vier medewerkers van het Libische staatsbedrijf General Post & Telecommunication Co., de instantie waar VASTech het Zebra surveillance systeem voor Libië heeft geïnstalleerd.

De Libiërs zullen Milipol bezocht hebben om andere producenten van surveillance apparatuur te ontmoeten. Het is niet duidelijk of zij door VASTech zijn ingezet als ervaringsdeskundigen in het gebruik van het Zebra systeem, om bijvoorbeeld het repressieve regime van Qatar te verleiden tot de aanschaf van de Zuid-Afrikaanse apparatuur. Het feit dat VASTech medewerkers, met hulp van AGT, visa regelen voor Libische overheidsfunctionarissen is echter zeer opmerkelijk.

Niet alleen voor VASTech is de Libische opdracht een succes dat nieuwe deuren in de regio kan openen. Ook voor AGT. In 2009 wordt VASTech samen met AGT uitgenodigd om te reageren op een aanbesteding van STE Syrian Telecommunications Establishment (STE). Het is niet vreemd dat beide bedrijven hiervoor gevraagd worden. AGT is al een aantal jaren actief in Syrië als reseller van antivirus licenties van producten van het cybersecurity bedrijf F-Secure. In de herfst van 2005 opent AGT zelfs een kantoor in de hoofdstad Damascus. Ook VASTech heeft een verleden in Syrië. Het is al enige jaren actief in het land.

Surveillance in Syrië

Als reseller van producten van Spescom Limited, zoals de Monitor Centre Solution, levert VASTech in de eerste jaren van haar bestaan aan verschillende telecomproviders, waaronder de Zuid-Afrikaanse MTN Group. De MTN Group heeft ook een vestiging in Syrië. MTN Syria is – naast Syriatel - een van de twee Syrische telecombedrijven voor mobiele telefonie.

Uitgangspunten voor de surveillance in Syrië zijn vastgelegd in de ‘Technical Specifications for the National Internet Backbone and STE ISP’ (nummer 18) van STE van augustus 1999. STE functioneert ook als cover voor de Syrische inlichtingendienst en dan vooral voor de interceptie van communicatie op het Syrische netwerk. Een van de onderdelen van de ‘national backbone’ is de ontwikkeling van een ‘electronic surveillance and monitoring system’ voor de Syrische machthebbers.

Het document bevat nadere details over de inhoud van het monitoring systeem. Het systeem: "shall provide law enforcement authority with the possibility to practice contents monitoring of the exchanged information and for all types of services according to the established legislation." In het document wordt gesproken over opsporingsdiensten. In Syrië was en is de scheiding tussen opsporings- en inlichtingendiensten echter diffuus.

Tevens wordt er in het document gesproken over inhoud surveillance: "contents monitoring of the exchanged information." De monitoring wordt omschreven als 'target (user) monitoring', het kopiëren van alle e-mails op een netwerk, 'full logging of accessed URLs' (het bewaren van de volledige browser geschiedenis van alle gebruikers), 'chat monitoring' en 'news monitoring (full copy of news articles)'. Naast alle persoonlijke communicatie wordt van Syrische burgers ook bijgehouden welke websites zij bezoeken en welke nieuwsbronnen zij raadplegen.

Het Duitse Siemens is een van de Europese bedrijven die begin deze eeuw het Syrische regime aan een surveillance systeem hielp. Dochteronderneming Siemens Syria schaft het LIMS (Lawful Interception Management System) aan van het eveneens Duitse Utimaco. Hiermee kunnen telefoongesprekken, tekst (sms en andere tekst), e-mails, VoIP gesprekken (voice-over-internet-protocol) en andere communicatie worden gemonitord.

Siemens was al aanwezig in Syrië via de joint venture met het Finse Nokia, Nokia Siemens Networks (NSN), dat de infrastructuur van de telecomproviders Syriatel en MTN Syria had aangelegd. VASTech heeft niet alleen met het Zuid-Afrikaanse MTN een zakelijke relatie, maar sinds 2002 ook met Nokia Siemens Networks.

Toenmalig CEO Frans Dreyer verklaart op 4 juni 2009 in een document in het kader van de aanbesteding van de STE tender dat VASTech sinds 2002 betrokken is bij een project in Syrië. Hij specificeert in het document niet waar deze betrokkenheid precies uit bestaat en of het uitsluitend gaat om leveranties aan MTN Syria en Nokia Siemens Network.

'Monitoring Equipment for international Exchange' voor Syrië

In 2007 schrijft STE een tender uit voor een "central monitoring system for public data network services (PDN) and the internet." Het doel is volgens het Technical Tender Book om de bestaande capaciteit uit te breiden: "The current network contains about 18600 dialup ports, and 3500 broadband ports (DSL) in service." STE wil de komende jaren uitbreiden: "The network is expected to scale up to 300 thousand broadband ports and 30 thousand dialup ports by the end of 2008." AGT ontvangt op 2 oktober 2007 een fax van Syrian Telecom (STE) met het verzoek om een projectvoorstel in te dienen. Net als in Libië werken VASTech en AGT samen om de opdracht binnen te halen.

Begin oktober 2008 logeren VASTech directeur Andre Scholtz en systeembeheerder Andre Vorster in het Four Seasons Hotel in Damascus. Ze geven een korte demonstratie van het Zebra systeem. Het Zuid-Afrikaanse bedrijf is bij dit bezoek versterkt met het voormalig Head of Regional Sales van Nokia Siemens Networks, Peter Habertheuer. Hij is woonachtig in Dubai en kent de situatie in Syrië goed.

Na de demonstratie van oktober volgt begin december 2008 een tweede demonstratie. Naast Scholtz, Vorster en Habertheuer komt ook Frans Dreyer naar de Syrische hoofdstad. De klant heeft aangegeven graag met de baas van het Zuid-Afrikaanse bedrijf te willen spreken. "Please confirm Frans can meet the customer on 3 December? We'll start working on site 23 November (Sunday). Peter will be there 22nd (evening) until Thursday 27th, and I'll be there from 29th Nov to full day 4th December," schrijft Scholtz op 13 november 2008 aan AGT.

De gesprekken van AGT en VASTech met STE Syrian Telecom zijn niet zonder resultaat. Nazem Bahsas, STE Director General, faxt het AGT-kantoor in Dubai een verzoek om een voorstel te doen voor een monitoring project van de internationale communicatie in Syrië (Project for supply and installation of Monitoring Equipment For the International Exchanges). AGT dient het voorstel voor 'Monitoring Equipment for international Exchange' in augustus 2009 in.

AGT en VASTech sturen in totaal acht documenten naar STE Syrian Telecom. VASTech dienst een verklaring, Adherece 20090604, te ondertekenen dat het voldoet aan de regels van de Syrische boycot van Israël en dat het bedrijf niet in dat land actief is. Daarnaast verklaren AGT en VASTech dat zij samenwerken bij de Syrische tender. VASTech schrijft dat het verantwoordelijk zal zijn voor 'content filtering': "Supply, Installation and Operation of the Equipment & Software of Content Filtering for Public Data Network Services (PDN) and the Internet in SAR and to be put into "Service" towards the STE."

Toenmalig CEO Frans Dreyer bezoekt in mei en in het najaar van 2009 nog een keer Damascus. Zijn overlijden bij de fatale vlucht Afriqiyah Airways-vlucht 771 op 12 mei 2010 is voor de Syrië deal een gevoelige klap. Dreyer had namelijk ook in juli 2010 een reis naar Syrië gepland.

Nu gaat directeur Andre Scholtz met zijn vrouw naar een ICT Security Forum van de Syrische overheid dat op 12 en 13 juli 2010 plaatsvindt in het Four Seasons Hotel. Het forum wordt mede georganiseerd door de Syrian Computer Society (SCS) waarvan president Assad de voorzitter is. Scholtz mailt AGT dat de bijeenkomst met de klant aan het eind van het forum of er vlak na gepland moet worden: "The meeting with the customer should be on 13th, or morning of 14th."

Uit de interne bedrijfsdocumenten over de relatie van het Nederlandse bedrijf Fox-IT met het Duitse bedrijf AGT en uit andere documenten wordt niet duidelijk of VASTech de opdracht daadwerkelijk heeft verkregen. Na de publicatie van het rapport 'Open Season, Building Syria's Surveillance State' van Privacy International in december 2016, waarin onder andere wordt ingegaan op de activiteiten van het bedrijf in Syrië, heeft VASTech echter nooit ontkend actief te zijn geweest in Syrië.

Wikileaks: VASTech in Egypte

Het bezoek van Scholtz aan Syrië in juli 2010 vindt plaats aan de vooravond van de Arabische Lente. De volksopstanden in grote delen van het Midden-Oosten en Noord-Afrika raken ook de landen waaraan VASTech apparatuur heeft verkocht, zoals Libië. Rond de Arabische Lente wordt meer duidelijk over de rol van Westerse bedrijven in de regio. Verschillende Westerse bedrijven raken in opspraak vanwege hun steun aan repressieve regimes en de bijdrage aan de opbouw van de surveillancestaat in verschillende landen in het Midden-Oosten.

Zo ook VASTech. Met het artikel in *Wall Street Journal* in augustus 2011 wordt duidelijk dat het bedrijf haar Zebra monitoringsysteem heeft verkocht aan Libië. In december 2011 publiceert Wikileaks een aantal documenten, 'The Spyfiles' die details bekend maken over bedrijven die verdienen aan de verkoop van monitoringapparatuur aan dictatoriale regimes.

In het persbericht over 'The Spyfiles' noemt Wikileaks ook de twee Zuid-Afrikaanse bedrijven VASTech en Seartech. Van de bedrijven worden ook documenten openbaar gemaakt, onder meer brochures van de producten die de twee bedrijven aanbieden. Beide bedrijven zijn nauw met elkaar verbonden. Drie personen staan bij de Zuid-Afrikaanse Kamer van Koophandel ingeschreven als directeur van zowel VASTech als Seartech: Cornelis Vamvadelis, Trevor Oosthuizen en Divan Dreyer, de zoon van Frans Dreyer.

Uit de Wikileaks documenten wordt duidelijk dat, net als in Libië, ook in Egypte apparatuur van VASTech is gevonden in de kantoren van de inlichtingendiensten. Amnesty International en Human Rights Watch rapporteerden uitgebreid over mensenrechtenschendingen in Egypte. Sinds 2006 staat het land ook op de lijst van Enemies of the Internet van Reporters without Borders. In dat jaar zet dictator Moebarak van Egypte vol in op controle, surveillance en vervolging van oppositionele geluiden op het internet. Tevens krijgt de Egyptische regering meer mogelijkheden om websites te sluiten vanwege mogelijke bedreiging van de 'nationale veiligheid'.

Het Zuid-Afrikaanse bedrijf heeft nooit gereageerd op de onthullingen van Wikileaks over de levering aan Egypte.

Spy Cables Leak: VASTech en Iran

Het Midden-Oosten is een belangrijke afzetmarkt voor VASTech. Het bedrijf leverde in ieder geval aan Syrië, de Verenigde Arabische Emiraten, Libië en Egypte. Daarnaast heeft VASTech ook geprobeerd om voet aan de grond te krijgen in Iran. In 2015 werden details bekend over de contacten tussen VASTech en het Iraanse regime. *Al Jazeera* maakte in februari 2015 documenten openbaar in het kader van de Spy Cables Leak, een verzameling documenten over voornamelijk de Zuid-Afrikaanse inlichtingendienst buitenland SASS (South African Secret Service).

Een van de documenten van de Spy Cables Leak is de 'Operational Target Analysis' van januari 2010 van het NIA (National Intelligence Agency), de binnenlandse veiligheidsdienst van Zuid-Afrika. In het document wordt verslag gedaan van een gesprek over de uitwisseling van nucleaire technologie tussen Zuid-Afrika en Iran in 2005, het bezoek van Iraanse medewerkers uit de luchtvaartindustrie aan de Zuid-Afrikaanse producent van drones Advanced Technical Engineering (ATE) in mei 2005, en een bezoek van een Iraanse delegatie van 21 tot en met 24 mei 2005 aan enkele Zuid-Afrikaanse bedrijven waaronder VASTech.

Het bezoek van Iraniërs aan Zuid-Afrika is op zich niets bijzonders. Beide landen bezoeken elkaar regelmatig en voeren gespreken over samenwerking. Zo bracht een Iraanse delegatie in 2003 een bezoek aan Zuid-Afrika, waarbij het de bedrijven Denel en Grintek aandeed. Het staatsbedrijf Denel is actief in de luchtvaart en militaire technologie. Saab Grintek, een dochter van het Zweedse Saab, zit in dezelfde branche.

Het bezoek van de Iraanse delegatie aan Denel en Grintek in 2003 zou bij de SASS zijn aangevraagd door een zakenman actief in de olieraffinage en tapijthandel. Zonder medeweten van de Zuid-Afrikaanse binnenlandse veiligheidsdienst NIA worden de Iraniërs door de SASS uitgenodigd en rondgeleid, terwijl de NIA is gewaarschuwd door de Israëlische geheime dienst Mossad dat de zakenman voor de Iraanse inlichtingendienst (MOIS) werkt. Of de NIA ook niet op de hoogte is van het bezoek van de Iraanse delegatie in mei 2005 aan Saab Grintek en VASTech staat niet in het document.

De Iraniërs waren volgens een lijst die de National Communication Centre (NCC) op 16 mei 2005, vijf dagen voor het bezoek, ontvangt vooral geïnteresseerd in afluister/surveillance technologie en drones: “Satellite interception, thuraya interception, microwave link interception, reconnaissance UAV, radio monitoring and radio location system in UN/UHF ranges, signal analysis and data decoding, passive GSM monitoring, deciphering (secure mails, A5.2 Algorithm), tactical jamming.”

Bij Saab Grintek was de focus van de delegatie gericht op informatie over elektronische oorlogsvoering en informatiemanagement: “The focus was information warfare and information management in terms of ground based, shipborne and airborne SIGINT systems Security systems for the professional and corporate markets.”

Bij VASTech kregen de delegatieleden informatie over afluistertechnologie en wordt er gesproken over onbeperkte monitoring, monitoring van de gehele bevolking dus: “Value Added Services Technologies that design and manufacture network based recording solutions for the worlds recording markets for government and commercial applications in terms of: Active Lawful Interception and Passive Unrestricted Monitoring.”

De interesse van VASTech in de Iraanse markt is logisch. Een partner van VASTech, het Zuid-Afrikaanse telecombedrijf MTN Group, neemt in 2005 bijna de helft van de Iraanse mobiele provider Irancell over. Sinds 2002 werkt VASTech in Syrië samen met een ander onderdeel van MTN Group, MTN Syria, waaraan het producten van Spescom Limited (Monitor Centre Solution) levert.

Uit de door *Al Jazeera* geopenbaarde documenten wordt niet duidelijk of het daadwerkelijk tot een deal is gekomen tussen de Iraanse overheid en VASTech. De sancties tegen het land kunnen een belemmering zijn geweest voor het bedrijf. In 2009 blijkt wel dat een partnerbedrijf van VASTech surveillance tools aan Iran heeft verkocht. In het artikel ‘Iran's web spying aided by Western technology’ van 22 juni 2009 in *The Wall Street Journal* wordt een bericht van de Oostenrijkse website *Futurezone* bevestigd dat Nokia Siemens Networks (NSN) in 2008 een monitoring centrum in Iran heeft aangelegd.

NSN Woordvoerder Ben Roome, bevestigt de berichten over de levering van surveillance tools: “The "monitoring center," installed within the government's telecom monopoly (TCI red.), was part of a larger contract with Iran that included mobile-phone networking technology. If you sell networks, you also, intrinsically, sell the capability to intercept any communication that runs over them.”

Op 28 mei 2011 registreert VASTech het dochterbedrijf VASTech LLC in de vrijhandelszone 'Knowledge Oasis' Muscat in Oman. Dit kan duiden op een hernieuwde poging om apparatuur aan Iran te leveren, gezien de neutraliteit van Oman ten aanzien van Iran. Oman speelt al decennia een rol in haar positie als intermediair met Iran, bijvoorbeeld bij de onderhandelingen tussen het Westen en Iran over de nucleaire deal.

Mondiale ambities

Het Midden-Oosten is altijd een belangrijke afzetmarkt geweest voor VASTech, maar het Zuid-Afrikaanse bedrijf heeft ook mondiale ambities. Dit blijkt uit de aanwezigheid op ISS World beurzen. Vanaf 2007 is het bedrijf aanwezig op de ISS World in Dubai en gaandeweg worden daar andere continenten aan toegevoegd. Vanaf 2008 Is VASTech ook te vinden op de ISS World beurzen in Praag (jaarlijks). Een jaar later wordt daar Azië aan toegevoegd, Kuala Lumpur (2009, 2010, 2017, 2019) en in 2010 ook Afrika (Johannesburg 2014, 2016) en Noord- en Zuid-Amerika (Washington 2010, 2011 en 2017, Brasilia 2011 en Mexico-stad 2015).

In een brochure uit 2016 onderschrijft VASTech haar mondiale ambities, en claimt het overal in de wereld aanwezig te zijn: "Current solutions in the Middle East, Europe, Africa, Asia, and the Americas."

Ook de communicatie over haar surveillance systeem verandert mettertijd. Tot 2016 sprak VASTech in haar externe communicatie over het Zebra monitoringsysteem. De naam Zebra wordt nu niet meer gebruikt, maar is vervangen door 'Portevia' dat alle data verzamelt van glasvezelverbindingen, 'Strata' voor het monitoren van mobiel dataverkeer en 'Galaxia' dat communicatie van satellieten verzamelt. Ook spreekt VASTech niet meer over het aantal miljoenen verbindingen en de hoeveelheid data die kunnen worden gemonitord en bewaard, maar over het verzamelen van alle communicatie op regionaal, landelijk en transnationaal niveau.

In de loop der jaren heeft het bedrijf ook een analyse tool ontwikkeld, Badger, die vooral wordt omschreven als social media monitoring tool. Met Badger kunnen afgeluisterde data zoals sociale media gegevens en e-mails worden gemonitord en geanalyseerd. Het bedrijf ontwikkelt daarnaast ook ander analyse- en monitoring tools, zoals de Satellite Signal Analyser (SSA) en de Fibre Signal Analyser (FSA).

Als onderdeel van de mondiale ambities van het bedrijf wordt, naast de kantoren in het Midden-Oosten, Dubai (2008) en Oman (2011), in 2013 ook een dochteronderneming in Zwitserland geregistreerd, VASTech AG.

In 2017 wordt ook in Nederland een dochteronderneming geregistreerd, Cyberupt BV. Nederland is volgens VASTech een aantrekkelijke vestigingsplaats vanwege onder meer de nabijheid van verschillende technische universiteiten. Verschillende onderdelen van de Nederlandse overheid ontvangen het Zuid-Afrikaanse bedrijf voor en na de registratie in 2017 ruimhartig en het bedrijf wordt bij diverse bestuursorganen en onderwijsinstellingen geïntroduceerd en uitgenodigd.

Zwitserse VASTech AG en de connectie met Elaman en Gamma Group

VASTech AG is op 6 februari 2013 opgericht in het Zwitserse Amriswil. Als bestuursleden staan ingeschreven de Zuid-Afrikanen André Rebb en Willem Johannes Barnard en de Oostenrijker Peter Habertheuer. Rebb staat sinds 2008 ingeschreven als uitvoerend directeur van VASTech in Zuid-Afrika, maar ook van de vestigingen in Dubai en Oman. Willem Barnard zit sinds 2007 in de Raad van Bestuur van VASTech. Habertheuer, afkomstig van Nokia Siemens Networks (NSN) en werkzaam voor VASTech, woont in Dubai en werkt sinds 2011 voor het Duitse Elaman GmbH. Later nemen ook de Zuid-Afrikaanse VASTech medewerker Petrus Jacobus Viljoen en de Zwitserse Monika Frech-Hänggi zitting in het bestuur van VASTech AG. Frech-Hänggi is betrokken bij het Zwitserse Elaman AG, de Zwitserse dochteronderneming van Elaman GmbH.

De eigenaar van het Duitse Elaman, Holger Günther Rumscheidt, en twee medewerkers van Elaman, Markus Michael Meiler en Henning Möller, hebben ook zitting in Elaman AG. Möller is tevens actief voor Trovicor AG, de naam die Nokia Siemens Networks na de onthulling over de levering van surveillance apparatuur aan Iran in 2009 heeft aangenomen. De namen en connecties van de bestuursleden maken duidelijk hoe VASTech gelieerd is aan een aantal controversiële bedrijven uit de surveillance industrie.

Elaman GmbH heeft vestigingen in Zwitserland (Elaman AG), de Emiraten (Elaman ME FZE) en Libanon (Alaman - German Security Solutions Sal). Het bedrijf is al sinds 2007 wederverkoper van het Zebra systeem van VASTech, van apparatuur van Nokia Siemens Networks, en ook van het product FinFisher van Gamma Group.

Gamma Group is een van oorsprong Brits bedrijf met takken en dochterondernemingen over de gehele wereld. Sinds 2008 biedt Gamma Group het digitale wapen FinFisher aan. Met de software FinFisher of FinSpy kan via een USB of vanaf afstand via wifi of een netwerk worden ingebroken op computers, laptops, tablets en smartphones. Het wapen is ook aangeschaft door een aantal repressieve regimes die het inzetten tegen oppositieleden, journalisten en mensenrechtenactivisten. Uit documenten die in 2014 door Wikileaks zijn gepubliceerd is duidelijk geworden dat ook de Nederlandse politie Finfisher gebruikt.

VASTech AG is gericht op de verkoop van VASTech producten, hoewel in de statuten wel staat vermeld dat er sprake is van ontwikkeling en productie: “Marketing und Verkauf sowie Entwicklung, Produktion und Auslieferung von Firmeneigener Software- und Hardware, einschliesslich Integration und Auslieferung von 3rd Party Software und Hardware im IT-Bereich und im Sicherheitsbereich.”

Opvallend is dat VASTech AG niet alleen financiële transacties kan doen in verband met verkoop, maar ook deel kan nemen in andere bedrijven: "Die Gesellschaft kann ebenfalls alle Handels- und Finanzgeschäfte tätigen, namentlich durch eine Beteiligung an anderen Gesellschaften, und im allgemeinen alle Geschäfte in der Schweiz und im Ausland eingehen."

Er is weinig bekend over VASTech AG. Het bedrijf heeft geen eigen website en geeft geen openheid van zaken over haar klantenkring. Los van de bestuurswisselingen en de connecties met andere firma's uit de surveillance wereld is weinig bekend over haar precieze functioneren.

Levering aan Mexico vlak voor de verkiezingen

Op 22 april 2013 wordt volgens gegevens van de Zuid-Afrikaanse douane een pakket met nummer 3042165 vanuit Zuid-Afrika naar Mexico verstuurd. Bestemming is het vliegveld van Mexico-stad, Aeropuerto Internacional de la Ciudad de Mexico. De apparatuur is afkomstig van Vastech (Pty) volgens de gegevens van het wereldwijd handelsgegevensbedrijf Panjiva Inc.

Uit de Wikileaks documenten over Gamma Group en het Italiaanse Hacking Team is gebleken dat Mexico een van de landen is die veel spyware aanschaft. Producenten zoals Hacking Team en VASTech zeggen dat de apparatuur en software bedoeld zijn voor opsporingsinstanties.

Finfisher van Gamma Group, Pegasus van de NSO Group en de DaVinci of Galileo RCS (Remote Control System) van Hacking Team zijn gericht op het bespioneren van individuen. Met Galileo RCS kan worden ingebroken op telefoons en computers en toegang worden verkregen tot alle aanwezige programma's en accounts, zoals Skype of Facebook.

In *Forbidden Stories* van 7 december 2020 vertelt een ex-medewerker van Hacking Team dat, hoewel de surveillance tools waren ontworpen voor de opsporing, ze al snel werden ingezet voor de monitoring van journalisten, activisten en de oppositie. “So they go to a different customer segment, governments that don’t have tools. Gradually there were more and more operations that were really borderline. Eventually, towards the end, most of the operations were on that side of the spectrum,” zegt de ex-medewerker over de verschuiving van het doel van de surveillance operaties.

In Mexico is hierbij van belang dat er duidelijke aanwijzingen bestaan voor relaties tussen opsporings- en inlichtingendiensten en criminele organisaties. Het risico is hierdoor reëel dat monitoringtools helemaal niet meer voor opsporing worden gebruikt, maar door criminele organisaties voor hun activiteiten. Zo beschrijft *Forbidden Stories* de waarneming van een technicus van Hacking Team, die bij een demonstratie een Mexicaanse ambtenaar herkent die banden met de georganiseerde criminaliteit zou hebben: “Then, one of the Hacking Team engineers panicked when he recognized Joaquin Arenal Romero, an official who he suspected had links to the Zetas cartel.” Een andere voormalig medewerker van Hacking Team voegt daar in Forbidden Stories aan toe: “Sometimes people would show up in front of us saying they worked for the intelligence.”

Deze vermoedens van Hacking Team medewerkers worden bevestigd door de Amerikaanse autoriteiten die stellen dat Mexicaanse drugskartels via corrupte functionarissen de beschikking hebben over surveillance apparatuur. De gevolgen van deze vermenging van de Mexicaanse staat en de georganiseerde criminaliteit worden bijvoorbeeld zichtbaar in de deelstaat Veracruz. Veracruz telt het hoogst aantal vermoordde journalisten in Mexico. De deelstaat heeft daarnaast een eigen spionage eenheid opgebouwd die gebruik maakt van surveillance technologie voor het monitoren van journalisten, activisten en politieke tegenstanders, compleet met persoonsdossiers met informatie over relaties, seksuele voorkeuren, politieke connecties en andere gegevens. Het voorbeeld van de deelstaat Veracruz maakt duidelijk dat de apparatuur van bedrijven als Hacking Team en VASTech zeker niet alleen worden ingezet voor opsporingsdoeleinden.

De levering van VASTech apparatuur aan Mexico in 2013 vindt plaats aan de vooravond van verkiezingen in veertien deelstaten van het land. Voor de zittende politieke partij de PRI (Partido Revolucionario Institucional) van president Enrique Peña Nieto staat er veel op het spel. Allerlei schandalen plagen zijn presidentschap en de ontevredenheid is groot. De jarenlange aanschaf en gebruik van surveillance apparatuur en software op grote schaal, de surveillance van journalisten, activisten en politieke tegenstanders roept dan ook de vraag op in hoeverre VASTech apparatuur is gebruikt bij mensenrechtenschendingen in Mexico.

Leverde VASTech apparatuur aan vijanden van de NAVO?

Het Zuid-Afrikaanse bedrijf trekt zich niets aan van de mogelijke impact van haar leveranties op het gebied van de mensenrechten. Het levert gedurende haar hele bestaan aan repressieve regimes, zoals bijvoorbeeld Libië en Syrië. De handelwijze van VASTech valt niet los te zien van de specifieke positie van Zuid-Afrika binnen de geopolitieke verhoudingen. Dit geldt zeker voor Libië, en in mindere mate voor Syrië en Iran.

Moammar al-Qadhafi steunde – in tegenstelling tot veel Westerse landen - het ANC vanaf een vroeg stadium in haar strijd tegen de apartheid. Nelson Mandela en andere ANC-leiders hebben dit nooit vergeten, hetgeen goed zichtbaar was in de houding van de Zuid-Afrikaanse regering ten aanzien van die landen. Zuid-Afrika onderhield handelsrelaties met de betreffende landen. Zo bezocht Mandela in 1999 Iran en Syrië. Kritiek uit het Westen pareerde hij door te zeggen dat: “The enemies of countries in the West are not our enemies.”

Ook relaties tussen Zuid-Afrika en Rusland moeten vanuit dit perspectief worden bezien. In de strijd tegen de apartheid was de Sovjet-Unie via de Zuid-Afrikaanse communistische partij SACP een belangrijke steunpilaar. De voormalig presidenten Jacob Zuma en Thabo Mbeki zaten in het SACP-bestuur en kregen een militaire opleiding in de Sovjet-Unie. Na het uiteenvallen van het Oostblok is die band blijven bestaan.

De Zuid-Afrikaanse krant *Mail & Guardian* suggereert in december 2015 op basis van geruchten uit de inlichtingenwereld afkomstig van journalist Sam Vaknin zelfs dat Russische inlichtingendiensten interesse toonden in financiering van VASTech: "But Vaknin said there were rumours in global intelligence circles that the government initially collaborated with Russian intelligence agencies to fund VASTech."

Of dit serieus genomen moet worden is de vraag. Opvallend is wel dat VASTech in 2021 door de Amerikaanse denktank Atlantic Council wordt afgeschilderd als een bedrijf dat apparatuur levert aan vijanden van de Verenigde Staten en NAVO. De Atlantic Council richt zich op de NAVO, de relatie tussen de Verenigde Staten en Europa en internationale zaken en heeft een invloedrijke plek verworven in de Amerikaanse politiek.

Spyware was lange tijd geen belangrijk issue, ook niet in de Verenigde Staten. Het rapport 'Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets' van november 2021 van de Atlantic Council is dan ook opmerkelijk. Het rapport is een inventarisatie van de bezoeken van bedrijven aan allerlei surveillance en militaire beurzen, zoals ISS World en Milipol. Volgens het rapport probeert het grootste deel van de bedrijven hun apparatuur buiten het continent van hun herkomstland te verkopen: "The authors found that 75 percent of companies likely selling interception/intrusion technologies have marketed these capabilities to governments outside their home continent."

VASTech krijgt, met vier andere bedrijven, een aparte vermelding in het rapport. Volgens de Atlantic Council levert het bedrijf apparatuur aan vijanden van de Verenigde Staten en de NAVO: "Five irresponsible proliferators - BTT, Cellebrite, Micro Systemation AB, Verint, and Vastech - have marketed their capabilities to US/NATO adversaries in the last ten years." Volgens het rapport heeft VASTech haar producten over de gehele wereld gepresenteerd aan bezoekers die niet alleen afkomstig waren uit parlementaire democratieën, maar ook uit repressieve regimes die niet allemaal op goede voet staan met de Verenigde Staten en de NAVO.

De onderbouwing van de claim van de Atlantic Council over leveringen van VASTech aan vijanden is, net als de bewering van Sam Vaknin over VASTech en de Russische inlichtingendiensten, nogal mager. Het is tevens de vraag in hoeverre VASTech zich onderscheidt van andere bedrijven uit de surveillance industrie. De mondialisering van de economie heeft ertoe geleid dat veel bedrijven met de 'vijand' handeldrijven. Bij de productie van surveillance apparatuur zijn, net als bij andere productieketens landen, betrokken die soms met elkaar in conflict zijn. Dit blijkt uit de handelsbetrekkingen van VASTech met verschillende landen in de voormalige Sovjet-Unie (Oekraïne en Georgië) en met India en Pakistan.

Toeleveranciers uit Oekraïne, surveillance van Abchazië en Zuid-Ossetië

Hoewel Zuid-Afrika en Rusland historische banden hebben, doet VASTech zaken met landen die op gespannen voet staan met Rusland, zoals Oekraïne en Georgië. Al ruim tien jaar zijn de Oekraïense bedrijven Sigmatech en VD Mais NVF PP toeleveranciers van VASTech. Van 21 april 2010 tot en met maart 2021 ontving het Zuid-Afrikaanse bedrijf tientallen keren onderdelen uit Oekraïne van deze twee bedrijven, met name van VD Mais NVF PP. VD Mais omschrijft zichzelf als ontwikkelaar, producent en distributeur van elektronische componenten en apparatuur. "Starting from R&D and ending at finished electronic module. Our core business includes distribution of electronic components, measuring and testing equipment, electromechanical products, production of printed circuit boards, contract manufacturing and repair of electronics." VD Mais is ook reseller voor het Duitse Siemens.

VASTech koopt niet alleen onderdelen van een voormalig Sovjetrepubliek, maar verkoopt ook haar apparatuur in de regio. Zo leverde het Zuid-Afrikaanse bedrijf haar apparatuur aan Georgië, een andere voormalige Sovjet staat waar Rusland mee op voet van oorlog staat. Het land heeft zich in de loop der jaren grotendeels ontworsteld aan de Russische invloedsferen. Begin 2021 sluit VASTech een deal voor de levering van apparatuur voor satelliet surveillance (compact Satellite Signal Analyzer, compact SSA) aan dat land.

De compact SSA van VASTech lijkt bedoeld voor de surveillance van alle communicatie in Abchazië en Zuid-Ossetië, delen van Georgië die onder Russische invloed staan, al wordt in de openbare productomschrijving aangegeven dat het bij Abchazië en Zuid-Ossetië slechts om voorbeelden gaat. In de productomschrijving van VASTech wordt gesproken over "monitoring telecommunications traffic in the pink areas from the white."

In een afgedrukte kaart in het document, die in de productomschrijving is overgenomen van wikimedia, zijn Abchazië en Zuid-Ossetië roze gekleurd en de rest van Georgië wit. VASTech geeft aan dat de communicatie in de roze delen gemonitord kan worden zonder fysieke toegang te hebben tot de netwerken: "Satellite monitoring is one of the easiest ways in which a Monitoring Agency located in one area can monitor the telecommunications taking place in another area where they might not have physical access to the telecommunications network being monitored."

Import uit India, surveillance door Pakistan

Ook India levert de Zuid-Afrikanen onderdelen voor haar apparatuur, terwijl Pakistan afnemer is van de apparatuur van VASTech. Gezien het langlopende conflict tussen India en Pakistan is de productie van onderdelen voor massasurveillance apparatuur voor Pakistan opmerkelijk.

Volgens het handelsgegevensbedrijf Panjiva Inc. produceren de Indiase bedrijven CoreEL Technologies en Valiant Communications zeker sinds 2015 onderdelen voor VASTech. CoreEL Technologies India Pvt Ltd is een elektronicabedrijf dat volgens haar website produceert voor onder andere de luchtvaartindustrie en defensie. Valiant Communications Limited is producent van telecommunicatie en cybersecurityapparatuur. Het heeft - naast de Amerikaanse overheid en de wapenfabrikanten Raytheon en Northrop Grumman - net als CoreEL Technologies het Duitse Siemens als klant.

De import uit India is opvallend omdat VASTech tegelijkertijd haar monitoring systemen levert aan Pakistan. Uit gegevens van Panjiva Inc. blijkt dat VASTech in maart 2014 apparatuur aan Pakistan heeft geleverd. De levering verliep via het VASTech kantoor in Dubai. De eindbestemming in Pakistan is voor deze levering niet bekend.

In augustus 2017 volgt een nieuwe verzending naar Pakistan. Ditmaal is de afnemer wel bekend, namelijk een bedrijf waar VASTech regelmatig mee samenwerkt: Trovicor (voorheen Nokia Siemens Networks (NSN)). Trovicor (Smc Pvt.) Ltd. is een dochteronderneming van Trovicor en al sinds 2009 in Pakistan gevestigd. NSN is bekend van levering aan Iran. Trovicor wordt in verband gebracht met leveringen aan Tajikistan in 2009 en Bahrein in 2010. In 2019 volgt nog een levering van VASTech aan Pakistan. Van deze levering is ook niet de eindbestemming bekend.

2018 - 2021 Monitoring centrum voor Saoedi-Arabië

Vanaf eind 2010, het begin van de Arabische Lente, komt de handel van de surveillance-industrie in het Midden-Oosten onder een vergrootglas te liggen. Dit weerhoudt Westerse bedrijven er echter niet van om toch zaken te blijven doen in de regio. Ook VASTech blijft actief in de regio.

Van 2018 tot en met 2021 werkt VASTech aan een monitoring centrum in Saoedi-Arabië. De Zuid-Afrikanen kennen de situatie in het land goed. Tien jaar eerder deed VASTech in april 2008 mee aan een vierdaagse bijeenkomst op het Saoedische Ministerie van Binnenlandse Zaken. De bijeenkomst was een van de voorbereidingsbijeenkomsten voor het opzetten van het Saoedische surveillance lab. Ook het Italiaanse RCS SpA, het Australische Senetas Corporation Ltd, het Nederlandse Fox-IT en later ook het Nederlandse Forensische Instituut (NFI) en TNO (Nederlandse Organisatie voor toegepast natuurwetenschappelijk onderzoek) namen deel aan deze bijeenkomst.

Het nieuwe project voor een surveillance systeem van satellietcommunicatie (Communications Intelligence of COMINT) voor het Ministerie van Defensie maakt deel uit van een samenwerkingsproject tussen de Franse en Saoedische overheid, Saudi Fransi Military Contract (SFMC).

Vanuit Zuid-Afrika wordt een 'Field Support Engineer' aangesteld om in Saoedi-Arabië het contact over het project tussen VASTech en het Ministerie van Defensie soepel te laten lopen. Saoedische engineers doorlopen in hetzelfde jaar 2018 een training voor het onderhouden en het repareren van VASTech apparatuur, 'RF System Maintenance and Support' (Radiofrequentie (RF)). Eind 2021 is het monitoring centrum voor het Saoedische regime afgerond.

Bij dit project werkt VASTech samen met het Franse Arpège, onderdeel van het Duitse Rohde & Schwarz en twee Amerikaanse bedrijven: General Dynamics en Rohn Product Industries. Het Zuid-Afrikaanse bedrijf werkt mee aan "SFMC03 & 04, Client MODA, Main Contractor, Arpège – France, VASTECH - South Africa, Supplier, General Dynamic, USA" schrijft een engineer van het project. Doel van het project is de installatie van satelliet antennes, installatie van een communicatiesysteem en het verbeteren van het datacentrum.

Arpège en VASTech voeren het project uit met het lokale bedrijf Datalink Technical Service Company (DLTSC). DLSTC schrijft dat het met VASTech het datacentrum inricht om ruwe communicatie af te luisteren: “DLTSC is partnered with one of the world’s leading technology company VASTECH on providing intelligence extraction from raw communication data.”

DLTSC schrijft op haar website dat VASTech surveillance van alle regionale, natonale en international communicatie in en uit Saoedi-Arabië levert: “VASTech’s unified systems provide a workbench with complete communication cover to gather regional, national and transnational intelligence through; Galaxia, Strata en Portevia.” Dit is communicatie via de kabel, mobile of satelliet: “In a unified system, these tools, application and systems, enable customers to analyse, monitor and investigate diverse communication deployed on satellite, Optic Fibre and Fixed & Mobile Networks for intelligence extraction from raw communication data.”

VASTech houdt zich op geen enkele wijze bezig met de mogelijke impact van het project op de mensenrechten, hoewel de mensenrechtensituatie in het land hiertoe wel aanleiding geeft. Op 2 oktober 2018 werd journalist Jamal Khashoggi vermoord door Saoediërs die een directe link hebben met de belangrijkste kroonprins van het land Mohammed bin Salman. Daarnaast zijn er al jaren grote zorgen over ernstige beperkingen van de vrijheid van meningsuiting, de behandeling van gevangen, het rechtssysteem, arbeidsrechten, de vervolging van mensenrechtenactivisten en andere burger- en mensenrechten. Sinds 2015 is Saoedi-Arabië tevens betrokken bij talloze mensenrechtenschendingen in Jemen.

Het project in Saoedi-Arabië past in de lijn van de betrokkenheid van VASTech bij surveillance projecten in repressieve regimes zoals de Verenigde Arabische Emiraten, Libië, Egypte en Syrië.

Naar inhoudsopgave Observant #79

Documenten bij onderzoek en profiel VASTech / Cyberupt

Het onderzoek van Buro Jansen & Janssen naar VASTech en Cyberupt is gebaseerd op openbare bronnen, interne bedrijfsdocumenten en e-mails die Buro Jansen & Janssen in 2017 heeft ontvangen over de relatie van het Nederlandse bedrijf Fox-IT met het Duitse bedrijf AGT, de door Wikileaks openbaar gemaakte Hacking Team files en diverse Wob/Woo verzoeken. Hier kunt u enkele van deze bronnen verifiëren.

Artikelen waar de stukken bij gebruikt zijn

- Nederlandse overheid rolt rode loper uit voor Zuid-Afrikaans surveillance bedrijf dat levert aan repressieve regimes (samenvatting)
- Nederlandse overheid rolt rode loper uit voor Zuid-Afrikaans surveillance bedrijf dat levert aan repressieve regimes
- Zuid-Afrikaans surveillance bedrijf VASTech leverancier van repressieve regimes

VASTech

18_200702-ISS-DXB-VASTECH
41_200810-ISS-PRG-VASTECH
182_VASTECH-201110-BROCHURES
284-vastech-zebra1
285_VASTECH-ZEBRA2
VasTech-Sanitized

SearTech

157_njala-model-ntxr-b-digital-audio-transmitter

Elaman

telephone-line-monitoring-zebra-e1-t1

Wob/Woo documenten
documentenWobverzoek

Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets
Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets
Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets, the report in pdf
Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets (artikel bespacific)
Swedish surveillance company criticized in US report

Algerije
Espionnage : VasTech, la surveillance numérique made in Afrique du Sud

Egypt
Africa: Dictators used SA surveillance equipment, says WikiLeaks
Dictators used SA surveillance equipment: WikiLeaks
The Spyfiles

Georgië
748bcc6aab75d02f3e374f1326c92edaebf1a99b7b9a5b8d04d6b66914e5969d.trusted

India

Panjiva-Consolidated_View-_Vas_Tech_SA_Pty_Ltd_-_results_1_to_7_of_7-2022-05-30-04-54.xlsx
Panjiva-Consolidated_View-Vastech_SA_Pty_Ltd-results_1_to_4_of_4-2022-05-30-04-47.xlsx
Panjiva-Consolidated_View-Vastech_SA_Pty_Ltd-results_1_to_4_of_4-2022-05-30-04-51.xlsx
Panjiva-Consolidated_View-VASTech-results_1_to_27_of_27-2022-05-30-04-56.xlsx
Panjiva-Vas_Tech_SA_(Pty)_)_Ltd.pdf
Panjiva-Vastech_Private_Ltd.pdf
Panjiva-Vastech_S.A._Ltd_(1).pdf
52wmb_Buyer_Vastech_S.a.pvt_Ltd._Import_Data_And_Contact.pdf
52wmb_buyer_Vastech_S.a.pvt_Ltd._Import_Data_And_Contact_alternative.pdf
52wmb_Buyer_Vastech_S.a_Pvt_Ltd._Import_Data_And_Contact_alternative_2.pdf
Import_Genius_Vastech_Ukraine.xlsx

Iran / Spy Cables

What do the #SpyCables say about SA's tech industry?
Say nothing – the spooks are listening
South African company selling spy technology to the world
What The #SpyCables Say About South Africa's Tech Industry
South African Spy Company Used by Gadaffi Touts its NSA-Like Capabilities
alj-spy-files-2015-02-21-23.pdf
alj-spy-files-2015-02-21-25.pdf
alj-spy-files-2015-0221-2.pdf
israel-mossad-warns-of-uranium-shipment.pdf
Mossad-On-Iran-Nuclear-Stat.pdf
south-africa-amp-ethiopia-intel-meet-on-dlamini(1).pdf
south-africa-amp-ethiopia-intel-meet-on-dlamini.pdf
south-africa-ethiopia-correspondence-22-october(1).pdf
south-africa-ethiopia-correspondence-22-october.pdf
south-africa-operational-target-analysis-of-iranocr.pdf
south-africa-operational-target-analysis-of-iran.pdf

south-africa-zimbabwe-joint-action-plan-2011-2012.pdf
south-korea-on-uae-seizure-of-arms-delivered.pdf
ssa-and-mi6-on-iran-october-2009.pdf
ssa-assessment-of-irans-interests-and-activities.pdf
ssa-counter-espionage-input-to-the-state.pdf
ssa-meets-iran-intelligence-may-2012.pdf
ssa-meets-iran-may-2012.pdf
ssa-meets-israel-mossad-october-2012.pdf
ssa-on-iranian-intelligence-in-africa-october-2012.pdf
ssa-on-security-vulnerabilities-in-south-african.pdf
uk-mi6-writes-to-ssa-on-ian-profileration.pdf

Libië
Firms Aided Libyan Spies

Maleisië
Intelligence gatherer

Mexico
SampleBillofLadingmexico.pdf

Oeganda
Datalink integrates French military surveillance systems sold to Riyadh

Oekraïne
VastechSapvtLtd

Oman
VASTechLLC.pdf

Pakistan
VastechMeFzePakistan2014.pdf
Panjiva-Vastech(Pty)Ltd.pdf
vastechptyltdpakistan2019

Saoedi-Arabië
attendees-in-MOI-Saudi-meeting 2008
Datalink integrates French military surveillance systems sold to Riyadh
Interceptions specialist Vastech seeks new pastures through German connections
Communication Intelligence Solutions

Qatar
2010octoberReCopyofpassportslibyanofficialsvastech

Syrië
bidinvitation_ex
STEtender2007
Ref768.20.1.1_3102007
TechTenderBkCMSRef768
2008novFWHotelAccommodationfordemo2vastech
Adherece20090604
Attestation20090604
Consortiumagreement20090604
Declaration20090604
LegalStatement20090604
request20090604
Statement20090604
Statementoffinndtechsituation20090604
STERef_83420.1.1_InternationalExchange_2872009
STEFax_ContentFiltering_diagram_14420090001
VASTech_Frans&Alex_ISS_Feb052008
InvitationVastech
Epson047
OpenSeason_0

Verenigde Arabische Emiraten
J-ICU-01-PRP-01IntelsatSystem SpecificationV1.2.pdf
J-IMS-01-PRP-01-AEMOIInmarsat1.1.pdf
J-LA-001-OFR-01LAMMSOffer1.pdf
J-LA-001-PM-01LAProjectPlan1.pdf
J-LA-001-SSP-01LASystemSpecification1.pdf
J-LA-001-URS-01LAUserRequirements1.1.pdf
J-LA-001-VT-01LAVASTechprofile2.pdf
J-LA-01-COMO-01LACommercialOffer1.pdf
LAcoverletter2JAS.pdf

Oeganda
Datalink integrates French military surveillance systems sold to Riyadh

Zimbabwe
Intelligence gatherer

Zuid-Afrika
South African Spy Company Used by Gadaffi Touts its NSA-like Capabilities
Say nothing – the spooks are listening
South African government provided funding for development of mass surveillance technologies found in Libya
SA government questioned over R3.5m investment in spy firm

ISS World documenten

ISS World 2006

ISS World Washington D.C. 2006
ISSWorld_LEA_web.pdf
iss-world-2006.pdf
issworld2006programfromwebsite.pdf
issworld2006sponsorsfromwebsite.pdf

ISS World 2007

ISS World Americas Washington 2007
ISSworldwashington2007brochure
ISSWorldwashington2007sponsorsfromwebsite

ISS World EMEA Dubai 2007
ISSWorldDubai2007brochure
ISSWorldDubai2007agendafromwebsite
ISSworldDubai2007sponsorsfromwebsite
ISSworlddubai2007visitors
ISSWorldDubaiListofAttendingCompanies

ISS World 2008

ISS World Americas Washington 2008
issworldamericasdecember2008programfromwebsite
issworldamericasdecember2008sponsorsfromwebsite

ISS World Asia Pacific 2008
ISSWorldAP_Bro06_web
ISSWorldAsiaPacificjune2008sponsorsfromwebsite
ISSWorldAsiaPacificjune2008programfromwebsite

ISS World EMEA Dubai 2008
issworldemeafeb2008programfromwebsite
issworldemeafeb2008sponsorsfromwebsite
issworldemea2008visitors

ISS World Europe Prague 2008
ISSWorldEuropebrochure2008
issworldeurope2008programfromwebsite
issworldeurope2008sponsorsfromwebsite
issworldeuropeoktober2008visitors

ISS World 2009
ISS World Americas Washington 2009
issworldamericas2009programfromwebsite
issworldamericas2009sponsorsfromwebsite

ISS World Asia Pacific 2009
ISSWorldAsiaPacific2009brochure

ISS World Europe Prague 2009
issworldeurope2009programfromwebsite
issworldeurope2009sponsorsfromwebsite

ISS World MEA Dubai 2009
ISSWorldMEA2009
issworldmea2009programfromwebsite
issworldmeafeb2009sponsorsfromwebsite

ISS World 2010
ISS World Americas Washington 2010
issworldamericasoktober2010
ISSWorldamericas2010programfromwebsite
ISSWorldamericas2010sponsorsfromwebsite

ISS World Asia Pacific 2010
ISSWorldAsiaPacificdecember2010.pdf

ISS World Europe Prague 2010
issworldeuropeagenda2010
ISSWorldeurope2010programfromwebsite
ISSWorldeurope2010sponsorsfromwebsite

ISS World MEA Dubai 2010
ISSWorldMEA2010
ISSWorldMEAfeb2010programfromwebsite
ISSWorldMEAfeb2010sponsorsfromwebsite

ISS World 2011
ISS World Americas Washington 2011
issworldamericas2011brochure
ISSWorldamericas2011programfromwebsite
ISSWorldamericas2011sponsorsfromwebsite

ISS World Asia Pacific 2011
ISSWorldAsiaPacificdecember2011

ISS World Europe Prague 2011
issworldeurope2011brochure
ISSWorldEuropejune2011programfromwebsite
ISSWorldEuropejune2011sponsorsfromwebsite

ISS World Latin America 2011
issworldlatinamerica2011brochure

ISS World MEA Dubai 2011
issworldmeabrochurefebruari2011
ISSWorldMea2011programfromwebsite
ISSWorldMea2011sponsorsfromwebsite

ISS World 2012
ISS World Americas Washington 2012
issworldamericas2012brochure
ISSWorldamericas2012programfromwebsite
issworldstatistics2012

ISS World Asia Pacific 2012
ISSWorldAsiadecember2012

ISS World Europe Prague 2012
ISSworldeurope2012brochure
ISSWorldeurope2012programfromwebsite
ISSWorldeurope2012sponsorsfromwebsite

ISS World Latin America 2012
issworldlatinamerica2012brochure

ISS World MEA Dubai 2012
issworldmea2012brochure
ISSWorldMea2012programfromwebsite
ISSWorldMea2012sponsorsfromwebsite

ISS World 2013
ISSWorldEurope2013brochure
ISSWorldAmericas2013brochure
ISSWorldAsiadecember2013
ISSWorldLatinAmericaoktober2013
ISSWorldMiddleEastmaart2013
issworldattendees2013
ProgramScheduleforYear

ISS World 2014
ISSWorldAmericas2014brochure.pdf
ISSWorldAsiadecember2014.pdf
2014-06_ISS-Europe-brochure
ISSWorldMiddleEastmaart2014.pdf
ISSWorldsouthafrica2014.pdf

ISS World 2015
ISSworldamericasseptokt2015.pdf
issworldeurope2015brochure.pdf
ISSWorldMiddleEastmaart2015.pdf
ISSWorldSouthAfricajuly2015.pdf
ISSWorldAsiadecember2015.pdf
ISSWorldLatinAmerica.pdf

ISS World 2016
ISSworldamericas2016brochure
ISSWorldEuropejune2016
ISSWorldLatinAmericaoktober2016
ISSWorldLatinAmerica2016
ISSWorldMiddleEastmaart2016
ISSWorldsouthafrica2016

ISS World 2017
ISSworldamericas2017brochure
ISSWorldAsiadecember2017
ISSWorldEuropejuni2017
ISSWorldMiddleEastmaart2017

ISS World 2018
ISSworldamericas2018brochure
ISSWorldAsiaPacific2018
ISSWorldEuropejune2018
ISSWorldLatinAmerica2018
ISSWorldMiddleEastmaart2018

ISS World 2019
ISSworldamericassepember2019
ISSWorldAsiaPacific2019
ISSWorldEuropejune2019
ISSWorldLatinAmericaoktober2019
ISSWorldMiddleEastmaart2019

ISS World 2020
ISSWorldEuropejune2020.pdf
ISSWorldMiddleEastmaart2020.pdf

ISS World 2021
ISSWorldEurope2021.pdf
ISSWorldMiddleEastmaart2021.pdf
ISSWorldNorthAmerica2021.pdf

ISS World 2022
BrochureEurope2022
Brochurelatin2022

Naar inhoudsopgave Observant #79

Je hoeft geen complotdenker te zijn om twijfels te hebben bij het gangbare vertoog over de oorlog in Oekraïne (selectie artikelen op nieuwsblog over export van wapens naar Rusland)

Je hoeft geen complotdenker te zijn om twijfels te hebben bij het gangbare vertoog over de oorlog in Oekraïne. Voor Buro Jansen & Janssen was en is Rusland een dictatuur sinds de aanslagen in 2004 in Beslan of misschien zelfs eerder. Rusland is in de huidige oorlog opnieuw duidelijk de agressor en pleegt op grote schaal oorlogsmisdaden.

Toch is het belangrijk om vragen te blijven stellen, net als bij elke crisis. De vragen die wij nu onder andere stellen is waarom Europa en de Verenigde Staten Rusland hebben geholpen met de militaire opbouw van Rusland. Ook na de bezetting van de Krim is de export naar Rusland niet aan banden gelegd. En waarom worden overtredingen van die sancties niet onderzocht of worden bedrijven die die overtredingen hebben begaan niet stevig aangepakt en fors veroordeeld?

Er worden in de verzamelde berichten verschillende voorbeelden genoemd. Een bedrijf, het Franse Thalens, heeft een paar jaar geleden nog het Nederlandse Gemalto overgenomen. Vraag is dan natuurlijk als Thalens genoemd wordt, wat is de rol van Gemalto?

Buro Jansen & Janssen heeft in 2021 een onderzoek over Fox-IT in Rusland gepubliceerd. Het onderzoek roept de vraag op of Fox-IT de sancties heeft overtreden. Onderzoek zal niet volgen en vergunningen zullen niet strenger worden beoordeeld, dit heeft Buro Jansen & Janssen namelijk in 2020 middels een onderzoek aangetoond.

Het lijkt erop dat de oorlog de Europese Unie en de Verenigde Staten eigenlijk goed uitkomt. Het heeft de kas in het verleden gespekt door Rusland te steunen en nu kunnen overheden goede sier maken door Oekraïne te steunen. Erg wrang is het wel, maar oorlog lijkt het perfecte verdienmodel.

Op nieuwsblog verzamelt Buro Jansen & Janssen artikelen over de export van wapens naar Rusland en de overtredingen van de sancties tegen Rusland. Hier kunt u zien welke artikelen wij hebben verzameld.

[How companies from Switzerland, Italy, and Germany help Russia circumvent sanctions to produce weapons]
30 juni 2022

The investigation was prepared by the Economic Security Council of Ukraine together with the InformNapalm international intelligence community. Instead of a Foreword This is Berenne Alinovi. She has her own business in Barcelona, Spain. She sews cocktail and wedding dresses and creates jewelry with Swarovski crystals. And this is Inna Soloshenko from Lebedyn, Sumy Oblast, […]

[Global arms industry getting shakeup by war in Ukraine – and China and US look like winners from Russia's stumbles]
30 juni 2022

Russia's war in Ukraine is upending the global arms industry. As the U.S. and its allies pour significant sums of money into arming Ukraine and Russia bleeds tanks and personnel, countries across the world are rethinking defense budgets, materiel needs and military relationships. Countries that historically have had low levels of defense spending such as […]

[Who armed Russia?]
30 juni 2022

Despite the embargo imposed in 2014, at least ten EU countries sold military equipment and weapons to the Russian Federation. According to the Working Party on Conventional Arms Exports (COARM) and all EU-27 arms export registers, between 2015 and 2020, France, Germany, Italy, Austria, Bulgaria, the Czech Republic, Croatia, Finland, Slovakia and Spain sold weapons […]

[Ukraine calls out Italian metal company for "supporting Russia's military complex"]
30 juni 2022

Ukraine calls out Italian metal company for "supporting Russia's military complex" Credit: Creative Commons The Defence of Ukraine called out an Italian steel-plant company for its collaboration with Russia, in supplying equipment allegedly destined to produce nuclear submarines and tank armour. Taking to Twitter to publicly call out the Italian company and its support of […]

[Italian company accused of supplying Russian military, even after invasion]
30 juni 2022

According to the message, these shipments have been ongoing even after Feb. 24 – the day Russia launched a full-scale invasion of Ukraine. "Supporting Russian military (-industrial) complex goes against lawful and moral considerations," the ministry said.

[Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain]
30 juni 2022

Since the invasion of Ukraine began, we have been tracking the responses of well over 1,200 companies, and counting. Over 1,000 companies have publicly announced they are voluntarily curtailing operations in Russia to some degree beyond the bare minimum legally required by international sanctions — but some companies have continued to operate in Russia undeterred. Originally […]

[Those who stay: how companies justify their stay in russia]
30 juni 2022

After the start of the full-scale attack of Russia on Ukraine, with tens of thousands killed and multiple war crimes documented, many companies (often under the pressure of their customers and shareholders) have left Russia. Others stayed, continuing to provide goods and services — to Russians and taxes — to the Russian government. Figure 1 […]

[French arms firm busts sanctions to help Russia build weapons]
30 juni 2022

It was the BMD-4 with the Thales-made Catherine FC thermal imaging camera that took part in the shelling of Ukrainian civilian cars in Bucha. I saw a post by volunteers on a social network, and together with my fellow lawyers we launched our own probe into the French manufacturer’s involvement in Russia’s military aggression against […]

[War in Ukraine: the Thales group has delivered kits to Russia until 2019 to assemble infrared cameras]
30 juni 2022

Thales acknowledges in a press release on Saturday April 30 having delivered until 2019 to the Russian company Vomz “kits for assembling thermal cameras”namely infrared cameras, confirming information from the Parisian. The French defense group, however, ensures that it does not have “nothing sold since 2014” and “the application of European sanctions against Russia”. “No […]

[France’s Thales Accused Of Selling To Russia Despite Sanctions, Denied By Company]
30 juni 2022

A senior Ukrainian official on Friday accused French defence electronics company Thales of violating European sanctions and selling Russia equipment that was used to kill civilians fleeing recent fighting outside Kyiv, claims strongly denied by Thales. “A family was trying to escape but was killed by Russian murderers,” tweeted presidential adviser Mykhaylo Podolyak. “Killed, as […]

[The French company Thales supplied Russia with its Catherine FC thermal imagers for the BMD-4M]
30 juni 2022

Pavlo Kashchuk, known as the founder of the infocar.ua project and host of the YouTube channel of the same name, published a video on it, shot after Bucha’s liberation from the ruscism occupiers. It shows not only traces of war crimes with the killing of civilians, but also abandoned equipment by retreating troops, which found […]

[EU'S SHAME France and Germany dodged Russia arms embargo to sell weapons to Putin – that are now being used to slaughter Ukrainians]
30 juni 2022

FRANCE, Germany and Italy side-stepped an arms embargo to sell weapons to Vladimir Putin that are being used to slaughter Ukrainians. On a day of shame for the EU, it emerged ten member states sold hundreds of millions of pounds of military kit to Russia between 2015 and 2020. Paris sent bombs, rockets and explosives, […]

[EU member states exported weapons to Russia after the 2014 embargo (2022)]
31 maart 2022

Missiles, aircraft, rockets, torpedoes, bombs. Russia continued to buy EU weapons until at least 2020. Despite the ongoing embargo, ten member states exported € 346 million worth of military equipment, according to public data analysed by Investigate Europe. Some of these weapons could be used against Ukraine now. "Our destinies are linked. Ukraine is part […]

[Staggering data shows NATO aided Putin by supplying arms being used against Ukraine (2022)]
31 maart 2022

STAGGERING unearthed data has revealed several NATO countries – including the UK – have supplied weapons and military equipment to Russia worth hundreds of millions of pounds, some of which are likely to be used against Ukraine today. NATO military alliance members including the UK, France and Germany, are being accused of supporting Russia's invasion of Ukraine by […]

Germany exported military equipment to Russia despite embargo: Report (2022)
31 maart 2022

$134 million worth of military equipment shipped between 2014 and 2020, despite EU sanctions on Russia, according to local media Germany shipped €122 million ($134 million) worth of military equipment to Russia despite the EU arms embargo in effect since 2014, local media has reported. Nine other EU member states also exported military goods during […]

France, Germany and Italy sold hundreds of millions of pounds worth of arms and military kit to Russia for years despite embargo (2022)
31 maart 2022

France, Germany and Italy sold hundreds of millions worth of arms to Russia They sold military kit to the Kremlin for years despite an EU embargo banning it They were three of at least 10 countries to use a loophole to get past the ban France alone sold €152million out of a total €350million (£293million) exported […]

France continued to deliver Russia weapons after 2014 embargo
31 maart 2022

France continued to issue arms export licences to Russia after the 2014 embargo, investigative website Disclose has revealed. According to leaked documents, French companies delivered arms to Russia after the EU imposed sanctions, including an arms embargo, against Russia in 2014. France has since issued more than 70 licences to export military equipment to companies […]

[A Third of EU Member States Exported Weapons to Russia (2022)]
31 maart 2022

A third of European Union (EU) member states exported weapons to Russia after the 2014 embargo banning them, according to data from the working group, which records all military exports from the 27, analyzed by Investigate Europe. The data, released today in the newspaper Public, indicate that 10 EU countries exported weapons to Russia after […]

[EU arms firms trying to flout Belarus and Russia ban (2021)]
31 maart 2022

Three EU-based firms are suspected of trying to smuggle arms to Belarus and Russia, in what might be the tip of a larger black market. Czech firm Česká zbrojovka tried to export over 100 rifles and pistols via Moldova to Russia in 2020, according to a Moldovan document seen by EUobserver. The shipment included 'CZ […]

[Up in arms: Warring over Europe's arms export regime (2019)]
31 maart 2022

The European Union's poorly co-ordinated arms export policy is undermining Europe's security, its foreign policy and its defence industry. The EU's arms export policy should have three aims. First, arms control, in order to keep arms out of the wrong hands. Second, targeted arms exports to allies and countries that share the EU's security challenges. […]

[EU arms embargo on Russia will make little impact if France can still sell Putin warships (2014)]
31 maart 2022

The Council of the EU is currently struggling over whether to impose an arms embargo on Russia as punishment for its role in destabilising Ukraine. Several governments in the EU, including the UK, have already announced that they are denying arms export licences for Russia and revoking those that have previously been granted. Also in […]

[From guns to warships: Inside Europe's arms trade with Russia (2014)]
31 maart 2022

The West has slapped stringent sanctions on Russia in response to the downing of Malaysia Airlines Flight 17, believed by the U.S. and others to have been shot down with a Russia-supplied Buk missile system by eastern Ukraine rebels. While the introduction of financial sanctions will create the most immediate squeeze on Russia, it is […]

[Weapons of the war in Ukraine. Russian entities acquired British, Czech, French, German, Spanish, and US-made components for use in the manufacture of these drones.]
28 februari 2022

Since 2014, the news media and other observers have provided accounts of weapon sourcing to armed formations operating in certain areas of the Donetsk and Luhansk regions of Ukraine. To date, efforts to verify these claims have relied largely on examinations of open-source photos and videos of weapons and ammunition, rather than systematic field-based investigations. […]

[The United States secretly captured 20 Russian military drones and tracked the entire technology supply chain. The key parts are all imported components]
28 februari 2022

The tough future of Russia's attack drones The rapid development of military drones around the world has raised a natural question time and time again-why is Russia so backward in design and production? In most cases, the main reason for this is the lazy thinking of the military and engineers. However, one of the most […]

[Western sanctions cause "huge problems" for Russia's war sector (but Israel probably still supplies drone parts) – military expert]
28 februari 2022

Editor's Note When we published the key points of the report "Weapons of War in Ukraine" by the UK-based investigative organization Conflict Armament Research, it caught our eye that between 2014 and 2018, the drone manufacturer Israel Aerospace Industries supplied a sanctioned Russian defense company with UAV components produced by various European and US manufacturers, […]

[Russian drones shot down over Ukraine were full of Western parts. Can the U.S. cut them off?]
28 februari 2022

The surveillance drones contained computer chips and components made in the United States and Europe In early 2017, Ukrainian forces battling Russia-backed separatists shot down a drone conducting surveillance over the eastern flank of Ukraine. The unmanned aircraft, nearly six feet long with a cone-shaped nose and a shiny gray body, had all the external […]

[Russian drones shot down over Ukraine had been filled with Western components. Can the U.S. minimize them off?]
28 februari 2022

The engine got here from a German firm that provides model-airplane hobbyists. Laptop chips for navigation and wi-fi communication had been made by U.S. suppliers. A British firm offered a motion-sensing chip. Different components got here from Switzerland and South Korea. "I used to be stunned after we checked out all of it collectively to […]

[British parts found on downed Russian spy drones in Ukraine and EU]
28 februari 2022

British components have been found in Russian-made spy drones captured by Ukrainian and Lithuanian forces, a report shows. The parts are among European kit discovered on Unmanned Aerial Vehicles (UAVs) deployed over Ukraine and neighbouring countries during the conflict in the country's eastern Donbass region, researchers have found. Ukraine is under the threat of invasion, […]

[Fears Russian military drones made with British components could target UK soldiers]
28 februari 2022

Russian-made military drones containing British components are being used by pro-Russian separatist forces in Ukraine and can now be used to target UK soldiers deployed there in the event of an invasion of Moscow, I to learn. Arms experts said an analysis of Russian-made surveillance planes intercepted over Ukraine showed they were made with electronics […]

Fears that Russian military drones built with British components could be used to attack British soldiers during the Ukraine crisis.
28 februari 2022

Pro-Russian separatist forces in Ukraine are using Russian-made military drones with British components, which could now be used to attack UK troops stationed there if Moscow invades.i has learned. An analysis of Russian-built surveillance drones intercepted over Ukraine found that they were built with electronics and mechanical parts from Western countries, including the United Kingdom, […]

Fox-IT in Rusland (samenvatting)
28 februari 2022

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 […]

Fox-IT en het Nederlandse exportbeleid voor dual-use goederen
28 februari 2022

Sinds de Arabische Lente zijn meerdere westerse computer- en beveiligingsbedrijven in opspraak geraakt vanwege hun leveranties aan repressieve regimes in het Midden-Oosten. Sommige bedrijven zijn daarvoor ook juridisch vervolgd. Ook in Nederland stond de export van Nederlandse bedrijven (waaronder Fox-IT) naar landen in het Midden-Oosten rond 2011 in de politieke en publieke belangstelling. Het Midden-Oosten […]
lees meer

Naar inhoudsopgave Observant #79

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 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.

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.

Naar inhoudsopgave Observant#79