MILITARISERING VAN SECURITY

Inventarisatie Nederlandse bedrijven

Campagne tegen Wapenhandel, november 2012
Mark Akkerman

Campagne tegen Wapenhandel

Kantoor Amsterdam
Anna Spenglerstraat 71
1054 NH Amsterdam
tel/fax 020 6164684

Kantoor Groningen
Postbus 7007
9701 JA Groningen
tel 050 3133247

info@stopwapenhandel.org
bank 39.04.07.380
www.stopwapenhandel.org

Colofon
Uitgave: Campagne tegen Wapenhandel, november 2012
Samenstelling: Mark Akkerman

De veiligheidsindustrie

Inleiding

Sinds de aanslagen in de VS op 11 september 2001 is de markt voor 'homeland security' in hoog tempo gegroeid.[1] De nadruk op veiligheid werd ook vertaald in grotere budgetten voor border security (grensbewaking) en cyber security (digitale beveiliging).
De nieuwe fixatie op veiligheid ging gepaard met een steeds verdere militarisering ervan. Mogelijkheden om militairen binnenlands in te zetten worden verruimd, terwijl er tegelijkertijd steeds meer militaire middelen ter beschikking komen voor politionele en paramilitaire inzet op veiligheidsgebied.
De militaire industrie loopt dan ook voorop in het binnendringen van deze markt. Nagenoeg alle grote wapenproducenten hebben inmiddels speciale afdelingen voor homeland security. Daarnaast steken vele nieuwe gespecialiseerde bedrijfjes de kop op.
Amerikaanse, Britse en Israëlische ondernemingen hebben vooralsnog een groot deel van de markt in handen. Ook voor Nederlandse bedrijven is deze sector van toenemend belang. Vooral op het gebied van border en cyber security spreekt Nederland internationaal een, zij het bescheiden, woordje mee. Europees onderzoeksgeld is belangrijke bron van inkomsten.

Veiligheid

Veiligheid is een centraal begrip in de politieke en maatschappelijke discussie geworden sinds 11 september 2001. Volgens criminoloog Hans Boutellier is "[v]eiligheid […] een onverzadigbare behoefte en het najagen daarvan kan een obsessie worden."[2] Elk (vermeend) incident wordt daarbij aangegrepen om nog drastischer maatregelen ter bevordering van de veiligheid af te kondigen.
Dit heeft geleid tot omstreden wetten, zoals de Patriot Act in de Verenigde Staten en het Kaderbesluit Terrorismebestrijding van de Europese Unie, waaruit in Nederland de Wet Terroristische Misdrijven voortvloeide. Mensenrechten en privacy komen hierbij onder druk te staan. Onderzoek wees uit dat sinds september 2011 de mensenrechten in westerse landen systematisch vaker zijn geschonden, veelal met een beroep op de noodzakelijkheid met het oog op veiligheid. "Het argument is dan dat het wringt tussen veiligheid en vrijheid en dat de balans in tijden van nationale nood door moet slaan naar veiligheid", aldus de Tilburgse onderzoeker Benedikt Goderis.[3]
Waar mensenrechten en privacy verliezen door de veiligheidsobsessie, stijgen de winsten van bedrijven. De Amerikaanse journalist Tom Engelhardt stelt: "Each time, the price of "safety" rises and some set of lucky corporations, along with the lobbyists and politicians

1 Tim Starks, Defense contracting: the war dividend; hardware demands at home and abroad readily reversed a downturn, Roll Call, 28 July 2011
2 Geciteerd op http://www.security.nl/artikel/32186/1/De_utopie_van_de_maakbare_veiligheid.html
3 Tilburg University, Mensenrechten systematisch geschonden na 9/11, 11 september 2012

that support them, get a windfall."[4]

Militarisering van security

In het huidige veiligheidsdenken is militaire veiligheid steeds minder een geïsoleerd begrip. De scheidslijnen tussen militaire, politionele en private inzet op veiligheidsgebied vervagen. Dit komt het duidelijkst tot uiting in 'terrorismebestrijding', waar sprake is van een gecombineerde, soms verweven, inzet vanuit deze verschillende sectoren, vaak onder de noemer 'Homeland security'.

Homeland security richt zich op de binnenlandse veiligheid, waarbij het vooral gaat om protectie tegen terroristische activiteiten en (gewelddadig) intern oproer. Zoals eerder al aangestipt wordt hierbij soms een wel erg breed dreigingsbeeld gehanteerd, waardoor ook legitieme oppositie onder druk komt te staan.

Border security richt zich op de het beveiligen van grenzen tegen ongewenste overschrijdingen. In de praktijk gaat het vooral om het tegenhouden van migranten.

Cyber security draait om beveiliging van computersystemen en -data tegen ongewenste digitale bedreigingen, zoals virussen, diefstal en hacken. Ook de offensieve inzet op dit vlak door statelijke actoren wordt hiertoe gerekend.

Het European Civil Liberties Network (ECLN) waarschuwde in 2009: "De EU bevindt zich in het midden van een paradigmaverschuiving met betrekking tot de manier waarop Europa en de wereld daarbuiten worden beveiligd. Dit is het gevolg van een aantal onderling samenhangende historische trends, waaronder de geleidelijke vervaging van de grenzen tussen politioneel en militair optreden en die tussen interne en externe veiligheid, de wijdverspreide toepassing van surveillancetechnologieën en de ontwikkeling van een security-industrieel complex, de economische motor voor deze ontwikkelingen. [...] Het resultaat is een toenemende security-militaristische benadering van langspelende sociale en economische problemen."[5]

Een toekomstbeeld dat voor wapenbedrijven een gouden kans is. Ze spelen op deze trend in door hun aanbod te verruimen en meer op deze security-markten te richten. Het belang van deze snel groeiende markt neemt bovendien verder toe, nu militaire budgetten en wapenaankopen in met name de westerse wereld stagneren onder invloed van de economische crisis.[6]

Er lijkt een oneindige vraag naar nieuwe security-toepassingen te zijn ontstaan. In de praktijk is lang niet altijd duidelijk of deze vraag het aanbod stuurt of dat overheden snel geneigd zijn alles wat de industrie ontwikkelt en in de aanbieding gooit maar aan te schaffen om niet achterop te raken.

De koepelorganisatie van de Nederlandse defensie-industrie, de NIDV, richt zich sinds enkele jaren expliciet op de veiligheidsmarkt naast de traditionele defensiemarkt. Ook de naam werd in 2008 in die richting veranderd: van Nederlandse Industriële Inschakeling Defensieopdrachten naar Nederlandse Industrie voor Defensie en Veiligheid. Met de naamswijziging wordt "duidelijker herkenbaar dat het werkterrein wordt gevormd door

4 Tom Engelhardt, How our "security" obsession costs us, Salon, 30 November 2010

5 ECLN, Oppose the 'Stockholm Programme' – Statement by the European Civil Liberties Network, on the new EU five-year plan on Justice and Home Affairs, April 2009; tot de 'founding organisations' van het ECLN behoren ondermeer Statewatch en het Nederlandse VD AMOK.

6 The Economist, Peace on the Rhine: a European defence gigant heals wounds and looks ahead, 29 December 2010

de nationale veiligheid in brede zin. Dit is in lijn met de ontwikkelingen in politiek en bedrijfsleven, waar de civiel-militaire samenwerking nadrukkelijk op de agenda is geplaatst."[7] De jaarlijkse bijeenkomt van de NIDV vindt in 2012 plaats onder de titel 'Veiligheid komt niet vanzelf'.[8]

Binnenlandse militaire inzet

De Nederlandse krijgsmacht heeft ook een binnenlandse veiligheidstaak. Daarvoor zijn permanent 4600 militairen paraat en heeft Defensie vertegenwoordigers bij alle veiligheidsregio's. De binnenlandse inzet van militairen richt zich tot nu toe met name op zaken als zoek- en observatieoperaties.[9]
De inzet van militair personeel en militaire middelen met het oog op binnenlandse veiligheid wordt sinds enige jaren op meer structurele wijze als serieuze mogelijkheid gezien.[10] Ook vanuit de krijgsmacht zelf presenteert men zich graag als partner voor binnenlandse aangelegenheden. Na de gebeurtenissen rond het zogenaamde Project X in Haren in september 2012 schreven de verenigingen van defensiepersoneel GOV/MHB dat de inzet van het leger rellen had kunnen voorkomen: "Veiligheid in Nederland staat hoog op de politieke agenda. De krijgsmacht heeft middelen en mensen om hieraan mede inhoud te geven. 5.000 militairen staan op afroep van de civiele autoriteiten gereed. In onze beleving had 'Haren' dan ook niet mogen gebeuren. Goede wederzijdse ondersteuning en een goede planning, waar de expertise en de capaciteit van de krijgsmacht had kunnen ondersteunen, zouden dit hebben kunnen voorkomen."[11]
Deze bewering wordt vervolgens gekoppeld aan een pleidooi tegen verdere bezuinigingen op Defensie.

Beurzen

Steeds meer wapenbeurzen zijn zich de afgelopen jaar ook op Homeland Security gaan richten. Specifieke beurzen schieten als paddestoelen de grond uit en al bestaande beurzen maken een forse groei door. Ook voor Nederlandse bedrijven zijn dergelijke beurzen een belangrijk middel om zich op de internationale markt te presenteren en buitenlandse klanten binnen te slepen.
Bekende specifieke security-beurzen zijn de IFSEC (Verenigd Koninkrijk), Milipol (Frankrijk en Qatar), Counter Terror Expo (Verenigd Koninkrijk), Security Essen

7 Bert van Elk, Een kwart eeuw belangenbehartiging: Stichting NIDV 25 jaar actief, NIDV-magazine, no. 3, 2009
8 http://symposium.nidv.eu/nl-NL/pages/1/Home.aspx
9 Martijn Delaere, Defensie helpt justitie en politie, Binnenlands Bestuur, 31 augustus 2012; Dat dergelijke 'hulp' nog een stuk verder kan gaan, blijkt bijvoorbeeld in de Verenigde Staten waar volgens een in 1997 ingesteld programma politie voorzien wordt van gebruikte militaire spullen door defensie, tot geweren en granaatwerpers aan toe; Benjamin Carlson, Battlefield Main Street – Pentagon project lets police forces - even in small towns – arm themselves with military gear, The Daily, 5 December 2011
10 Ministerie van Defensie en Ministerie van Binnenlandse Zaken, Catalogus Civiel-Militaire Samenwerking, juli 2007
11 GOV/MHB, Brief aan informateurs, GOV|MHB/12/0204-256, Den Haag, 26 september 2012

(Duitsland), Homsec (Spanje), Intersec (Dubai), ISS World (divers), Security Israël (Israël) en Sfitex (Rusland).

Financiering uit Brussel

Framework Programmes Europese Unie

Financiële steun aan defensie-onderzoek vanuit de Europese Unie ligt politiek erg gevoelig, maar via de omweg van 'veiligheid' gaat er veel geld vanuit Brussel naar de defensie-industrie en militair gerelateerd onderzoek. De Europese Unie subsidieert onderzoek en ontwikkeling van technologie op security-terrein, in het kader van de zogenaamde Kaderprogramma's voor Onderzoek.[12] Veel grote opdrachten worden gegund aan consortia, waarin naast bedrijven ook regelmatig onderzoeksinstituten en universiteiten deelnemen.[13]

Vooral EADS en TNO zijn erg bedreven in het binnenslepen van Europees onderzoeksgeld. De projecten waar zij bij betrokken zijn, worden verderop beschreven. In onderstaande tabel een overzicht van andere Nederlandse bedrijven en instellingen die op kleinere schaal betrokken zijn bij Europees security-onderzoek.

Een voorbeeld is het BS-UAV-project, een studie naar de mogelijkheden van het gebruik van drones voor grensbewaking (zowel boven land als boven zee) in Europa. Daartoe worden de problemen die er nu met grensbewaking zouden zijn in kaart gebracht, en bekeken hoe en welke drones ingezet kunnen worden om oplossingen te bieden.[14] Vanuit Nederland is het Nationaal Lucht- en Ruimtevaartlaboratorium (NLR) betrokken in een consortium waarin ook wapenfabrikanten SAAB, Thales en Rolls-Royce deelnemen. Het NLR is ook bezig met het opzetten van het eerste Europese trainingscentrum voor operators van drones in het Brabantse Rijen. Daarbij werkt het NLR samen met onder meer de Universiteit van Tilburg.[15]

[12] http://europa.eu/legislation_summaries/energy/european_energy_policy/i23022_nl.htm
[13] Ben Hayes, Neoconopticon, TNI / Statewatch, September 2009
[14] EU Directorate General Enterprise and Industry Security Research, Border Surveillance – UAV, 2005
[15] NLR, Trainig Academy for unmanned aviation, 5 July 2012

Betrokkenheid Nederlandse bedrijven bij Europees Kaderprogramma onderzoek			
Naam	**Omschrijving**	**Hoofdaannemer**	**Betrokken Nederlandse bedrijven/instellingen**
SUPPORT	Ontwikkeling beveiliging havens oa ter voorkoming van illegale immigratie	BMT Group (Verenigd Koninkrijk)	ECOSLC (voorheen Stichting Ecoports) Gemeente Amsterdam
SECTRONIC	Observatie en beveiliging maritieme infrastructuur	Maritime and Remote Sensing Solutions (Verenigd Koninkrijk)	Uniresearch Havenbedrijf Rotterdam
HUMBOLDT	Integratie ruimtelijke data voor oa grensbewaking (GMES)	Fraunhofer (Duitsland)	Maris OTB (TU Delft)
BS-UAV	Onderzoek gebruik van drones voor grensbewaking	Dassault Aviation (Frankrijk)	NLR
CRISIS	Ontwikkelen simulatie-omgeving voor voorbereiding hulpverleners en coördinatoren crisissituaties luchthavens	School of Engineering & Information Sciences (VK)	NLR
E-SPONDER	Ontwikkelen informatie- en communicatiesysteem voor 'first responders' in crisissituaties	Exodus (Griekenland)	CrisisPlan BV
EMILI	Ontwikkelen nieuwe generatie besturingssystemen voor grootschalige kritieke infrastructuur	Fraunhofer IAIS (Duitsland)	Centrum voor Wiskunde en Informatica
EUSECON	Ontwikkelen analytisch kader voor aanvullend onderzoek op het vlak van veiligheidseconomie	German Institute for Economic Research (Duitsland)	Institute of Social Studies
INDIGO	Ontwikkelen systeem voor integreren nieuwste ontwikkelingen in de virtuele werkelijkheid en simulatie mbt rampen en crises	Diginext (Frankrijk)	CrisisPlan BV
INEX	Analyse van de waardegebaseerde premissen en ethische consequenties van het interne/externe veiligheidscontinuüm	Peace Research Institute Oslo (Noorwegen)	Vrije Universiteit
OPTIX	Ontwikkelen mobiel systeem voor detectie en identificatie van explosieven	Indra Sistemas (Spanje)	Avantes
SEREN	Versterken onderzoeksnetwerk van nationale contactpunten voor security-onderzoek	Commissariat à l'Energie Atomique (Frankrijk)	SenterNovem
bron: cordis.europa.eu			

EADS

EADS is het op een na grootste Europese wapenbedrijf. Het hoofdkantoor zit in Nederland (Leiden), productie vindt met name in Duitsland, Frankrijk en Spanje plaats. De laatste jaren is EADS steeds actiever op de security-markt. Cassidian, het primaire militaire onderdeel van het bedrijf, verwacht in 2020 50% van de inkomsten uit deze sector te halen. In 2009 was dit 20 %.[16]

[16] http://www.hstoday.us/focused-topics/airport-aviation/single-article-page/market-monitor-eads-boosts-security-growth-priority.html

EADS is op alle security-gebieden actief. Zo werd in 2012 een nieuwe Cyber Security Business Unit gelanceerd. Op dit vlak beperken de klanten zich nu nog tot het Verenigd Koninkrijk, Duitsland en Frankrijk, maar een snelle groei, ondermeer door het opkopen van kleinere bedrijven, wordt verwacht.[17]

EADS heeft zich het meest geprofileerd op het terrein van grensbeveiliging. In het Midden-Oosten wist het bedrijf in 2007 een contract binnen te halen voor de bouw van een grens- en maritiem beveiligingssysteem ('National Security Shield') in Qatar.[18] Twee jaar later volgde een megacontract met Saoedi-Arabië, met een geschatte waarde van meer dan 2 miljard euro, voor het aanleggen van een hightech hek langs de volledige grens van het land. Ook radar-, camera- en communicatieapparatuur maakten deel uit van de deal.[19] Thales Nederland levert in het kader van deze zelfde zogenaamde MIKSA-deal Squire grondradars. Van de 225 in 2009 bestelde Squires zijn in 2011 25 geleverd.[20]

In de zomer van 2012 werd bekend dat de TRS-3D radar van Cassidian op het nieuwe patrouilleschip van de Finse Border Guard geïnstalleerd gaat worden.[21] EADS (Cassidian) leverde ook communicatieapparatuur aan grensbewakingseenheden in Bulgarije en Roemenië. Deze aankopen zijn gefinancierd door de EU, om toetreding tot de Schengenzone mogelijk te maken. EADS voorzag Bulgarije van 4000 TETRA (Terrestrial Trunked Radio) radio's.[22] Roemenië kreeg een TETRA netwerk en een TETRA nationaal platform voor alle veiligheidsdiensten in de grensregio's.[23] Ook warmtebeeldapparatuur en documentscanners maken deel uit van het omstreden contract van 545 miljoen euro. Volgens politici en experts werd er teveel geld aan uitgegeven en was een deel ervan overbodig wegens overlap met bestaande EU-programma's[24].

EADS was aanwezig als standhouder op de European Day for Border Guards in Warschau in mei 2012. Een van de doelen van deze dag was het bediscussiëren van "the latest technologies and their use and influence in border management."[25] Het hoofd van de "R&T projects for Border Surveillance and Protection of Critical Infrastructure" van Cassidian was bovendien een van de sprekers tijdens het conferentiedeel van deze dag.[26]

EADS maakt deel uit van een zestal consortia die in het kader van het Europees Kaderprogramma (zie hierboven) onderzoek uitvoeren (zie tabel). Het meest in het oog springende project is OPARUS, dat zich richt op de ontwikkeling van een open architectuur voor grensbewaking door middel van drones. Het gaat erom een zo kostenefficiënt mogelijk ontwerp te maken voor de bewaking van de land- een zeegrenzen van de Europese Unie, waarbij alles van communicatienetwerken tot surveillancesensoren aan de orde moet komen. EADS werkt hierbij samen met een aantal andere grote wapenbedrijven (Sagem, BAE Systems, Finmeccanica, Thales, EADS, Dassault Aviation, ISDEFE, Israel Aircraft Industries), die gezamenlijk 11,8 miljoen euro aan EU-subsidie

17 Pierre Tran, EADS unveils Cybersecurity Business Unit, DefenseNews, 27 April 2012
18 AFP, Qatar signgs 240M Euro defense deal with EADS, 5 June 2007
19 EADS, EADS wins national security Program for the Kingdom of Saudi Arabia, press release, 30 June 2009
20 SIPRI Arms Transfers Database
21 Asian Defence Journal, Border Guard Patrol Vessel with High-performance Naval Radar, September 2012
22 Cassidian, Cassidian and Ericsson complete extension of TETRA network to secure Bulgarian borders, press release, 17 January 2011
23 Cassidian, Cassidian provides interoperable TETRA network to Border Police in all Romanian Border counties, press release, 8 November 2010
24 Iulian Bulandra, Controversial EADS border security contract signed, Romanian Daily, 14 November 2005
25 http://www.ed4bg.eu/what_is_ed4bg.html
26 http://www.ed4bg.eu/programme.html

ontvingen.[27]

Betrokkenheid EADS bij Europees Kaderprogramma Onderzoek			
Naam	**Omschrijving**	**Hoofdaannemer**	**Betrokken Nederlandse bedrijven/instellingen**
OPARUS	Ontwikkeling open architectuur voor grensbewaking mbv drones	Sagem Defense Securite (Frankrijk)	EADS
PERSEUS	Ontwikkeling maritiem surveillance-systeem voor grensbewaking	Indra Sistemas (Spanje)	Ecorys EADS
G-MOSAIC	Verzamelen van intelligence data voor oa grensbewaking	E-Geos (Italië)	TNO EADS (Astrium)
EUFOREO	Gebruik van Earth Observation voor GMES	Telespazio (Italië)	Argoss Netherlands Geomatics and Earth Observation EADS (Astrium)
MARISS	Combineren informatie uit verschillende bronnen voor oa grensbewaking	Telespazio (Italië)	EADS (Astrium)
bron: cordis.europa.eu			

Waar EADS op het gebied van grensbeveiliging dus al een stevige voet aan de grond heeft in Europa en het Midden-Oosten, probeert het bedrijf ook in andere delen van de wereld grote contracten binnen te halen. In samenwerking met Thales zou EADS een poging doen een contract een groot Braziliaans grensbeveiligingsproject, ter waarde van 10 miljard dollar, te verkrijgen.[28]

In maart 2012 verschenen berichten over een mogelijke samenwerking van EADS met de Amerikaanse wapenproducent General Dynamics voor een contract voor grensbeveiliging tussen de Verenigde Staten en Mexico.[29] Na een geannuleerd contract met Boeing is het Amerikaanse Department for Homeland Security nu op zoek naar een of meer bedrijven die een netwerk kunnen opzetten waarbinnen radars, camera's en andere sensoren langs de grens aan elkaar gekoppeld kunnen worden.

De afgelopen jaren leverde EADS North America al een groot deel van in totaal 345 UH-72A Lakota-helikopters aan de Amerikaanse krijgsmacht. Deze worden onder meer ingezet voor grenspatrouilles aan de Amerikaans-Mexicaanse grens.[30] Daarnaast is het bedrijf, in samenwerking met Amerikaanse universiteiten, recentelijk begonnen met het ontwikkelen van modellen voor gedragsanalyse om bewaking aan dezelfde grens te verbeteren.[31]

Ook op andere vlakken van 'homeland security' is EADS North America succesvol. Het leverde helikopters aan ondermeer de Amerikaanse kustwacht, de FBI en de National Guard voor binnenlands gebruik. In het Midden-Oosten en Latijns-Amerika probeert EADS eveneens een voet aan de grond te krijgen in de 'homeland security'-markt. Daartoe werd een business unit in Abu Dhabi opgezet en een joint venture met het Braziliaanse

27 http://neoconopticon.wordpress.com/2010/11/15/euro-drones-update-more-funding-from-fp7-frontex-and-eda/

28 http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=19657:eads-open-to-thales-tie-up-for-brazil-contract-paper&catid=7:Industry&Itemid=116

29 Andrea Shalal-Esa, GD, EADS eye team for US border security work-sources, Reuters, 13 March 2012

30 http://www.uh-72a.com/about/program-overview.asp

31 http://www.eads.com/eads/int/en/flash/upmagazine-en.html#/issuesoverview/5/article/8/1

bedrijf Odebrecht aangegaan.[32]

TNO

TNO is het grootste onderzoeksinstituut van Nederland. Defensie en veiligheid behoren tot de kerngebieden. Die zijn steeds dichter bij elkaar gekomen, aldus TNO: "Externe en interne veiligheid, oftewel Defensie en maatschappelijke veiligheid raken [...] steeds nauwer met elkaar verweven. TNO zet daarom in op integrale veiligheid en werkt nauw samen met defensie, politie, hulpdiensten en het bedrijfsleven. Wij doen dit met zowel technologische innovaties als met innovaties in gedrag, zodat zij effectiever kunnen handelen."[33]

Zo ontwikkelde TNO "Bluetrace Crowd Control", waarmee politie en beveiliging mensenmassa's en hun bewegingen in kaart kunnen brengen door het schatten van aantallen aanwezigen per vierkante meter op basis van aanwezige bluetooth telefoons.[34] Het had volgens een woordvoerder bijvoorbeeld ingezet kunnen worden bij rellen in het Verenigd Koninkrijk in 2011.[35]

Samen met Europese partners bracht TNO het LOTUS-surveillancesysteem op de markt: "Dit systeem, dat de veiligheid in de stad moet gaan vergroten, bestaat uit een uiterst gevoelige chemische sensor op het dak van een politiewagen, die via gsm stoffenconcentraties, met daaraan gekoppeld een GPS-ruimtestempel plus meteorologische gegevens als windsnelheid, regen of temperatuur, naar een centrale stuurt."[36]

Op security-gebied is TNO verder vooral succesvol in het binnenhalen van Europees onderzoeksgeld, het is actief in twintig Kaderprogramma-projecten (zie tabel). In het kader van het SEABILLA-project wordt een systeem voor bewaking van de Europese zeegrenzen ontwikkeld. Dit omvattende systeem moet bestaande en binnenkort beschikbaar komende systemen integreren, om beter (kleine) onbekende schepen te kunnen detecteren. De bijdrage van TNO bestond met name uit het organiseren van drie bijeenkomsten, waarbij de ontwikkelingen met de voorziene eindgebruikers besproken worden.[37]

ADABTS richt zich op het ontwikkelen van een automatisch detectiesysteem voor afwijkend menselijk gedrag in de publieke ruimte. Daarvoor wordt data van audio- en videosensoren gecombineerd met informatie over de omgeving en vervolgens langs de meetlat van de definitie van 'afwijkend gedrag' gelegd. Daarmee moeten potentiële bedreigingen op de gebieden van criminaliteit, rellen en terrorisme opgespoord worden.[38]

---

32 Philip Finnegan, Market monitor: EADS boosts security growth priority, Homeland Security Today, 1 February 2011

33 http://www.tno.nl/content.cfm?context=thema&content=thema_hoofd&laag1=893&item_id=893

34 http://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=2&item_id=2011-10-24%2011:22:30.0

35 http://www.agentschapnl.nl/onderwerp/wereldwijde-crowd-control

36 http://www.technischweekblad.nl/lotus-sensor-leidt-politie-naar-bommen.184581.lynkx

37 http://www.tno.nl/content.cfm?context=kennis&content=expertise_euproject&laag1=1&laag2=20&item_id=1805&Taal=2

38 http://www.tno.nl/content.cfm?context=kennis&content=expertise_euproject&laag1=3&laag2=37&item_id=899&Taal=2

Betrokkenheid TNO bij Europees Kaderprogramma Onderzoek			
Naam	**Omschrijving**	**Hoofdaannemer**	**Betrokken Nederlandse bedrijven/instellingen**
SEABILLA	Ontwikkeling van een maritiem grensbewakingssysteem	Selex Sistemi Integrati (Italië)	HITT TNO Thales Nl[39]
VIRTUOSO	Ontwikkeling toolkit informatie-verwerking voor oa grensbewaking	CEA (Frankrijk)	TNO Tilburg Institute for Law and Technologie (UvT)
G-MOSAIC	Verzamelen van intelligence data voor oa grensbewaking	E-Geos (Italië)	TNO EADS (Astrium)
GMOSSFP	Integratie van security research voor oa grensmonitoring	DLR (Duitsland)	TNO
DOLPHIN	Gebruik Earth Observation Satellites voor maritieme surveillance (oa voor grensbewaking)	E-Geos (Italië)	TNO
TANGO	Ontwikkeling nieuwe satelliet telecommunicatiediensten voor GMES	EADS (Astrium)	Synoptics TNO Infram International
SOBCAH	Ontwikkeling surveillancesystemen voor grensbeveiliging	Galileo Avionica (Italië)	TNO
ADABTS	Automatische detectie van afwijkend gedrag en bedreigingen in mensenmassa's	FOI (Zweden)	TNO Universiteit van Amsterdam
CPSI	Ontwikkeling methodologie om inzicht te krijgen in determinanten werkelijke en vermeende veiligheid	TNO	Sociaal Cultureel Planbureau VLC
CREATIF	Creëren netwerk van experts en testcentra voor detectie NBC-wapens	Austrian Research Centers (Oostenrijk)	TNO
CRESCENDO	Stimuleren publiek-private netwerkvorming veiligheidsonderzoeksinstituten, eindgebruikers en technici	CEA LIST (Frankrijk)	TNO
DECOTESSC1	Ontwikkelen systeem van maatregelen om aanslagen met NBC-wapens te voorkomen of te beperken	TNO	TNO
DEMASST	Ontwikkelen routekaart voor system-of-system oplossingen voor veiligheid massatransport	FOI (Zweden)	TNO
DITSEF	Verbeteren effectiviteit en veiligheid 'First responders' in crisissituaties bij kritieke infrastructuur	Sagem (Frankrijk)	EADS TNO
EULER	Ontwikkeling draadloze Europese Software Defined Radio voor gezamenlijke security-operaties	Thales (Frankrijk)	EADS TNO
EURACOM	Identificieren gemeenschappelijke benadering voor risicobeoordeling en -management mbt energieinfrastructuur	European Organisation for Security (EU)	JRC TNO
FRESP	Ontwikkeling adembeschermende middelen voor 'First responders'	Koninklijke Militaire Academie (België)	TNO NORIT Nederland

[39] http://www.ttinorte.es/en/?page_id=343

Betrokkenheid TNO bij Europees Kaderprogramma Onderzoek			
Naam	**Omschrijving**	**Hoofdaannemer**	**Betrokken Nederlandse bedrijven/instellingen**
LOTUS	Geintegreerd surveillancesysteem voor chemische achtergrondmonitoring	FOI (Zweden)	TNO
SAFIRE	Inzicht geven in processen van radicalisering en werkzame (elementen van) preventieve interventies	TNO	FORUM Hogeschool Utrecht Universiteit van Amsterdam
TWOBIAS	Ontwikkelen demonstratiemodel alarmsysteem voor locaties beschouwd als doelwit bioterroristische aanslagen	FFI (Noorwegen)	TNO
bron: cordis.europa.eu			

In oktober 2011 sloot TNO een overeenkomst met de Nederlandse tak van G4S, het grootste beveiligingsbedrijf ter wereld, om informatie uit te wisselen over technologische ontwikkelingen en marktkansen, met als doel het ontwikkelen van nieuwe beveiligingsproducten. Daarnaast is men van plan samen te gaan werken bij training en opleiding, cybersecurity en EU-projecten.[40]

Nederlandse aanbieders in verschillende werk-velden

TNO en EADS zijn spelers in de volle breedte van de security-markt en kwamen al uitgebreid aan de orde. Veel andere Nederlandse bedrijven richten zich op specifiekere marktsegmenten. Wat nu volgt is een inventarisatie van ondernemingen die goederen of diensten aanbieden achtereenvolgens de homeland-, border- en cyber security-markt.

Homeland security

Wereldwijd werd in 2009 zo'n 118 miljard euro gespendeerd op de Homeland Security-markt, met de verwachting dat dit in 2018 gegroeid zal zijn tot ongeveer 215 miljard euro.[41] In de Verenigde Staten explodeerde het budget voor Homeland Security van 20 miljard dollar in 2001 tot een niveau van rond de 70 miljard dollar tien jaar later. Ongeveer tweederde van dit bedrag zou rechtstreeks te koppelen zijn aan de gevolgen van 9/11.[42]
De grootverdieners op het vlak van Homeland Security zijn in de eerste plaats Amerikaanse bedrijven. Ook Nederlandse ondernemingen proberen een (bescheiden) graantje mee te pikken. Er worden uiteenlopende producten en diensten aangeboden.

Algemeen

Het Wassenaarse **Axxiflex** treedt op als makelaar in 'homeland security'-toepassingen: “Axxiflex is een onafhankelijk adviesbureau dat zich gespecialiseerd heeft in het

[40] G4S, G4S samen met TNO in beveiligingstechniek, persbericht, 3 oktober 2011
[41] HSRC, Outlook 2009-2018, zoals geciteerd in: Hervé Guillou, Security business – a growth plan, EADS, March 2010
[42] Anita Dancs, Homeland Security spending since 9/11, www.costsofwar.org, 13 June 2011

ontwikkelen van industriële samenwerking tussen de internationale Homeland Security Sector en Nederlandse bedrijven met een technologische hoogwaardig produkt."[43] Tot het netwerk van buitenlandse bedrijven behoren ondermeer Thales, Rafael, General Dynamics, Boeing, Northrop Grumman en Honeywell.[44]

Siqura uit Gouda is leverancier van videobewakingssystemen. Op de klantenlijst staan het Amerikaanse Department of Homeland Security en het Secure Border Initiative, de Israëlische grensbewaking, de politie in Praag en het presidentieel paleis in Jemen.[45]

Diverse Nederlandse bedrijven zijn op de internationale markt actief met camera-, nachtzicht- en warmtebeeldtoepassingen voor security-doeleinden. **FLIR Systems** uit Eindhoven maakt onderdeel uit van een wereldwijd concern op dit vlak. Het Apeldoornse **IMIX Vision Support Systems** en **Videology Imaging Solutions** uit Uden staan op de hele wereld op beurzen om hun goederen aan de mens te brengen.

Crowd en riot control

De Zwarte Cross, een groot meerdaags festival in de Achterhoek, wordt medebeveiligd door Gatekeeper-systemen van **Thales Netherlands**. Een aantal warmtebeeldcamera's houdt vanaf hoogte het hele terrein in de gaten. Ze zijn via een controlekamer gekoppeld aan iPhones van dienstdoende politieagenten, die zo snel op mogelijke incidenten af kunnen gaan. De Gatekeeper is ontwikkeld voor militaire toepassingen, bijvoorbeeld op de nieuwe Nederlandse marinekorvetten, maar Thales hoopt er ook de civiele markt mee te bereiken.[46]

De rellen in het Verenigd Koninkrijk in augustus 2011 werden door **Apex Global** (Apeldoorn) aangegrepen om zijn producten op het gebied van 'Crowd and riot control' te promoten.[47] Het bedrijf heeft ondermeer de 'Soundcommander' ("a dual capability system that projects clear, undistorted voice audio and warning sounds to a range of up to 1000 meters"), beschermende kleding en diverse bepantserde voertuigen in de aanbieding. Apex mikt duidelijk op de internationale markt, het was dit jaar ondermeer met een stand op de beurzen Milipol (Parijs) en de Counter Terror Expo (Londen) aanwezig.

Het Eindhovense **Vigilance** prijst voor zowel militaire als security-toepassingen de DB-16 aan, een Rapid Deployable Aerostat System. Het is een soort luchtballon die uitgerust kan worden met sensoren. Het systeem is inzetbaar voor bijvoorbeeld surveillance en crowd control.[48]

Er zijn meer bedrijven die artikelen voor 'crowd control' in de aanbieding hebben. Naast het hierboven al genoemde Bluetrace Crowd Control van TNO gaat het om onder meer Long Range Acoustic Devices, uit de catalogus van **SurCom International** uit Rhenen. Dit is "equipment that is used for projecting a audible voice or deterrent tone at a specific target at a distance dependent upon the device used. These "acoustic hailing and warning

43 http://www.axxiflex.com/wp/about/

44 http://www.axxiflex.com/wp/onzedoelgroep/lijst-internationale-defensiebedrijven/

45 http://www.siqura.com/optelecom_C01/Modules/ItemBankC/ItemBankC_Module.asp?comid=6&modid=400&OrderBy=String6,Titel&Direction=DESC,ASC&UnfoldedItems=&UnfoldedItemKind=fold&CurrentPage=1&FilterSearchKey=&FilterCat=656

46 Noël van Bemmel, Gatekeeper detectiesysteem houdt alle Zwarte Cross-bezoekers in de gaten, Volkskrant, 15 juli 2011

47 http://www.apexglobal.eu/london-riots-emphasizes-the-need-for-good-crowd-riot-control-solutions/

48 http://www.vigilance.nl/tactical-aerostat-systems.html

devices" provide clear communication to limit unneccessary escalation of force."[49] Dit product is ook geschikt voor 'force protection', bijvoorbeeld om schepen te beschermen tegen piraterij of aanslagen. Om die reden wordt het gebruikt door bijvoorbeeld de marines van Singapore, Japan en Zuid-Korea.[50]
Het in Zeewolde gevestigde **General Armour** heeft ook beschermende, kogelwerende producten voor "defensie, politie en persoonlijke/civiele bescherming" in de aanbieding.[51]
Voor groter materieel kan men terecht bij **Plastisol** uit Wanroij. Dit bedrijf maakt rellenbestrijdingsvoertuigen, onder meer voor de Nederlandse en de Zwitserse politie. In het eerste geval werd samengewerkt met **Terberg Techniek** uit IJsselstein.[52]
Vaak is onduidelijk of de genoemde bedrijven hun producten ook aan het buitenland leveren en zo ja, aan welke landen.

Border security

Het Britse onderzoeksbureau Visiongain becijferde dat de markt voor grensbeveiliging in 2011 een waarde van 17 miljard dollar had.[53] Het ligt in de lijn der verwachting dat dit alleen maar zal groeien, gezien het feit dat grenzen overal ter wereld steeds zwaarder beveiligd worden. Daarbij wordt meer en meer ingezet op gebruik van nieuwe technologieën.[54] Het is de paradox van een globaliserende wereld waarin grenzen op bepaalde gebieden steeds opener worden en tegelijkertijd de selectie aan grenzen voor zowel mensen als goederen steeds strenger wordt.
Daarbij is sprake van een duidelijk militarisering van grensbeveiliging om (illegale) immigranten buiten te houden. Het gebruik van militair personeel, middelen en technologie is een standaardpraktijk geworden. Waar grensbeveiligingstaken eerder uitgevoerd werden door (militaire) politie-eenheden leidt de inzet van zwaarder geschut en fijnmazigere controle tot steeds grotere risico's voor immigranten, bijvoorbeeld omdat men uitwijkt naar gevaarlijkere migratieroutes.[55]
Voor Europa patrouilleren een toenemend aantal marineschepen en helikopters in en boven de Middellandse Zee in operaties die worden gecoördineerd door het EU grensbewakingsagentschap Frontex om een 'oorlog tegen immigratie' te voeren, zoals het door verschillende NGO's en academici wordt genoemd.
Met deze ontwikkelingen is ook een nieuwe markt voor de militaire industrie ontstaan. Bijna alle grote wapenproducerende bedrijven profiteren van de militarisering van grenscontrole. Sinds 2011 zijn hun afzetmogelijkheden verder vergroot. Het Europees Parlement gaf toen groen licht aan Frontex om eigen materieel te kopen of te huren. Voorheen was Frontex afhankelijk van EU-lidstaten voor middelen als patrouilleschepen en helikopters, wat niet altijd even soepel verliep.[56]
Frontex is daarbij steeds meer afhankelijk van nieuwe defensietechnologie, vooral

[49] http://www.surcom.nl/page/products/force_protection/lrad.html
[50] http://www.surcom.nl/upload/File/Order_for_Asia.pdf
[51] http://www.generalarmour.com/index.htm
[52] http://www.plastisol.com/Default.aspx?branch=politie
[53] Homeland Security News Wire, Border security market booming, 1 November 2011
[54] IHS, Border security: shifting priorities, 13 June 2012
[55] Huub Dijstelbloem, Albert Meijer and Michiel Besters, The migration machine, in: Huub Dijstelbloem and Albert Meijer (eds), Migration and the new technological borders of Europe, Basingstoke, Palgrave MacMillan, 2010
[56] Jim Brunsden, Frontex pushes the boundaries, European Voice, 15 May 2008

surveillancesystemen, en toont grote belangstelling voor de ontwikkeling van drones. Dit moet uitmonden in een alles omvattend Europees grens- en surveillancesysteem (EUROSUR), dat "het dagelijks technisch raamwerk dat nodig is om de efficiëntie van de samenwerking en de 24-uurs-communicatie tussen de autoriteiten van de lidstaten en het gebruik van de allernieuwste technologie voor grenssurveillance moet bevorderen."[57]
De ontwikkeling van EUROSUR is fel bekritiseerd, bijvoorbeeld door de Groenen in het Europees Parlement, die waarschuwden voor "het spenderen van publieke gelden voor het ontwikkelen van nieuwe technologieën, zoals robots en drones, om de buitengrenzen van Europa te bewaken".[58]
Meer in het algemeen is de militarisering van grenzen, zoals de buitengrenzen van de EU en de grens tussen de Verenigde Staten en Mexico, onderhevig aan forse internationale kritiek. Mensenrechtenorganisaties als Amnesty International en Human Rights Watch, maar ook het Europees Hof voor de Rechten van de Mens, veroordelen bij herhaling grensbeveiligingspraktijken en het asielbeleid van de EU en de Verenigde Staten.
Desondanks is ook voor Nederlandse bedrijven de border security-markt een groeisector. De verrichtingen van EADS en TNO op dit vlak werden hierboven al toegelicht. Voor het overige speelt het Nederlandse bedrijfsleven vooral op maritiem gebied een rol.

Schepen

Scheepsbouwer **Damen** leverde patrouilleschepen voor ondermeer grensbewakingstaken aan Roemenië, het Verenigd Koninkrijk, Albanië, Jamaica en Bulgarije.[59] Bij de bouw van het schip voor Roemenië, een Offshore Patrol Vessel, was ook het Nijmeegse bedrijf **Alewijnse** betrokken.[60] Deze deal werd gefinancierd door het 'Schengen Facility' programma, een EU financieringsplan ontworpen om nieuwe lidstaten te steunen in de beveiliging van de buitengrenzen van de EU.[61]
Merwede Shipyard uit Rotterdam voorzag in 2006 de Nieuw-Zeelandse marine van een Multi Role Vessel voor grensbeveiligingstaken. De bouw vond plaats onder een licentieovereenkomst met de hoofdaannemer, het toenmalige Australische defensiebedrijf Tenix Defence, dat inmiddels onderdeel is van BAE Systems. De bijbehorende Landing Craft waren afkomstig van **Zwijnenburg**, ook uit Rotterdam.[62]

Border Security Innovation Center

In Den Haag bevindt zich sinds 2009 het zogenaamde **Border Security Innovation Center** (BIC). Dit werd opgericht door een aantal bedrijven, met name uit de regio.[63] Het centrum

---

57 Communication of 13 February 2008 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Examining the creation of a European border surveillance system (EUROSUR)

58 The Greens / European Free Alliance in the European Parliament, Commission proposes 'Fortress 2.0'; skewed approach to immigration misses the point, press release, 12 December 2011

59 http://en.wikipedia.org/wiki/Damen_Stan_4207_patrol_vessel; http://www.damen.nl/en/news/deliveries/2010/09/opv-950-stefan-cel-mare; http://www.ukba.homeoffice.gov.uk/aboutus/organisation/cutters/; Damen News, Edition 13, September 2010, p. 22; http://www.damen.nl/en/news/deliveries/2010/07/spa-4207-obzor; Damen, Second Damen Patrol Vessel deliverd to Albanian Coast Guard, 17 July 2012

60 http://www.alewijnse.nl/alewijnse/en/news/new-project-for-alewijnse-retec-romania

61 http://www.damen.nl/en/markets/offshore-patrol-vessel?type=950

62 Royal New Zealand Navy, MRV takes to the Water, Navy Today, No. 108, March 2006

63 Road Consultants bv (Leidschendam), AMTB (Leidschendam), E-Semble (Delft), IQ Vision Benelux (Wassenaar),

is gericht op "het bieden van een platform aan MKB-bedrijven in de grenscontrole en -beveiliging om zich met de hulp van BIC bij de vaak diverse en versplinterde nationale en internationale vraagzijde te kunnen profileren."[64] Het opzetten van het BIC werd zowel door de gemeente Den Haag als het Ministerie van Economische Zaken met ruim 1 miljoen euro gesubsidieerd.[65]

Frontex

De mogelijkheid voor Frontex om eigen materieel aan te schaffen heeft vooralsnog niet tot concrete aankopen geleid. Wel hebben inmiddels een aantal wapenbedrijven hun producten, met name drones, aan Frontex gedemonstreerd.[66] Nederlandse bedrijven zijn hier (nog) niet bij betrokken. De enige bekende rechtstreekse levering aan Frontex door een Nederlands bedrijf is van het op Schiphol gevestigde **Dartagnan** afkomstig. Het gaat om IT-diensten, die het bedrijf in 2010 ruim 50.000 euro opleverden.[67] Dartagnan is voorts verantwoordelijk voor het Privium biometrische iris-herkenningssysteem dat op Schiphol in gebruik is.[68]

Overig

Ook 's werelds grootste beveiligingsbedrijf, **G4S**, is actief op de border security-markt. De Nederlandse tak biedt op dit gebied enkel ondersteunende diensten aan: "We beschikken over internationale expertise op het gebied van risicoconsultancy, techniek, projectmanagement en logistiek. Deze expertise gebruiken we om samen met de immigratie- en grensbewakingsautoriteiten, effectieve grensbeveiligingsdiensten te leveren. Door diensten aan te bieden op het gebied van grensbewaking assisteert G4S overheden in de hele wereld bij het opbouwen en behouden van het vertrouwen in grensveiligheid en het verlagen van operationele kosten."[69]

De grens tussen de Verenigde Staten en Mexico is een ander bekend voorbeeld van gemilitariseerde grensbewaking. Het Utrechtse **WCC** maakt kans technologie voor het hele Amerikaanse grensbewakingssysteem te gaan leveren, zo liet het bedrijf begin 2012 weten.[70] Sindsdien is hier geen nieuws meer over vernomen. In Estland wordt software van WCC al gebruikt in combinatie met een systeem van wapengigant Raytheon om passagierslijsten door te nemen aan de hand van een serie risico-criteria.[71] Ook in niet nader genoemd Centraal-Amerikaans land en een ander Europees land worden toepassingen van WCC voor grensbeveiliging gebruikt. In het laatste geval werkt WCC

OSC BV (Amsterdam), NCIT bv (Zoetermeer), TSIF Products & Serives bv (Den Haag)

64 R.P.B. Goosen, Openbare samenvatting 'Border Security Innovation Centre', Road Consultants BV, 12 november 2009

65 Gemeente Den Haag, Cofinanciering projectaanvragen Pieken in de Delta / tender najaar 2009, BSD/2009.5278 – RIS 169867, 12 januari 2010

66 Mark Akkerman, Militarisation of border security – profit opportunities for the arms industry, http://stopwapenhandel.org/node/1304, April 2012

67 Frontex, Annual list of law value contracts (between 25,000 and 60,000 EUR) concluded by Frontex in 2010

68 Frontex, BIOPASS – Study on automated biometric border crossing systems for registered passenger at four European airports, Warshaw, August 2007

69 http://www.g4s.nl/nl-nl/oplossingen/sector/Publieke%20sector/Binnenlandse%20veiligheid/

70 Anne-Greet Haars, Nederlands bedrijf in biometrische markt, BNR, 13 januari 2012

71 WCC, WCC Delivers Europe's First Automated Traveler Management System for Estonia's E-Border, 3 November 2011

samen met computerbedrijf Oracle.[72]

Cyber security

Op het vlak van cyber security volgen de ontwikkelingen elkaar in hoog tempo op. Het gaat hierbij allang niet meer alleen om verdediging tegen criminele cyberactiviteiten, maar ook om cyber warfare op het niveau van staten en om interventies van staten op internet en andere digitale communicatiemedia. De opstanden in Noord-Afrika en het Midden-Oosten, die in 2011 hun hoogtepunt kenden, zijn een voorbeeld van zowel het gebruik van sociale media door oppositiebewegingen als pogingen van overheidszijde om dit gebruik, ook technologisch, onmogelijk te maken, te verstoren of aan te grijpen voor repressie en vervolging.[73]

Defensie op weg naar offensieve cybercapaciteit

Cyber security is nog veelal defensief gericht, maar opbouw van een offensieve capaciteit krijgt steeds meer aandacht. De Adviesraad Internationale Vraagstukken (AIV) schreef in een advies eind 2011: "Een digitale aanval die voldoet aan de voorwaarden van een gewapende aanval kan een respons met conventionele gewapende middelen rechtvaardigen." Het moet dan gaan om "een georganiseerde digitale aanval op essentiële functies van de staat [...], ook wanneer deze geen fysieke schade of letsel tot gevolg heeft, maar mogelijk of daadwerkelijk leidt tot ernstige verstoring van het functioneren van de staat of ernstige en langdurige gevolgen voor de stabiliteit van de staat."[74]

De regering nam dit advies over en toonde zich ook van plan de digitale capaciteiten van Defensie te versterken.[75] Dit werd verder uitgewerkt in de eind juni 2012 gepubliceerde Defensie Cyber Strategie. Daarin wordt naast het ontwikkelen van een defensieve capaciteit om een cyberaanval het hoofd te kunnen bieden ook ingezet op het ontwikkelen van een offensieve capaciteit, die "kan fungeren als een *force multiplier* en daarmee de effectiviteit van de krijgsmacht vergroten."[76]

Sinds januari 2012 heeft Defensie een 'Taskforce Cyber', die, langs de lijnen van de genoemde cyber strategie, werkt aan de oprichting van een Defense Cyber Expertise Centrum (DCEC, gepland voor eind 2013) en van een Defensie Cyber Commando (DCC, gepland voor eind 2014).[77]

De Taskforce wordt geleid door kolonel Hans Folmer, die nadrukkelijk inzet op het ontwikkelen van offensieve cybercapaciteit: "De aanval is onderdeel van het totale pakket van mogelijkheden die we hebben in een operatie. We moeten in cyberspace kunnen aanvallen."[78] Daarvoor zal een pool met 'cyberreservisten' aangelegd gaan worden, waarvoor contacten gelegd zijn met universiteiten en het bedrijfsleven.[79]

---

72 http://www.findbiometrics.com/interviews/i/9802/

73 Ben Wagner, Exporting censorship and and surveillance technology, Hivos, January 2012

74 Adviesraad Internationale Vraagstukken en Commissie van Advies inzake Volkenrechtelijke Vraagstukken, Digitale oorlogvoering, No 77/AIV, No 22/CAVV, december 2011

75 Ministeries van Buitenlandse Zaken en van Defensie, Brief aan de Eerste Kamer betreffende het AIV/CAVV-advies over digitale oorlogvoering, DVB/VD-39/12, 6 april 2012

76 Ministerie van Defensie, Defensie Cyber Strategie – brief aan de Tweede Kamer, 33 321 – nr. 1, 27 juni 2012

77 Nationaal Cyber Security Centrum, Cybersecuritybeeld Nederland, Ministerie van Veiligheid en Justitie, juni 2012

78 Radio 1, Defensie wil cyberaanvallen uitvoeren, 27 juni 2012

79 Evert Brouwer, Taskforce Cyber komt van de grond, Defensiekrant, nr. 38, 10 november 2011

In dit alles zal fors geïnvesteerd moeten worden. Dat blijkt ook al uit de Defensiebegroting 2012, waarin, te midden van vele bezuinigingen, gesproken wordt over 50 miljoen euro extra voor verdere ontwikkeling van de cyber capaciteit in de periode 2011-2015.[80]
Hierbij wordt ook verder nadrukkelijk ingezet op samenwerking met bedrijven: "Nieuwe mogelijkheden tot strategische samenwerking moeten worden onderzocht. Defensie draagt bij aan de Nationale Cyber Security Research Agenda en, in het kader van het bedrijfslevenbeleid van het kabinet, aan de specifieke aandacht die in de topsector *High Tech* wordt geschonken aan *cyber security*. Ook in dit verband zal Defensie nauw met andere departementen, de kennisinstellingen en het bedrijfsleven optrekken. Ten aanzien van het ontwikkelen van middelen zal worden gezocht naar mogelijkheden van allianties met het bedrijfsleven."[81]
In de genoemde Cyber Security Research Agenda wordt gemeld dat defensiegerelateerde onderzoeksopdrachten door het ministerie vrijwel allemaal aan TNO gegund worden: "This research is often of a highly confidential nature, which makes it difficult to include other partners into the research projects."[82]

Clean IT

De Nederlandse Nationaal Coördinator Terrorismebestrijding en Veiligheid is de voortrekker van het door de EU gefinancierde Clean IT-project, dat samen met België, Duitsland, Spanje en het Verenigd Koninkrijk werd opgezet.[83] Dit project richt zich op het bestrijden van 'terroristisch' internetgebruik. Organisaties voor internetvrijheid maken zich echter grote zorgen over de breedte van de voorgestelde maatregelen. "Een uitgelekt document onthult gedetailleerde en verstrekkende voorstellen voor de aanpak van terrorisme op internet. Zouden die voorstellen er ook komen, dan blijft van de internetvrijheid weinig over", aldus Bits of Freedom.[84] D66-Europarlementariërs In 't Veld en Schaake hebben inmiddels vragen gesteld aan de Europese Commissie over de verregaande voorstellen.[85]
Tot de betreffende voorstellen behoren de mogelijkheid om snel omstreden content van internet te laten verwijderen, politiesurveillance op sociale media, het illegaal verklaren van hyperlinks naar websites met "terroristische content" en een wettelijke plicht voor internetbedrijven alle klantinformatie over te dragen die een opsporingsinstantie nodig heeft. Ook zouden internetbedrijven gebruikers in staat moeten stellen terroristische of radicaliserende inhoud als zodanig aan te merken en aan te geven, eventueel met een zogenaamde 'police button' waarmee direct de politie op de hoogte gesteld kan worden. Bovendien moeten internetgebruikers gestimuleerd worden dan ook daadwerkelijk "unusual behavior and radicalization" van andere gebruikers te melden.[86]

---

80 Ministerie van Defensie, Vaststelling begrotingsstaten voor het jaar 2012 – Memorie van Toelichting, X – nr. 2, 16 september 2011
81 Ministerie van Defensie, Defensie Cyber Strategie – brief aan de Tweede Kamer, 33 321 – nr. 1, 27 juni 2012
82 H. Bos, S. Etalle and E. Poll (ed.), National Cyber Security Research Agenda: Trust and Security for our Digital Life, version 1.2, 2011
83 http://www.cleanitproject.eu/partners-and-participants/
84 Janneke Slöetjes, CleanIT: absude voorstellen tegen terrorisme uitgelekt, 21 september 2012; https://www.bof.nl/2012/09/21/cleanit-absurde-voorstellen-tegen-terrorisme-uitgelekt/
85 René Schoemaker, Anti-terrorismeplan beknot internetvrijheid burgers, Webwereld.nl, 3 oktober 2012
86 Clean IT Project, Detailed recommendations document for best practices and permanent dialogue, 28 August 2012

Fox-IT

Op de internationale markt is **Fox-IT** het meest in het oog springende Nederlandse bedrijf. Het werd opgericht in 1999, door twee personen die eerder werkzaam waren bij het Nederlands Forensisch Instituut en de toenmalige Binnenlandse Veiligheidsdienst (nu AIVD).[87]

Fox-IT werkte in eerste instantie met name voor andere bedrijven en voor de Nederlandse overheid. Later ging het bedrijf ook de internationale markt op. Dat leverde controversiële contacten met dubieuze regimes op als die van de Verenigde Arabische Emiraten, Iran en Egypte op. Technologie om internet te tappen was een van de succesnummers en 'de eerste keuze van veel politie- en inlichtingendiensten over de hele wereld', aldus het bedrijf. Daartoe behoort in ieder geval een niet nader genoemde geheime dienst in het Midden-Oosten.[88]

In 2003 nam Fox-IT deel aan de 'International Police, Safety & Security Equipment Exhibition' in Iran. Later deed directeur Ronald Prins dit af als 'naïef': "Nu zouden wij nooit meer die keuze maken."[89] Voor het overige is Prins tamelijk ambigue. Hij zegt dat "het [wel] is [...] gebeurd dat landen waar een hoop commotie is opeens aan de lijn hangen en onze spullen willen kopen. En dan ben ik heel duidelijk: dat doen we dus niet", maar "[t]och leveren we aan landen waarvan het beleid ons niet helemaal aanspreekt."[90] Desondanks stelt Prins ook dat "we [...] nog nooit zaken [hebben] gedaan met foute regimes."[91]

Eind 2009 verkocht Fox-IT zijn internettapdivisie aan het Amerikaanse bedrijf NetScout.[92] Daarmee is echter geen eind gekomen aan de offensieve capaciteiten die Fox-IT in de aanbieding heeft. In augustus 2012 bepleitte Prins het terughacken en stilleggen van buitenlandse servers in het geval van virusaanvallen: "Fox-IT staat te popelen, maar we kunnen het niet doen zonder toestemming van de politiek. Dit zou het moment kunnen zijn om die hele soevereiniteitsdiscussie op dit vlak eens te voeren."[93]

Het Nationaal Cyber Security Centrum liet in een reactie weten dat het juridisch niet mogelijk is buitenlandse servers plat te leggen. Wel werkt minister Opstelten van Veiligheid en Justitie aan voorstellen voor meer bevoegdheden op dit vlak.[94]

Spy Leaks

De documenten van de zogenaamde 'Spy Leaks' over leveringen van apparatuur aan dictatoriale regimes, die eind 2011 door Wikileaks gepubliceerd werden, bevatten ook een aantal Nederlandse bedrijven. Naast het al genoemde Fox-IT gaat het om **Group 2000** en **Pine Digital Security**. Beide bedrijven ontkenden leveringen aan controversiële staten. Richard Coppens, managing director van Group 2000: "[...] we clearly reject any form of relation with such kind of 'customers'. We strive to openness. As a company we comply

87 René Schoemaker, Fox-IT: Is er dan wat aan de hand in Egypte?, Webwereld.nl, 3 december 2011
88 Harry Lensink en Maurits Martijn, Schieten met hagel, Vrij Nederland, 8 december 2011
89 NOS, WikiLeaks onthult industrie voor spionage, 1 december 2011
90 Harry Lensink en Maurits Martijn, De geheimen van een supertapper, Vrij Nederland, 12 augustus 2011
91 Harry Lensink en Maurits Martijn, Schieten met hagel, Vrij Nederland, 8 december 2011
92 Fox-IT, Fox-IT divests business unit Replay to US-based NetScout Systems Inc., press release, 26 September 2011
93 NOS, 'Nederland moet 'terughacken'', 10 augustus 2012
94 NOS, 'Waarborgen bij terughacken', 10 augustus 2012

with Legislation and do respect human rights."[95]

Zowel Group 2000 als Pine hebben wel afluister- en interceptieapparatuur in de aanbieding. Afzetlanden worden niet benoemd, maar Pine stelt "market leader in the Netherlands" te zijn een "a strong presence throughout Europa and the USA" te hebben.[96] Group 2000 is in ruim twintig landen actief, waaronder voor het Amerikaanse Ministerie van Justitie.[97]

Het Rotterdamse **Digivox** is een andere leverancier van dergelijke apparatuur.[98] Politie, justitie en veiligheidsdiensten in vijftien niet met naam genoemde landen behoren tot het klantenbestand.[99]

Digivox, Group 2000 en Fox-It namen begin 2011, terwijl in het Midden-Oosten volksopstanden met harde hand werden neergeslagen, deel aan de ISS World MEA-conferentie in Dubai, over aftappen en filteren van telecommunicatie. Arjan El-Fassed, toenmalig Kamerlid voor GroenLinks, stelde vragen aan minister Verhagen van Economische Zaken, die beloofde met de bedrijven om tafel te gaan zitten. "Bedrijven hebben een bijzondere verantwoordelijkheid om er zelf voor te zorgen dat hun technologie niet in verkeerde handen valt", aldus Verhagen.[100] Dat mag zo zijn, het lijkt ook op het afschuiven van het probleem van gebrekkige overheidscontrole op dit vlak.

Digivox liet het ministerie later onder meer weten dat het bedrijf bij leveringen van interceptieapparatuur vraagt "om een end-user certificaat waarbij de eindgebruiker (overheid) schriftelijk verklaart dat de LI systemen alleen ingezet worden voor het bestrijden van criminaliteit en terrorisme. Deze clausule is ook opgenomen in het supportcontract voor het LI systeem, dat jaarlijks verlengd dient te worden."[101] Probleem hierbij is de invulling van het begrip 'terrorisme', dat veel overheden graag zodanig oprekken dat ook legitieme oppositiebewegingen en politieke activisten hieronder geschaard worden.[102]

Group 2000 was na de deelname in Dubai in 2011 ook een van de sponsoren van de ISS World Europe 2012. Tijdens deze conferentie in Praag kwamen talloze aspecten van overheidsinterventies in de digitale wereld aan de orde, van opsporing via sociale media tot offensieve IT-inlichtingenoperaties.[103]

---

95 Group 2000, Wikileaks Spy Files benefits Group 2000, press release, 8 December 2011

96 http://www.lawfulinterception.com/

97 NIDV Magazine, Gevoelige markt – Group 2000: Nederlandse veiligheidsbedrijven welkom, 2012 – nr. 1, september 2012

98 Bas Bareman, Grootste leverancier niet in Wikileaks Spy Files, Webwereld.nl, 2 december 2011

99 http://www.digivox.nl/home/References.htm

100 Ministerie van Economische Zaken, Landbouw en Innovatie, Verhagen spreekt bedrijven aan op misbruik internetfilters, nieuwsbericht, 11 april 2011

101 Ministerie van Economische Zaken, Landbouw en Innovatie, Beantwoording vragen over de export van internetfilters en aftaptechnologie, BEB/HPG/11153702, 16 januari 2012

102 Martin Broek, Versleutelen en tappen, http://broekstukken.blogspot.nl/2012_01_01_archive.html, 26 januari 2012; Dit fenomeen beperkt zich overigens niet tot voor de hand liggende voorbeelden als bekende dictaturen, ook in de VS en de EU wordt bij herhaling geprobeerd de definities van 'terrorisme' te verbreden teneinde zwaardere middelen in te kunnen zetten tegen bijvoorbeeld activisten. Zie bijvoorbeeld: Wil van der Schans, Ook activist kan terrorist zijn, Ravage, 19 december 2003; Trouw, Wet tegen terreur is gevaarlijk, 2 september 2003; Jelle van Buuren, Tussen terrorisme en politiek activisme, Fabel van de Illegaal, zomer 2002; RT.com, FBI targeting political activists as terrorists, 26 May 2011

103 Telestrategies, ISS World Europe 2012 Brochure, http://www.issworldtraining.com/iss_europe/brochure.pdf

Exporten

Een deel van de apparatuur voor cyber security valt onder de dual use-regelingen. De overheid hobbelt hierbij echter achter de elkaar snel opvolgende ontwikkelingen in deze markt aan. Staatssecretaris Bleker liet begin 2012 in antwoord op Kamervragen van D66 weten dat "de meeste goederen die naast lawful interception ook voor [...] mensenrechtenschendingen gebruikt kunnen worden, [...] zonder vergunning uitgevoerd [kunnen] worden." Wel gaf hij aan binnen de EU te pleiten voor verruiming van de dual use-verordening, zodat "het mogelijk [wordt] een ad-hoc vergunningplicht op te leggen voor individuele gevallen indien er aanwijzingen zijn dat de goederen geheel of gedeeltelijk zullen worden gebruikt voor mensenrechtenschendingen."[104]
Onderzoeker Martin Broek becijferde dat er in de eerste helft van 2011, de meest recente beschikbare gegevens, voor 1,67 miljard euro vergunningsplichtige apparatuur voor informatiebeveiliging van Nederland naar landen buiten de EU werd uitgevoerd. Navraag bij het Ministerie van Economische Zaken leerde hem dat een van de grootste vergunningen exporten binnen een bedrijf behelst, maar dan nog gaat het om een miljard aan vergunningen. De daadwerkelijke afnemers en hun bedoelingen met de inzet van de geleverde apparatuur zijn veelal onbekend.[105]

The Hague Security Delta

In maart 2012 werd The Hague Security Delta opgericht, een netwerk van bedrijven, overheden en (wetenschappelijke) instellingen die in verschillende security-sectoren actief zijn. Tot de deelnemers behoren Fox-IT, TNO, Thales, G4S, de Gemeente Den Haag, Europol, de Ministeries van Defensie en van Veiligheid en Justitie, de Haagse Hogeschool, de Universiteit Leiden en het Hague Centre for Security Studies (HCSS) van Rob de Wijk.[106] Rob de Wijk is ook benoemd als directeur van dit samenwerkingsverband.
De oprichtende bedrijven staken gezamenlijk 650.000 euro in het netwerk, de gemeente Den Haag en het Ministerie van Economische Zaken, Landbouw en Innovatie deden daar nog 1,5 miljoen euro bovenop. Doel van het netwerk is het samenbrengen van middelen om producten te ontwikkelen en in de (internationale) markt te zetten. "Door gezamenlijk op te trekken, kunnen we de regio Den Haag wereldwijd positioneren als hét cluster waar je terecht kunt met al je veiligheidsvraagstukken", aldus René Willems, senior beleidsadviseur bij TNO.[107]
Inmiddels is vanuit The Hague Security Delta een Cyber Security Academy opgezet, zijn handelsmissies naar Turkije, Canada en de Verenigde Staten gehouden en hebben enkele partners een European Network for Cyber Security opgericht.[108]

[104] Ministerie van Economische Zaken, Landbouw en Innovatie, Beantwoording vragen over het gebruik van Europese technologie bij mensenrechtenschendingen, BEB/HPG 11153702/11163290, 16 januari 2012
[105] Martin Broek, Versleutelen en tappen, http://broekstukken.blogspot.nl/2012_01_01_archive.html, 26 januari 2012
[106] http://www.thehaguesecuritydelta.com/partners-landkaart.html
[107] NIDV-magazine, 'De hele wereld voor veiligheid naar Den Haag', 2012 – nr. 1, september 2012
[108] http://www.thehaguesecuritydelta.com/milestone.html

Consequenties van militarisering van veiligheid

Het afgelopen decennium is het streven naar veiligheid door (technologische) controle steeds verder doorgeschoten. Daarbij zijn binnenlandse veiligheid (homeland security), grensbewaking (border security) en digitale veiligheid (cyber security) steeds meer gemilitariseerd waarbij 'oplossingen' steeds meer vanuit de wapenindustrie worden aangedragen. Voor bestaande wapenbedrijven en nieuwe gespecialiseerde ondernemingen creëerde dit een nieuwe lucratieve markt. Er komen nieuwe geldstromen beschikbaar voor de ontwikkeling van militaire producten, niet alleen vanuit Defensie maar ook vanuit Binnenlandse Zaken en de Europese Unie. Ook Nederlandse bedrijven weten hiervan te profiteren.

Deze snel opkomende sector vraag om een nieuwe stap in het wapenexportbeleid. De voortdurend voortschrijdende technologie, vooral op het gebied van cyber security, maakt dat de overheid op het gebied van exportcontrole van nieuw ontwikkelde producten en technieken sneller zou moeten reageren. Het is zaak controlelijsten constant actueel te houden door snel op nieuwe ontwikkelingen te reageren. Voorkomen moet worden dat Nederlandse technologie wordt gebruikt tegen legitieme oppositie of bij mensenrechtenschendingen. Daarnaast moet het risico van proliferatie in het oog gehouden worden. In het geval van toepassingen voor cyber warfare is verdere verspreiding ervan bijvoorbeeld nauwelijks controleer- en beheersbaar.

Overigens willen we benadrukken dat de groeiende obsessie om veiligheid met technologie en andere ((para)militaire) middelen af te dwingen de vraag opwerpt of het middel niet erger is dan de kwaal. Waar een verstandige toepassing van nieuwe security technologie zijn nut kan hebben, lijkt het er nu vaak op dat het vooral draait om de inzet van steeds meer middelen zonder acht te slaan op de mogelijk negatieve gevolgen ervan.
Er zou veel kritischer gekeken moeten worden naar wiens belang er gediend wordt, dat van de samenleving of dat van de beveiligings- en wapenindustrie. Een kritische houding is geboden geboden ten aanzien van wat door overheden als veiligheid en terrorismebestrijding wordt gepresenteerd. In de praktijk kan het uitdraaien op een zeer onwenselijke afkalving van burgerlijke vrijheden en privacy.

Militarisation of security

Inventory of Dutch companies

English summary

Since 9/11 the security market has grown immensely. On Homeland Security alone the world spend 118 billion euro in 2009, this is expected to rise to 215 billion in 2018. Homeland security, border security and cyber security are becoming more and more militarized, and 'solutions' are sought in technologies developed by or in cooperation with the defence industry. Now that national defence budgets are shrinking due to the economic crisis, the security market becomes even more important for the arms industry. Security is often funded from non-traditional sources such as the home office and the European Union.

In some cases, supply is directing the market more than demand is. Privacy and civil liberties are under pressure. Homeland security is protection against internal terrorist attacks and (violent) internal upheaval. Some governments define terrorism very broadly, including legitimate opposition. Border security is the protection against unwanted border crossings, most often by migrants. Cyber security is protection of computer and data systems but increasingly includes developing an offensive cyber capacity.

The global security market is dominated by American, British and Israeli companies. For Dutch companies it is also of growing importance. The Dutch lobby organisation of the arms industry has renamed itself into NIDV, Dutch Industry for Defence and Security.

An increasing number of fairs and exhibitions are focussing on security, most important are IFSEC (UK), Milipol (France and Qatar), Counter Terror Expo (UK), Security Essen (Germany), Homsec (Spain), Intersec (Dubai), ISS World (several), Security Israël (Israël) and Sfitex (Russia).

The European Union is not subsidizing defence production but through security budgets in the Framework Programs on innovation and technical development EU money is going to the arms industry. Many projects go to consortia where the arms industry works closely together with research institutions an universities.

In the Netherlands EADS and TNO are profiting from EU budgets. EADS' military division Cassidian expects to earn 50% of its income in the security sector by 20120. TNO is participating in 20 Framework Programme funded projects. Many smaller Dutch companies are developing specific products for niches in the security market. The report gives an overview of these companies.

The most recent figures show that in the first half of 2011, 1,67 milliard euro of cyber

equipment has been exported from the Netherlands under dual use permits. The fast developments in this sector needs a permanent updating of arms exports and dual use lists.

Recente publicaties van de Campagne tegen Wapenhandel

- Beleggingen pensioenfondsen in kernwapens, oktober 2012

- Duurzame energie voor duurzame vrede, september 2012, factsheet (i.s.m. Peakoil Nederland)

- Nederlandse export van dual-use goederen in kaart gebracht, juli 2012

- Alternatief jaarverslag wapengigant EADS, mei 2012

- Brochure Europa en de wapenhandel: van exportcontrole tot industriebeleid, voorjaar 2012

- Lessons from MENA – Appraising EU transfer of military and security equipment to the Middle East and North Africa, november 2011 (i.s.m. Universiteit Gent en Saferworld)

- Introductie Nederlandse wapenhandel, oktober 2011, factsheet

- European technology arming the world - European Aeronautic Defence and Space Company EADS, mei 2011

- Vrij verkeer - Nederlandse wapendoorvoer onder de Algemene Douanewet, januari 2011

- De opkomst van de nieuwe huurling. Over private diensten in de militaire- en veiligheidssector, januari 2011

- **Analyse Nederlandse wapenexportbeleid 2009**, november 2010

- **Ontwikkelingscriterium voor wapenexport. Regels, belangen en Millenniumdoelen**, oktober 2010, factsheet

- **Wapenwedloop in Zuid-Amerika**, maart 2010

- **Nederlandse patrouilleschepen voor Nigeriaans leger**, februari 2010, factsheet

Zonder donateurs geen Campagne tegen Wapenhandel

Steun ons met een gift op rekening 39 04 07 380
t.n.v. Campagne tegen Wapenhandel, Amsterdam