

Een Europese agenda voor veiligheidstechnologie: van innovatiebeleid tot exportcontroles

Jocelyn Mawdsley

Rapport
Februari 2013



Inhoudsopgave

SAMENVATTING	4
LIJST MET AFKORTINGEN	5
1	INLEIDING 6
1.1	Onderzoeksvragen 6
1.2	Methodologie 7
1.3	Structuur van het rapport 8
2	VEILIGHEID EN DEFENSIE: CONCEPTEN EN HOE ZE GEBRUIKT WORDEN 9
2.1	Inleiding 9
2.2	Wijzigende visie op veiligheid in academische en beleidskringen: verbreden en verdiepen 9
2.2.1	Het concept nationale veiligheid / defensie tijdens de Koude Oorlog 9
2.2.2	Nieuwe veiligheidsbekkernissen – de verbreding van de agenda 10
2.2.3	Menselijke veiligheid en de verantwoordelijkheid om te beschermen – de verdieping van de agenda 11
2.2.4	Gevolgen voor het beleid 12
2.3	Het concept ‘homeland security’ 13
2.3.1	Oorsprong 13
2.3.2	‘Homeland security’ in de EU en de VS: convergentie of divergentie? 14
2.4	Veiligheid en defensie: gebruik binnen de EU-context 16
2.4.1	De EU en defensie 16
2.4.2	De vervagen van het onderscheid tussen veiligheid en defensie 16
2.5	Samenvatting 17
3	DE KENMERKEN VAN DE VEILIGHEIDS- EN DEFENSIEMARKT IN DE EU 19
3.1	Inleiding 19
3.2	De veiligheids- en defensiesector gedefinieerd: problemen en beperkingen 19
3.2.1	Wat is de Europese veiligheidssector? 20
3.3	Veiligheids- en defensietechnologieën 24
3.3.1	Uitgaven en trends inzake defensie-O&O: implicaties voor veiligheidstechnologie? 24
3.3.2	Kan men veiligheids- en defensietechnologieën onderscheiden? 26
3.3.3	Innovatieve technologieën en de veiligheids- en defensiesector 28

3.4	Aanbodzijde	28
3.4.1	Hoe defensiebedrijven de veiligheidssector benaderen	28
3.4.2	Niet-defensiebedrijven en hoe zij de veiligheidssector benaderen	32
3.4.3	Opkomende trends?	33
3.5	Vraagzijde	34
3.5.1	Voornaamste gebruikersgroepen van en vereisten voor defensie- en veiligheidstechnologieën: vervaagd of verschillend?	35
3.5.2	Civiele en militaire klanten: verschillen in aankoopprocedures en behoefteomschrijving onoverbrugbaar groot?	36
3.6	Samenvatting	37
4	BEOORDELING VAN EU-MAATREGELEN MET EEN IMPACT OP DE VEILIGHEIDS- EN DE DEFENSIE-INDUSTRIE	39
4.1	Inleiding	39
4.2	Wetgevende basis van EU-optreden inzake veiligheid en defensie	40
4.2.1	Verdragsbasis en beperkingen	40
4.2.2	Uitspraken door het Hof van Justitie	41
4.3	Beleid van de Europese Commissie	42
4.3.1	Ontstaan en evolutie van het programma voor veiligheidsonderzoek	43
4.3.2	Beleidsacties door het DG Ondernemingen en Industrie onder de noemer concurrentievermogen van de sector	53
4.3.3	Actie om de aankoop van defensie- en veiligheidsproducten te reguleren en barrières op intracommunautaire handel weg te werken	55
4.3.4	Ontwikkeling van een beleid naar analogie met de Amerikaanse 'homeland security' en daaraan verbonden technologische behoeften door DG Binnenlandse Zaken	57
4.4	Europees Defensieagentschap	58
4.5	EU-lidstaten	60
4.5.1	Voornaamste bilaterale en multilaterale overeenkomsten	61
4.5.2	Is de NAVO relevant?	63
4.6	Samenvatting	64
5	VEILIGHEIDSTECHNOLOGIEËN EN HUN IMPACT OP EXPORTCONTROLES VAN STRATEGISCHE GOEDEREN	67
5.1	Inleiding	67
5.2	De controle van strategische goederen: de contouren van het debat	70
5.3	Bestaande en potentiële controleregimes	73
5.3.1	EU-verordening inzake producten voor tweeërlei gebruik	73

	5.3.2 Gemeenschappelijk standpunt inzake wapenuitvoer	77
	5.3.3 De EU-folterverordening	79
	5.3.4 Sancties en embargo's	81
	5.3.5 Vrijwillige codes op initiatief van de sector	82
5.4	Is controle nodig? De externe aspecten van de EU-interne veiligheidsstrategie	83
5.5	Samenvatting	86
6	CONCLUSIES	87
7	LITERATUURLIJST	91

Samenvatting

Dit rapport houdt de EU-agenda inzake veiligheidstechnologie tegen het licht. Het onderzoekt of veiligheid en defensie - ofwel interne en externe veiligheid - sinds het einde van de Koude Oorlog grotendeels in elkaar zijn opgegaan, zodat tussen de twee sectoren geen betekenisvol verschil meer zou bestaan qua behoeften van de eindgebruikers, qua technologieën, en qua leveranciers. De overtuiging dat dit zo is, heeft het afgelopen decennium aanleiding gegeven tot verschillende door de Europese Commissie aangestuurde beleidsacties rond de veiligheids- en defensietechnologie en -industrie. Het rapport gaat na of het vervagen van de grenzen tussen defensie en veiligheid, zoals dit in de academische en beleidsliteratuur wordt vooropgesteld, ook zijn weerslag vindt in het daadwerkelijke beleid. Het komt tot de vaststelling dat de verschillen zeker wat vereisten van eindgebruikers betreft nog aanzienlijk zijn, hoewel er overlappingsen zijn ontstaan wanneer het gaat over technologieën en leveranciers.

De inspanningen van de Commissie om een EU-beleid rond veiligheidsindustrie en -technologie in de steigers te zetten zijn grotendeels onopgemerkt gebleven. Het rapport doet een poging om de reikwijdte en strekking van deze markt af te bakenen en de soorten gebruikte technologieën te definiëren. Verder evalueert het de beleidsacties waarmee de EU tracht het concurrentievermogen van de Europese veiligheids- en defensiesector te vergroten. Daarmee schetst het rapport een duidelijk beeld van een complexe sector in ontwikkeling. Het rapport benadrukt ook dat het toenemende belang van binnenlandse veiligheid in de EU moeilijke ethische vragen op werpt over het correcte evenwicht tussen burgerrechten en veiligheid. De technologische ontwikkelingen die voortvloeien uit veiligheidsonderzoek gefinancierd vanuit het zevende Kaderprogramma van de EU, zetten deze kwesties extra in de verf. Naar aanleiding van de Arabische Lente stelde zich nog een prangende vraag, namelijk of de EU voldoende controle heeft op de uitvoer van deze technologieën naar regimes die, zoals blijkt uit talrijke mediabijdragen, bewakingstechnologieën en andere politie-uitrusting inzetten om politieke dissidenten te onderdrukken. Het rapport schetst bestaande controlemechanismen en hun zwaktes en onderzoekt de mogelijkheden om controles in de toekomst te verscherpen.

Over de auteur

Dr Jocelyn Mawdsley geeft les over Europese en EU politiek aan de Universiteit van Newcastle upon Tyne in Groot-Brittannië. Ze heeft uitgebreid gepubliceerd over bewapening, recent nog over de Frans-Britse defensierelaties en over de groei van de industriële veiligheidssector.

Lijst met afkortingen

ASD: Aerospace and Defence Industries of Europe
CBRNE: chemische, biologische, radiologische, nucleaire en explosieven met hoge kracht
CCTV: gesloten televisiecircuit
CEA: Commissariat à l'Énergie Atomique
COARM: Raadsgroep export van conventionele wapens
DITB: technologische en industriële basis voor defensie
GVDB: gemeenschappelijk veiligheids- en defensiebeleid
HvJ: Hof van Justitie
EAVO: Europese Adviesraad voor veiligheidsonderzoek
EDA: Europees Defensieagentschap
EDEM: Europese markt voor defensie-uitrusting
EDITB: Europese technologische en industriële basis voor defensie
EVDB: Europees veiligheids- en defensiebeleid
GNI: Global Network Initiative
GoP: Groep van prominenten op het gebied van veiligheidsonderzoek
ICISS: Internationale Commissie inzake Interventie en Soevereiniteit van de Staat
ICT: informatie- en communicatietechnologie
KMO: kleine en middelgrote ondernemingen
MENA: Midden-Oosten en Noord-Afrika
MEP: lid van het Europees Parlement
MoD: ministerie van Defensie
OCCAR: Organisation Conjointe de Coopération en Matière d'Armement
OESO: Organisatie voor Economische Samenwerking en Ontwikkeling
UAV: onbemand luchtvaartuig
UGV: onbemand grondvaartuig
UNDP: Ontwikkelingsprogramma van de Verenigde Naties
WEAG: West-Europese Bewapeningsgroep
WEU: West-Europese Unie

1 Inleiding¹

1.1 Onderzoeksvragen

Sinds het ontstaan in Europa van het moderne statenstelsel heeft men veiligheidsbedreigingen voornamelijk als een extern militair gevaar omschreven en zijn strijdkrachten ook als dusdanig ingericht. Deze gerichtheid naar buiten toe heeft er, in combinatie met het Weberiaanse principe dat de staat het monopolie moet hebben op het legitieme gebruik van geweld, voor gezorgd dat hoewel het staatsbestel in andere beleidsdomeinen steeds meer is uitgehold, defensie daarvan grotendeels is gevrijwaard gebleven. Als antwoord op een nieuwe definitie van veiligheidsbedreigingen (verbreding en verdieping van de veiligheidsagenda) sinds het einde van de Koude Oorlog, hebben strijdkrachten in Europa een aanzienlijk andere rol toebedeeld gekregen. Ook is de private sector vandaag veel nauwer betrokken bij veiligheidsoopdrachten, waardoor de grens tussen civiele en militaire taken is vervaagd.

De aanslagen van 11 september 2001 hebben interne veiligheid onder de aandacht gebracht, vooral in de VS maar ook elders. Sindsdien heeft de opkomst van nieuwe technologieën, aangedreven door de ambitie van overheden om hun burgers en kritieke infrastructuur te beschermen tegen elke terroristische aanval, wereldwijd het ontstaan van een markt voor 'homeland security' in de hand gewerkt. In de EU heeft de complexe verdragsbasis om inzake veiligheid stappen te ondernemen ertoe geleid dat de omliggende beleidsdynamiek niet geheel rechtlijnig verloopt. Edler en James (2012) stellen dat de Europese Commissie als beleidsondernemer een agenda rond technologische ontwikkeling voor interne veiligheid heeft opgezet, waar echter de lidstaten noch de industrie volledig betrokken partij in waren. Doordat de opvattingen over veiligheid zoals hierboven beschreven zo zijn vervaagd, zijn de ambigue termen veiligheidsindustrie en veiligheidstechnologie gelijkgesteld geraakt aan defensie-industrie en defensietechnologie, een domein waar het wettelijke mandaat van de Commissie allesbehalve duidelijk is. Maar geeft dit onduidelijker wordende onderscheid ook de realiteit accuraat weer? Of blijft het mogelijk de civiele en militaire technologieën en hun industriële leveranciers en klanten te differentiëren?

De EU-agenda inzake veiligheidstechnologie vertrekt van de vraag of ook in de 21^e eeuw de opdeling in interne en externe veiligheid, militaire en civiele inmenging en in veiligheid en defensie blijft bestaan, maar raakt daarnaast ook een aantal deelvragen aan. Het is volgens deze deelvragen dat het rapport zich structureert:

- Hoe is het veiligheidsconcept veranderd in de periode na de Koude Oorlog? En hoe heeft de EU dit begrepen?
- Wat is de veiligheidsmarkt? Welke parameters zijn bepalend voor haar technologieën en geven vraag en aanbod vorm? Kunnen deze worden gedifferentieerd van de meer gevestigde defensietechnologieën, bedrijven en klanten / gebruikers?
- Welke beleidsinitiatieven neemt Europa op dit vlak en wat stuurt ze aan? Hoe beïnvloeden zij de markt? Wie zijn de beleidsondernemers – de Europese instellingen of de lidstaten? Bestaat er samenhang tussen de verschillende beleidsdoelstellingen? Is het bevorderlijk of gevaarlijk om

¹ De auteur bedankt Ulpia Botezatu, doctoraatsstudente aan Newcastle University, die met haar enthousiasme en uitstekend onderzoekswerk aan dit project heeft meegewerkt.

defensie en veiligheid in elkaar te laten opgaan? Welke impact hebben kwesties gerelateerd aan veiligheidsindustrie en –technologie op andere EU-beleidsdomeinen?

- Ten slotte is er analyse vereist naar de plaats die veiligheidstechnologieën in het strategische exportcontrolesysteem innemen. Zijn de bestaande controleregimes voorzien op veiligheidstechnologieën? Moeten veiligheidstechnologieën worden gecontroleerd? Wat zijn de ethische vraagstukken?

1.2 Methodologie

Om een antwoord te vinden op de onderzoeksvragen hebben we verschillende kwalitatieve onderzoeksmethodes gehanteerd. De reden waarom we voor kwalitatieve eerder dan voor kwantitatieve methodes hebben geopteerd, was louter pragmatisch. Zoals zal blijken uit de inleiding bij onderdeel 3 van het rapport, is het erg moeilijk om over betrouwbare gegevens te kunnen beschikken. Zo zijn de uitgaven voor defensieonderzoek nationaal te vergelijken, terwijl dit voor het veiligheidsonderzoek niet het geval is. Dit beperkt op zijn beurt het soort kwantitatieve analyse die men kan uitvoeren.

Zoals Edler en James (2012) het stellen, is er verhoudingsgewijs naar dit onderwerp ook weinig academisch onderzoek gevoerd. De analyse dient zich dus grotendeels op primaire documenten eerder dan op secundaire studies te baseren. Het rapport maakt tevens intensief gebruik van semiofficiële publicaties en studies van de hand van mensen uit de beleids- en NGO-wereld. Naast officiële documenten en grijze literatuur konden we voor onderdeel 3, 4 en 5 terugvallen op een reeks semigestructureerde interviews uit april 2008 (uitgevoerd met financiering van de British Academy) en januari 2012. In beide gevallen kwamen daarin ambtenaren van de Europese Commissie, het Europees Parlement en het Europees Defensieagentschap alsook industriële vertegenwoordigers aan het woord. De eerste gespreksronde vond plaats in 2008, kort nadat binnen de prioritaire onderzoekslijn ‘veiligheidsonderzoek’ van het zevende Kaderprogramma de eerste financieringsschijven waren toegewezen. Het financieren van dit onderzoek was het eerste omvattende optreden van de EU op het gebied van de veiligheidsindustrie. De bedoeling van de interviews was te vernemen welke beleidsdoeleinden de sector nastreefde, hoe deze pasten binnen een ruimer EU-beleid en hoe ze initieel door andere instellingen, gebruikersgroepen en de industrie werden ontvangen. De tweede gespreksronde trachtte van alle betrokken groepen te weten te komen of de initiatieven van de EU naar hun aanvoelen de veiligheidsindustrie met succes hadden ondersteund, in welke mate zij hadden bijgedragen of zouden bijdragen tot ruimere beleidsdoelen en het industriële concurrentievermogen en hoe respondenten voorstellen tot toekomstige optredens zagen. Soms bestond de mogelijkheid om de eerste respondent weer te kunnen spreken. In de meeste gevallen echter zaten mensen ondertussen op een nieuwe functie, waren bevoegdheden herverdeeld of was de agenda anders gericht. In dergelijke gevallen was het interessanter om iemand anders te spreken. In dit rapport worden de gesprekspartners niet met naam of functie maar met instelling of sector genoemd, dit om de vertrouwelijkheid waar veel van hen om vroegen te vrijwaren. Onderdeel 5 gaat ook voort op een aantal telefoongesprekken met deskundigen inzake exportcontroles die tussen mei en juli 2012 hebben plaatsgevonden. Deze moesten eerder een inkijk bieden in het lopende debat over de controle van veiligheidstechnologieën en de meest adequate methodes daarvoor en niet zozeer specifieke informatie verstrekken. Onderdeel 4 ten slotte omvat een evaluatie van het programma voor veiligheidsonderzoek. Om na te gaan of kritische rapporten de juiste pijnpunten blootlegden, is een databank met vóór juli 2012 gefinancierde projecten ontwikkeld en voor analyse gebruikt.

1.3 Structuur van het rapport

Het rapport gaat op basis van de beschikbare literatuur na hoe en waarom de concepten veiligheid en defensie, interne en externe veiligheid en civiel en militair steeds meer in elkaar lijken over te lopen. Het begint met een overzicht van de voornaamste pogingen die de academische en de beleidswereld hebben ondernomen om, in het licht van de uitdagingen na de Koude Oorlog, het begrip veiligheid te herschrijven. Daarna werpt het zijn licht op de opgang van het concept 'homeland security' en stelt het zich de vraag of de Europese en Amerikaanse manier om hier theoretisch en praktisch mee om te gaan, verschilt. Tot slot komt het tot een bondig overzicht van hoe deze concepten binnen de EU precies worden gehanteerd en waarom de praktijk in deze arena mogelijk anders is dan elders. Dit onderdeel heeft een conceptueel karakter.

Het tweede deel gaat na of er wat betreft de industrie, technologie en gebruikersgroepen werkelijk sprake is van vervagende grenzen tussen veiligheid en defensie, tussen interne en externe veiligheid en tussen het civiele en het militaire. Het onderzoek wil met name verduidelijken wat de Europese Commissie verstaat onder veiligheidsindustrie, –technologieën en –klanten en of haar begrip hier afwijkt van wat ze onder de defensie-industrie, defensietechnologieën, en eindgebruikers verstaat. Ook beschrijft het hoe de vraag- en aanbodzijde al dan niet inspelen op dit, door de Commissie vooropgestelde, nieuwe veiligheidsdomein.

Deel 3 maakt een beoordeling van de verschillende beleidsinitiatieven waarmee de EU poogt om het concurrentievermogen van de veiligheids- en defensiesector te versterken en desbetreffende technologische ontwikkeling te stimuleren. Daarnaast vraagt het zich af of er een samenhangende aanpak bestaat. Na eerst de juridische basis voor EU-optreden op dit terrein, inclusief de beperkingen daarvan, te hebben uitgetekend, maakt dit onderdeel een kritische analyse van de EU-financiering voor veiligheidsonderzoek, het beleid inzake veiligheids- en defensie-industrie, binnenlandse of interne veiligheidsmaatregelen en het intergouvernementele werk van het Europees Defensieagentschap. Dan neemt het de bilaterale, multilaterale en NAVO-samenwerking op dit vlak onder de loep en onderzoekt het of deze het EU-beleid kan versterken of ook verstoren. Om af te ronden stelt het vragen bij de tendens in de EU om de convergentie tussen veiligheid en defensie sterk te benadrukken, en vraagt het zich af of zowel vraag- als aanbodzijde gebaat zouden zijn bij een meer gedifferentieerde aanpak.

Het laatste onderdeel kijkt naar de impact van veiligheidstechnologieën op de agenda inzake de controle op wapenuitvoer. Het schetst waarom het uitvoeren van bepaalde technologieën problematisch is geworden. Dan stelt het de vraag of het debat zich in hetzelfde kader moet afspelen als dat rond de wapenexportcontrole. Het stelt een overzicht samen van bestaande controles binnen verschillende stelsels en brengt mogelijke aanpassingen voor deze stelsels aan die de toestand zouden moeten verbeteren. Wat als slot nog aan bod komt, is de spanning die bestaat tussen de wens om de export van bepaalde technologieën te controleren omwille van een bezorgdheid om de schending van mensenrechten enerzijds, en externe vereisten van de interne veiligheidsprioriteiten van de EU anderzijds.

2 Veiligheid en defensie: concepten en hoe ze gebruikt worden

2.1 Inleiding

In de discussie rond veiligheid en defensie zijn academici én beleidsmakers het er roerend over eens dat het steeds moeilijker wordt om correct te omschrijven wat veiligheid tegenwoordig precies betekent. Dit beknopte conceptuele overzicht tracht de relevante debatten in kaart te brengen. Zo moet duidelijk worden hoe en waarom concepten zoals interne en externe veiligheid, civiele en militaire inmenging en veiligheid en defensie misschien niet meer zo duidelijk zijn afgelijnd. In de plaats van de duidelijk nationaal-militaire definitie van bedreigingen tijdens de Koude Oorlog is een myriade gekomen van transnationale veiligheidsuitdagingen (die gezien hun aard vaak internationale samenwerking vereisen), veranderende opvattingen over de rol die strijdkrachten en andere veiligheidsleveranciers moeten spelen en natiestaten die door privatisering en wijzigende bestuursvormen niet langer zelf de middelen hebben om de veiligheid te garanderen. In de Europese Unie, waar institutionele bevoegdheden overlappen en rivaliteit speelt, wordt dit een nog moeilijker kwestie.

Dit onderdeel onderzoekt eerst hoe de academische en de beleidswereld de uitdagingen na de Koude Oorlog zijn aangegaan. Daarna beschrijft het hoe het concept 'homeland security' ingang heeft gevonden en bekijkt het of EU en VS in hun besluitvorming en benadering naar mekaar toe of eerder uit elkaar groeien. Het derde onderdeel kijkt naar de Europese lidstaten en haalt verschillende praktijken naar voren op het domein van interne veiligheid. Het laatste onderdeel richt zijn blik op de EU zelf en naar hoe de concepten veiligheid en defensie worden gebruikt in de beeldvorming.

2.2 Wijzigende visie op veiligheid in academische en beleidskringen: verbreden en verdiepen

2.2.1 Het concept nationale veiligheid / defensie tijdens de Koude Oorlog

Misschien is het onjuist te denken dat tijdens de Koude Oorlog geheel duidelijk was wat nationale veiligheid inhield. De dominantie van het realisme tijdens de Koude Oorlog, en dit zowel bij beleidsmakers als bij academici, liet beleidsmakers toe om simpel te veronderstellen dat landen rationeel handelen om hun belangen te maximaliseren en in de eerste plaats hun voortbestaan te garanderen. Maar zelfs tijdens de Koude Oorlog werden veiligheidsbeslissingen genomen die niet uitsluitend waren gebaseerd op rationele berekeningen van nationale belangen. Als we de Koude Oorlog enkel beschouwen als een, om het met Katzenstein (1996: 2) te zeggen, "bipolair, ideologisch gevecht" dan is het niet nodig om nationale veiligheid vanuit een meer gecompliceerd standpunt te trachten te begrijpen. Maar wanneer de complexe aard van de Koude Oorlog mee in het spel komt, duiken ook daar kwesties omtrent normen, identiteiten en belangen op die we in de

periode na de Koude Oorlog terugvinden. Het is evident dat de militaire bedreiging tijdens de Koude Oorlog duidelijk voelbaar was en dat deze voor de meeste Europese landen voorrang kreeg op alle andere veiligheidsbepinningen. Toen de dekolonisatiestrijd was afgelopen zouden enkel die landen die op hun eigen grondgebied met een doorgezette en ernstige vorm van terrorisme te maken kregen nog middelen vrijmaken ter bestrijding van andere veiligheidsproblemen dan de Oost-Westconfrontatie.

Voor dit onderzoek is het nodig te bespreken hoe nationale veiligheid als concept is ontstaan. Het concept 'nationale veiligheid' werd met name ontwikkeld in de Verenigde Staten. De term dook een eerste keer op in documenten over de Amerikaanse deelname aan de Eerste Wereldoorlog. Als idee ging de Amerikaanse regering het vooral gebruiken in de nasleep van de Tweede Wereldoorlog, om een onderscheid te duiden tussen de nationale defensie (waaronder de activiteiten van de strijdkrachten werd verstaan) en de nationale veiligheid, waaronder men de ganse nationale capaciteit voor oorlogsvoering verstond, inclusief haarindustrie, onderzoek en natuurlijke hulpbronnen (Relyea, 2002). Academics verwijzen doorgaans naar Wolfers (1952) als de eerste die een definitie voor nationale veiligheid heeft kunnen ontwikkelen, namelijk door te suggereren dat wanneer men spreekt over nationale veiligheid, de veiligheid van de natie voorrang krijgt op die van de ruimere internationale gemeenschap. Algemeener werd het omschreven als het vermogen van een natie om haar interne waarden te beschermen tegen externe bedreigingen. Hoewel vaak wordt aangenomen dat nationale veiligheid tijdens de Koude Oorlog een universeel begrepen academisch concept was, ontbrak het in academische publicaties, zoals Baldwin (1997) aangeeft, vaak aan definities. In deze context betreurde Buzan (1991) het gebrek aan conceptueel werk over veiligheid.

Omdat de Oost-Westconfrontatie zo centraal stond in het wereldwijde veiligheidsbeleid, en omdat bovendien zowel kernwapens als grote staande legers gestationeerd in Oost- en West-Duitsland een cruciale rol speelden, werd veiligheid gedefinieerd in functie van deze strijdkrachten en hun wapenarsenaal. Centrale concepten om de Koude Oorlog te analyseren waren machtsverevenwicht, bipolariteit, indamming en afschrikking. Met een natiestaat die zich concentreerde op harde veiligheid en daarvoor de middelen moest voorzien, was het ook voor academics en beleidsmakers moeilijk om tot een ruimer of idealistischer beeld over wereldwijde veiligheid te komen. Het einde van de Koude Oorlog, zonder dat er zich onmiddellijk een duidelijke nieuwe militaire dreiging voordeed, creëerde echter ruimte om het concept veiligheid te herdenken. In dit debat tekenden zich twee kampen af, het ene dat de nationale veiligheidsagenda wil verbreden tot niet-militaire bedreigingen, en het andere dat een verdieping voorstaat met ook oog voor de veiligheid van individuen en niet alleen landen.

2.2.2 Nieuwe veiligheidsbepinningen – de verbreding van de agenda

De veiligheidsagenda verbreden was in academische kringen vooral een stokpaardje van de neorealisten¹, die de noodzaak inzagen om staten tegen meer dan louter militaire dreigingen te gaan beschermen. Ullman (1983) was een van de eersten om de overdreven aandacht voor externe militaire bedreigingen te bekritisieren, omdat men een niet-militaire dreiging van een omvang om landen te destabiliseren daardoor misschien uit het oog zou verliezen en bedreigingen van binnenuit zou kunnen onderschatten. Hij betoogde dat:

“een bedreiging voor de nationale veiligheid een actie is dan wel een reeks gebeurtenissen die (1) de levenskwaliteit voor de inwoners van een land drastisch en op relatief korte termijn dreigt aan te

¹ De verdiepingsagenda wordt eerder in combinatie gezien met sociaal-constructivistische en kritisch-theoretische denkers, terwijl de Kopenhaagse School voor een parallelle verbredings- en verdiepingsagenda pleitte.

tasten, of (2) de mogelijke beleidskeuzes waarover de regering van een land of private, niet-gouvernementele entiteiten (individueen, groeperingen, ondernemingen) in een land kunnen beschikken aanzienlijk dreigt in te perken" (1983: 133).

Hierop verder bouwend hebben academici verschillende soorten bedreigingen aangebracht die de veiligheid in het gedrang zouden kunnen brengen. De Kopenhaagse School bijvoorbeeld onderscheidt vijf algemene veiligheidscategorieën of –sectoren; militaire, ecologische, economische, maatschappelijke en politieke veiligheid (Buzan et al, 1998). Migratie, internationaal terrorisme en milieuschade krijgen stevast een hoofdstuk toebedeeld in een handboek veiligheidsstudies.

Toch is niet iedereen onverdeeld blij met het verbreden van de veiligheidsagenda. Sommige critici, zoals Ayoob (1997), vinden dat het door veiligheid in een bredere zin te omschrijven moeilijker en verwarrender wordt om de discussie te voeren, en zien er daarom geen nut in om vraagstukken met betrekking tot globaal beheer gelijk te stellen aan vraagstukken van internationale veiligheid. Scherpere kritiek komt uit de hoek van aanhangers van de verveiligingstheorie, die beargumenteren dat politici die in hun discours naar bepaalde kwesties als veiligheidsproblemen verwijzen, voor zichzelf de mogelijkheid creëren om buitengewone maatregelen te nemen om de vermeende bedreiging een halt toe te roepen (Buzan et al, 1998). Als aanvulling op de analyse van de Kopenhaagse School stelt Bigo (2002) dat verveiliging niet enkel tot uiting komt in een discours, maar ook in de specifieke praktijken van veiligheidsprofessionals die door een proces van verveiliging toepasbaar worden op de vermeende dreiging. Deze veiligheidspraktijken kunnen in strijd zijn met de vrijwaring van mensenrechten. Zoals verder in deze tekst zal blijken, is deze kritiek met name van toepassing op het domein van de 'homeland security'.

2.2.3 Menselijke veiligheid en de verantwoordelijkheid om te beschermen – de verdieping van de agenda

De verdieping van de agenda in academische veiligheidsstudies heeft met name vragen gesteld bij de traditionele focus op de staat als referentieobject voor veiligheid, dus datgene wat moet worden beveiligd. De vraag is of er naast de staat nog andere entiteiten zijn die in zulke mate bedreigd worden dat ze onderwerp worden van een veiligheidsbeleid. Sommige onderzoekers stelden voor om – naar boven toe – het internationale niveau als referentie object te nemen. Anderen stelden het regionale of het niveau van de maatschappij voor. Veruit de meeste aandacht in de academische en de beleidswereld ging echter naar de notie 'menselijke veiligheid' en naar de veiligheidsbedreigingen voor individuen. Deze verdiepingsagenda moet niet in de plaats komen van de verbredingsagenda: wie buiten de staat ook andere referentieobjecten in overweging neemt, beseft snel dat existentiële bedreigingen veel verder gaan dan enkel militaire dreigementen. Het 1993 Human Development Report stelt het als volgt: *"Het veiligheidsconcept moet de nadruk voor een stuk verleggen van nationale veiligheid naar meer aandacht voor de veiligheid van mensen, van veiligheid via bewapening naar veiligheid door menselijke ontwikkeling, van territoriale veiligheid naar veiligheid van voedsel, werk en milieu"* (UNDP Human Development Report 1993: 2).

In haar Human Development Report van 1994 heeft de UNDP dit onderwerp verder uitgewerkt met de argumentatie dat vrijheid van angst en gebrek voor iedereen de beste manier was om een oplossing te vinden voor de mondiale veiligheidsproblemen, die zeven dimensies hebben (economische veiligheid, voedselveiligheid, gezondheidsveiligheid, milieuveiligheid, persoonlijke veiligheid, veiligheid van de gemeenschap en politieke veiligheid). Deze argumenten kregen flink wat aandacht van academici en beleidsmakers en men neemt aan dat ze bijdroegen aan twee

beleidsontwikkelingen: het Verdrag van Ottawa inzake het verbod op landmijnen en de totstandkoming van de richtlijnen inzake de 'verantwoordelijkheid om te beschermen' voor humanitaire interventies.

Vooraf deze laatste ontwikkeling is van belang voor dit rapport. Deze heeft namelijk de manier waarop de EU is beginnen nadenken over haar mogelijke militaire rol zwaar beïnvloed. Een korte schets: in 2001 heeft de Canadese regering kort de Internationale Commissie inzake Interventie en Soevereiniteit van de Staat (ICISS) gesponsord om een antwoord te formuleren op de vraag van Kofi Annan over hoe de VN moest reageren op wreedheden zoals die in Rwanda en Srebrenica indien een humanitaire interventie een onaanvaardbare aanval op de soevereiniteit van een staat zou zijn. De ICISS (2001) kwam tot de conclusie dat het recht op humanitaire interventie kon worden uitgeoefend. Het recht op veiligheid van het individu moest immers voorrang krijgen op dat van de staat wanneer mensen intern door hun eigen staat of extern door andere staten worden bedreigd. Ook achtte zij het cruciaal dat de onderliggende oorzaken van instabiliteit werden begrepen en aangepakt, en was het volgens de commissie beter te voorkomen dan te interveniëren. Wel legde de ICISS (2001) zes criteria vast die een militaire interventie rechtvaardigden, namelijk; *“juiste autorisatie, gerechtvaardigde zaak, juiste intentie, laatste redmiddel, proportionele middelen en redelijke vooruitzichten”*. Interventie werd als concept later ook overgenomen door de VN wanneer het ging over genocide, etnische zuiveringen, oorlogsmisdrijven en misdrijven tegen de menselijkheid. Militaire interventie blijft controversieel. De inconsistente houding, en vooral ook praktijk, van de VN heeft kritiek uitgelokt. Bovendien zijn er kritische stemmen, zoals Chandler (2008), die stellen dat de menselijke-veiligheidsagenda bedreigingen in de nasleep van de Koude Oorlog heeft overdreven, ze naar ontwikkelingslanden heeft doen verschuiven met negatieve gevolgen voor het ontwikkelingsbeleid, en ontwikkelde landen heeft aanzet tot interventies op korte termijn in plaats van een strategie op lange termijn te ontwikkelen.¹

2.2.4 Gevolgen voor het beleid

Zulke debatten hebben allerhande gevolgen gehad voor het beleid. Door veiligheid niet langer te definiëren via externe militaire bedreigingen voor de integriteit van de natiestaat zijn Europese landen en de EU bedreigingen anders gaan omschrijven en behandelen. De EU-veiligheidsstrategie bijvoorbeeld identificeert de vijf voornaamste dreigingen waarmee de EU geconfronteerd wordt: terrorisme, verspreiding van massavernietigingswapens, regionale conflicten, mislukte staten en georganiseerde misdaad (Europese Raad, 2003). Deze veronderstellen een geheel andere veiligheidsaanpak dan wat er tijdens de Koude Oorlog courant was. En waar toch militair geweld noodzakelijk is, moeten de strijdkrachten anders worden getraind, bewapend en georganiseerd. Ten tweede vertrekt de menselijke-veiligheidsagenda vanuit een meer holistische benadering van conflictpreventie in alle fasen, wat betekent dat de types publiek- en privaatrechtelijke actoren betrokken bij interventies zijn gewijzigd. Daardoor zijn de voordien eerder duidelijke lijnen tussen civiele en militaire categorieën vervaagd.

Bovendien vinden die academici die zich zorgen maken over de verveiliging van een brede waaier aan uitdagingen, gehoor bij beleids mensen. Wanneer men in de academische wereld snel was om nieuwe veiligheidsbedreigingen te identificeren, liepen beleids makers daarin maar al te graag mee. In een breed variërend aantal beleids domeinen voert de EU steeds vaker een veiligheidsdiscours. We zien beleidsmaatregelen, comités en wetten opduiken over luchtvaartbeveiliging,

¹ Zo kwam er kritiek op de GVOB-missies van de EU omdat ze geen strategische onderbouwing kenden (Flechtner, 2006).

grensbeveiliging, energieveiligheid, milieuveiligheid, voedselveiligheid, gezondheidsbeveiliging om er maar enkele te noemen. Het is wellicht vooral op het domein van interne veiligheid dat we ons zorgen moeten maken over het risico dat politici en beleidsmakers buitengewone beleidsmaatregelen zullen legitimeren door een bepaalde uitdaging als een veiligheidsdreiging voor te stellen.

2.3 Het concept ‘homeland security’

2.3.1 Oorsprong

Vaak wordt de term ‘homeland security’ toegeschreven aan George W Bush tijdens een speech die hij gaf kort na de aanslagen van 11 september. Het concept werd echter al eerder gebruikt, aan het einde van de jaren 1990, door Amerikaanse militaire analisten die het veiligheidsbeleid van de VS na de Koude Oorlog uittekenden. Zij achtten ‘homeland security’ een voorname bezorgdheid. Zo formuleerde de U.S. Commission on National Security/21st Century in een rapport uit 2000 de aanbeveling dat de VS beveiligingscapaciteit op het gebied van ‘homeland security’ zou uitbouwen (2000: 14). Volgens Cohen et al (2006) stelden er zich toen drie problemen; ten eerste bleef de verantwoordelijkheid voor interne veiligheid erg versnipperd vanuit een bezorgdheid voor te veel centralisering van de macht, ten tweede dat de verschillende agentschappen die actief waren rond ‘homeland security’ bijna altijd andere primaire verantwoordelijkheden hadden, en ten derde dat de coördinatie tussen de agentschappen soms onvoldoende was. Na de aanslagen van 11 september werden, met de oprichting van eerst een dienst en vervolgens een ministerie van ‘homeland security’ en de benoeming van een adviseur voor ‘homeland security’, die de verschillende activiteiten moest coördineren, snelle pogingen ondernomen om deze problemen op te lossen. De PATRIOT Act van oktober 2001, die politiemensen minder beperkingen oplegde en het medewerkers van veiligheids- en immigratiediensten makkelijker maakte om Amerikaanse burgers en buitenlanders te schaduwen, gaf heel duidelijk uiting aan het concept ‘homeland security’.

Morag (2011) voert aan dat het concept ‘homeland security’ strikt Amerikaans van aard is, en *“een product van Amerikaanse geografische isolatie en de sterke neiging doorheen de geschiedenis van Amerika om te vinden dat gebeurtenissen, aangelegenheden en problemen buiten Amerikaanse grenzen losstaan van wat er daarbinnen gebeurt”* (Morag, 2011: 1). Hij wijst erop dat de VS in tegenstelling tot haar bondgenoten altijd een duidelijk onderscheid heeft gemaakt tussen de instrumenten waarvan zij zich thuis en elders kon bedienen. Vanuit wettelijk of institutioneel oogpunt mochten technieken voor nationale veiligheid met andere woorden niet op Amerikaans grondgebied worden ingezet. ‘Homeland security’ was een poging om deze kloof te overbruggen. Het moest een integratief concept worden dat paraatheid, reactievermogen en herstelcapaciteit bundelt in reactie op gebeurtenissen die een grootschalige sociale of economische ontwrichting teweeg kunnen brengen. Critici zien er de kiemen van een autoritaire veiligheidsstaat in. Ondanks deze kritiek heeft het concept ook buiten de VS doorgang gevonden, deels simpelweg omdat men zich genoodzaakt zag te reageren op de Amerikaanse ‘homeland security’. Morag (2011), stipt aan dat dit niet altijd gepaard ging met een duidelijk begrip van het concept.

Ook binnen de Verenigde Staten heerst onduidelijkheid over de betekenis van ‘homeland security’. Bellavita (2008:1-2) stelt bijvoorbeeld dat er minstens zeven plausibele definities zijn:

- een gezamenlijke nationale (federale, regionale en lokale) poging tot terrorismebestrijding;
- een gezamenlijke nationale poging tot terrorismebestrijding en bescherming tegen, antwoord op, en herstel van door de mens veroorzaakte en natuurlijke gevaren;
- wat het ministerie van Homeland Security doet om terroristische aanvallen en rampen te voorkomen, bestrijden en herstellen;
- een lokaal gestuurde poging om incidenten, waarvan men kan verwachten dat ze de veiligheid van de burgers in het gedrang brengen, te voorkomen en er zich op voor te bereiden;
- een nationale inspanning om elke sociale trend te voorkomen of af te zwakken die de stabiliteit van de Amerikaanse levenswijze zou kunnen bedreigen;
- een onderdeel van de nationale veiligheid of
- een door een overheid gebruikt symbool om de inperking van burgersvrijheden te rechtvaardigen.

Dit wijst er sterk op dat er binnen de VS geen consensus bestaat over het integratieve concept 'homeland security'. Ook heerst er flinke controverse rond het Amerikaanse ministerie van Homeland Security, dat ervan beschuldigd wordt burgersvrijheden te schenden en projecten te financieren enkel en alleen om het kiespubliek te paaien (Mueller en Stewart, 2012; Coats, Karahan en Tollison, 2006).

2.3.2 'Homeland security' in de EU en de VS: convergentie of divergentie?

Als trouwe bondgenoten en handelspartners van de VS moesten de EU en haar lidstaten tegemoetkomen aan de eisen van de Amerikaanse 'homeland security'-agenda en niet enkel op het vlak van terrorismebestrijding maar ook met betrekking tot de Amerikaanse poging om haar grenzen te beveiligen. Dit is geen vanzelfsprekende samenwerking geweest. Zoals Rees en Aldrich (2005) aangeven, zijn de strategische cultuurverschillen wanneer het over terrorisme gaat aan deze en gene zijde van de Atlantische Oceaan erg groot. Ten eerste zijn zij van mening dat, daar waar de VS wereldwijd een 'war on terror' is aangegaan, Europese landen terrorismebestrijding als een politionele en interne-veiligheidskwestie hebben beschouwd. De meer legalistisch ingestelde Europese aanpak hield in dat Amerikaanse beleidsbeslissingen zoals de 'extraordinary rendition' en Guantánamo Bay voor Europese politici moeilijk te aanvaarden waren (Archick, 2011). Ten tweede wijzen Rees en Aldrich (2005) erop dat bepaalde EU-lidstaten op het eigen grondgebied reeds lang vertrouwd waren met terrorisme, wat ze deed vermoeden dat Al Qaeda niet zo radicaal anders was als de VS beweerde. Ten derde speelt het verschil tussen hoe men tegen burgerrechten aankijkt inzake elektronisch toezicht en de bescherming van persoonsgegevens. Met name het Europees Parlement uitte zijn bezorgdheid over, en vroeg een herziening van, akkoorden in verband met de overdracht van bankgegevens (SWIFT-akkoord) en passagiersgegevens (PNR-gegevens) aan de VS (Archick, 2011). Ten slotte mag de EU dan wel een coördinator voor terrorismebestrijding hebben, diens taken en bevoegdheden zijn oneindig veel beperkter dan die van het Amerikaanse ministerie van Homeland Security.

Volgens veel commentatoren zijn de EU en de VS in hun houding rond 'homeland security' echter naar mekaar toe gegroeid. Deels heeft dit te maken met de meer multilaterale koers die de VS is gaan varen, reeds tijdens de tweede ambtstermijn van Bush maar vooral door de regering-Obama, waarbij meer aandacht ging naar de bezorgdheid in de EU rond burgerrechten, met name de manier waarop gevangenen werden behandeld (Archick, 2011). Anderen benadrukken echter het feit dat de Commissie het schokeffect van 9/11 heeft aangewend om nationale bevoegdheden inzake interne veiligheid versneld naar het EU-niveau over te hevelen, iets waar de lidstaten

traditioneel voor op hun hoede waren geweest. Dit betekent dat de EU haar nieuwe interne-veiligheidsmaatregelen deels heeft geënt op de VS en op de nood aan trans-Atlantische samenwerking (Lodge, 2004; Pawlak, 2009). Archick (2011) verwijst specifiek naar het akkoord van de EU in 2010 over een eerste interne-veiligheidsstrategie, die tenminste qua omvang parallel loopt met de opdrachten die het Amerikaanse ‘homeland security’-concept worden toevertrouwd. Ook het vermelden waard hierbij is dat de EU misschien wel de indruk moest wekken dat ze de strijd tegen het terrorisme ter harte nam. Dit creëerde ruimte om maatregelen goed te keuren die vroeger al op de agenda hadden gestaan maar waarover geen akkoord bestond. Bossong (2008) wijst er bijvoorbeeld op dat veertien van de achttien maatregelen die de Commissie voorstelde aan de bijzondere Europese Raad van 21 september 2001 slechts deels of zijdelings met terrorismebestrijding te maken hadden. De toenemende belangstelling voor bewakingstechnologieën geldt net zozeer voor andere domeinen in de Ruimte van Vrijheid, Veiligheid en Recht, zoals migratie en georganiseerde misdaad. Volgens critici zoals Hayes (2006; 2009) en Lodge (2004) heeft dit de EU in staat gesteld om maatregelen door te drukken die haaks staan op de waarden waarop de EU is gesticht. Lodge (2004: 253) stelt het als volgt: *“De binnenlandse-veiligheidsagenda van de EU en de daaraan gekoppelde biometrische instrumenten duiden op de toenemende verveiliging van de EU maar passen niet binnen de voor de EU fundamentele beginselen van vrijheid, democratie en rechtvaardigheid, en houden mogelijke risico's in voor het recht van burgers op privacy.”*

De maatregelen die de EU inzake ‘homeland security’ neemt, getuigen volgens Lodge (2004) niet zozeer van een interne noodzaak dan wel van een totale overgave aan de VS. Andere commentatoren zoals Archick (2011) en Bossong (2008) stellen zich duidelijk vragen bij de mogelijkheid tot concrete implementatie van de afgesproken maatregelen. Beide wijzen op de grote nationale verschillen tussen de lidstaten qua visie op interne veiligheid als reden waarom de tenuitvoerlegging moeilijk zal verlopen. Elke poging om in de EU een gemeenschappelijke interne-veiligheidsstrategie uit te werken, stuit op een verscheidenheid aan problemen. Inzet van politie-, intelligentie- en douanediensdiensten is iets wat binnen de EU behoorlijk kan verschillen, wat ook geldt voor de rol die het leger voor de interne veiligheid speelt. Bovendien hanteren de EU-lidstaten 29 verschillende rechtssystemen¹, elk met eigen procedures, jurisprudentie- en gewoonterecht. Een laatste element is dat een nationaal Grondwettelijk Hof EU-maatregelen ongrondwettelijk kan verklaren; denken we maar aan wat het Duitse Hof met het Europees aanhoudingsbevel heeft gedaan.

Toch houden critici het voor bewezen dat Europese landen, net als de VS, tot veiligheidsstaten evolueren. Hallsworth en Lea (2011: 142) suggereren dat er *“drie domeinen zijn waarin de veiligheidsstaat opgang maakt – de overgang van welfare naar workfare en risicobeheer; nieuwe maatregelen in de strijd tegen terrorisme en georganiseerde misdaad; en het vervagende onderscheid tussen oorlogvoering en misdaadbestrijding”*. De EU oogstte vooral kritiek voor haar pogingen om de buitengrenzen te bewaken, met name via het EUROSUR-voorstel rond geïntegreerd grensbeheer dat intensief gebruik zou gaan maken van bewakingstechnologieën aan de grenzen zelf en in derde landen als manier om het grensgebied te controleren. Critici zien hierin het bewijs dat grenscontroles toenemend militariseren (Hayes en Vermeulen, 2012). Deze ontwikkelingen werpen belangrijke ethische vragen op, die nog in deel 5 aan bod zullen komen.

¹ In het VK hebben Schotland en Noord-Ierland andere rechtssystemen dan Engeland en Wales.

2.4 Veiligheid en defensie: gebruik binnen de EU-context

2.4.1 De EU en defensie

De EU beschikt dan wel over een gemeenschappelijk veiligheids- en defensiebeleid, het moet worden benadrukt dat dit weinig te maken heeft met defensie in de traditionele zin van het woord. Zoals het vandaag is opgevat, is het vooral een mechanisme waarmee de EU humanitaire interventies kan opzetten (Mérand, 2008). Lidstaten houden eraan de intergouvernementele aard van het beleid te behouden. Een bijkomend probleem voor dit beleidsdomein bestaat erin dat lidstaten de NAVO blijven beschouwen, of zelfs steeds meer beschouwen als het primaire instrument voor klassieke defensietaken, en ook dat er buiten de EU om intergouvernementele defensiesamenwerkingen worden opgezet, zoals de Frans-Britse akkoorden van 2010. Ondanks dit alles onderneemt de Commissie al jaren pogingen om een rol in het defensiebeleid te spelen, zonder veel succes weliswaar, behalve het recente initiatief betreffende veiligheidsonderzoek.¹ Het nationaal-protectionistische beleid ten opzichte van verlieslatende defensiebedrijven is één reden voor dit gebrek aan succes. Verder spelen ook gevoeligheden over een beleid dat de kern uitmaakt van nationale soevereiniteit mee. Een andere belangrijke reden was dat de Commissie zelf niet eenduidig optrad.

Mörth (2000 en met Britz, 2004) brengt het relatieve falen van de Commissie in verband met met de bestuurskundige aspecten 'framing' (2000) en 'organisatie' (2004). Wellicht *had* de Commissie al eerder een defensierol kunnen opnemen, ware het niet dat dit moeilijk was als gevolg van interne conflicten en het relatieve succes van lidstaten om intergouvernementele organisatiedomeinen in te richten. De lidstaten richtten bijvoorbeeld OCCAR op om multinationale defensieaankopen te beheren en ze sloten een Raamovereenkomst voor de industriële herstructurering van defensie. Volgens Mörth (2000) was het te wijten aan de rivaliteit tussen de commissaris voor Handel en die voor Buitenlandse Betrekkingen (Bangemann en van den Broek) in de jaren '90 over wie nu verantwoordelijk was dat twee mededelingen over kwesties in verband met de defensie-industrie niet zo goed werden ontvangen als mogelijk was geweest en uiteindelijk dan ook door de Raad werden verworpen. Omdat het niet duidelijk was of bewapeningsbeleid nu onder de portefeuille Eenheidsmarkt, Ondernemingen of Buitenlandse Betrekkingen valt, heeft de Commissie hierover niet altijd een eensgezinde of samenhangende visie kunnen ontwikkelen.

2.4.2 De vervagen van het onderscheid tussen veiligheid en defensie

In de EU lijken bepaalde elementen erop te wijzen dat het de Commissie zelf is geweest die onduidelijkheid heeft geschapen over de concepten veiligheid en defensie, om zo haar rol in de defensiesector te kunnen uitbreiden (Mawdsley, 2011; Edler en James, 2012). Twee belangrijke rapporten uit 2002 (STAR21 en ACARE), opgemaakt door lobbygroepen van de ruimtevaart- en de luchtvaartsector, stelden dat technologische innovaties voor defensie- en ruimtevaartdoeleinden de economie in de EU in bredere zin ondersteunden. In haar mededeling van maart 2003 'Naar een EU-beleid voor defensiematerieel' onderschreef de Commissie deze thesis. Onder het punt *Naar een coherenter Europese inspanning voor hoogwaardig onderzoek op het gebied van veiligheid* riep de Commissie op tot meer coördinatie van het veiligheidsonderzoek. Ze gaf aan dat ze

¹ De inspanningen van de Commissie en de beperkingen ervan worden uitvoerig beschreven in deel 4 van het rapport.

ationale overheden, de bedrijfswereld en onderzoeksinstituten zou vragen hoe een Europese onderzoeksagenda er in dit domein zou moeten uitzien en zou proberen *“om een voorbereidende actie op te zetten, met de bedoeling dergelijk onderzoek op Europees niveau te coördineren, gericht op een beperkt aantal concrete technologieën die aan de Petersbergtaken zijn gekoppeld”* (Europese Commissie, 2003a). De Commissie gaf de indruk defensieonderzoek te gaan financieren maar de oprichting in 2003 van het Europees Defensieagentschap met een opdracht op dat vlak maakte dit politiek onmogelijk (Mawdsley, 2011). Ze stelde een Groep van prominenten samen die de kwestie moest bekijken. In 2004 rapporteerden zij dat militair en civiel onderzoek zich amper van elkaar onderscheidde en zagen zij in de Amerikaanse investering in ‘homeland security’ nogmaals geïllustreerd hoe de EU achterop raakte. Mede dankzij hun rapport kreeg de onderzoeksprioriteit op het gebied van civiele veiligheid in het zevende Kaderprogramma vorm. Recenter nog besloten de Europese ministers van Defensie in mei 2009, het Europees Defensieagentschap op te dragen om samen met de Europese Commissie een Europees samenwerkingskader voor veiligheid en defensie in te richten, met de bedoeling om *“onderzoeksactiviteiten rond defensie en civiele veiligheid waar mogelijk te laten aanvullen en op elkaar af te stemmen”*.¹ Met andere woorden, voor wat research betreft maakt de EU geen onderscheid meer tussen de twee types van onderzoek.

Is dit van belang? Voor sommigen is dit een puur semantische kwestie. Tim Robinson, senior vicepresident van de veiligheidsafdeling bij Thales merkt bij de veranderende binnenlandse veiligheidsmarkt het volgende op: *“Ik zie de klemtoon verschuiven en merk dat de verschillen uitvlakken tussen wat we als defensie en als ‘homeland security’ beschouwen. ‘Veiligheid’ is een politiek correctere term die omschrijft wat we voordien defensie noemden.”* (Euractiv, 2006) Anderen, zoals Hayes (2006; 2009) zien de vervagende grenzen tussen militaire en civiele toepassingen als een onrustwekkende ontwikkeling met zorgelijke gevolgen voor de burgersvrijheden in Europa. Bovendien kunnen we uit de manier waarop deze ontwikkelingen hebben plaatsgegrepen opmaken dat de Commissie zich vooral met het industriële en technologische aspect van defensie heeft ingelaten, waardoor ze mogelijk het geheel uit het oog verliest.

2.5 Samenvatting

Nu we kort de debatten hebben besproken die zich onder beleidsmakers en in de academische wereld afspelen, en die bepalen of we nog een duidelijk onderscheid kunnen maken tussen een nationale veiligheid met civiele grondslag en een militair gebaseerde defensie, staat het vast dat dit een complexe materie is. Duidelijk is dat academische debatten over wat veiligheid in het post-Koude Oorlog tijdperk kan betekenen, nu ook onder EU-beleidsmakers worden gevoerd. In eerste instantie zijn het nu verdiepte veiligheidsconcept om niet enkel landen maar ook individuen als mogelijke dreiging te beschouwen en de ontwikkeling van de ‘Verantwoordelijkheid om te beschermen’-doctrine, die stoelt op een concept van menselijke veiligheid, van doorslaggevend belang geweest in de ontwikkeling van het Gemeenschappelijk Veiligheids- en Defensiebeleid, dat zich eigenlijk niet op militaire defensie maar eerder op humanitaire interventies focust. Met als gevolg dat naast het leger verscheidene niet-militaire publiek- en privaatrechtelijke actoren hier een rol in spelen. Ten tweede vormt het opentrekken van het veiligheidsconcept naar ook niet-militaire bedreigingen de onderbouw van de Europese veiligheidsstrategie en aanverwante beleidsmaatregelen. De vrees bestaat echter dat naarmate de verveiliging zich in een toenemend

¹ Raad van de Europese Unie, 2943e zitting van de Raad Externe Betrekkingen, Conclusie over Europees veiligheids- en defensiebeleid (EVDB), Brussel, 18 mei 2009

aantal domeinen doorzet, dit optreden zal rechtvaardigen dat niet geheel binnen het waardenpatroon van de EU past.

Het tweede deel van het overzicht behandelde de opkomst van het 'homeland security'-concept in de Verenigde Staten en de invloed daarvan op de Europese Unie. Het beargumenteerde dat de verschillende wijze waarop de Europese lidstaten en de VS met terrorisme omgaan na een decennium trans-Atlantische samenwerking sinds 9/11 deels is weggewerkt. Deels had dit te maken met het feit dat bepaalde in de EU bestaande denkbeelden ingang vonden in de VS, maar meer nog omdat 'homeland security' aanzienlijke sporen heeft nagelaten in een Europese Unie die voordien geen duidelijk beleid ter zake voerde en de Amerikaanse vraag tot samenwerking niet naast zich neer kon leggen. Deze context maakte bepaalde beleidsontwikkelingen binnen de EU mogelijk. Niet iedereen was tevreden met deze ontwikkeling, zeker waar burgervrijheden in het spel waren. Anderen vonden dan weer dat de EU te verdeeld was om inzake interne veiligheid een efficiënte actor te worden.

Als laatste element wierp het overzicht een blik op de opkomst van defensie in de EU. Daar de meeste lidstaten enkel heil zagen in een intergouvernementele aanpak, heeft de Commissie pogingen ondernomen om een ander defensiemodel uit te werken waarbinnen wel mogelijkheden lagen. Pas zodra er binnen de Commissie eensgezindheid bestond, werden de portefeuilles Industrie en Onderzoek naar voren geschoven als meest geschikte beleidsdomeinen. Met de oprichting echter van het Europees Defensieagentschap dat ook op die domeinen actief was, zag de Commissie zich genoodzaakt om haar financieringsplannen onder de noemer veiligheid onder te brengen en van het 'homeland security'-model te vertrekken. Dit heeft ertoe geleid dat de grenzen tussen civiele en militaire toepassingen nog verder vervaagden, en dat de Commissie zich uitsluitend op het industriële en het technologische aspect ging richten. Dit overzicht stelt kortom dat we ons terecht mogen afvragen of we in de EU nog een onderscheid mogen maken tussen veiligheid en defensie, civiele en militaire inmenging of interne en externe veiligheid. Echter, het gebrek aan een duidelijk concept in de manier waarop deze terminologie wordt gebruikt, betekent dat er een empirisch onderzoek naar de materiële factoren (markt en technologieën) en de beleidsaspecten moet plaatsvinden.

3 De kenmerken van de veiligheids- en defensiemarkt in de EU

3.1 Inleiding

Dit deel van het rapport wil de kenmerken schetsen van zowel de veiligheids- als de defensiemarkt in de EU. Daarvoor moeten we de vraag- (gebruikers) en de aanbodzijde (ondernemingen) van de markt(en) onder de loep nemen, net als het onderzoek, de ontwikkeling en de aankoop van producten. In wat volgt trachten we te begrijpen of de veiligheids- en de defensiemarkt losstaande entiteiten zijn, op bepaalde punten overlappen of grotendeels als inwisselbaar kunnen worden beschouwd. Eerst worden de methodologische problemen op een rijtje gezet om de veiligheids- en de defensiesector te kunnen definiëren. Vervolgens geeft dit hoofdstuk een definitie van de veiligheidssector en van wat deze inhoudt. Het volgende punt behandelt onderzoek en technologieën; het gaat kort over onderzoeksfinanciering, de mogelijkheden en beperkingen van de taxonomische aanpak en vraagt zich af of we veiligheids- en defensietechnologieën van elkaar kunnen onderscheiden. Als laatste probeert het te antwoorden op de vraag welke rol de defensie- en de veiligheidssector vandaag in innovatiesystemen spelen. Dan komt de industrie aan bod. Daarbij poogt dit deel om een discussie op gang te brengen over hoe de veiligheidssector kan worden gedefinieerd en in dit rapport zal worden behandeld, gevolgd door een analyse van hoe zowel defensie- als andere ondernemingen de sector toen die in volle opgang was hebben benaderd, en welke trends er merkbaar zijn. Het laatste belangrijke punt kijkt naar gebruikersgroepen; na identificatie van de voornaamste groepen stelt het de vraag of civiele en militaire rollen en technologievereisten in de huidige veiligheidsomgeving minder duidelijk zijn afgelijnd. Om af te ronden gaat het na of erg uiteenlopende civiele en militaire aankoopprocedures en behoefteomschrijvingen ertoe leiden dat de vraagzijde van de markt gefragmenteerd blijft, en als dit zo is of daarvoor een oplossing bestaat.

3.2 De veiligheids- en defensiesector gedefinieerd: problemen en beperkingen

In eerste instantie moet duidelijk zijn dat geschikte kwantitatieve gegevens om de EU-defensiesector te analyseren moeilijk te verkrijgen zijn, iets wat nog meer geldt voor de veiligheidssector. Defensie-economen wijzen reeds geruime tijd op hoe moeilijk het is om, bijvoorbeeld aan de hand van OESO-categorieën, het defensieonderzoek in kaart te brengen. Aangezien steeds meer technologieën immers een duale en civiele toepassing hebben (Mollas-Gallart, 1999) of de industriële basis voor defensie moeilijk is te omschrijven, ontstaan problemen om tot geloofwaardige meetresultaten te komen (Dunne, 1995; Hartley, 2011). Zelfs ondernemingen die algemeen bekend staan als defensiebedrijven halen hun omzet zelden uitsluitend uit defensieprojecten maar ontwikkelen daarnaast ook heel wat civiele toepassingen. Bovendien werken de NAVO en het Europees Defensieagentschap dan wel met standaardprocedures om defensie-uitgaven van EU-lidstaten en wat daarvan aan materieel wordt

besteed te verzamelen¹ waardoor vergelijken mogelijk wordt, toch blijft het moeilijk te achterhalen waar het budget voor materieel, los van de behoorlijk correct gedocumenteerde grote aanbestedingsprojecten, heen gaat. Evenmin zijn er, om commerciële redenen, maar weinig bedrijven die hun resultaten publiceren. Daarbij komt nog dat tot dusver geen voor alle EU-lidstaten vergelijkbare gegevens beschikbaar zijn gesteld over vanuit de overheid vrijgemaakte budgetten ter ondersteuning van de defensiesector, denken we maar aan steun voor de wapenexport, compenserende overeenkomsten, onderzoekssubsidies ten behoeve van door de overheid gefinancierde universiteiten en onderzoeksinstituten, regionale financiering en preferentiële aanbestedingsprocedures om er maar enkele te noemen. Al deze lacunes maken uitgebreid cross-nationaal kwantitatief onderzoek onmogelijk.

De veiligheidssector kampt op dit vlak met nog grotere problemen. Ten eerste is er geen eenstemmigheid over een precieze afbakening van de veiligheidssector (de voor deze studie gebruikte definitie van de veiligheidsindustrie en de achterliggende principes worden toegelicht in punt 3.2.1). Zelfs de Europese Commissie (2012a) erkent dat er geen algemeen aanvaarde definitie bestaat. Ten tweede is betrouwbare statistische informatie, ook vergeleken met de defensiesector, moeilijk te vinden. Volgens Martí Sempere (2011) verstrekt Eurostat dan wel bepaalde gegevens die nuttig kunnen zijn om uitgaven, import en export te berekenen, maar geven de NACE-codes¹¹ voor sommige beveiligingsproducten en -diensten (bv. code 80 voor beveiligings- en opsporingsdiensten en 84.24 voor openbare orde en veiligheid) aanleiding tot problemen omdat ze niet sluitend zijn. Evenzeer zijn er codes die andere types beveiligingsmaterieel moeten classificeren maar geen onderscheid maken tussen materieel voor beveiligings- of andere doeleinden. Zo wordt het onmogelijk om de veiligheidssector vanuit een classificatie van industriële activiteiten correct te identificeren en te definiëren. Even problematisch wordt het wanneer we gegevens van nationale overheden op elkaar willen afstemmen. Veel landen hebben meer dan één begrotingslijn voor veiligheid. Doorgaans gaan verschillende ministeries en agentschappen over veiligheid en is dit een bevoegdheid die in federale staten vaak over het federale en regionale niveau is verspreid (Masson en Marta, 2011). Landen met elkaar vergelijken wordt zo erg moeilijk. En om commerciële redenen zijn ondernemingen niet snel bereid om informatie te verspreiden. Hoewel dit rapport gebruik zal maken van allerlei gegevens aangeleverd door Europese bedrijfsfederaties en de gegevens uit twee ten behoeve van de Europese Commissie opgestelde omvangrijke rapporten (ECORYS et al (2009) inzake het industriële concurrentievermogen van de veiligheidsindustrie en IRIS et al (2010) inzake het vervagen van de scheidslijnen tussen defensie en veiligheid), moet worden erkend dat de cijfers schattingen inhouden of een onvolledig dan wel een tegenstrijdig beeld scheppen (Hartley, 2011). IRIS et al (2010: 26) stellen bijvoorbeeld dat het onmogelijk bleek om de omvang van de veiligheidssector precies te omschrijven omdat de beschikbare gegevens niet verifieerbaar waren.

3.2.1 Wat is de Europese veiligheidssector?

Wat is de Europese industriële veiligheidssector? Dit lijkt een eenvoudige vraag, maar ze is verrassend moeilijk te beantwoorden. In feite is het een verzamelnaam voor een hele reeks bedrijven die producten en diensten leveren aan individuele klanten maar ook natiestaten die daarmee een breed spectrum aan veiligheidsproblemen wensen aan te pakken. Vertrekkend van de definities die onder andere de EAVO (2006) voorstelt, vindt Martí Sempere dat de veiligheidsindustrie in deze zin als volgt kan worden gedefinieerd:

¹ Daarnaast zijn de jaarlijkse analyses van wereldwijde militaire uitgaven door het Internationaal Instituut voor Vredesonderzoek van Stockholm en het Internationaal Instituut voor Strategische Studies betrouwbare gegevensbronnen.

¹¹ Algemene nomenclatuur van de economische activiteiten in de Europese Gemeenschap

“De veiligheidsindustrie omvat alle producten en diensten die mensen met name gebruiken om zich voor te bereiden op, als preventie, bescherming en reactie tegen, als inperking en verlichting van en als oplossing voor bedreigingen en effecten die onverwachte gebeurtenissen voor onze samenleving kunnen inhouden. Deze effecten vormen een bedreiging voor mensenlevens, de gezondheid, de bezittingen of andere activa zoals informatie.” (Martí Sempere, 2011: 246)

Maar Martí Sempere (2011) beseft ook dat het om analytische redenen nodig is tot een engere definitie te komen. Volgens hem moeten we de focus daarbij best leggen op de industrie die een oplossing wil bieden voor het onveiligheidsgevoel naar aanleiding van nieuwe bedreigingen van internationaal terrorisme en georganiseerde misdaad, die hij vandaag als de voornaamste gevaren beschouwt. Met deze suggestie laat hij echter leveranciers van traditioneel militair materieel buiten beschouwing (Martí Sempere, 2011: 248), iets wat voor dit rapport problemen oplevert. Hierin concentreren we ons namelijk op de positie van de EU en de Europese Commissie hechtte net veel belang aan vertegenwoordiging van de defensie-industrie en dichtte haar een prominente tol toe in de overleg- en adviesgroepen die voor de Europese Commissie de industriële veiligheidssector moesten doorlichten (zie onderdeel 4). Bovendien is het zo dat, net zoals ‘homeland security’ in de VS een vlag is die meerdere ladingen dekt, ook uit de beschikbare EU-regelgeving zoals Richtlijn 2008/14/EG inzake de bescherming van kritieke infrastructuren blijkt dat terrorisme als voornaamste bedreiging wordt gezien maar dat de wetgeving moet gelden voor alle dreigingen, ook als gevolg van natuurrampen (Raad van de EU, 2008b).

Net als Martí Sempere benadrukten ECORYS et al (2009) in hun verslag voor het DG Ondernemingen en Industrie over de concurrentiepositie van de veiligheidssector in Europa de noodzaak om tot een meer afgebakende definitie te komen. Om de sector af te bakenen werkten ze met een model dat deze opdeelde in de traditionele veiligheidsmarkt waar vooral de private beveiligingsfirma’s sterk staan, de defensiemarkt en de ‘nieuwe veiligheidsmarkt’ als reactie op ‘nieuwe’ veiligheidsbedreigingen zoals terrorisme, georganiseerde misdaad, computercriminaliteit en bescherming tegen en reactie op grote rampen. Daarbij zou deze laatste markt nog in haar kinderschoenen staan, daar deze pas echt is opgekomen na de aanslagen van 11 september en de daaropvolgende lancering in de VS van een grootschalig ‘homeland security’-programma. Wel wijzen ze erop dat de scheidslijnen tussen deze drie categorieën niet altijd even duidelijk zijn. Martí Sempere (2011) en ECORYS et al (2009) zien dan wel andere ‘nieuwe bedreigingen’ opduiken, toch zijn ze het eens dat een andersoortige industriële veiligheidssector nu een antwoord moet vinden voor deze problemen.¹

IRIS et al (2010) hanteren een andere benadering, omdat zij vooral willen analyseren in welke mate de scheidslijnen tussen veiligheid en defensie zijn vervaagd en niet echt tot een definitie van de industriële veiligheidssector willen komen. In hun analyse gaan ze eerst de relevant geachte taakgebieden identificeren om vervolgens een omschrijving te geven van de veiligheidsopdrachten. Dit zijn dan de vier types die ESRAB (2006) heeft omschreven (bescherming tegen terrorisme en georganiseerde misdaad, grensbewaking, bescherming van kritieke infrastructuur en herstel van veiligheid in geval van crises) en de inzet van strijdkrachten op drie door Franse, Italiaanse en Duitse beleidsrichtlijnen inzake defensie² afgebakende terreinen (traditionele territoriumverdediging en afschrikking, crisisbeheersoperaties en steun aan civiele bescherming). Dan wordt onderzocht op welke domeinen vervaging is opgetreden en bepalen ze welke technologieën en apparaten vereist zijn om daar missies te kunnen uitvoeren. Zij stellen terecht dat de interne en externe veiligheidsmissies zijn samengevloeid. We komen daar nog op terug in punt

¹ Deze mening deelden ambtenaren van de Europese Commissie, DG Onderzoek en DG Ondernemingen en Industrie die in april 2008 werden geïnterviewd.

² Dit wijst toch op raakvlakken tussen deze documenten die dit rapport misschien te sterk benadrukt.

3.5.2. Deze benadering heeft hen het desbetreffende marktsegment wel als volgt doen omschrijven: *“uitermate complex en gefragmenteerd, met talrijke industriële spelers uit verschillende bedrijfstakken die elk hun eigen oplossingen aandragen”* (IRIS et al, 2010: 139). Martí Sempere (2011) en ECORYS et al (2009) van hun kant slaagden erin de veiligheidssector op een meer gerichte manier te typeren. Voor alle drie de analyses geldt dat ze zich (al dan niet expliciet) richten op technologische producten¹, dus niet op het gehele spectrum aan veiligheidsproducten en -diensten. Ook gaan ze allen uit van de premisse dat de klant een overheidsorganisatie is. Dit ligt in de lijn van de EU-beleidsagenda voor deze sector. De Commissie (2012a) zegt inderdaad uitdrukkelijk dat ze in haar beleid inzake de veiligheidssector van dienstverlening geen aandachtspunt maakt. In dit rapport wordt de industriële veiligheidssector aldus verstaan als ondernemingen met verschillende industriële achtergronden die overheidsklanten technologische producten aanleveren om veiligheidsproblemen aan te pakken. De analyse richt zich daarmee wel degelijk op alle defensiebedrijven en sluit geen veiligheidsproblemen uit, enkel op voorwaarde dat de producten een technologische gerichtheid hebben. Uitgesloten van de analyse worden commerciële en private klanten, dit ten voordele van overheidsactoren die tot dusver de doelgroep van EU-beleidsacties zijn geweest. De European Organisation for Security (EOS), vertegenwoordiger van technologiefabrikanten en dienstverleners voor private beveiligingsdoelstellingen, heeft opdracht gegeven om de veiligheidsmarkt zoals die er 2011 uitzag door te lichten. Hoewel ook zij de beperkingen van de beschikbare kwantitatieve gegevens benadrukken, hebben zij een poging ondernomen om de door hun leden aangebrachte cijfers over de interne markt naast gegevens uit commercieel onderzoek te leggen. Op basis daarvan zien zij hun sector opgedeeld in vier takken:

- Grenscontrole
- Civiele en burgerbescherming
- Cyberbeveiliging
- Bescherming van kritieke infrastructuur.

Hun schattingen wijzen op een totale omzet in de hele EU van 10,5 mld. euro voor 2009, inclusief export buiten de EU (geschatte interne omzetcijfers - grenscontrole 1,54 mld. euro, civiele en burgerbescherming 2,69 mld. euro, cyberbeveiliging 1,85 mld. euro, bescherming van kritieke infrastructuur 1,57 mld. euro dus in totaal 7.65 mld. euro) met een tewerkstellingscijfer in de hele EU van naar schatting 50.000 (EOS, 2011). ECORYS et al (2009) berekenden de totale waarde van de veiligheidssector in 2008 op ongeveer 36 mld. euro. De publieke sector was daarbij goed voor 80% van de vraag. Welke technologieën zijn hiervoor nodig? Volgens het EAVO-rapport (2006: 50) zijn volgende technologieën vereist:

¹ Er gaapt hier een interessante kloof tussen de academische literatuur over de industriële veiligheidssector, die veiligheidstechnologieën grotendeels links heeft laten liggen en zich in plaats daarvan heeft geconcentreerd op bedrijven die personeel en diensten aanleveren voor conflictgebieden, en deze door de Europese Commissie gefinancierde beleidsstudies met een sterke focus op technologie.

Tabel 1: Veiligheidstechnologieën

Technologisch domein	Voornaamste technologische toepassingen
Signaal- en informatietechnologie	Datafusietechnieken, gegevens verzamelen/classificeren, beeld-/patroonverwerking, technologie om informatie te integreren, technologie voor gegevens- en informatiebeheer (DB, enz.)
Artificiële intelligentie en beslissingsondersteuning	Tekstmining/datamining, IKBS/AI/experttechnieken, kennisbeheer, modellering en simulatie, optimalisatie- en beslissingsondersteunende technologie
Sensorapparatuur	Camera's, radarsensor-apparatuur, NRBC-sensoren (met name opsporingstechnologieën voor biologische en chemische bedreigingen), passieve IR-sensorapparatuur
Sensortechnologieën	Hyperspectrale/multispectrale beeldsensoren, hyperspectrale/multispectrale verwerking, autonome kleine sensoren/smart dust technologieën, IR-sensortechnologieën, Terahertz-sensoren, optische-sensortechnologieën, geluidssensoren — passief
Communicatieapparatuur	Herconfigureerbare communicatie, mobiele beveiligde communicatie, communicatienetwerkbeheer en controleapparatuur, netwerksupervisor, netwerk- en protocolafhankelijke beveiligde communicatie, informatiebeveiliging, beveiligde, draadloze breedband gegevensverbindingen voor beveiligde communicatie, bescherming van communicatienetwerken in agressieve omgevingen
Menswetenschappen	Analyse en modellering van het menselijk gedrag, bevolkingsgedrag, menselijke factoren in het besluitvormingsproces, teams, organisaties en culturen
Technologieën voor informatiebeveiliging	Encryptie en sleutelbeheer, datamining, toegangscontrole, filtertechnologieën, authenticatietechnologieën, encryptietechnologieën (cryptografie)
Computing-technologieën	Protocoltechnologie, SW-architecturen, beveiligde gegevensverwerkingstechnieken, krachtige computers, high integrity en safety critical computing
Informatieoorlog-/inlichtingsystemen	Infrastructuur om informatiebeheer en –verspreiding te ondersteunen, beheersinstrumenten voor cyberbeveiligingsbeleid, optimalisatie, planning- en beslissingsondersteunende systemen
Scenario- en beslissingssimulatie	Concepten van impactanalyse en impactbeperking, geavanceerde modellering en simulatie van het menselijk gedrag, simulatie voor besluitvorming (realtime simulatie), voorspelling van structurele kwetsbaarheid, evacuatie- en gevolgbeheerstechnieken, missiesimulatie
Informatiesystemen	Infrastructuur om informatiebeheer en –verspreiding te ondersteunen, beheersinstrumenten voor cyberbeveiligingsbeleid, optimalisatie, planning- en beslissingsondersteunende systemen
Navigatie, begeleiding, controle en tracking	RFID-tags, tracking, GPS, radionavigatie, sturing en kartografische navigatie, op streepjescode gebaseerde opsporing
Forensische technologieën — biometrie	Vingerafdrukherkenning (digitale vingerafdrukken), gelaatsherkenning, herkenning van iris/netvlies, stem, handschrift, handtekening
Geïntegreerde platformen	UAV's (lucht/land/water), lichter dan luchtplatformen, bewakings- en navigatiesatellieten
Overlevings- en verhardingstechnologie	EMC-beoordeling en -versterking, slimme kledij en uitrusting, ontploffingsbestendig glas/beton, enz., kritieke gebouwen, specifieke architecturen, impact- en schokeffecten

Elektronische authenticatie	Systemen voor elektronisch toezicht, chipkaarten
Biotechnologie	Snelle analyse van biologische agentia en menselijke vatbaarheid voor ziektes en giftige stoffen, decontaminatietechnieken, technieken om water te testen en te zuiveren, technieken voor voedseltests en -controles
Simulatoren, trainers en synthetische omgevingen	Virtuele en aangevulde realiteit, systemen voor tactische training/opleiding van personeel, systemen voor commando- en personeelstraining, synthetische omgevingen
Chemische, biologische en medische materialen	Chemische en biologische opsporingstechnieken
Signaalbescherming (oorlogssituaties)	Niet-coöperatieve doelwitherkenning, geografische informatiesystemen
Ruimtevaartsystemen	Observatie van de aarde (beeld en communicatie)
Lichte en sterke materialen, coatings, ...	Lichte materialen voor menselijke bescherming, slimme stoffen, lichte materialen voor locatiebescherming, zelfbeschermende en explosiebestendige materiaaltechnologie, oppervlaktebehandelingen om de levensduur te verlengen, roestwering
Opslag en distributie van opgewekte energie	Generatoren, accu's, energiedistributie

Uit de tabel blijkt dat sommige technologieën vereist voor de voornaamste toepassingen in dit nieuwe marktsegment duidelijk ook in de defensiesector hun nut hebben. Denken we maar aan onbemande luchtvaartuigen, sensortechnologieën en mobiele beveiligde communicatiesystemen. Zijn de technologieën daarom inwisselbaar?

3.3 Veiligheids- en defensietechnologieën

Dit onderdeel gaat in op de verbanden tussen veiligheids- en defensietechnologieën. Eerst wordt kort toegelicht hoe financiering van onderzoek en ontwikkeling op defensiegebied in de EU tot dusver verliep, aangezien dit duidelijk zijn stempel zou kunnen drukken op de toekomstige financieringsmechanismen voor O&O inzake veiligheid. Vervolgens bespreekt het of de technologieën wel of niet inwisselbaar zijn, en wat het betekent dat beide domeinen zo sterk afhankelijk zijn van generische technologieën.

3.3.1 Uitgaven en trends inzake defensie-O&O: implicaties voor veiligheidstechnologie?

Dit korte onderdeel tracht in grote lijnen enkele elementen toe te lichten die van invloed zijn op de Europese financiering van onderzoek en ontwikkeling op defensiegebied en die wellicht ook van tel zullen zijn voor de O&O inzake veiligheid. Om te beginnen toont het overzicht hieronder dat twee landen, Frankrijk en het Verenigd Koninkrijk, goed zijn voor het leeuwendeel van de Europese uitgaven aan defensie-O&O, met Duitsland op de derde plaats. Veel EU-lidstaten besteden weinig of geen geld aan onderzoek en ontwikkeling op defensiegebied. Bovendien zijn hier ook de

gevolgen van de financiële crisis duidelijk merkbaar. Kijk maar naar de uitgaven van Italië en Spanje na 2008.

Tabel 2: EU-uitgaven defensie-O&O 2006-10 (in miljoen euro)

	2006	2007	2008	2009	2010
Oostenrijk	0,81	1	0,87	7,5	1
België			9,66	9,3	9,2
Bulgarije	0,42	0,42	0,244	0	0
Cyprus				0	0
Tsjechië	18,5	18,4	21,8	20,8	20,2
Estland	1	1	1,8	0,3	0,7
Finland	30,7	44	27,6	44,1	38,3
Frankrijk	3777	3231	3281	3704	3580
Duitsland	1035	1213	1183,1	1088	1455
Griekenland	0,06	7,3	10,89	4,7	10
Hongarije	0,82	0,974	2,79	3,5	0,3
Ierland	0			0	0
Italië	252	341	251,7	139	64
Letland	0,423	0,27	0,171	0,2	0,03
Litouwen				0	0
Luxemburg				1,6	2,1
Malta				0	0
Nederland	112	107	105	105	75
Polen	37,6	53,9	50,89	88,9	121
Portugal	5,624	4,699	4	9	7
Roemenië	3,4	15,3	7,3	2,3	2,1
Slowakije	3,7	2,49	3,5	5,3	0,1
Slovenië	19,5	12,8	17,5	11,2	7,8
Spanje	201	276,6	314	229	162
Zweden	266	299	235	151	107
VK	4012	4011	3214	2770	2895

Bron: Europees Defensieagentschap

Masson en Marta (2011) wijzen erop dat deze trends zich schijnbaar ook vertalen in de budgetten die op regeringsniveau voor onderzoek en ontwikkeling inzake veiligheid worden vrijgemaakt. Enkel Groot-Brittannië, Frankrijk en Duitsland hebben hiervoor noemenswaardige programma's opgezet: *“Het Duitse federale ministerie van Onderwijs en Onderzoek heeft voor de periode 2007-2011 ten behoeve van onderzoek inzake civiele veiligheid 123 miljoen euro gebudgetteerd. In Frankrijk realiseert de Délégation Générale pour l'Armement (binnen het ministerie van Defensie), samen met het Agence National pour la Recherche een programma rond “concepten, systemen en instrumenten voor globale veiligheid”, dat in 2009 met 12,7 miljoen euro werd gefinancierd. In het*

VK krijgt het ministerie van Binnenlandse Zaken in de uitvoering van zijn opdracht ondersteuning vanuit zijn eigen afdeling voor wetenschappelijke ontwikkeling, wat een investering inhoudt van ongeveer 65 miljoen euro op jaarbasis.” (Masson en Marta, 2011: 113)

Dit is duidelijk geen volledig overzicht van alle uitgaven voor veiligheidsonderzoek in de lidstaten. Maar indien, zoals punt 3.4 suggereert, zowel defensie- als andere bedrijven hun onderzoek moeilijk gefinancierd krijgen en daarvoor in grote mate afhankelijk zijn van overheidsgeld, dan lijkt alles erop te wijzen dat een verhoudingsgewijs klein aantal landen in onderzoek en ontwikkeling investeert. Wat bijvoorbeeld opvalt, is dat tot de EU een initiatief nam inzake veiligheidsonderzoek enkel Zweden en Oostenrijk voor het onderzoek naar - en de ontwikkeling van - veiligheidsproducten een bijzondere financiering voorzagen, en dit ondanks de hoge instapkosten voor de bedrijven die de markt wensen te betreden.

Het Europees Defensieagentschap heeft sinds zijn oprichting geprobeerd om samenwerkingsverbanden rond onderzoek en ontwikkeling te ondersteunen. Uit onderstaande tabel blijkt echter dat het opnieuw minder actief is op dit vlak, en dat het EDA het niet veel beter doet dan de gezamenlijke inspanningen van de West-Europese Bewapeningsgroep (WEAG).

Tabel 3: EU-uitgaven onderzoek en technologie in samenwerkingsverband (in miljoen euro)

Jaar	Bedrag
2005	206
2006	254
2007	332.75
2008	412
2009	290
2010	246

Bron: Europees Defensieagentschap

Dit lijkt erop te wijzen dat de Europese Commissie het moeilijk zal hebben om lidstaten meer te laten participeren in samenwerkingsverbanden rond veiligheidsonderzoek die niet binnen de EU-kaderprogramma's voor onderzoek en andere EU-financieringsinstrumenten vallen.

3.3.2 Kan men veiligheids- en defensietechnologieën onderscheiden?

In Europa en wereldwijd zijn er verschillende taxonomieën in gebruik om technologieën te identificeren, bijvoorbeeld die van het Europees Defensieagentschap (EDA), de West-Europese Bewapeningsgroep (WEAG), de Europese Adviesraad voor veiligheidsonderzoek (EAVO), de Militarily Critical Technologies List (MCTL) en de Developing Science and Technologies List (DSTL). Het STACCATO-project (platform van belanghebbenden voor het in kaart brengen van de toeleveringsketen, analyse van marktvoorwaarden en technologische opportuniteiten) heeft gepoogd om wat WEAG en EAVO hebben gedaan samen te brengen tot een taxonomie waarvan zowel vraag- als aanbodzijde gebruik zou kunnen maken.¹ De taxonomie moest niet enkel dienen om gebruikte technologieën in kaart te brengen en te vernemen hoe deze in de apparatuur kunnen worden geïntegreerd, maar ook hoe de vereisten van door EU-beleid gedefinieerde missies konden worden geclassificeerd. De zeven secties zijn:

¹ De hele taxonomie is terug te vinden op: http://www.asd-europe.org/site/fileadmin/user_upload/STACCATO_final_taxonomy.pdf

- (I) Technologieën en onderdelen
- (II) Apparaten en subsystemen
- (IIIA) Systeem- en servicefuncties
- (IIIB) Ontwerp en fabricage
- (IV) Geïntegreerde platformen en systemen en menselijke factoren
- (VA) Mogelijkheden tijdens missies
- (VB) Beleid en ondersteuning

Naderhand heeft het Gemeenschappelijk Centrum voor Onderzoek nog een poging ondernomen, een overzicht samen te stellen van de technologieën die bedrijven in handen hebben om tijdens missies meer mogelijkheden en ondersteuning te bieden. Maar omdat ondernemingen niet verplicht waren deel te nemen, heeft dit weinig resultaat opgeleverd. De STACCATO-taxonomie werd ook verweten onvoldoende aandacht te besteden aan veiligheidstechnologieën die door niet-defensieleveranciers waren aangeleverd. Wat problematisch is als er meerdere taxonomieën of classificaties in gebruik zijn, is dat het soms moeilijk is (zeker tijdens onderhandelingen over wapenbeheersing/-export) om te bepalen hoe een specifieke technologie moet worden geclassificeerd.ⁱ

Vast staat dat de scheidslijn tussen aan eindgebruikers in defensie en veiligheid geleverde militaire en niet-militaire producten enigszins is vervaagd. Deels heeft dit te maken met enige convergentie in hun missies. Zo hebben de bestrijding van opstanden en terrorismebestrijding wel wat gemeen, maar speelt ook de dynamiek van technologische innovatie hier een rol. We moeten dit echter ook niet overdrijven. Hoewel sommige producten nuttig zijn voor zowel militaire als niet-militaire gebruikers, denken we dan bijvoorbeeld aan beveiligde communicatiesystemen en bewakingstechnologieën zoals onbemande luchtvaartuigen en sensoren, blijft de kloof tussen militaire en niet-militaire producten toch erg groot.ⁱⁱ Vliegdekschepen, gevechtsvliegtuigen en geavanceerde rakettechnologie blijven eenduidig militaire producten. Een raketfabrikant als MBDA zal zich wellicht niet op de veiligheidsmarkt wagen, net omdat zijn technologieën hem daar van weinig nut zullen zijn. Stankiewicz et al (2009) benadrukken dat deze scheidslijn zal blijven bestaan. Ministeries zullen immers proberen om de controle over en de investeringen in bepaalde defensietechnologieën te behouden, dit om redenen van nationale veiligheid en continuïteit van de voorziening. De verschillen zijn kleiner in de technologieën ter ondersteuning van de producten. Indien we van oordeel zijn dat de STACCATO-technologieclassificaties interessant zijn voor veiligheids- en defensiegebruikers, dan argumenteert James (2009a: 7) dat er nog verschillende technologiecategorieën zijn die “in essentie specifiek voor defensie zijn bedoeld en in andere domeinen beperkt (of niet) inzetbaar zijn (namelijk 102 – Afschrikingsmaterialen; 103 – Stealthmaterialen en technologieën; en 105 – Energetische materialen).”ⁱⁱⁱ De meerderheid van de producten voor defensie en civiele veiligheid is echter op een ruime waaier generische technologieën gebaseerd.

ⁱ Er zijn al datamining-technieken ingezet om dit op te lossen. Zie bijvoorbeeld Thorleuchter en van den Poel (2011).

ⁱⁱ Overlapping zien we ook op niet-technologische domeinen, bv. uniformen, beschermende kleding, logistiek, enz.

ⁱⁱⁱ Eén in januari 2012 geïnterviewde vertegenwoordiger van de industrie opperde dat de overlapping tussen veiligheids- en defensietechnologieën zoals aangeduid in de Staccato-taxonomie mogelijk overdreven was. De deelnemers aan het onderzoek kwamen immers uit de defensiesector. Mogelijk had de oefening met deelnemers van telecommunicatie- of ICT-bedrijven andere resultaten opgeleverd.

3.3.3 Innovatieve technologieën en de veiligheids- en defensiesector

Terwijl men er tijdens de Koude Oorlog van uitging dat defensietechnologieën baanbrekend waren, en dat er zonder gevaar voor de technologieën zelf commerciële toepassingen uit voortkwamen, luidt de visie van Stankiewicz et al (2009: 21) vandaag als volgt:

"Niemand is vandaag nog zelfvoorzienend. Dit geldt voor ondernemingen, industrietakken, sectoren en landen. De verticaal geïntegreerde technisch-militaire complexen zijn niet meer de beveiligde plaatsen waar de meest relevante technologieën hun oorsprong vinden. Producten voor defensie en civiele veiligheid maken intensief gebruik van generische, overal verkrijgbare technologieën, niet in de laatste plaats informatie- en communicatietechnologieën (ICT). De geboekte vooruitgang in microsystemen, nanotechnologie, onbemande systemen, communicatie en sensoren, digitale technologie, bio- en materiaalwetenschap bleek telkens belangrijk voor de defensiesector. De meeste, indien niet al deze technologieën kunnen als generisch worden beschouwd."

Het model van innovatieve defensie dat tijdens de Koude Oorlog gold, is dus in verval. Vertegenwoordigers uit de industrie waren tijdens gesprekken in januari 2012 graag bereid toe te geven dat defensiebedrijven de innovatie al geruime tijd niet meer trokken. Gezien het feit dat zowel militaire als niet-militaire producten van generische technologieën vertrekken, doet dit de grenzen van zowel kenniscreatie als de toepassing van de technologieën vervagen, niet enkel tussen militaire en niet-militaire veiligheidsproducten, maar ook ten opzichte van de ruimere innovaties in civiele en commerciële technologieën (James, 2009b). Ook het feit dat veel defensie- en veiligheidsproducten van commercieel verkrijgbare technologieën gebruik maken, en dan vooral ICT-technologieën, betekent dat ook vijandige gebruikers daarover kunnen beschikken als zij daarvoor de nodige systeemintegratiecapaciteiten in hun bezit hebben of aankopen. Europese systeemintegratiecapaciteiten en de bescherming daarvan zullen daarom uiteindelijk misschien belangrijker worden dan de technologieën op zich. Respondenten uit de industrie wezen in januari 2012 op het feit dat dit weer nieuwe dilemma's rond de continuïteit van het aanbod opwerpt. Microchips bijvoorbeeld zijn cruciaal voor veel van de huidige defensieproducten, maar de frequentie en de hoeveelheden waar defensiebedrijven in Europa om vragen zijn te laag om voor leveranciers in Azië en Noord-Amerika een interessante afzetmarkt te zijn. Diegenen die zich zorgen maken over de proliferatie van defensie- en veiligheidstechnologieën staan aldus ook voor nieuwe uitdagingen. We kunnen daarmee besluiten dat het niet zozeer een kwestie is van vervagende grenzen tussen defensie- en veiligheidsproducten, maar eerder dat zij beide vertrouwen op generische technologieën, waardoor het tegenover vroeger moeilijker wordt ze te beschermen.

3.4 Aanbodzijde

3.4.1 Hoe defensiebedrijven de veiligheidssector benaderen

Beslist niet alle defensiebedrijven benaderen de veiligheidssector op eenzelfde manier, maar wanneer we de structuur van de industriële defensiesector opdelen per categorie producenten, wordt het toch mogelijk enkele algemene lijnen te onderscheiden. De industriële defensiesector heeft de vorm van een piramide. Helemaal bovenaan staan de systeemintegratoren zoals BAE, EADS, Thales en Finmeccanica, met de gespecialiseerde fabrikanten van subsystemen daar net onder. Onderaan bevindt zich een grote groep leveranciers van onderdelen en diensten die in

onderaanneming werken voor de hogere niveaus en vaak KMO's zijn.^I Misschien onverwacht, maar na een periode van terugval na het einde van de Koude Oorlog doen veel Europese defensiebedrijven het erg goed. Sinds 2003 is de tewerkstelling in de ruimtevaart- en de defensie-industrie gestaag gegroeid. Ook de defensiesector, en dan zeker die van de landmacht, stelt heel wat mensen tewerk, dit terwijl nog altijd ruime winsten worden geboekt. Deels is dit te verklaren doordat landen als Duitsland en Nederland de tewerkstelling in de sector via andere statistische modellen berekenen, maar de voornaamste reden is de bestendige exportgroei naar vooral Azië en het Midden-Oosten (ASD-Europe, 2010).^{II} Door de financiële crisis en de besparingsmaatregelen ziet de toekomst in Europa er minder rooskleurig uit. Het punt dat we hier echter willen maken is dat de defensiesector zich niet gedwongen zag om de veiligheidsmarkt te betreden, maar dat bedrijven dit onder hun eigen voorwaarden hebben kunnen doen. Elke onderneming heeft dan ook haar eigen strategische berekeningen kunnen maken. Vertegenwoordigers van de defensiesector gaven tijdens gesprekken in 2012 aan dat, toen de VS rond 2003 aankondigde gelden vrij te maken voor haar 'homeland security'-programma, defensiebedrijven aanvankelijk dachten dat dit nieuwe marktsegment hen heel wat commerciële opportuniteiten zou bieden. Maar aangezien de vraag vanuit Europese overheden uiteindelijk onder de verwachtingen bleef, zijn deze vooruitzichten nooit bewaarheid geworden.

Defensiebedrijven hebben drie mogelijkheden om de veiligheidsmarkt te betreden; ten eerste kunnen zij via hun bestaande defensietechnologieën een plaats trachten te verwerven; ten tweede kunnen zij diversifiëren door de overname van beveiligingsfirma's; en ten derde kunnen zij zich via partnerschappen toegang tot de markt verschaffen. Volgens IRIS et al (2010: 143-44) echter kunnen defensiebedrijven de veiligheidsmarkt enkel met succes benaderen op voorwaarde dat aan drie businessvoorwaarden is voldaan:

- Technologieën die in de ogen van veiligheidsklanten waardevol en kenmerkend zijn, en die een commercieel voordeel te bieden hebben in vergelijking met het aanbod van niet-defensiebedrijven. (Opgelet: sommige defensiebedrijven beschikken over technologieën die vlotter naar verschillende sectoren te diversifiëren zijn.)
- Toegang tot de vereiste aanvullende capaciteiten – hier stellen zij dat defensiebedrijven het nadeel dat zij nieuwe klanten moeten zoeken, dienen te compenseren (eventueel door de overname van bedrijven die al actief zijn in de sector).
- Haalbaar business model dat aanvaardt dat de veiligheidssector anders werkt dan de defensiesector en dat de verschillende overheadkosten, investeringsbehoeften en reglementeringen realistisch inschat.

In punt 3.5 gaan we verder in op de verschillen in cliënteel, bedrijfsklimaat en reglementering.

Laat ons even bekijken hoe de systeemintegratoren zich op de veiligheidsmarkt hebben ingesteld. In de eerste plaats hebben zij allen een aantal kleine firma's overgenomen zoals blijkt uit onderstaande tabel).^{III}

^I Veel ondernemingen doen zich dan wel voor als defensiebedrijven maar zijn vooral civiel actief, met name in de luchtvaartsector. Mensen uit de sector die we in 2012 spraken, suggereerden dat het verschil in bedrijfsactiviteiten eerder langsheen een civiel-militaire dan een defensie-veiligheidsgrens liep.

^{II} Deze statistieken gaan niet over leveranciers voor wie defensie geen prioriteit is. In de toeleveringsketen zijn dit heel wat bedrijven.

^{III} Verschillende respondenten lieten in januari 2012 uitschijnen dat met name defensiebedrijven wel eens KMO's hadden overgenomen om aan te vereisten te voldoen voor deelname aan het programma voor veiligheidsonderzoek (nl. geografisch evenwicht en KMO-participatie.)

Tabel 4: grote overnames door Europese defensiebedrijven 2005-10

Bedrijven	Datum	Overnames	Domeinen
EADS	2005	Professionele mobiele radioactiviteiten (PMR) van Nokia	Beveiligde telecommunicatie
	2006	Franse onderneming Sofrelog	Systemen voor scheepsverkeersdiensten (VTS) en kustbewakingssystemen (CSS)
	2008	Amerikaanse PlantCML	Noodoproep-oplossingen en -diensten
	2010	EADS DS en Atlas Elektronik (AE) hebben besloten hun marktpositie in maritieme beveiliging en veiligheid te consolideren via een fusie van hun filialen Sofrelog en Atlas Maritime Security, een spin-off van AE, waaruit "Sofrelog Atlas Maritime Security" (SA Maritime Security) is ontstaan	
Thales	2007	Afdeling spoorwegsignalisatie en veiligheidssystemen overgenomen van Alcatel-Lucent	
	2008	Brits bedrijf n-Cipher	Encryptie (systeembeveiliging van internet en communicatie)
Safran	2008	Nederlands bedrijf Sdu-Identification	Beveiligde identificatiedocumenten, onder andere elektronische en biometrische paspoorten, identiteitskaarten en rijbewijzen
	2009	Biometrieactiviteiten van Motorola USA	Merk Printrak. Automatisch vingerafdrukidentificatiesysteem (AFIS)
	2009	81% van Amerikaanse GE Homeland Protection	Systemen om gevaarlijke of illegale materialen te detecteren (detectiesystemen met röntgentomografie). Deze technologie wordt vaak ingezet bij controles op luchthaven.
Finmeccanica	2007	Britse VEGA Consulting Services Ltd (VEGA)	Projectbeheer en geavanceerde oplossingen voor simulatie en training
	2008	Amerikaanse DRS Technologies	VTMS, havenbeveiliging, ordehandhaving, grensbewaking; onderaannemer van Boeing voor SBInet
BAE Systems	2008	Britse DETICA	Technologieën voor analytische beslissingsondersteuning, realtime omgevingsbewustzijn en controle, beveiligde gegevensverwerking en communicatie (terrorisme- en fraudebestrijding)
	2000-2009	Meer dan tien Amerikaanse overnames in de IT-sector, in defensie-elektronica en bewapening van de landmacht	

Bron: Masson en Marta (2011: 122)

Een overname die recent in het oog sprong maar niet in dit overzicht is opgenomen, was in 2010 die van de biometrische, identiteits- en controleafdelingen van L-1 Identity Solutions ter waarde van ongeveer 1 miljard euro door de Franse defensie- en luchtvaartgroep Safran. Hierdoor werd Safran de wereldleider in biometrische identificatie. Ook BAE heeft in 2010 haar positie op de veiligheidsmarkt verstevigd door de overname van L-1 Intelligence Services Group en OASYS Technology, een onderdelenproducent voor bewakings- en verkenningstoepassingen. De golf van overnames lijkt sinds kort te zijn afgezwakt.

Maar hoewel dit een eenduidig verhaal lijkt te zijn, bestaan er grote verschillen tussen de bedrijven onderling. Thales had al een veiligheidsafdeling die ze sindsdien heeft geconsolideerd door extra overnames te doen. Het bedrijf ontwikkelt vooral technologieën voor bewakingsdoeleinden, identiteitscontrole, inlichtingendiensten en voor de bescherming van kritieke infrastructuur en stond daarom sterk om contracten binnen te halen. Het hanteert een strategie van dual-use technologieën. IRIS et al (2010) wijzen erop dat Thales, in tegenstelling tot zijn concurrenten, veiligheid als een kernactiviteit beschouwt. In 2008 was de afdeling goed voor 25% van de omzet en daarmee is de onderneming misschien een buitenbeentje onder de Europese integratoren van defensiesystemen. Het Franse Safran is ook interessant, hoewel het een leverancier is van subsystemen. Het is prominent aanwezig op de veiligheids- en de defensiemarkt, maar onderscheidt zich van zijn concurrenten doordat het zijn veiligheidsactiviteiten heeft trachten af te splitsen van zijn werk als defensieproducent om zo een doelgerichte groeistrategie om te zetten. Safran is eigenaar van Morpho, vroeger onder de naam Sagem Sécurité actief en wereldleider in biometrische technologieën. Zoals IRIS et al (2010) meldden, gonsde het in 2009-10 van de geruchten dat Thales en Safran onderhandelden over een eventuele ruil van hun veiligheids- en defensieactiva. Thales zou zich dan gaan toeleggen op defensie en Safran op veiligheid. Doel was om daarmee de dubbele onderzoeksinspanningen te beperken. Deze gesprekken sprongen af in 2010. En ondanks druk van de Franse regering leidde ook een volgende onderhandelingsronde in november 2011 over een swap van avionics- en optronicsactiviteiten door syndicale druk over de tewerkstelling tot niets.¹

EADS heeft een eigen defensie- en veiligheidsafdeling (Cassidian) maar tot dusver haalt het zijn omzet geheel uit niet-defensiecontracten. Daarbij blijft alle focus op zijn traditionele civiele en militaire producten liggen. Het mag dan wel pogingen ondernemen om zijn geïntegreerde communicatietechnologieën op de veiligheidsmarkt te lanceren, en dan vooral buiten de EU, tot op heden worden de producten vooral militair ingezet. Cassidian zag een groeipotentieel in orderhandhaving, cyberbeveiliging en bewakingsdrones (IISS, 2012). Het heeft meegewerkt aan het programma voor veiligheidsonderzoek en zal zich dan ook sterk kunnen profileren, zou de EU-markt voor veiligheidsproducten aantrekken (IRIS et al, 2010). EADS maakte in 2011 echter vooral indruk met de overname van Vector Airspace en Satair. In beide gevallen zal dit de positie versterken van haar support- en serviceafdeling, een domein dat volgens EADS winstgevend en anticyclisch is. Ook Finmeccanica heeft zich met zijn defensietechnologieën in de veiligheidssector trachten in te kopen. Dit verliep echter niet vlot door de slabakkende vraag naar zowel defensie- als veiligheidsproducten in het eigen Italië. Bovendien had het bedrijf de geconsolideerde vraag in de EU te optimistisch ingeschat. Voor zijn veiligheidsactiviteiten heeft het zich dus vooral op de export buiten de EU moeten richten. Ondanks het feit dat Finmeccanica op papier een indrukwekkend veiligheidsportfolio heeft, vonden IRIS et al (2010) dat het veiligheidsaspect, de exportcontracten niet te na gesproken, licht doorwoog in het totale activiteitenpakket. Finmeccanica heeft zich graag bereid getoond om EU-activiteiten in de industriële veiligheidssector te begeleiden, vooral dan het programma voor veiligheidsonderzoek. BAE daarentegen is niet actief geweest op EU-niveau maar heeft zich vooral gefocust op het binnenhalen van veiligheidscontracten op zijn Britse en Amerikaanse thuismarkten. Daar heeft het zijn troeven uitgespeeld door zich vooral op information-based systemen voor inlichtingendiensten toe te spitsen. Defensie blijft evenwel de voornaamste opdracht. EADS en BAE houden goed stand op hun klassieke markten. Dit maakt dat ze weliswaar oog hebben voor de veiligheidsmarkt, maar dat deze geen prioriteit krijgt.

Wanneer we tweede- en derdelijns-defensieproducenten bekijken, krijgen we vaak een wazig beeld. Vooral in de IT-sector en in defensie-elektronica konden bedrijven, mits overname van

¹ <http://www.reuters.com/article/2011/12/13/thales-safran-idUSWEA540420111213>

enkele kleinere ondernemingen, zonder al te veel moeite zo goed als hetzelfde product bij zowel veiligheids- als defensieklanten aan de man brengen. Heel succesvol op dit vlak was bijvoorbeeld Smiths Detection dat deel uitmaakt van Smiths Group en zich specialiseert in opsporings- en screeningstechnologieën. Voor anderen, raketfabrikanten bijvoorbeeld, heeft de nieuwe veiligheidsmarkt dan weer weinig te bieden. Of neem nu de Duitse firma Diehl (die recent besloot zich in de civiele ruimtevaartindustrie in te kopen), die meer heil ziet in alternatieve diversificatiestrategieën. Voor de derdelijns-leveranciers bepaalt het product weer sterk of er al of niet een duidelijke afscheiding bestaat. Maar sowieso zijn de meesten niet enkel actief op de defensiemarkt.

Een respondent van het Europees Defensieagentschap liet in januari 2012 optekenen dat indien de veiligheidssector bevolkt zou worden door klanten van vergelijkbare omvang als die op de defensiemarkt, daar vooral de alom bekende defensiebedrijven een sterke positie zouden kunnen verwerven. Ze hebben goede contacten bij de overheid, weten hoe ze aanbestedingen moeten binnenhalen en beschikken in veel gevallen over relevante technologieën. Toch is dit nog geen garantie op succes. De defensiesector kreeg voor het eerst een grote opdracht toegewezen met de keuze in 2007 voor Raytheon als voornaamste leverancier voor het Britse E-Borders-programma rond geavanceerde grensbewaking en -beveiliging. Gemiste deadlines en ondermaats werk deden de Britse regering echter in 2010 besluiten, het contract op te zeggen. Momenteel daagt Raytheon de Britse regering voor de rechter (Curtis, 2011). Defensiebedrijven aarzelen ook om grote opdrachten aan te gaan zolang er geen akkoord is over de aansprakelijkheid, zouden hun systemen niet werken.

3.4.2 Niet-defensiebedrijven en hoe zij de veiligheidssector benaderen

Ecorys et al (2009) maakten op de veiligheidsmarkt onderscheid tussen drie soorten niet-defensieleveranciers: de traditionele beveiligingsbedrijven enerzijds, die algemene beveiligingstoepassingen aanleveren, bv. beschermende kleding, toegangscontrole, branddetectie, CCTV, en nieuwe spelers anderzijds, ofwel uit andere civiele industrietakken die hun technologieën tot veiligheidstoepassingen ombouwen (vooral ICT en telecommunicatie) ofwel hoogtechnologische opstartende bedrijven. Ecorys et al (2009) zien in de bovenlaag van de 'nieuwe veiligheidsmarkt', die de steun krijgt van het EU-programma voor veiligheidsonderzoek, echter betrekkelijk weinig traditionele beveiligingsbedrijven actief zijn, met uitzondering van enkele domeinen van bewakingstechnologieën. Misschien is het geen verrassing dat traditionele veiligheidsleveranciers zich niet echt roeren. Hun markt is er een van producten met een korte of middellange levensduur, privaat gefinancierde O&O, een erg gefragmenteerde vraag en lage instapkosten die vooral naar productie gaan. Het heeft er alle schijn naar dat het nieuwe segment heel verschillend zal zijn. ECORYS et al (2009) wezen erop dat de vraagzijde van dit bovenste marktsegment maar door een beperkt aantal klanten wordt bevolkt. Meestal zijn dit nationale overheden, aangezien zij de enigen zijn die de producten legitiem mogen gebruiken. Aangezien hun vraag erg specifiek is, doet zich daar in de levering van veiligheidsmaterieel ook een desbetreffende concentratie voor. Verder stelden zij dat in het topsegment van de nieuwe veiligheidsmarkt de instap moeilijk verloopt, gezien de aanzienlijke hindernissen te wijten aan

- de hoge investeringskosten voor technologische ontwikkeling en vervolgens voor de commercialisering (dit is ook een bekommernis voor defensiebedrijven, hoewel zij natuurlijk vertrouwd zijn met heel andere O&O-financieringsmodellen dan wat niet-defensiebedrijven hanteren).

- de hoge kosten om een marktpositie te verwerven (lobbyen, marketing en contacten op overheidsniveau) – volgens ECORYS et al (2009: iv) speelt hierbij ook de nood om klanten ‘op te leiden’ in technologische mogelijkheden en keuzes in plaats van gebruiksklare technologie te verkopen aan voornamelijk niet-overheidsklanten, wat zulke bedrijven beter gewend zijn.

Hoewel er dus behoorlijk wat KMO's de sector bevolken, vechten zij allemaal voor marktaandeel.¹ En wanneer ze dan een technologie ontwikkelen, worden ze dikwijls overgenomen door de grote systeemintegratoren of verkopen ze hen hun licentie om de technologie te ontwikkelen. Aan de andere kant van het commerciële spectrum kampen niet-defensiebedrijven met andere woorden met gelijkaardige problemen als defensiebedrijven. Dit betekent niet dat niet-defensiebedrijven in het nieuwe marktsegment altijd in het nadeel zullen zijn. IRIS et al (2010) halen het voorbeeld aan van een Brits contract voor een nationaal radiosysteem voor hulpdiensten. In plaats van dat een consortium geleid door defensiebedrijf EADS de opdracht in de wacht sleepte, ging deze naar het O2 Airwave-consortium onder leiding van telecommunicatiebedrijf BT. ECORYS et al (2009) merkten evenwel op dat bedrijven afkomstig uit de civiele markt maar belangrijke spelers waren in een klein aantal sectoren. Een voorbeeld is Motorola, dat gespecialiseerd is in beveiligde communicatie.

De meeste studies over de sector kijken daarom vooral naar de rol van defensiebedrijven, deels omdat zij op de meer ontwikkelde Amerikaanse veiligheidsmarkt eerste viool spelen, deels wegens de manier waarop het beleidsdomein binnen de EU vorm heeft gekregen (deel 4 zal daar dieper op ingaan). Het is best mogelijk dat niet-defensiebedrijven moedwillig werden uitgesloten van de voorbereidende onderhandelingen over de toenemende EU-aanwezigheid in de veiligheidssector. Bigo en Jeandesboz (2010) besluiten bijvoorbeeld dat *“leidende defensie- en veiligheidsbedrijven een centrale rol hebben gespeeld om een richting aan te geven en prioriteiten op te stellen voor het Europese onderzoeks- en ontwikkelingsbeleid inzake veiligheidsgerelateerde systemen.”* Dit neemt evenwel niet weg dat niet-defensiebedrijven zich een heel andere werkwijze eigen zullen moeten maken indien, zoals de Europese Commissie hoopt, sterke overheidsklanten zich gaan roeren. Voor sommige niet-defensiebedrijven die de defensiemarkt hebben betreden, is dit niet eenvoudig gebleken. Door de nieuw opgerichte Airbus-dochter Airbus Military Company de A400M transporter te laten bouwen, vertrouwde men op de commerciële ervaring die Airbus had met de bouw van burgerluchtvaartuigen om de aanbesteding vlot te laten verlopen. Het probleem was dat Airbus nog nooit een militair vliegtuig had gebouwd, veel van zijn middelen moest inzetten op problemen met zijn grootste burgerluchtvaartproject en de risico's van het project volledig had onderschat (Masseret en Gauthier, 2009: 46-8). Afgezien van bepaalde ICT- en communicatiesectoren lijkt het er momenteel tenminste op dat niet-defensiebedrijven in het nadeel zijn.

3.4.3 Opkomende trends?

Algemeen heerst vandaag de indruk dat de grote defensiebedrijven zich op de veiligheidsmarkt hebben gepositioneerd, sommige met meer overtuiging dan anderen, maar dat ze wachten tot de vraag in de EU echt aantrekt. Tot dusver is die van overheidswege echter betrekkelijk beperkt gebleven, om niet te zeggen nog gekrompen. Masson en Marta (2011) stellen dat a) de huidige veiligheidscontracten tegenover defensieopdrachten klein uitvallen, b) de meerderheid van de

¹ Masson en Marta (2011) stellen dat opstartende innovatoren, ontwikkelaars en leveranciers van nieuwe veiligheidstechnologieën volgens de European Security Directory 2009 heel actief zijn op het vlak van veiligheid. Er zouden zowat 668 KMO's op een of andere manier bij betrokken zijn via EU-beleidsacties, vakorganisaties en registratie in de directory. In een casestudy over Nederland maakt Akkermann (2012) ook melding van een uitgebreide interesse onder kleinere Nederlandse ondernemingen.

bestaande grote contracten afloopt en er zich geen nieuwe aandienen (sommige grootschalige opdrachten hebben politiek ook heel wat controverser opgeroepen, vooral dan in het VK voor wat identiteitskaarten en e-grenzen betreft); en c) zij dikwijls verband houden met specifieke evenementen zoals de Olympische Spelen in Londen of er komen naar aanleiding van een natuurramp. De ruime aandacht die het dossier rond G4S heeft gekregen, dat niet in staat bleek om de veiligheid voor de Olympische Spelen in Londen te verzorgen, heeft ook geleid tot twijfels of de overheid beveiligingsfuncties wel aan de privésector zou moeten uitbesteden. Dit maakt dat de veiligheidssector momenteel niet veel inkomsten genereert, met uitzondering van die spelers die klaarstonden om in te spelen op de vraag naar bewakings-, screening- en identiteitstechnologieën. Sommige grote defensiebedrijven richten hun aandacht daarom verder op defensieactiviteiten, terwijl anderen uit noodzaak buiten de EU zijn gaan exporteren. Iedereen neemt daarin zijn eigen beslissingen, maar veel hangt ook af van hoe gezond of ongezond hoog de defensie-uitgaven op de binnenlandse markt oplopen.

Behalve in communicatie en ICT nemen niet-veiligheidsbedrijven blijkbaar een minder benijdenswaardige positie in. Voor een deel is dit te wijten aan bepaalde EU-beleidsbeslissingen en deels aan de vele KMO's die maar moeilijk aan de marktvoorwaarden kunnen voldoen. Nog een ontwikkeling die mogelijk positief zal uitdraaien voor defensiebedrijven, is dat de Europese Commissie het programma voor veiligheidsonderzoek heeft aangewend om een samenwerking aan te gaan met het Europees Defensieagentschap. Het EDA en de Commissie zijn met name trots op twee projecten.

- Software Defined Radio, dat toepassingen heeft voor zowel militair gebruik als voor hulpdiensten (politie, brandweer en dergelijke).
- een project over de inzet van onbemande vliegtuigen in de burgerluchtvaart. (James, 2009a)

Deze ad-hoc samenwerking heeft de Europese ministers van Defensie in mei 2009 doen beslissen om het Europees Defensieagentschap op te dragen, samen met de Europese Commissie een Europees samenwerkingskader voor veiligheids- en defensieonderzoek in te richten, met de bedoeling te komen tot een *“maximale complementariteit en samenwerking tussen onderzoeksactiviteiten met het oog op defensie en de veiligheid van burgers”*. Volgens het EDA is omgevingsbewustzijn (sensorechnologieën, bediening en controle van netwerkkassets) een domein waar samenwerking mogelijk is (James, 2009a). Ook zijn er gesprekken aan de gang over de mogelijkheid om defensieonderzoek op te nemen in het achtste Kaderprogramma. Al deze ontwikkelingen zullen wellicht tot een ruimere capaciteit op de nieuwe veiligheidsmarkt leiden, waar defensiebedrijven in de meeste maar niet in alle veiligheidssectoren goed geplaatst zijn en enkel succesvol kunnen zijn als de geconsolideerde vraag aantrekt. Blijft de vraag gefragmenteerd, dan zijn niet-defensiebedrijven en zelfs KMO's misschien wel in het voordeel.

3.5 Vraagzijde

Zoals reeds eerder besproken is de aard van de vraag in de sectoren traditionele veiligheid, nieuwe veiligheid en defensie heel belangrijk om te bepalen hoe de aanbodzijde zal worden opgebouwd en hoe onderzoek en ontwikkeling in het nieuwe marktsegment kunnen worden gefinancierd. De gefragmenteerde aard van de Europese vraag leidt onveranderlijk tot kritiek. Is deze kritiek terecht en zou het de nieuwe veiligheidssector goed uitkomen indien daar dezelfde militaire of defensiekanten zouden worden bediend? Dit onderdeel schetst kort de voornaamste gebruikersgroepen van veiligheids- en defensieproducten, vraagt zich af in hoever er in het huidige

veiligheidsbeleid onduidelijkheid is ontstaan over de rollen en vereisten en bespreekt vervolgens hoe de civiele en de militaire overheidsklant andere reglementen, aankoopprocedures en behoeften hanteert.

3.5.1 Voornaamste gebruikersgroepen van en vereisten voor defensie- en veiligheidstechnologieën: vervaagd of verschillend?

Beweringen dat de scheidslijnen tussen defensie en veiligheid of meer bepaald tussen interne en externe veiligheid voor gebruikers van deze technologieën zijn vervaagd, worden vaak gevoed door de premisse dat hun missies met elkaar verweven zijn geraakt. Zoals IRIS et al (2010) aangeven, hebben crisisbeheeroperaties tegenwoordig vaak niet enkel een militair karakter. In het geval de interventie doorloopt tot in de postconflictfase, dragen civiele dan wel ngo-missies dikwijls bij aan het herstel van het politieapparaat, de administratieve diensten en de rechtsorde of begeleiden ze de hervorming van de humanitaire en de veiligheidssector. Ook legerpersoneel zal in sommige gevallen bepaalde interne-veiligheidsmissies ondersteunen, bijvoorbeeld operaties in de strijd tegen het terrorisme, meewerken aan de bescherming van burgers, bescherming van kritieke infrastructuur en grensbewaking.¹ Welke rol een krijgsmacht al of niet mag opnemen, is vaak grondwettelijk bepaald en verschilt dus van het ene EU-land tot het andere. Maar de scheidslijn tussen militaire en civiele functies is ontegensprekelijk vaag, iets wat nog meer geldt in landen met een paramilitair apparaat (bv. Rijkswacht).

De overlapping gaat verder dan een 'doelverschuiving' – indien militaire en civiele machten moeten samenwerken aan gezamenlijke operaties, dan vereist dit natuurlijk een zekere interoperabiliteit, hetzij op het vlak van training, communicatieapparatuur hetzij door een integratie van de commandostructuren. Verwijzend naar deze studie krijgt deze overlapping echter misschien een interessantere dimensie, namelijk wanneer civiel en militair personeel voor gelijkaardige opdrachten gebruikmaken van vergelijkbare technologieën, maar dan wel in een heel andere omgeving. Onbemande luchtvaartuigen bijvoorbeeld zijn van doorslaggevend belang geweest in militaire operaties, vooral om in Afghanistan en Pakistan gericht doelwitten uit te schakelen, maar kunnen onbewapend ook nuttig zijn om politietaken uit te voeren (zoals observaties van voetbalsupporters). Nog een voorbeeld zijn Trojaanse paarden of andere malware: bekend daarin is Stuxnet, dat is gebruikt om het Iraanse nucleaire programma te saboteren. Blijkt echter dat ook de Duitse politie malware op pc's van haar eigen burgers installeerde, met de bedoeling hen te bespioneren.² IRIS et al (2010) besloten dat er op volgende domeinen sprake was van een functionele vervaging:

- detectie, identificatie en authenticatie
- omgevingsbewustzijn en -bewaking
- risicoanalyse en -berekening
- communicatie
- informatiebeheer
- positionering en lokalisatie

Na de bomaanslagen in Londen op 7 juli 2005 kwam er kritiek op het feit dat de communicatie tussen de hulpdiensten moeilijk was verlopen. Waarom zijn er, ondanks de gedeelde

¹ Omdat G4S onvoldoende veiligheidspersoneel had kunnen opleiden, moest het Britse leger zelfs tussenbeide komen om de veiligheid tijdens de Olympische Spelen in Londen te verzekeren.

² Dit is overal op het internet verschenen. Een betrouwbare bron is de blog van het magazine New Scientist: <http://www.newscientist.com/blogs/onepercent/2011/10/german-hackers-find-possible-g.html>

gebruiksmogelijkheden, dan niet meer gezamenlijke aankopen gedaan? Waarom blijft de vraag dermate gefragmenteerd?

3.5.2 Civiele en militaire klanten: verschillen in aankoopprocedures en behoefteomschrijving onoverbrugbaar groot?

Ten eerste is het belangrijk te benadrukken dat terwijl het ministerie van Defensie (ondanks spanningen tussen verschillende diensten) in eigen land altijd de enige militaire klant is, interne-veiligheidsklanten heel wat gevarieerder zijn. Om te beginnen zijn zij niet allen op nationaal niveau terug te vinden: vaak zijn het regionale en lokale operatoren die veiligheidsfuncties op zich nemen, dikwijls met een ruime autonomie en eigen budgetten. Bovendien zijn veiligheidsklanten, hoewel zij in dit rapport niet centraal staan, niet altijd overheidsdiensten. Commerciële en private klanten kunnen grote infrastructuurexploitanten zijn (zoals energieleveranciers, luchthavenuitbaters), maar ook kleine particulieren. Sommige van deze privéklanten, met name dan diegenen die kritieke infrastructuur beheren, zullen betrokken moeten worden in rampenplannen van de overheid. Dit maakt het, zelfs wanneer er nog geen militaire klanten in het spel zijn, erg moeilijk om een gezamenlijke aankoop te doen. Iets dergelijks grensoverschrijdend organiseren wordt nog gecompliceerder gezien de verschillende manieren waarop EU-lidstaten hun interne veiligheid organiseren. Het mag geen verrassing heten dat noch IRIS et al (2010) noch Masson en Marta (2011) veel voorbeelden kunnen geven van waar dit is gelukt, zelfs niet in één land. Twee in Groot-Brittannië vaak aangehaalde voorbeelden van gezamenlijke aankopen, het e-Borders-initiatief voor grensbewaking en het 'Fire Control'-project om brandweerinfrastructuur te concentreren in negen regionale centra, zijn allebei op een mislukking uitgedraaid. Wat echter misschien nog meer doorweegt zijn de fundamenteel andere reglementeringen en verschillende behoefteniveaus die spelen tussen civiele en militaire klanten, zelfs wanneer ze gelijkaardige producten aanschaffen. De militaire of defensieklanten en hun toeleveranciers zijn actief in een uiterst ongewoon milieu. Briani en Sartori (2011) vatten deze omstandigheden als volgt samen:

- Monopsoniestructuur aan de vraagzijde
- Monopolie-/oligopoliestructuur aan de aanbodzijde
- Intensieve O&O en langlopende productiecycli
- Afnemende productiekosten
- Overheidssubsidies in de O&O-fase
- Aanverwante spin-offs

Wat binnen de EU-context misschien nog het meest speelt, is het artikel 346 van het Verdrag van Lissabon. Ondanks het 'defensiepakket' van 2009 op grond van de richtlijnen inzake de overdracht van defensie- en veiligheidsgerelateerde aankopen binnen de EU doet artikel 346 aankopen van defensie-uitrusting nog grotendeels buiten de interne-markt-voorschriften vallen.¹

Marktbeschermende maatregelen en subsidies die onder de mededingingswetgeving verboden zijn, worden daardoor tot op zekere hoogte weer mogelijk. Eerder haalden we al aan dat dit een erg specifiek milieu is. Diegenen die gewoon zijn binnen zulke structuren te werken, passen zich dan ook maar moeilijk aan normalere bedrijfsomgevingen aan. En het omgekeerde geldt ook. Respondenten bij het Europees Defensieagentschap wezen er in 2012 bovendien op dat militaire gebruikers gewoonlijk veel meer aangepaste en duurdere apparatuur wilden dan andere gebruikers. Zelfs al gaat het dus om vergelijkbaar materieel, in zo'n geval wordt het moeilijk om tot een gezamenlijke behoefteomschrijving te komen.

¹ Zie Eguren Secades (2011) voor een volledige bespreking van de beperkingen van deze richtlijnen.

Zou er, aangezien de richtlijn overheidsopdrachten van 2009 ook gaat over veiligheidsmaterieel, een mogelijkheid bestaan dat interne-veiligheidsklanten zich – binnen de grenzen van de wetgeving – een militaire aankoopprocedure kunnen eigen maken? Immers, net zoals defensietechnologie vereist dit nieuwe type veiligheidstechnologie een bijzondere manier van werken. Daar lijkt de EU toch van uit te gaan wanneer we zien hoe zij haar activiteiten uitzet, bijvoorbeeld de belofte dat ze gaat onderzoeken of de aansprakelijkheid van bedrijven kan worden beperkt (Europese Commissie, 2012a). Zoiets veronderstellen kan echter problemen opleveren. Het rapport heeft al besproken hoe complex het is om zelfs interne-veiligheidsklanten uit hetzelfde land materieel gemeenschappelijk te laten aankopen. Maar zelfs als hiervoor oplossingen zouden bestaan, stelt zich de vraag of een markt voor veiligheidstechnologie efficiënter zou werken dan de bestaande defensiemarkt? Het lijkt onwaarschijnlijk dat interne-veiligheidsklanten bereid zijn na hun behoefteomschrijving zo buitengewoon lang te wachten tot hun apparaat in gebruik is, iets waarbij defensieklanten zich hebben neergelegd. Vooral wanneer de gevraagde uitrusting al beschikbaar is voor verkoop, wordt dit ondenkbaar. Daarnaast wordt de kritiek luider dat een dergelijk aankoopmodel in feite onbetaalbaar is. Misschien verklaart dit waarom nationale gebruikers onwillig zijn om, in tegenstelling tot wat de Europese Commissie en het GoP-rapport in 2003 verwachtten, de vraag naar veiligheidstechnologieën gecoördineerd en geconsolideerd in te vullen.

3.6 Samenvatting

Dit onderdeel besprak eerst de methodologische problemen om kwantitatief een omschrijving te geven van wat verschillende studies zagen als een nieuw segment op de veiligheidsmarkt, nauw verbonden met het tot stand komen van het concept 'homeland security' (beschreven in onderdeel 2), maar met een sterke link naar de defensiesector. Dit industriële segment kreeg een voorlopige omschrijving als ondernemingen met verschillende industriële achtergronden die overheidsklanten technologische producten aanleveren om veiligheidsbepaaldingen aan te pakken. Het richtte zich daarmee wel degelijk op alle defensiebedrijven en sloot geen veiligheidsbepaaldingen uit, enkel op voorwaarde dat de producten een technologische gerichtheid hadden. Uitgesloten van de analyse werden commerciële en private veiligheidsklanten, dit ten voordele van overheidsactoren.

Het tweede deel bekeek de cross-over tussen veiligheids- en defensietechnologieën. Een eerste vaststelling was dat trends binnen defensie-O&O waarschijnlijk ook zouden optreden in andere hoogtechnologische sectoren met een overheidsklant. Dit zou betekenen dat de O&O zich wellicht zal concentreren in relatief weinig landen en dat EU-inspanningen om ter compensatie samenwerking rond O&O te stimuleren normaal gezien weinig zoden aan de dijk zullen zetten. Daarop bekeek het rapport de taxonomieën ontwikkeld om technologieën en aanverwante apparatuur te classificeren. Het erkende de grote mate aan cross-over tussen defensie- en veiligheidstechnologieën, maar plaatste ook enkele kanttekeningen. Wat voor deze studie het belangrijkste was, was dat ze beide gebruikmaakten van generische technologieën, met moeilijkheden voor de non-proliferatie en de exportcontroles als gevolg. Tevens bracht het kwesties ter sprake zoals de continuïteit van het aanbod voor de EU.

In dit deel kwam ook het aanbod aan bod. Daarbij bleek dat defensiebedrijven het in zekere mate makkelijker hebben om de nieuwe sector te benaderen, maar dat succes geen garantie is. Omdat de vraag vanuit de overheid ondermaats bleef, hadden de grote systeemintegratoren andere strategieën ontwikkeld; sommigen gingen hun veiligheidsmaterieel exporteren, anderen richtten zich op hun defensieportfolio's. Allen hadden zij in zekere zin positie ingenomen om, zodra de vraag aantrok, een EU-markt te betreden. Leveranciers van de tweede rang moesten al meer

definitief beslissen of hun technologieën wel nut hadden voor de nieuwe markt. Producten van leveranciers in de derde rang waren soms wel relevant, maar zij richtten zich vrijwel nooit uitsluitend op defensie. Behalve in de domeinen veilige communicatie en ICT hadden niet-defensiebedrijven het moeilijk. De voornaamste reden was dat traditionele veiligheidsleveranciers en KMO's moeilijker met overheidsklanten konden omgaan, maar de beperkte vraag maakte het moeilijk om sluitende conclusies te trekken.

Ten slotte nam dit hoofdstuk de moeilijkheden van de gefragmenteerde vraag onder de loep. Niemand stelde zich nog vragen bij het feit dat gebruikers van militaire en civiele veiligheidssystemen samenwerkten tijdens steeds meer missies, en daarbij – zij het dan voor andere doeleinden – erg gelijkaardige technologieën gebruikten. Maar in dit punt bleek duidelijk dat het niet zo eenvoudig was om de vraag te consolideren. Een eerste punt was de complexiteit om diverse interne-veiligheidsgebruikers uit de private en de openbare sector, op nationaal, regionaal en lokaal bestuursniveau samen te brengen. Ten tweede werd de specifieke omgeving besproken waarin defensieaankopen plaatsvinden, en de verschillen op wetgevend vlak voor militaire en civiele aankopen. Een laatste element in dit onderdeel was of civiele gebruikers wel geneigd waren om de vraag te consolideren, als ze daarvoor militaire procedures moesten overnemen.

We mogen besluiten dat de gebruikersbehoeften en technologieën ontegenzeggelijk raakvlakken hebben. Evenwel niet vergeten dat de moeilijkheden om de gefragmenteerde vraag te consolideren aanwezig blijven. Dit betekent dat defensiebedrijven alles hebben om een rol te spelen in de veiligheidssector als de vraag er komt, maar dat de vooruitzichten niet echt veelbelovend zullen zijn. We kunnen ons afvragen in hoever lidstaten de EU eigenlijk volgen in haar visie dat deze sector zo belangrijk is. De manier waarop de EU haar activiteiten heeft ontwikkeld, zal verklaren waarom de doelstellingen van de Commissie en die van de lidstaten misschien niet parallel lopen.

4 Beoordeling van EU-maatregelen met een impact op de veiligheids- en de defensie-industrie

4.1 Inleiding

De Europese Unie is een betrekkelijk nieuwe speler op de markt van veiligheid en defensie. Ze was er slechts zijdelings bij betrokken, maar daar is sinds de komst van het Europees en momenteel het Gemeenschappelijk Veiligheids- en Defensiebeleid, en omdat interne veiligheid na 11 september 2001 bovendien ruimer wordt geïnterpreteerd, verandering in gekomen. De Europese Commissie heeft echter lang de ambitie gekoesterd, het industriële defensiebeleid mee vorm te geven. Via interne-markt-voorschriften, een mededingingsbeleid en regionaal beleid heeft ze geprobeerd om daar greep op te krijgen. Tot dusver hebben deze inspanningen enkel op volgende terreinen tot enig succes geleid:

- het beheer van de Kaderprogramma's voor onderzoek en ontwikkeling, met sommige projecten voor tweërlei gebruik,
- grote bedrijfsfusies goedkeuren, ook als die een defensiedimensie hadden,
- regionale ontwikkelingsfondsen toewijzen aan getroffen regio's wanneer militaire bases of bedrijven sluiten (KONVER), en
- in 1995 een stelsel opzetten voor de handel in producten voor tweërlei gebruik binnen de EU (Taylor, 1997).

Vóór de ontwikkeling van het GVDB waren binnen de Raad twee werkgroepen actief rond bewapening. De eerste heette COARM; deze in 1991 opgerichte werkgroep trachtte het exportcontrolebeleid inzake derde landen af te stemmen. De tweede was POLARM, opgestart in 1995, en dit was een ad-hoc werkgroep voor bewapeningsbeleid (Colvin, 1998). Het Europees Parlement was daar niet bij betrokken. Dit betekent dat de Europese samenwerking rond kwesties in verband met de defensie- en de veiligheidsindustrie historisch gezien plaatsvond buiten de EU, in de NAVO, de West-Europese Unie of andere multi- en bilaterale fora.

Dit deel van het rapport wil de EU-maatregelen om het concurrentievermogen van de Europese veiligheids- en defensie-industrie op te drijven kritisch op hun samenhangend karakter en efficiëntie beoordelen. Omdat de EU op dit vlak pas recent bevoegdheid heeft verworven, wordt eerst de juridische basis voor EU-optreden besproken. Vervolgens kijkt dit deel naar het beleid van de Commissie, met aandacht voor het programma voor veiligheidsonderzoek, haar optreden om de sector competitiever te maken, het defensiepakket¹ en ten slotte de betrokkenheid van DG Binnenlandse Zaken in de ontwikkeling van een beleid naar analogie met de Amerikaanse 'homeland security'. Vervolgens richt het zijn blik op het Europees Defensieagentschap. Het laatste grote punt gaat over gelijkaardige Europese activiteit buiten de EU, in casu de Frans-Britse

¹ Het zogenaamde 'Europees defensiepakket' bestaat uit: 1) een overkoepelende mededeling van de Commissie met aanbevelingen voor de versterking van de concurrentiekracht van de Europese defensieindustrie, 2) een voorstel van richtlijn met betrekking tot het intra-communautair verkeer van defensiegerelateerde goederen, 3) een voorstel van richtlijn met betrekking tot het aankopen van defensiematerieel met het oog op meer openheid en concurrentie op de defensiemarkt.

defensieakkoorden, OCCAR, de Raamovereenkomst en de NAVO, met een poging om te beoordelen of welke betekenis zij mogelijk hebben voor het welslagen van het EU-beleid.

4.2 Wetgevende basis van EU-optreden inzake veiligheid en defensie

De wetgevende basis voor EU-optreden inzake veiligheid en defensie is behoorlijk complex en verdient dan ook aandacht. Dit punt geeft kort de essentie weer van de verdragen die dienen als basis voor EU acties in het domein van de veiligheids- en defensie-industrieën en –technologieën, zowel binnen het kader van het Gemeenschappelijk Veiligheids- en Defensiebeleid als van de interne-veiligheidsclausules. Ook licht dit deel toe hoe artikel 346 van het Verdrag betreffende de werking van de Europese Unie (voordien artikel 296) een beperking inhoudt op de activiteiten van de EU. Tevens zal het uitleg geven bij een aantal belangrijke uitspraken door het Hof van Justitie over het gebruik van artikel 346.

4.2.1 Verdragsbasis en beperkingen

De verdragsbasis voor het Gemeenschappelijk Veiligheids- en Defensiebeleid berust op Titel V van het Verdrag betreffende de Europese Unie (VEU)¹ inzake de "Algemene bepalingen inzake het extern optreden van de Unie en specifieke bepalingen betreffende het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB)", en meer bepaald hoofdstuk 2, artikel 42 tot 46, met als titel "Bepalingen betreffende het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB)", alsmede protocol 10 (betreffende de permanente gestructureerde samenwerking), 11 (inzake het VEU) en verklaring 13 en 14 (die beide benadrukken dat het GVDB geen afbreuk mag doen aan de specifieke aard van het veiligheids- en defensiebeleid van de lidstaten; verklaring 14 stelt daarenboven dat geen nieuwe bevoegdheden worden geschapen voor de Commissie of het Parlement). Wat er voor dit rapport erg toe doet, is dat de bepalingen van het Europees Defensieagentschap stellen dat het zal toezien op de definitie van de vermogens en het ontwikkelingsproces en daarbij ook als doel heeft "om de industriële basis van de defensiesector te versterken" en deel te nemen "aan het bepalen van een Europees beleid inzake vermogens en bewapening" (artikel 42.3 en 45 VEU).

Er staat evenwel een belangrijke beperking op wat het EDA of elke andere EU-instelling kan doen om de markt van defensie-uitrusting te reguleren, namelijk artikel 346 (1) van het Verdrag betreffende de werking van de Europese Unie, dat als volgt luidt:

"De bepalingen van de Verdragen vormen geen beletsel voor de volgende regels:

(a) geen enkele lidstaat is gehouden inlichtingen te verstrekken waarvan verbreiding naar zijn mening strijdig zou zijn met de wezenlijke belangen van zijn veiligheid;

(b) elke lidstaat kan de maatregelen nemen die hij noodzakelijk acht voor de bescherming van de wezenlijke belangen van zijn veiligheid en die betrekking hebben op de productie van of de handel in wapenen, munitie en oorlogsmateriaal; die maatregelen mogen de mededingingsverhoudingen

¹ Het Verdrag betreffende de Europese Unie is te vinden op:
<http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0013:0045:NL:PDF>

op de interne markt niet wijzigen voor producten die niet bestemd zijn voor specifiek militaire doeleinden.”

Dit is vrijelijk geïnterpreteerd als een “algemene en automatische vrijstelling van zwaar defensiematerieel van de toepassing van het verdrag” (Trybus, 2000: 665), wat mede werd gevoed door de geheimdoenerij over een lijst met producten waarop deze vrijstelling van toepassing zou zijn, samengesteld in 1958 en bijgewerkt in 1978.ⁱ Enkele uitspraken door het Hof van Justitie en een richtlijn van de Commissie van 2008 hebben hier duidelijkheid in geschept. We zullen deze later bespreken.

Acties ondernomen inzake het interne veiligheidsbeleid berusten op het herziene Verdrag van Rome, vandaag gekend als het Verdrag betreffende de werking van de Europese Unie (VWEU)ⁱⁱ, Titel V ‘Ruimte van vrijheid, veiligheid en recht’ (RVVR). De met het Verdrag van Lissabon overeengekomen wijzigingen laten de RVVR onder het dispositief van het verdrag vallen, en dus ook onder het normale gerechtelijk toezicht van de Gemeenschap. Sommige juristen stelden zich vragen bij de snelle uitbreiding van het beleidsdomein sinds 9/11, omdat bepaalde evoluties zware gevolgen zouden hebben voor de burgerrechten en zij vreesden dat daarvoor onvoldoende aandacht bestond. De veranderingen die het Verdrag van Lissabon voorziet, stemden hen daarom tevreden, aangezien het Hof, mochten bepaalde beslissingen niet stroken met het vandaag wettelijk bindende Handvest van de grondrechten, met de maatregelen die het nu kan nemen hier extra op kan toezien (Craig, 2010). Ook interessant is dat artikel 4 (2) van het VEU specifiek bepaalt dat *“nationale veiligheid de uitsluitende verantwoordelijkheid blijft van elke lidstaat”* en dat het VWEU in plaats daarvan over interne veiligheid spreekt. Over dit onderscheid dat voor sommige lidstaten belangrijk was, werd duidelijkheid verschaft tijdens de onderhandelingen over het Verdrag van Lissabon. Artikel 71 van het VWEU bepaalt dat *“binnen de Raad een permanent comité wordt opgericht om ervoor te zorgen dat binnen de Unie de operationele samenwerking op het gebied van de binnenlandse veiligheid wordt bevorderd en versterkt.”* Dit comité staat bekend als COSI. Artikel 72 van het VWEU luidt echter als volgt: *“Deze titel (Titel V) laat de uitoefening van de verantwoordelijkheid van de lidstaten voor de handhaving van de openbare orde en de bescherming van de binnenlandse veiligheid onverlet.”*

4.2.2 Uitspraken door het Hof van Justitie

Het Hof van Justitie van het Europese Unie heeft talrijke zaken behandeldⁱⁱⁱ waarbij de gedaagde te zijner verdediging artikel 346 heeft ingeroepen. Alhoewel de analyse misschien kort door de bocht gaat, komt het standpunt van de Commissie erop neer dat uitzonderingen in overeenstemming met artikel 346 net als elke andere uitzondering aan een toetsing van de evenredigheid moesten worden onderworpen, terwijl artikel 346 volgens de lidstaten automatisch een uitzondering toestond. Het Hof van Justitie heeft hierin doorgaans het midden tussen beide interpretaties gehouden. Enerzijds heeft het Hof in enkele zaken geoordeeld dat lidstaten artikel 346 mogen gebruiken om hun soevereiniteit te beschermen. In zaak C-252/01 bijvoorbeeld over een overeenkomst betreffende luchtfotografie aan de Belgische kust kon het Hof zich vinden in het argument van België dat de opdracht gepaard moest gaan met speciale veiligheidsmaatregelen zonder dat daarbij nauwkeurig diende te worden onderzocht of veiligheidsmaatregelen nodig waren. In dezelfde zin aanvaardde het Hof in zaak T-26/01 betreffende Fiocchi Munizioni dat

ⁱ De lijst van artikel 346 is nu te raadplegen op <http://register.consilium.europa.eu/pdf/nl/08/st14/st14538-re04.nl08.pdf>.

ⁱⁱ Het Verdrag betreffende de werking van de EU is beschikbaar op: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0047:0199:nl:PDF>

ⁱⁱⁱ De aangehaalde uitspraken zijn terug te vinden op http://curia.europa.eu/en/content/juris/c2_juris.htm.

lidstaten wel degelijk discretionaire bevoegdheid hebben bij de beoordeling van de behoeften om hun belangen te beschermen.

Anderzijds heeft het Hof van Justitie altijd geoordeeld dat vrijstellingen krachtens artikel 346 beperkt zijn. Zo oordeelde het bijvoorbeeld in zaak 367/89 Richardt dat de uitzondering strikt moet worden geïnterpreteerd en dat enkel producten die daadwerkelijk in de lijst van 1958 voorkwamen, waren vrijgesteld. Voorts bleek uit de beslissing in zaak 337/05 (helikopters van het merk Agusta) dat artikel 346 enkel gold voor producten die specifiek voor militaire doeleinden waren bedoeld, wat betekende dat dual-use-goederen of apparatuur geleverd aan een strijdmacht maar met een civiele bestemming niet waren vrijgesteld. Het Hof heeft eveneens geoordeeld dat er geen sprake is van automatische vrijstelling – artikel 346 is enkel van toepassing indien de voorwaarden zijn vervuld (zaak 273/97 Sirdar) – en dat het enkel om veiligheidsredenen mag worden ingeroepen, niet vanuit economische overwegingen (zaak 414-97 Spaanse wapens). In 2009 benadrukten de uitspraken in de zogenaamde ‘eigen middelen’-zaken (C284/05 en anderen), waarbij lidstaten artikel 346 wilden invoeren als rechtvaardiging waarom zij btw-inkomsten uit wapenimport niet aan de Commissie hadden gerapporteerd, ook dat een automatische vrijstelling niet mogelijk was. Deze uitspraken inzake artikel 346 hebben de Commissie in haar recent optreden op het vlak van defensie en veiligheid als inspiratiebron gediend, en hebben haar positie verstevigd.

4.3 Beleid van de Europese Commissie

De acties die de Europese Commissie onderneemt om het concurrentievermogen van de veiligheids- en defensie-industrie te versterken gaan niet allemaal uit van één directoraat-generaal, hoewel DG Ondernemingen en Industrie wel eenheden heeft die gespecialiseerd zijn in zowel de veiligheids- als de defensie-industrie. We mogen niet vergeten dat op dit vlak verschillende DG's activiteiten ontplooiën. Dit zijn DG Ondernemingen en Industrie (veiligheidsonderzoek en concurrentievermogen van de sector), DG Interne Markt en Diensten (defensiepakket) en DG Binnenlandse Zaken (binnenlandse veiligheid). DG Informatiemaatschappij en Media speelt door zijn betrokkenheid bij cyberbeveiliging ook een rol, maar het werk van dit DG is voor wat dit rapport betreft minder relevant. DG Handel ten slotte is verantwoordelijk voor de exportwetgeving van producten voor tweeledig gebruik. Dat zoveel DG's hierin actief zijn, duidt erop dat de Commissie genooddakt is een gemeenschappelijk standpunt te ontwikkelen over een erg veelzijdig onderwerp. De afgelopen jaren lijkt het erop dat de Commissie het desbetreffende beleid op een meer eenduidige manier tot stand heeft kunnen brengen. Eerdere pogingen in de jaren '90 om bevoegdheid te verwerven zijn wellicht op niets uitgedraaid omdat commissarissen het niet eens waren of ze dit als een industrieel beleid dan wel een mededingingskwestie van de interne markt moesten aanpakken. Dit maakte het de lidstaten, die de Commissie daarbuiten wilde houden, eenvoudiger om haar mededelingen links te laten liggen (Mörth, 2000).

Twee ontwikkelingen net voor en net na de eeuwwisseling speelden echter in de kaart van de Commissie. Ten eerste nam Romano Prodi commissarissen Liikanen en Busquin op in zijn Commissie. Beiden waren overtuigd van het belang van de defensie-industrie voor de economische toekomst van Europa en gaven het beleid vorm. De idee dat Europa in staat zou zijn haar hightechproblemen op te lossen door haar defensie-industrie uit te bouwen, lijkt zich sedertdien in het denkpatroon van de Commissie te hebben genesteld (Merritt, 2004: 216). Vanuit de sector rees dan ook de vraag om de Commissie meer beleidsverantwoordelijkheid te geven. Twee belangrijke rapporten uit 2002 (STAR21 en ACARE) opgemaakt door lobbygroepen van de ruimtevaart- en de

luchtvaartsector stelden dat technologische innovaties voor defensie- en ruimtevaartdoeleinden de economie in de EU in bredere zin ondersteunden. Ten tweede legde de beslissing om het EVDB te ontwikkelen snel de tekortkomingen inzake infrastructuur en technologie bloot en deed deze de politiek weer oog krijgen voor de trans-Atlantische kloof. 11 maart 2003 was de dag waarop de Commissie haar denkbeelden wereldkundig maakte, toen ze een mededeling publiceerde over de industriële en marktvraagstukken van Europese defensie. De Commissie stelde maatregelen voor op zeven domeinen; normalisatie, toezicht op de defensiegerelateerde industrie, overbrenging binnen de Gemeenschap, mededinging, aanbestedingsregels, controle op de uitvoer van goederen voor tweëerlei gebruik en onderzoek (Europese Commissie, 2003a). Zoals zal blijken heeft de beslissing van de Europese Raad in 2003 om het Europees Defensieagentschap op te richten de Commissie in haar mogelijkheden om wetgevende voorstellen te doen beknot, maar desalniettemin heeft ze sindsdien haar macht duidelijk kunnen uitbreiden. Dat Michel Barnier, de commissaris voor Interne markt, op 7 november 2011 aankondigde dat de Commissie had besloten om een task force voor het defensiebeleid te vormen, met daarin wellicht de commissaris voor Interne markt, Onderzoek, Industrie, Vervoer, Energie en de juridische dienst, aangevuld door het EDA en de Europese dienst voor extern optreden, geeft blijk van verdere ambities.

4.3.1 Ontstaan en evolutie van het programma voor veiligheidsonderzoek

Binnen het DG Onderzoek van de Europese Commissie hebben bepaalde afdelingen lange tijd geprobeerd om defensiegerelateerd onderzoek te financieren, maar veel lidstaten, leden van het Europees Parlement en zelfs sommige ambtenaren van de Commissie hebben zich daar om twee redenen altijd tegen verzet: a) defensie bleef een nationaal prerogatief en b) de EU was een civiele, geen militaire macht, wat iets dergelijks ongepast zou maken. Maar hoewel de kaderprogramma's voor onderzoek¹ nooit formele toestemming hebben gekregen om defensiegerelateerd onderzoek te financieren, is met de jaren steeds meer geld naar dual-use onderzoek gevloeid.² Maar zij die voorstander waren om van defensiegerelateerd onderzoek een taak voor de Commissie te maken, met name Liikanen en Busquin, hebben in 2003-2004 toch stappen ondernomen. Daarop zagen enkele mededelingen het licht over aanverwante domeinen zoals defensie-uitrusting (Europese Commissie, 2003a) en ruimtevaartindustrie (Europese Commissie, 2003b), die de ambitie uitspraken dat de Commissie een rol kon spelen in het defensieonderzoek. Onder het punt "naar een coherenter Europese inspanning voor hoogwaardig onderzoek op het gebied van veiligheid" riep de Commissie (2003a) bijvoorbeeld op tot meer coördinatie van het veiligheidsonderzoek. Ze gaf aan dat ze nationale overheden, de bedrijfswereld en onderzoeksinstellingen zou vragen hoe

¹ De EU-kaderprogramma's voor onderzoek zijn voor de EU het voornaamste vehikel om onderzoek te financieren. Ze bestaan sinds 1984. Het zijn meerjarenprogramma's (de eerste zes liepen telkens vijf jaar, het huidige zevende Kaderprogramma en zijn opvolgers zullen een looptijd hebben van zeven jaar). Elk kaderprogramma heeft eigen onderzoeksprioriteiten vooropgesteld en heeft deze ook anders gefinancierd. Het huidige kaderprogramma heeft vier programma's: samenwerking met tien onderzoeksprioriteiten (gezondheid; voeding, landbouw en visserij en biotechnologie; informatie- en communicatietechnologieën; nanowetenschappen, nanotechnologieën, materialen en nieuwe productietechnologieën; energie; milieu (inclusief klimaatverandering); vervoer (met inbegrip van luchtvaart); sociaal-economische wetenschappen en geesteswetenschappen; ruimtevaart; veiligheid, ideeën (ERC-subsidies voor startende onafhankelijke onderzoekers), mensen (Marie Curie-acties ter ondersteuning van de mobiliteit van onderzoekers) en capaciteit (ter verbetering van de onderzoeks- en innovatiecapaciteit). Niet-EU-lidstaten kunnen ook deelnemen aan het programma als zij mee de begroting financieren. Volgende landen zijn op die manier verbonden aan het huidige kaderprogramma: Zwitserland, Israël, Noorwegen, IJsland, Liechtenstein, Turkije, Kroatië, FYROM, Albanië, Montenegro, Bosnië en Herzegovina, Faeröer en Moldavië.

² De prioriteit veiligheidsonderzoek, zoals aanvankelijk gedefinieerd in de voorstellen van de Commissie, had geen geheel duidelijk karakter. Maar tijdens de medebeslissingsprocedure over het zevende Kaderprogramma stonden het VK, Frankrijk en Duitsland er samen met het Europees Parlement op de civiele aard van de kaderprogramma's te behouden. Dat is waarom het thema veiligheidsonderzoek formeel uitsluitend een civiele focus heeft (zie Besluit nr. 1982/2006/EG van het Europees Parlement en de Raad van 18 december 2006 betreffende het zevende kaderprogramma van de Europese Gemeenschap voor activiteiten op het gebied van onderzoek, technologische ontwikkeling en demonstratie (2007-2013)).

een Europese onderzoeksagenda er in dit domein zou moeten uitzien en zou proberen “om een voorbereidende actie op te zetten, met de bedoeling dergelijk onderzoek op Europees niveau te coördineren, gericht op een beperkt aantal concrete technologieën die aan de Petersbergtaken zijn gekoppeld”. De denkpiste zag er in deze fase behoorlijk duidelijk uit; de Commissie probeerde om het defensieonderzoek te financieren als steun aan defensiebedrijven die volgens haar technologisch in staat waren om economisch de concurrentie aan te gaan. Een ambtenaar van de Commissie deed officieel volgende uitspraak: “Het EU-kaderprogramma ondersteunt dual-use onderzoek in al deze domeinen, dus het zou wel zinvol zijn om alles op het puur militaire in te zetten... Belangrijk is dat we het precedent scheppen” (Tigner, 2003a). In mei 2003 suggereerde nog een andere functionaris van de Commissie dat er een grootschalige heroriëntatie van het onderzoeksbudget zat aan te komen. Zo zouden, om Europa inzake defensie een sterkere identiteit te geven, “Europese gelden flexibeler inzetbaar moeten worden, ten voordele van defensiegerichte projecten” (Tigner, 2003b). Maar tijdens de zomer van 2003 besloot de Europese Raad om het Europees Defensieagentschap op te richten, dat onder andere zou instaan voor de coördinatie van het defensieonderzoek. Omdat dit het de Commissie erg moeilijk maakte om openlijk te pogen defensieonderzoek te financieren, verlegde ze haar aandacht naar het veiligheidsonderzoek. In maart 2004 publiceerde de Commissie een mededeling over veiligheidsonderzoek (Europese Commissie, 2004) en een besluit betreffende de tenuitvoerlegging van een voorbereidende actie¹. En op 15 maart 2004 legde de door de Commissie samengestelde Groep van prominenten op het gebied van veiligheidsonderzoek (GoP) haar rapport voor aan Romano Prodi (zie figuur 1 op blz. 47). Edler en James (2012) benadrukken dat de Commissie deze weg op geheel eigen houtje is ingeslagen en wijzen erop dat noch de lidstaten noch de sector initieel om deze maatregelen hadden gevraagd.

Daarop publiceerde de Commissie op 31 maart 2004 de eerste oproep tot het indienen van voorstellen voor projecten en ondersteunende acties onder de nieuwe ‘vorbereidende actie inzake de versterking van het Europese industriële potentieel op het gebied van veiligheidsonderzoek’ (PASR 2004). Deze actie spendeerde 65 miljoen euro over een periode van drie jaar en fungeerde als pilootfase voor de ruimere ambitie van de Commissie om een afzonderlijk programma voor veiligheidsonderzoek te lanceren, met de bedoeling de veiligheidscultuur in de EU te stimuleren. Critici vonden dat er onvoldoende overleg had plaatsgevonden met veiligheidsgebruikers², dat er onvoldoende overeenstemming was met de beleidsprioriteiten in de strijd tegen het terrorisme, dat de doelstellingen onvoldoende duidelijk bleven en dat de implantatie overhaast gebeurde (Hayes, 2006; Mawdsley, 2004). De prioriteit veiligheidsonderzoek in het zevende Kaderprogramma financierde zelf projecten op vier taakgebieden, tegen een achtergrond van drie horizontale thema's:

Taakgebieden:

- **“Beveiliging van burgers verbeteren** - technologische oplossingen voor civiele bescherming, bioveiligheid, bescherming tegen criminaliteit en terrorisme;
- **Beveiliging van de infrastructuur en nutsvoorzieningen verbeteren** - het analyseren en beveiligen van infrastructuur zoals die voor ICT, vervoer, energie en financiële en bestuurlijke diensten;

¹ Besluit 2004/213/EG

² Belangrijk is te weten dat toen van de lidstaten enkel Oostenrijk en Zweden het nodig hadden gevonden om een nationaal programma voor veiligheidsonderzoek op te zetten – het is goed mogelijk dat de GoP de vraag daardoor veel te hoog had ingeschat.

- **Intelligente grensbewaking en -beveiliging** - technologieën, apparatuur, gereedschappen en methodes om Europa's grenzen en kusten te beveiligen;
- **Herstel van de beveiliging en veiligheid in crisissituaties** - technologieën en communicatie, coördinatie ter ondersteuning van civiele, humanitaire en reddingstaken”;

Horizontale thema's:

- **“Integratie, interconnectiviteit en interoperabiliteit van beveiligingssystemen verbeteren** - informatievergaring voor civiele bescherming, bescherming van vertrouwelijkheid en traceerbaarheid van transacties;
- **Beveiliging en de samenleving** - sociaal-economische, politieke en culturele aspecten van veiligheid, ethiek en waarden, het aanvaarden van beveiligingsoplossingen, sociaal milieu en het veiligheidsgevoel;
- **Coördinatie en structurering van het veiligheidsonderzoek** - coördinatie tussen Europees en internationaal veiligheidsonderzoek inzake civiel, veiligheids- en defensieonderzoek.”ⁱ

Het is een taakgericht en grotendeels ontwikkelingsgericht onderzoek, dus geen "blue skies"-research zoals dat onder de door het DG Onderzoek beheerde prioriteiten wordt gefinancierd. In sommige projecten lijkt het erop dat men zelfs liever systemen aankoopt, in plaats van op onderzoek en ontwikkeling te focussen, aangezien ook demonstratiemodellen zijn geproduceerd (een late fase in de ontwikkeling van technologie). Het had een totale begroting van 1,4 miljard euro voor de periode 2007-13. De Commissie hoopte dat de onderzoeksprioriteit zou bijdragen aan het algemenere doel om de fragmentatie van zowel vraag als aanbod terug te dringen, en om via EU-standaardiseringsoefeningen wereldwijd een marktleiderspositie te veroveren.ⁱⁱ Doorheen de voorbereidende en de eerste fasen van de eigenlijke prioriteit, organiseerde de Commissie een dialoog tussen overheid en bedrijfsleven via adviesgroepen, in aanvulling op de comitologie-comitésⁱⁱⁱ die gewoonlijk al bij onderzoeksprogramma's worden ingezet. Deze groepen en hun rapporten worden kort beschreven in figuur 1. Zij zijn belangrijk en hun samenstelling doet ertoe, want de Europese Commissie heeft de meeste van hun aanbevelingen overgenomen in daaropvolgende mededelingen (Europese Commissie, 2004a, 2009). Deze dialoog lijkt grote impact te hebben gehad op de bepaling van de financieringsprioriteiten. Maar als we kijken wat het veiligheidsonderzoek beoogde, hadden we mogen verwachten dat dit aan de hand van een wetenschappelijk sluitende risicoanalyse zou zijn gebeurd.

Dat de Groep van prominenten in haar rapport toen nog opriep om elk jaar minstens 1 miljard euro extra te voorzien voor veiligheidsonderzoek, komt nu totaal onrealistisch voor. Volgens vertegenwoordigers van de industrie kwam de overtuiging dat lidstaten bereid zouden zijn om budgetten van het niveau dat de VS aan 'homeland security' uit geeft vrij te maken en hun beleid in een bepaalde richting te sturen minstens voor een deel voort uit een situatie van groepsdenken, gevoed door een Commissie en een Europese defensiesector die vreesden dat de miljarden dollars die Amerikaanse defensiebedrijven in de nabije toekomst zouden binnenhalen hun Europese concurrenten hopeloos achterop zouden doen geraken. Maar in werkelijkheid begrepen ze toen

ⁱ De hoofdpunten van de prioriteit veiligheidsonderzoek zijn te vinden op: http://cordis.europa.eu/fp7/cooperation/security_en.html (geraadpleegd op 7 maart 2011).

ⁱⁱ Gesprekken met ambtenaren van de Commissie in april 2008.

ⁱⁱⁱ Er is ook een adviesgroep voor veiligheidsonderzoek (SecAG) van deskundigen, aangeduid door de Commissie om haar te begeleiden in de planning van toekomstige programma's voor veiligheidsonderzoek. De twintig leden tellen zeven grote defensiebedrijven, drie veiligheidsbedrijven, het EDA, vier eindgebruikers (Polen, Malta, Roemenië en Estland) drie onderzoeksinstituten (Finland, Israël, Nederland), het Zweeds agentschap voor defensieonderzoek en het Oostenrijkse Rode Kruis.

onvoldoende (net als Amerikaanse bedrijven - Beidel, 2011) hoe de 'homeland security'-begroting eigenlijk zou worden besteed.

Ten eerste bepalen concrete gebeurtenissen hoe de VS haar geld uitgeeft. Orkaan Katrina leidde ertoe dat veel dollars in een eerste fase terecht kwamen bij bedrijven die werken rond crisis respons, niet bij defensiefirma's. Pas vanaf 2009 begonnen belangrijke defensieproducenten zoals Lockheed echt grote contracten binnen te halen (Beidel, 2011). Grote bedragen gaan ook naar het ministerie van Homeland Security zelf, dat in vergelijking met de 13 medewerkers in 2002 in 2010 60.000 mensen in dienst had. Ten tweede is men het er nu over eens dat de VS door de begrotingscrisis voortaan minder geld zal besteden aan 'homeland security' dan tijdens het eerste decennium. Beidel (2011) stelt ook dat de mogelijkheid dat de veiligheidsmarkt met de defensiesector zou gaan wedijveren *"nu eerder klein is, deels ten gevolge van de toenemende budgettaire beperkingen en omdat beide markten door verschillende factoren worden aangedreven"*. Nu men tot het besef komt dat grootschalige bewakings- en opsporingsprogramma's enorme financiële en commerciële inspanningen hebben gevraagd en het veiligheidsniveau amper hebben kunnen optrekken,¹ en burgers steeds meer vragen hebben bij de vergaande veiligheidsmaatregelen, zijn bepaalde programma's afgeblazen, bijvoorbeeld het Advanced Spectrographic Portal-programma om gesmokkeld nucleair materiaal te detecteren of SBI-net, een 'virtuele omheining' om grenzen te bewaken. Bovendien stelt Beidel (2011) dat de VS zich, behalve wanneer het op cyberbeveiliging aankomt, in de toekomst gaat richten op het integreren van bestaande, beproefde technologie en financiering van nieuw onderzoek achterwege zal laten. Volgens Hayes en Vermeulen (2012) trekt de Europese Commissie ook geen lessen uit wat er zich in de VS heeft afgespeeld. Ze blijft immers het soort grensbewakingsprojecten financieren waarvan men in de VS heeft vastgesteld dat ze niet naar behoren werken, zoals bijvoorbeeld het SBI-net. Naast eigen projecten is het programma voor veiligheidsonderzoek uitgemond in een inter-institutionele samenwerking tussen de Commissie en het EDA. Het EDA en de Commissie zijn met name trots op twee projecten.

- Software Defined Radio, dat toepassingen kent voor zowel militair gebruik als voor hulpdiensten (politie, brandweer en dergelijke).
- een project over de inzet van onbemande vliegtuigen in de burgerluchtvaart (James, 2009a).

Deze ad-hoc samenwerking heeft de Europese ministers van Defensie in mei 2009 doen beslissen om het Europees Defensieagentschap op te dragen om samen met de Europese Commissie een Europees samenwerkingskader voor veiligheids- en defensieonderzoek in te richten, met de bedoeling te komen tot een "maximale complementariteit en samenwerking tussen onderzoeksactiviteiten met het oog op defensie en de veiligheid van burgers".¹¹ Volgens het EDA is omgevingsbewustzijn (sensorentechnologieën, bediening en controle van netwerkkassetten) een domein waar samenwerking mogelijk is (James, 2009a). Gesprekken in januari 2012 met ambtenaren van zowel het EDA als de Commissie leken aan te geven dat beide partijen tevreden waren met deze samenwerking. Vooral het EDA zag er een manier in om bijkomende financieringsmogelijkheden te creëren.

¹ Mueller en Stewart (2012: 107) berekenen dat wat de VS uitgaf aan 'homeland security' pas kostefficiënt zou zijn indien het zou dienen als "afschrikking tegen, preventie of verijdeling van of bescherming tegen 333 grootschalige aanvallen per jaar die anders wel waren gelukt. Dat is er dus ongeveer één per dag." Volgens het artikel hebben zich tussen 2001 en 2012 slechts 50 gevallen van moslimterrorisme voorgedaan, de meesten op de kleine schaal.

¹¹ Raad van de Europese Unie, 2943e zitting van de Raad Externe Betrekkingen, Conclusie over Europees veiligheids- en defensiebeleid (EVDB), Brussel, 18 mei 2009

Figuur 1: adviesgroep voor veiligheidsonderzoek en hun rapporten

Groep van prominenten, rapport van 2004

Leden - 27 leden vooral afkomstig uit de defensiesector of met militaire achtergrond. Beperkte vertegenwoordiging van gebruikers.

Voornaamste aanbevelingen

- Programma voor veiligheidsonderzoek van de Commissie moet worden ingericht
- De Commissie moet bovenop bestaande uitgaven 1 miljard euro per jaar aan veiligheidsonderzoek besteden
- Programma moet onderzoeksprojecten gerelateerd met capaciteitsopbouw financieren tot in de fase van de demonstratiemodellen
- Er mag geen opdeling bestaan tussen civiel en militair veiligheidsonderzoek – synergiën zijn aan te moedigen
- Het programma moet het concurrentievermogen van de sector bevorderen en marktontwikkeling stimuleren

Europese Adviesraad voor Veiligheidsonderzoek, rapport “Meeting the Challenge” van 2006

Leden - 50 leden - combinatie van publieke gebruikers (18), vertegenwoordigers van de sector (14) en enkele veiligheidsdeskundigen - meer defensiegericht dan misschien verwacht.

Voornaamste aanbevelingen

- Er moet multidisciplinair, missiegericht onderzoek inzake veiligheid plaatsvinden over vermogensontwikkeling, systeemontwikkeling en geïntegreerde systeemdemonstratie
- Vijf demonstratieprogramma's werden aanbevolen: beheer van de nasleep van een crisis; Europees geïntegreerde grensbewaking; veiligheid van logistiek en aanvoerketen; veiligheid van massavervoer; en CBRNE-bedreigingen
- Maatschappelijke ongerustheid over privacy en ethiek mag tijdens pogingen om de veiligheid te verhogen niet worden genegeerd
- Systeem voor veiligheidsonderzoek moet worden ingericht door gebruik te maken van *“innovatieve precommerciële inkoop door de overheid, grootschalige demonstratieprogramma's, meer KMO-betrokkenheid en door Europese normen te definiëren en gebruiken”*

***Europees Forum voor onderzoek en innovatie op het gebied van veiligheid (ESRIF),
eindverslag 2009***

Leden - 65 plenaire leden - alle belanghebbenden vertegenwoordigd, met inbegrip van EU-instellingen. Bijkomende leden (600), vooral bekende industriëlen, maakten mee deel uit van werkgroepen. Weinig vertegenwoordiging van het middenveld.

Voornaamste aanbevelingen

- De menselijke en maatschappelijke aspecten van veiligheid moeten centraal staan in het veiligheidsonderzoek en veiligheidsoplossingen moeten ook ethisch en juridisch zijn onderbouwd.
- Industrieel beleid – fragmentatie van de markt wegwerken en de industriële basis van veiligheid versterken om zich vooraan op de wereldwijde veiligheidsmarkt te positioneren
- Europese agenda voor onderzoek en innovatie op het gebied van veiligheid – 5 clusters
 - o klassieke veiligheidscyclus van preventie, bescherming, voorbereiding, reactie en herstel;
 - o verschillende aanvalsmiddelen beantwoorden;
 - o kritieke activa/infrastructuren beveiligen;
 - o identiteit, toegang en beweging van mensen en goederen beveiligen;
 - o horizontale stimulansen, met name informatie- en communicatietechnologieën.
- Vereiste om daarenboven de externe dimensie van veiligheid in de toekomst te bekijken
- Verdere dialoog tussen overheid en bedrijfsleven, gecoördineerde trans-Europese samenwerking en oprichting van een Fonds voor interne veiligheid

Is het programma voor veiligheidsonderzoek geslaagd? Om deze vraag te beantwoorden dienen we te onderzoeken hoe de Commissie, de sector en critici van de Commissie dit bekijken. Ten eerste was het programma voor veiligheidsonderzoek vanuit het standpunt van de Commissie minstens deels een succes. Het was populair. Gesprekken met ambtenaren van het DG Ondernemingen en Industrie en vertegenwoordigers van de sector in januari 2012 bevestigden dat het programma zwaar overbevraagd was. Bovendien wijst het feit dat veiligheidsonderzoek ook een plaats zal krijgen in het achtste Kaderprogramma Horizon 2020 onder het punt 'Inclusieve, innoverende en veilige samenlevingen' op een zeker succes, hoewel op dit ogenblik nog geen duidelijkheid bestaat over het budget. De mogelijkheid is zelfs ter sprake gekomen om defensieonderzoek te financieren via de kaderprogramma's.¹ Wat marktvorming betreft echter heeft de Commissie, zeker aan de vraagzijde, zoals eerder besproken in onderdeel 3 minder succes geboekt.

¹ Er was een voorstel om defensieonderzoek te financieren via het Horizon 2020-programma (de opvolger van het zevende Kaderprogramma), maar het DG Onderzoek en de lidstaten waren het daarmee niet eens. Edler en James (2012) stellen dat

Vanuit het standpunt van de sector kwam er uit de in januari 2012 gevoerde gesprekken heel wat interessants naar voor. Die had het erg lastig met de naderhand gebrekkige vraag door gebruikers, omdat het weinig zin had technologieën (of nuttige contacten om de gebruiker in het project te vertegenwoordigen) te delen met projectpartners in het programma voor veiligheidsonderzoek als dit niet uitmondde in een opdracht. Dit was vooral een probleem voor bedrijven in landen waar de beschikbare onderzoeksgelden beperkt waren en geen aankopen werden gedaan. Zij konden voor de onderzoeksfase dan wel EU-financiering aanvragen, maar daarna was niet duidelijk hoe het dan verder moest; uitvoeren was moeilijk zonder klanten, wat de vraag opwierp of onderzoek en ontwikkeling dan geen verloren moeite was. De Commissie, die geen klant is, heeft maar beperkte capaciteit om hier iets aan te doen. Ook werd aangevoerd dat, omdat offertes geografisch evenwichtig moesten zijn en ook KMO's konden meedingen, niet altijd de beste partners werden gekozen.

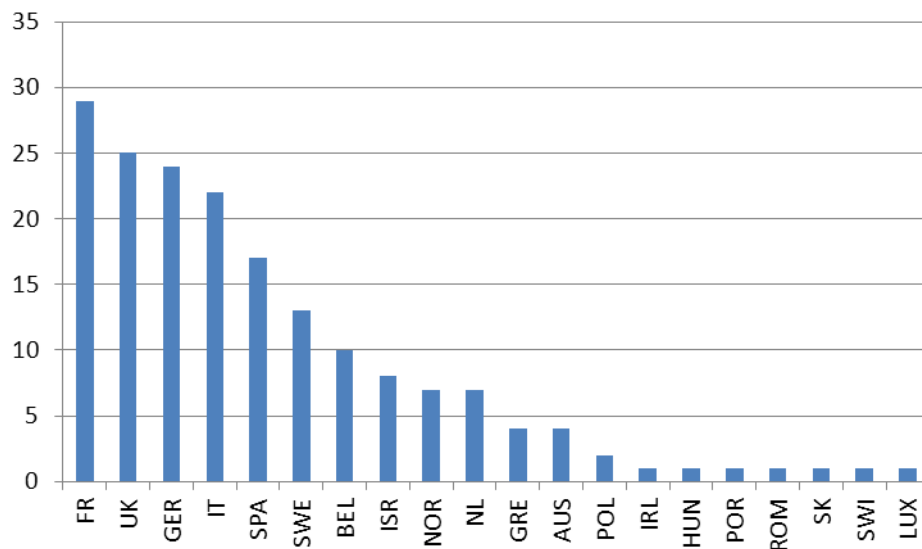
De critici van de Commissie laten zich negatiever uit. Hayes (2006; 2009; 2010) is van oordeel dat het programma voor veiligheidsonderzoek het lobbywerk van defensiebedrijven heeft beloond. Volgens hem waren zij te sterk vertegenwoordigd in alle adviesgroepen, dit ten nadele van echte stemmen uit het middenveld. Jeandesboz en Ragazzo (2010) stellen verder dat de dialoog tussen overheid en bedrijfsleven binnen de adviesgroepen gesloten en beperkt was, maar hebben ook een heleboel interessante gegevens verzameld om hun kritiek te staven dat het programma een geografische scheeftrekking kende, werd overheerst door grote defensiebedrijven en zich concentreerde op controversiële bewakingstechnologieën. Volgens hen waren onevenredig veel begunstigen afkomstig uit zes landen (VK, Frankrijk, Duitsland, Italië, Zweden en Israël). Jeandesboz en Ragazzo (2010) beweerden verder dat bijna uitsluitend grote defensiebedrijven hun voordeel hadden gehaald uit het programma voor veiligheidsonderzoek, wat zij verklaren met verwijzing naar hun te sterke vertegenwoordiging in de adviesgroepen. Hun laatste punt van kritiek was dat het programma zich te zeer focuste op bewakingstechnologieën die in sommige gevallen voor wat burgervrijheden en privacy betreft veel controversie opwerpen. Zij wezen erop dat projecten voor bewaking en detectie tot mei 2009 40,1% van het budget hadden opgebruikt, vergeleken met de 1,09% voor twee projecten die over ethische en wettelijke kwesties nadachten. Voor hun stelling vertrokken zij van een analyse van vóór mei 2009 toegekende projecten. In het kader van dit onderzoek werd een databank opgesteld met projecten die tot juli 2012 waren toegewezen en waaruit meer gegevens werden gehaald om de visie van Jeandesboz en Ragazzo bij te treden. De gegevens waren afkomstig van de CORDIS-website.¹ Uit een analyse van het totale aantal projecten dat elk land coördineerde en hun waarde (zie figuren 1 en 2 hieronder) blijkt duidelijk dat er sprake is van concentratie. De zes landen die tot juli 2012 de meeste en grootste projecten gefinancierd hadden gekregen, waren Frankrijk, het VK, Duitsland, Italië, Spanje en Zweden. Frankrijk, dat tot dan ruim 19% van de toegewezen fondsen had gecoördineerd, is op dat vlak het meest succesvol geweest. België heeft het ook goed gedaan, waarbij wel moet worden opgemerkt dat de helft van het aantal gecoördineerde projecten in handen ligt van Europese organisaties met standplaats in Brussel, zoals de European Organisation for Security. Israël en Noorwegen (niet-EU-lidstaten kunnen ook deelnemen aan de kaderprogramma's als zij mee de begroting financieren) scoorden eveneens sterk. Zoals kon worden verwacht gaat industriële defensiekracht samen met een bovengemiddeld coördinatiepercentage. De zes best presterende landen zijn de zes leden die de intentieverklaring ondertekenden. Dit lijkt erop te wijzen dat de in

deze nederlaag aangeeft dat de Commissie maar beperkt in staat is om zich op dit beleidsdomein te begeven. Ook is niet geheel duidelijk of financiering voor defensieonderzoek een toegevoegde waarde zou creëren. Wellicht zal er niet voldoende budget worden gevonden om een verschil te maken, en het probleem dat het EDA geen garantie kon bieden dat het kopers zou vinden voor het gefinancierde onderzoek zou ook voor de Commissie gelden. Het lijkt erop dat EU-onderzoeksfinanciering efficiënter op andere domeinen kan worden gebruikt.

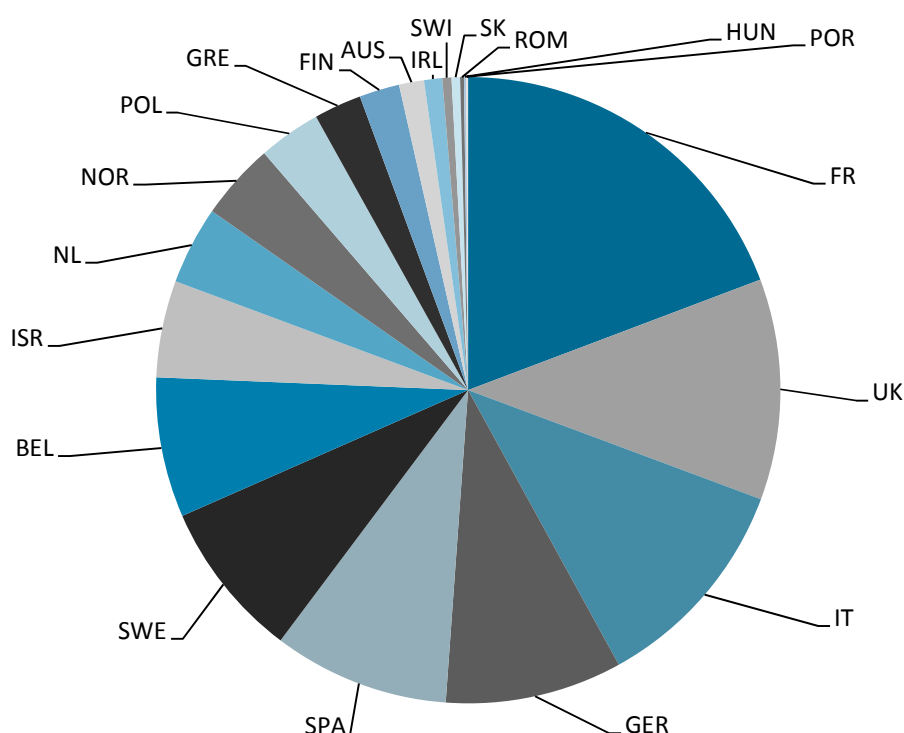
¹ CORDIS-lijst van projecten gefinancierd onder de prioriteit veiligheidsonderzoek:
http://cordis.europa.eu/fp7/security/projects_en.html

onderdeel 3 uitgesproken vrees dat het veiligheidsonderzoek net zoals defensieonderzoek mogelijk geografisch geconcentreerd zou verlopen, terecht is. De gehele participatie levert misschien een complexer beeld op. Maar omdat het aan elke partner toegewezen bedrag niet bekend is, was het voor dit rapport niet mogelijk een diepere analyse uit te voeren. Aangezien respondenten uit de sector zich bezorgd hadden getoond dat zij, omdat de Commissie trachtte een betere geografische spreiding te bewerkstelligen, genoodzaakt waren om voor minderwaardige partners te kiezen, schept een diepere analyse misschien ook geen correct beeld over waar de expertise in veiligheidsonderzoek precies te vinden is.

figuur 1: aantal projecten in de veiligheidsprioriteit van het zevende Kaderprogramma met financiering van projectcoördinatoren per deelnemend land (tot juli 2012)



Figuur 2: waarde van projecten gefinancierd in de veiligheidsprioriteit van het zevende Kaderprogramma naar projectcoördinatoren per deelnemend land (tot juli 2012)



De gegevens geven een gemengd beeld van wie het programma vooral heeft begunstigd. Vier van de vijf bedrijven in de lijst maken ofwel deel uit van bedrijven met een defensieportfolio of zijn dochters van defensiebedrijven. De twee voornaamste begunstigden (Thales en Indra) hebben belangen in zowel de defensie- als de veiligheidssector. Morpho (in handen van Safran) en Selex Sistemi Integrati SPA (in handen van Finmeccanica) verkopen bewakings- en detectietechnologieën. Ook Verint is een fabrikant van bewakings- en detectietechnologieën maar levert eerder systemen voor ordehandhaving dan voor defensie. In de top tien vinden we daarnaast het Zweedse agentschap voor defensieonderzoek, de Belgische Koninklijke Militaire School, de onderzoeksinstituten Fraunhofer-Gesellschaft uit Duitsland en TNO uit Nederland (met enkele groepen die aan defensieonderzoek doen) en het Franse CEA, dat onderzoek uitvoert naar civiele en militaire toepassingen van kernenergie (en, sinds 2010, alternatieve energie). Dit betekent dat het beeld niet zo eenduidig is als Jeandesboz en Ragazzo (2010) het voorstelden. Maar als we beseffen dat het programma voor veiligheidsonderzoek voor civiel gebruik bedoeld is, valt niettemin op hoeveel defensiespelers we erin terug vinden. Het dient opgemerkt dat de analyse weer de financiering per coördinator bekijkt - in verschillende gevallen bestaat er duidelijk een

vervolgproject dat gecoördineerd wordt door , maar dit is een factor waarmee geen rekening kon worden gehouden.

Tabel 5: tien hoogst gefinancierde projectcoördinatoren uit de veiligheidsprioriteit van het zevende Kaderprogramma (tot juli 2012)

Projectcoördinator	Totale waarde van financiering (in euro)
Thales Communications and Security SA (Frankrijk)	37640021
Indra Sistemas S.A. (Spanje)	35459846
Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung (Duitsland)	31437774
Totalforsvarets Forskningsinstitut (Zweden)	30806584
Ecole Royale Militaire - Koninklijke Militaire School (België)	30549645
Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek – TNO (Nederland)	22998389
Selex Sistemi Integrati SPA (Italië)	22143064
Morpho (Frankrijk)	22048026
Verint Systems Ltd (Israël)	21108212
Commissariat à l’Energie Atomique et aux Energies Alternatives (Frankrijk)	18300468

Tenslotte beweerden Jeandesboz en Ragazzo (2010) dat het programma erg op bewakings- en detectietechnologieën was gericht en dat daardoor slechts twee projecten de ethische en wettelijke implicaties van veiligheidstechnologieën hadden bestudeerd. De meeste projecten met financiering onder de categorieën ‘beveiliging van burgers’, ‘beveiliging van de infrastructuur en nutsvoorzieningen’ en ‘intelligente grensbewaking en –beveiliging’ gaan wel degelijk over bewakings- en detectietechnologieën. Deze drie categorieën nemen 48,5% van de uitgaven voor zich. Hoewel minder budget is opgegaan aan voornamelijk sociale-wetenschapsprojecten (niet te verwonderen, omdat zij goedkoper zijn dan technologieprojecten), hebben veertien projecten financiering gekregen die (volgens de beschikbare omschrijving, de wettelijke of ethische implicaties behandelen. Mogelijk wijst dit erop dat de Commissie eerdere kritiek heeft aanvaard en het anders wil aanpakken. Maar over bepaalde technologieën die maatschappelijk geen draagvlak hebben, zegt de Commissie (2012a: 5) het volgende:

“De problemen in verband met de maatschappelijke aanvaarding van veiligheidstechnologieën hebben een aantal negatieve consequenties. Voor de industrie bestaat het gevaar dat er geïnvesteerd wordt in technologieën die vervolgens niet door het publiek worden geaccepteerd, zodat de investering tevergeefs is. De afnemers worden gedwongen een minder omstreden product te kopen dat echter niet volledig aan de veiligheidsnoden tegemoet komt.”

Dit kan worden gezien als een argument ter ondersteuning van de stelling van Jeandesboz en Ragazzo (2010) dat de Commissie zich niet echt bekommert om de ethische en wettelijke implicaties van veiligheidstechnologieën.

Zoals eerder aangestipt, biedt een analyse die tot juli 2012 loopt een gemengd beeld van de aard van het programma. Desondanks blijken de critici van de Commissie terecht aan te geven dat het programma disproportioneel veel overhelde naar bepaalde types technologieën, bedrijven en landen waar de defensiesector goed verankerd zat. Dit mag geen verrassing heten als we de ontstaansgeschiedenis van het programma bekijken. Wel is dit misschien zorgwekkend als we ons, zoals in deel 3 van het rapport beschreven, afvragen of het wenselijk of realistisch was om te proberen een markt op gebied van interne veiligheid te ontwikkelen naar analogie met de defensiemarkt.

4.3.2 Beleidsacties door het DG Ondernemingen en Industrie onder de noemer concurrentievermogen van de sector

Tussen 2001 en 2004 richtte de Europese Commissie een aantal beleidsadviesgroepen op om verschillende met defensie verbonden industrietakken te bestuderen: STAR 21 voor de lucht- en ruimtevaartindustrie,^I LeaderSHIP 2015 over scheepsbouw^{II} en de reeds besproken Groep van prominenten over veiligheids- en defensieonderzoek en -ontwikkeling, die onder andere ambieerde hun contacten met de sector aan te halen en zodoende steun te vergaren voor een optreden van de Commissie in de defensie- en veiligheidssector (Slijper, 2005). Zelfs zij die de aanpak van de Commissie steunen, geven openlijk toe dat ze *“binnen de sector op zoek is gegaan naar bondgenoten om haar boodschap kracht bij te zetten”* (Merritt, 2004: 238). De Commissie werkt ook nauw samen met ASD (Aerospace and Defence Industries of Europe), de belangrijkste lobbygroep van de sector. ASD coördineert door de Commissie gefinancierde onderzoeksprojecten zoals SETRAS, een onderzoek over de uitbreiding van maatregelen en veiligheidsnormen voor de bescherming van kritieke infrastructuur. Daarnaast beheert het voor de Commissie enkele samenwerkingsprojecten met derde landen. De activiteiten van de Commissie rond het concurrentievermogen van de veiligheids- en defensiesector krijgen langzamerhand vorm in mededelingen en actieplannen.

In juli 2012 publiceerde de Commissie een mededeling inzake het EU-beleid op het gebied van de veiligheidsindustrie en stelde ze daarin een actieplan voor om het concurrentievermogen en de innovatie van de Europese veiligheidsindustrie te vergroten. De mededeling erkent dat er geen duidelijke definitie van de veiligheidsindustrie is en vertrouwt voor haar cijfers die de waarde ervan inschatten erg op het werk van Ecorys (2011), hoewel dat onderzoek de beperkingen van haar gegevens nadrukkelijk erkende. In tegenstelling tot eerdere documenten, wordt nu aanvaardt dat de veiligheids- en de defensiemarkt, met verschillende eindgebruikers, behoeften en toepassingen, verschillend zijn. Vreemd genoeg wordt dit ook als een interne fragmentatie omschreven (Commissie, 2012a: 8). Interessant is wel dat ze de industriële basis van toeleveranciers aan beide markten enkel als ‘niet geheel identiek’ (Europese Commissie, 2012a: 8) beschrijft, hoewel (zoals besproken in onderdeel 3) andere commentatoren een grotere diversiteit suggereerden. Het actieplan ziet er als volgt uit:

Beëindiging van de fragmentatie van de markt door:

- stappenplannen voor normalisatie
- geharmoniseerde certificatie voor controleapparatuur voor luchthavens en alarmsystemen
- de synergiën tussen veiligheids- en defensietechnologieën via hybride normen te benutten

^I Het STAR21-rapport is hier te raadplegen: ftp://ftp.cordis.europa.eu/pub/era/docs/report_star21_en.pdf

^{II} Het LeaderSHIP-rapport is hier te raadplegen: http://ec.europa.eu/enterprise/sectors/maritime/documents/shipbuilding/index_en.htm

Verkleining van de kloof tussen onderzoek en markt door:

- financieringsprogramma's (met name Horizon 2020 en de ruimte van vrijheid, veiligheid en recht) op elkaar af te stemmen en intellectuele-eigendomsrechten te benutten om gefinancierde projecten te controleren en te valideren
- publieke gebruikers aan te moedigen om technologische innovatie te financieren aan de hand van regels voor pre-commerciële aankopen
- manieren te zoeken om aansprakelijkheid van derden voor bedrijven te beperken

Betere integratie van de maatschappelijke dimensie door:

- het maatschappelijke effect tijdens de O&O-fase te controleren
- een industriële norm in te voeren voor 'privacy by design' (ingebouwde privacy) en 'privacy by default' (standaard-privacy) voor producten.

De mededeling legt duidelijk de nadruk op het belang van exportmarkten en de nood om de handel in veiligheidsproducten niet enkel binnen de EU maar wereldwijd mogelijk te maken (welke gevolgen dit heeft voor exportcontroles, komt aan bod in onderdeel 5). Ook is uit de mededeling de teleurstelling van de Commissie op te maken over het feit dat lidstaten weigeren die technologieën aan te kopen die volgens de Commissie noodzakelijk zijn. Nationale regeringen zijn zichtbaar niet geïnteresseerd in een beleid op het gebied van de veiligheidsindustrie. Tijdens de raadpleging voorafgaand aan de publicatie van de mededeling was amper 7% van de antwoorden afkomstig van de lidstaten. Met slechts 59¹ antwoorden in totaal betekent dit dat vier van de zevenentwintig lidstaten hieraan hun medewerking verleenden. Met maatregelen die beschrijven hoe de begroting van de Commissie voor controle en validering in de toekomst zal worden ingezet en door de precommerciële inkoop te stimuleren tracht de Commissie hier iets aan te doen. Burgers staan weigerachtig tegenover bepaalde veiligheidstechnologieën en lidstaten hebben elk hun geheel eigen visie op privacy en rechten. Deze twee elementen maken dat onderzoek misschien tevergeefs is, wat het industriële concurrentievermogen niet ten goede zou komen.

Dit is evenwel niet louter een probleem van nationale verschillen. Het programma voor veiligheidsonderzoek heeft 13 miljoen euro vrijgemaakt voor de ontwikkeling van een operationeel prototype van een "verplaatsbare autonome patrouille voor de bewaking van vastelandsgrenzen" of "Talos". Het systeem bestaat uit twee onbemande grondvoertuigen (UGV's). Het ene voertuig registreert verdachten die proberen om EU-grenzen over te steken, het andere houdt hen tegen. De UGV's staan in contact met bemande commando-eenheden en brengen deze op de hoogte zodra verdachten werden tegengehouden en opgespoord. Het is mogelijk de UGV's uit te rusten met niet-dodelijke wapens. Het consortium met daarin een Israëliisch bedrijf (Israeli Aerospace Industries) is op zoek naar extra EU-financiering om het product verder te ontwikkelen. Nielsen (2012a) meldt dat een woordvoerder van Frontex het niet waarschijnlijk achtte dat UGV's aan EU-grenzen zouden opduiken maar dat *"Israël er misschien meer mogelijkheden in ziet als systeem om hun grenzen te bewaken"*. Dit impliceert dat de tijdens de O&O-fase beoogde controle van het maatschappelijke effect streng moet zijn.

Tot dusver heeft de Commissie vooral mededelingen verspreid (Europese Commissie, 1996; 1997; 2003; 2007) en opdracht gegeven tot studies zoals IRIS et al (2010) om het concurrentievermogen van de defensiesector te vergroten. De enige omvangrijke wetgevende actie zijn de richtlijnen geweest, dus het defensiepakket dat in 2009 is goedgekeurd en dat we in het volgende punt zullen bespreken. De Commissie koestert echter aanzienlijke ambities op dit beleidsvlak, en de

¹ 51 antwoorden waren afkomstig van bedrijven en vakorganisaties en vier van ngo's.

aankondiging in november 2011 dat ze een task force voor het defensiebeleid samenstelde, is mogelijk veelzeggend. De task force zal vier kernopdrachten hebben:

- *“Ervoor zorgen dat een EU-richtlijn inzake overheidsopdrachten op defensiegebied en een richtlijn inzake de overdracht van defensiegerelateerde producten binnen de EU worden omgezet in nationale wetgeving*
- *De sector tot overleg aansporen om de strategische domeinen te bepalen waar Europa een industriële basis moet vrijwaren om zo strategische autonomie te behouden*
- *Synergiën benutten tussen de veiligheids- en de defensiesector*
- *Problemen met de aanvoorzekerheid coherent aanpakken” (Hale, 2011)*

Op dit ogenblik kunnen we in het volgende punt echter enkel een voorlopige inschatting maken van de impact die het defensiepakket zal hebben.

4.3.3 Actie om de aankoop van defensie- en veiligheidsproducten te reguleren en barrières op intracommunautaire handel weg te werken

Het in september 2004 gepubliceerde Groenboek betreffende overheidsopdrachten op defensiegebied (Europese Commissie, 2004b) gaf de aanzet tot een vergaand overleg met nationale regeringen, de sector en instellingen voor veiligheidsbeleid over wat de beste manier zou zijn om de nationale defensiemarkten, die lange tijd afgeschermd werden, in Europa open te stellen voor concurrentie. Het zag twee mogelijke methodes:

- Een mededeling om te verduidelijken tot waar artikel 296 reikt
- Een bindende richtlijn inzake overheidsopdrachten om de aankoop van items te regelen die niet in de lijst van artikel 296 voorkomen

Tijdens de overlegronde droeg de Britse regering nog een derde optie voor die snel steun kreeg van veel lidstaten:

- Een vrijwillige gedragscode betreffende het gebruik van het artikel, waarbij landen zouden bekendmaken wanneer en waarom ze gebruikmaakten van artikel 296, aangereikt door het EDA

Daarop stelde het EDA in naam van de nationale regeringen een dergelijke code op. Er bestond zo weinig enthousiasme voor de twee voorstellen van de Commissie vooral omdat, zoals Schmitt et al (2005) aangeven, niet duidelijk was of deze maatregelen invloed zouden hebben op de manier waarop de aankoop van hoogwaardig defensiematerieel zou verlopen. En daarin zagen de lidstaten een probleem. De maatregelen zouden gevolgen hebben voor de aankoopprocedures van items die niet op de lijst van artikel 296 voorkomen. Het was en is echter onduidelijk in welke mate protectionisme bij deze aankopen van courant defensiematerieel de handel binnen de EU echt belemmert. Desondanks bracht de Commissie eerst een mededeling naar buiten waarin ze toelichtte hoe artikel 296 (Commissie, 2006) moest worden begrepen. Vervolgens maakte ze twee richtlijnen op die we het defensiepakket zijn gaan noemen; Richtlijn 2009/43/EG betreffende de overdracht van defensieproducten binnen de EUⁱ en Richtlijn 2009/81/EG betreffende aanbestedingen op defensie- en veiligheidsgebied.ⁱⁱ Deze voorstellen verliepen conform artikel 114 van het VWEU, dat wetgevende voorstellen toelaat om nationale wetten te harmoniseren en zo de

ⁱ Richtlijn 2009/43/EG: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:146:0001:0036:NL:PDF>

ⁱⁱ Richtlijn 2009/81/EG: http://ec.europa.eu/enterprise/sectors/defence/files/full_text_of_directive_en.pdf

werking van de interne markt te verbeteren. Terwijl de eerste richtlijn bedrijven administratieve verlichting zou moeten bieden,ⁱ is het de tweede richtlijn die aanzienlijk zou kunnen inwerken op de kracht en het concurrentievermogen van de Europese defensie- en veiligheidssector. De richtlijn stelt de uitwerking voor van een gespecialiseerd systeem van aanbesteding voor de veiligheids- en de defensiesector, met specifieke aandacht voor moeilijke kwesties zoals de zekerheid van aanvoer en de veiligheid van informatie, waardoor aankopers niet langer hun toevlucht zouden moeten zoeken tot artikel 346. In twee belangrijke uitzonderingen is de richtlijn niet van toepassing: in geval van verkoop tussen regeringen en bij multinationale samenwerkingsprojecten (Eguren Secades, 2011). Bovendien zal pas over enkele jaren, wanneer we weten hoe het Hof van Justitie in desbetreffende zaken uitspraken zal doen, ten volle duidelijk worden waartoe de richtlijn heeft geleid. Wellicht zullen de gevolgen het ingrijpendst zijn voor ten eerste die landen met een sterk verankerde defensiesector en die de meeste producten nationaal aankopen, en ten tweede landen die veel wapens importeren en compensatieregelingen gebruiken als een instrument van industrieel beleid.

Het zijn dezelfde paar lidstaten, vooral Groot-Brittannië, Frankrijk en Duitsland, die het grootste defensiebudget maar ook de meest performante industrie hebben. Wat er aan EU-overheidsopdrachten op defensiegebied wordt uitgegeven, heeft met andere woorden vooral betrekking op die landen en hun defensiebedrijven. De richtlijn wil openbare aanbestedingen stimuleren, zodat de concurrentie meer kan spelen en prijzen worden gedrukt. Hier duiken dan wel twee potentiële problemen op. Ten eerste zegt de richtlijn niets over onderzoek en ontwikkeling. Maar zodra de ontwikkelingsfase voorbij is, moet voor de opdracht een openbare aanbesteding worden gelanceerd. Bepaalde landen kunnen daarom aarzelen om onderzoek te financieren, indien ze niet zeker zijn dat een opdracht wordt gegund aan een van hun eigen bedrijven (Edwards, 2011). Verder is wellicht zo dat lidstaten zullen kunnen aangeven welke technologieën vitaal zijn voor hun nationale veiligheid, bijvoorbeeld systemen die worden ingezet bij kernwapens of complexe bewapening, en zo er dus op kunnen aansturen dat die opdrachten in nationale handen blijven. Maar, zo stelt Edwards (2011), de Commissie zou kunnen verzoeken om opdrachten voor grote platformen op te delen, waarbij voor het niet-gevoelige deel een openbare aanbesteding kan worden uitgeschreven. In dit scenario is het niet duidelijk of dit zou bijdragen aan de efficiëntie of betaalbaarheid. Als de Commissie bovendien verzet aantekent tegen deze landen, bestaat er een reëel gevaar dat zij de Europese industrie zullen ondermijnen. Want omdat er weinig Europese alternatieven zijn, zullen ze meer opdrachten moeten openstellen voor Amerikaanse bedrijven.

Ten tweede zullen landen die defensie- en veiligheidsproducten importeren gevolgen ondervinden. Binnen de wereldwijde wapenhandel zijn compensatiesⁱⁱ iets heel normaal.ⁱⁱⁱ De Commissie vindt echter dat deze de aanbestedingsprocedure verstoren omdat op die manier de voorgestelde compensatieregeling zwaarder gaat doorwegen in de beslissing dan de kwaliteit en de prijs. Compensaties zijn volgens de richtlijn niet verboden, maar de Commissie heeft wel duidelijk gemaakt dat ze zal proberen om het voortdurende gebruik ervan te blokkeren. Wat dit betreft kunnen EU-landen in vier groepen worden verdeeld. Frankrijk en Duitsland voeren erg weinig in.

ⁱ Er zouden evenwel problemen kunnen ontstaan om de export terdege te controleren. Dit komt verder aan bod in deel 5. Zie Depauw (2010) voor een volledige bespreking van de richtlijn.

ⁱⁱ De VS omschrijft compensaties als "Industriële praktijken als voorwaarde om een aankooptransactie tussen regeringen of op commerciële basis te laten plaatsvinden, van defensieartikelen en/of diensten zoals omschreven door de Amerikaanse Arms Export Control Act en de International Traffic in Arms Regulations." De volledige definities zijn hier terug te vinden: <http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/offsets/offsetsdefinitions.html>

ⁱⁱⁱ Directe compenserende overeenkomsten gaan uit van producten en diensten die rechtstreeks verband houden met de apparatuur die een land aankoopt (bv. lokale coproductie van onderdelen van het aangekochte wapensysteem. Meestal zijn deze militair van aard. Indirecte compenserende overeenkomsten echter kunnen uitgaan van militaire of civiele producten/diensten die losstaan van de desbetreffende aangekochte defensieapparatuur. Dit mogen buitenlandse investeringen of ruilhandelsacties zijn.

Italië, Nederland, Zweden en het VK zijn netto-exporteurs maar voeren ook aanzienlijke hoeveelheden materieel in uit de VS. Doorgaans koppelen zij indirect een compensatie aan dergelijke opdrachten. Finland, Griekenland, Polen, Portugal en Spanje voeren veel in uit de EU en verwachten directe compensaties. De andere landen hebben een beperkte industriële defensiecapaciteit en werken daarom het meest met civiele indirecte compensatieregelingen (Edwards, 2011). De derde groep, die compensaties gebruikt ter ondersteuning van hun eigen en meestal niet-concurrentiële industrie, heeft het meest te verliezen. De Commissie heeft al eerste pogingen ondernomen om in te gaan tegen het gebruik van compensaties. Het eerste land dat ze daarover aanpakte,¹ was Griekenland, naar aanleiding van een openbare aanbesteding voor zes accukits voor onderzeeërs. De oproep tot inschrijving vereiste onder andere dat 35% van het in de accu gebruikte materiaal in Griekenland was geproduceerd. Hoewel de Griekse regering redenen van nationale veiligheid inriep (artikel 346), besloot de Commissie dat de Grieken in overtreding waren van EU-wetgeving. Zij hadden immers niet gemotiveerd waarom het gebruik van de EU-aanbestedingsvoorschriften Griekse veiligheidsbelangen in gevaar zou brengen. Hoewel we de economische gevolgen van een verbod op de compensatieregeling niet kunnen aantonen, valt te vermoeden dat sommige defensiebedrijven in de betrokken landen hier wel nadeel van zullen ondervinden (Mawdsley, 2008a). De tweede groep landen, die hun materieel in de VS aankopen, zijn mogelijk ook in het nadeel. Zij hebben de compensatie immers vaak gebruikt als manier om subcontractanten in lucratieve Amerikaanse toeleveringsketens te verankeren. Het VK maakt voor haar invoer reeds geen gebruik meer van compensatieregelingen (UK MoD, 2012), wat suggereert dat de impact niet zo groot wordt ingeschat.

We kunnen besluiten dat de richtlijn de markt ongetwijfeld efficiënter zal maken, maar dat we niet weten of deze de Europese defensiesector meer kracht en concurrentievermogen zal geven. Dat enkele niet-concurrentiële bedrijven van de markt verdwijnen, kan op lange termijn een voordeel zijn. Maar aan de operatie zijn wel twee significante risico's verbonden. Ten eerste kan de richtlijn er ongewenst toe leiden dat de VS haar marktaandeel in de EU vergroot ziet. Ten tweede raakt de industriële defensiecapaciteit misschien nog meer geconcentreerd in nog minder landen, met het risico dat het aantal landen toeneemt dat niet meer bereid is om defensie-O&O te financieren. Uit gesprekken in januari 2012 met vertegenwoordigers van de industrie bleek dat de sector de gevolgen bang afwachtte. Daarbij wezen zij erop dat de richtlijn niets ondernam om de vraag te consolideren. Er bestaat geen garantie dat landen die hun eigen industriële defensiecapaciteit zien slinken daarom ook 'Europees kopen'. De VS en Rusland zullen hun producten maar al te graag aan de man brengen en het valt niet uit te sluiten dat hun producten aantrekkelijker blijken dan een eventueel Europees alternatief. De richtlijn geldt ook voor gevoelige veiligheidsproducten. Maar de gevolgen wegen waarschijnlijk minder zwaar door op een markt die nog niet is volgroeid.

4.3.4 Ontwikkeling van een beleid naar analogie met de Amerikaanse 'homeland security' en daaraan verbonden technologische behoeften door DG Binnenlandse Zaken

Het werk van het DG Binnenlandse Zaken vult in veel opzichten dat van het DG Ondernemingen en Industrie aan. Parallel aan het programma voor veiligheidsonderzoek leidt het DG Binnenlandse Zaken ook een kaderprogramma betreffende veiligheid en bescherming van de vrijheden, dat bestaat uit twee specifieke programma's: 'Terrorisme: preventie, paraatheid en beheersing van de gevolgen' en 'Preventie en de bestrijding van criminaliteit'. De totale begroting voor de periode

¹ Persbericht IP/10/1558 is hier te raadplegen:
<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1558&format=HTML&aged=0&language=en&guiLanguage>

2007-13 bedraagt 740 miljoen euro. Dit programma wil steun bieden aan “*operationele, hoogst specifieke en beleidsgerichte activiteiten*”. Vooral het terrorismeprogramma is gericht op de bescherming van kritieke infrastructuur, een doelstelling die het deelt met die van het programma voor veiligheidsonderzoek.

Schengenlanden kunnen ook financiering aanvragen bij het Buitengrenzenfonds, dat die lidstaten financieel wil bijstaan van wie “de implementatie van de gemeenschappelijke normen om de buitengrenzen van de EU te bewaking een zware inspanning vereist”.ⁱ Landen die hun grensbewakingsapparatuur zoals materieel, schepen en helikopters willen moderniseren, kunnen een aanvraag doen. Het fonds financiert sommige projecten tot 90%, hoewel dit in de meeste gevallen 80% zal zijn. In totaal is voor de financiële periode 2007-13 1.820 miljoen euro vrijgemaakt. Vooral voor landen waar de financiële crisis hard heeft toegeslagen, is dit fonds een manier om de aankoop van bepaalde interne en externe veiligheidsapparatuur grotendeels te financieren. Voor de volgende begrotingscyclus 2014-20 heeft de Commissie voorgesteld om een Fonds voor interne veiligheid op te richten met 4.648 miljoen euro financiering. Dit fonds moet een hulp zijn bij de tenuitvoerlegging van de interne veiligheidsstrategie.ⁱⁱ Zulk een instrument dient als financiële ondersteuning voor “*voor politionele samenwerking, voorkoming en bestrijding van criminaliteit, en crisisbeheer*” en voor uitgaven in verband met de buitengrenzen en visa en brengt daarmee de twee reeds besproken programma’s efficiënt samen. Met de mededeling over haar begrotingsplannen beoogt de Commissie specifiek de kloof tussen het programma voor veiligheidsonderzoek en aanbestedingen te dichten. “*Daarnaast zal er financiering ter beschikking worden gesteld voor bijzonder innovatieve projecten die de ontwikkeling van nieuwe methoden of technologieën als doel hebben, vooral het testen en valideren van de resultaten van door de EU gefinancierd veiligheidsonderzoek. Dit zal helpen om de kloof te dichten die bestaat tussen de onderzoeksresultaten die met steun uit het achtste kaderprogramma zijn bereikt en de opeenvolgende toepassing van die resultaten in de praktijk ten behoeve van de rechtshandhavingsautoriteiten.*” (Commissie, 2011: 7) Verdere verbanden lopen via het voorgestelde grensbewakingssysteem EUROSUR, dat bijvoorbeeld het volgende stelt: “*Het gebruik van de EU-programma's voor onderzoek en ontwikkeling zal ten goede komen aan de technische werking van bewakingsinstrumenten en -sensoren (bv. satellieten, onbemande vliegtuigen, enz.)*” (Europese Commissie, 2008).ⁱⁱⁱ De mededeling van de Europese Commissie (2012a: 9) inzake het beleid op het gebied van de veiligheidsindustrie stelt ook uitdrukkelijk dat het Fonds voor interne veiligheid kan worden aangewend ter financiering van de controle en validering van gefinancierde projecten voor veiligheidsonderzoek. Zelfs ondanks het feit dat de lidstaten zoals besproken in deel 3 niet zeker zijn of zij hun vraag naar interne veiligheidstechnologieën wel moeten opdrijven, doet de Europese Commissie er blijkbaar toch alles aan om de markt te maximaliseren.

4.4 Europees Defensieagentschap

De rol van het Europees Defensieagentschap wordt als volgt gedefinieerd:

“Er wordt een agentschap op het gebied van de ontwikkeling van defensievermogens, onderzoek, aankopen en bewapening (hierna: ‘het Europees Defensieagentschap’ te noemen) opgericht, dat de operationele behoeften bepaalt, maatregelen bevordert om in die behoeften te voorzien, bijdraagt

ⁱ Voor informatie over het Buitengrenzenfonds zie: http://ec.europa.eu/home-Affairs/funding/borders/funding_borders_en.htm

ⁱⁱ EU-interneveiligheidsstrategie: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/113055.pdf

ⁱⁱⁱ Voor een uiterst kritisch rapport over beide initiatieven en met name over hoe de Europese Commissie de beweringen van bedrijven over hun uitrusting zonder meer voor waar nam, zie Hayes en Vermeulen (2012).

tot de vaststelling en, in voorkomend geval, tot de uitvoering van alle nuttige maatregelen om de industriële en technologische basis van de defensiesector te versterken, deelneemt aan het bepalen van een Europees beleid inzake vermogens en bewapening, en de Raad bijstaat om de verbetering van de militaire vermogens te evalueren". (VEU artikel 42(3))

Het is daarom logisch dat het EDA de opdracht krijgt om op de kracht en het concurrentievermogen van de Europese industriële en technologische defensiebasis (EDITB) toe te zien. Het EDA zal de bewapeningsinspanningen van de EU strategisch moeten sturen. Daarom loont het de moeite een analyse te maken van hoe het de toestand van de Europese industriële defensiebasis van de toekomst (2007) inschat, om zo na te gaan of zij coherente en haalbare beleidsvoorstellen hebben kunnen formuleren. Vanuit de wetenschap dat harmonisatie van de vraag vereist is om het aanbod te kunnen consolideren, stelt het EDA (2007) dat de EDITB er als volgt moet uitzien:

- Capaciteitsgedreven (er dus op gericht, de echte operationele behoeften van de krijgsmacht van de toekomst in te vullen en tegelijk de vereiste niveaus aan Europese en nationale operationele soevereiniteit aan te houden);
- Competent (met name duiden op het snel inzetten van de beste technologieën); en
- Concurrentieel (zowel binnen als buiten Europa).

Volgens het EDA kunnen we dit enkel bereiken door meer te consolideren, werk te delen, onderlinge afhankelijkheid op EU-basis te creëren, met meer (correct regionaal verspreide) expertisecentra, meer integratie in de civiele industriebasis, met *"voor cruciale defensietechnologieën minder Europese afhankelijkheid van niet-Europese bronnen"*, zonder echter een Fort Europa-aanpak te hanteren (EDA, 2007). Dit mogen dan wel lovenswaardige doelen zijn, het is duidelijk dat we door nog verder te consolideren monopolies in plaats van concurrentie zullen creëren (Hartley, 2006) en dat een regionale verspreiding (hoewel gewenst) de ogen sluit voor de toestand waarin de EDITB zich werkelijk bevindt (Mawdsley, 2008b). Eigenlijk is, zoals Hartley (2011) aangeeft, de industriële defensiecapaciteit in de EU nog altijd te groot, zodat deze bedrijven niet kunstmatig moeten worden ingedekt. Het EDA heeft in veel opzichten de zo goed als onmogelijke opdracht geërfd, de ambities te verzoenen van grote en kleine wapenproducerende landen, Fort Europa- en vrijemarktadepten die vooruitgang binnen de WEAG hebben geblokkeerd. En dit alles moet dan gebeuren in tijden van besparingsmaatregelen, wanneer steeds meer lidstaten, volgens de eigen cijfers van het EDA, afhaken voor wat defensieonderzoek betreft en hun uitgaven voor defensie krimpen. Ook heeft het EDA het moeilijk omdat het een beleid moet zien te ontwikkelen zonder de geschikte gegevens; zoals Hartley stelt zijn de *"data erg beperkt: met onvolledige gegevens kan men niet over de cijfers beschikken die toelaten, de individuele sectoren van de EDITB zoals het hoort economisch te beoordelen."* (Hartley, 2011: 96-7)

Twee problemen zitten het EDA echter het meest in de weg. Ten eerste beschikt het niet over het budget om de stimulansen aan te bieden die lidstaten zullen doen participeren.¹ Ten tweede heeft het Verenigd Koninkrijk van bij het begin met de handrem op gereden en vraagt het land zich af of het nog verder betrokken wil blijven. Reeds in november 2006, toen het EDA-stuurcomité een driejarig onderzoeksprogramma betreffende troepenbescherming ter waarde van 54,23 miljoen euro opstartte, weigerde het VK om deel te nemen. Frankrijk lijkt ook niet helemaal overtuigd dat het EDA kan instaan voor wat het voor zijn eigen DITB belangrijk vindt. Wanneer de twee landen met het grootste budget voor defensieonderzoek en –opdrachten niet actief mee aan boord klimmen, is het moeilijk denkbaar hoe het EDA zulke aanzienlijke doelstellingen ooit kan halen. Net zoals de Commissie is het EDA geen klant. Het kampt dus met hetzelfde probleem dat zelfs

¹ Hoewel de begroting steevast is toegenomen, bedroeg ze in 2010 nog altijd maar 31 miljoen euro.

wanneer het de ontwikkeling van technologieën tot in de demonstratiefase financiert, het lidstaten niet kan dwingen om apparatuur aan te kopen. Men begrijpt dat dit geen incentive is voor sterkere bedrijven om technologieën met elkaar te delen. Het is daarom beperkt in zijn mogelijkheden om de EDITB kracht bij te zetten. Dit betekent niet dat het Europees Defensieagentschap niets nuttigs heeft bereikt. Het heeft verschillende projecten opgezet die militair echt bruikbaar zijn. De introductie van de vrijwillige gedragscode om defensieaanbestedingen openbaar te laten verlopen, heeft het de weg geëffend voor de richtlijn van de Commissie. Bovendien heeft wat het rond de compensatiemaatregelen heeft gedaan een nuttige inkijk opgeleverd in de Europese manier van werken.

Hoewel de samenwerking tussen de Commissie en het EDA nu vastligt in het Europees samenwerkingskader voor veiligheid en defensie en doorgaans goed lijkt te verlopen, is het ook moeilijk om de aanpak om te zetten die de Commissie in verband met de 'Europese markt voor defensie-uitrusting' (EDEM) voorstaat en de defensiemarkt zo veel mogelijk blijkt te willen behandelen als een interne markt (zoals al bleek in de uitleg over de aankooprichtlijn), en tegelijk een EDITB te behouden. Hartley (2011) zet volgende moeilijke keuzes die zich opdringen op een rijtje:

*“i) **Onverenigbaarheden tussen EDEM en EDITB.** Er moeten keuzes worden gemaakt: ofwel alleen bedrijven uit lidstaten de concurrentie laten aangaan, ofwel ook andere bedrijven van elders ter wereld toegang verlenen tot EU-defensiemarkten (bv. Amerikaanse defensiebedrijven). Concurrentie kan ook een gevaar betekenen voor de voornaamste industriële defensiecapaciteiten en het voor de EDITB vereiste regionale evenwicht verstoren. Als de concurrentie wordt uitgeschakeld, zal men private bedrijven met een defensie-monopolie moeten behandelen als gereguleerde bedrijven, met alle problemen van prijsbepaling, efficiëntie en winstmarges van dien.*

*ii) **Belangrijke gespecialiseerde industriële defensiecapaciteiten ook bij een gering ontwikkelings- en productieniveau op peil houden.** Sommige gespecialiseerde bedrijven kunnen hun installatie en mensen niet voor andere doeleinden inzetten maar moeten naderhand toch inzetbaar zijn (bv. capaciteit in kernonderzeeërs, zware gevechtstanks, vliegdekschepen). Dergelijke specialisten kunnen grote contractanten zijn, of kleine en middelgrote ondernemingen in de aanvoerketen van de defensiesector. Kiezen welke kerncapaciteiten men wil behouden, is maar de eerste stap. Ook wordt het moeilijk wanneer er wordt gesproken over manieren om dit te doen (bv. tussentijdse bestellingen; installaties buiten gebruik, enz.), de kostprijs van alternatieve maatregelen, wie beslist en wie betaalt.” (Hartley, 2011: 111)*

Dit zijn beslissingen die politiek heel moeilijk liggen en vereisen een zekere intra-institutionele samenwerking die niet evident is.

4.5 EU-lidstaten

Sommige lidstaten zien de Europese Unie vandaag als de natuurlijke habitat voor beleidsvorming over de defensie- en de veiligheidssector. Maar andere actoren zitten niet op diezelfde lijn. Ten eerste heeft een toenemend aantal landen zoals Duitsland, het VK en Frankrijk duidelijk gesteld dat voor hen het GVDB een vehikel is voor crisisbeheer, maar niet voor defensie (Auswärtiges Amt, 2012; Haine, 2011). Vooral de Frans-Britse akkoorden van Lancaster House uit 2010 hebben het

potentieel om in de defensiesector een omwenteling in gang te zetten. Ten tweede bestaan er verschillende multilaterale initiatieven die zich buiten de EU afspelen, zoals OCCAR (Organisation Conjointe pour la Coopération en matière d'Armement) en de Raamovereenkomst. De NAVO ten slotte engageert zich in samenwerkingen rond terrorismebestrijding en cyberoorlogvoering.

4.5.1 Voornaamste bilaterale en multilaterale overeenkomsten

Belangrijk is dat we benadrukken dat multilaterale en bilaterale samenwerking inzake defensie niet van het toneel is verdwenen. Formele verbanden zoals de sterk ontwikkelde Nordic Defence Cooperation (NORDEFCO) en de steeds actiever wordende Visegradgroep proberen om hun capaciteiten te vergroten via nauwere samenwerking tussen een klein aantal gelijkgezinde landen. Maar het zijn vooral de Frans-Britse akkoorden van 2010 inzake defensiesamenwerking die belangrijk lijken te worden; de parameters die zij vastleggen zullen wellicht richtinggevend zijn voor de toekomstige Europese samenwerking rond bewapening. Gezien de focus op conventionele en nucleaire wapens loont het de moeite na te gaan tot waar de afspraken reiken. Binnen het kader van twee wettelijk bindende verdragen gingen beide landen het engagement aan om hun strijdkrachten meer te doen samenwerken en samen de ontwikkeling van hun nucleaire wapentechnologie op zich te nemen. Dit betekende een drastische wijziging in de reikwijdte en diepgang van hun bilaterale samenwerking. Bovenop het baanbrekende verdrag inzake nucleaire samenwerking, de inrichting van een gezamenlijke expeditiemacht en verschillende 'pooling and sharing'-maatregelen spraken Londen en Parijs ook af om voor defensie een vergaande industriële samenwerking aan te gaan.

De overeengekomen samenwerking inzake defensietechnologie en -industrie gaat ook uit van strategische overwegingen die met de loop der jaren steeds meer gemeenschappelijk tot stand zijn gekomen.^I Het tienjarenplan op het vlak van complexe wapens dat in 2011 van start moet gaan met de ontwikkeling van het FASGW(H)/ANL antischeepswapen, een onderzoek naar de uitbreidingen op de Scalp/Storm Shadow kruisraketten en een gemeenschappelijk technologie-stappenplan voor kortereafstand luchtafweerraketten gaf aan hoe belangrijk de intensievere industriële samenwerking voor beide landen is. Om Britse en Franse defensiebedrijven meer te doen samenwerken is een financieringsbudget voor gezamenlijke onderzoeks- en ontwikkelingsprojecten ten bedrage van 100 miljoen euro per jaar vastgelegd. Volgens Chick (2011) heeft de Frans-Britse samenwerking veel te maken met het behoud van industriële defensiecapaciteiten. Verdere overeenkomsten in 2010 én 2012 om samen te werken rond MALE-drones en toekomstige luchtgevechtssystemen zouden dat marktsegment – met sponsoring van overheidswege – kunnen consolideren. In dat geval zouden andere Europese landen buitenspel komen te staan (Kempin, Mawdsley en Steinicke, 2012).^{II}

Parijs en Londen hadden ook de mogelijkheid om de afgesproken projecten binnen het EU-kader van permanent gestructureerde samenwerking uit te voeren en zo lidstaten de kans te bieden inzake defensie flexibel samen te werken. Hun beslissing toont aan hoe weinig beide landen geloofden dat het GVDB nog tot enige substantiële vooruitgang inzake capaciteitssamenwerking zou komen, en vooral hoe teleurgesteld Frankrijk was omdat het tijdens zijn EU-voorzitterschap in 2008 en in de nasleep van de missie in Tsjad geen echte stappen vooruit had kunnen zetten (Haïne, 2011). Deze houding zal ook zijn gevolgen hebben voor het Europees Defensieagentschap (EDA). Het lijkt erop dat beide landen niet tevreden waren met wat het EDA had kunnen

^I In 2007 startten beide landen een innovatie- en technologiepartnerschap op dat naar synergieën moest zoeken in het onderzoek en de vereisten op het vlak van complexe wapens.

^{II} Het bezwaar dat Italië bij de Commissie aantekende als zou de Frans-Britse samenwerking de concurrentie fnuiken, werd van tafel geveegd (Kington, 2011).

bewerkstellingen in de ontwikkeling van dringend vereiste militaire capaciteiten en daarom besloten hadden om buiten de EU-instellingen om samen te werken. Frankrijk is tot dusver altijd vooropgegaan in de ondersteuning van het werk dat het EDA leverde. Dat het land nu deze beslissing heeft genomen, zal wellicht leiden tot een verzwakking van het EDA. Groot-Brittannië en Frankrijk hebben de EU-samenwerking rond bewapening niet de rug toegekeerd maar hebben duidelijk gesteld dat deze onder hun voorwaarden moet verlopen. Wellicht zullen zij ook weigerachtig staan tegenover enige betrokkenheid van de Commissie bij defensie, als zij aanvoelen dat deze hun industriële defensiecapaciteiten in het gedrang kan brengen.

Het is ook interessant even aandacht te besteden aan de Raamovereenkomst betreffende de industriële herstructurering (VK, Frankrijk, Duitsland, Italië, Zweden en Spanje) en de Organisation Conjointe de Coopération en matière d'Armement (OCCAR – VK, Frankrijk, Duitsland, Italië, België en Spanje), niet omdat zij wellicht hun stempel zullen drukken op het optreden van de EU, maar omdat wat zij op dit terrein meemaken sprekend is voor sommige problemen waarop het EDA en mogelijk de Commissie zullen stoten. De raamovereenkomst kwam tot stand door de afsluiting van de zogenaamde intentieverklaring, waarvoor de ministers van Defensie van Frankrijk, Duitsland, Spanje, Italië, Zweden en het VK zich in juli 1998 inschreven. Deze intentieverklaring wilde een kader ontwikkelen voor samenwerking met het oog op de herstructurering en werking van de West-Europese defensiesector en daarnaast een door de industrie aangevoerde herstructurering begeleiden van de sector voor zowel ruimtevaart- als defensie-elektronica. In 2000 ondertekenden dezelfde ministers de Raamovereenkomst die maatregelen vastlegde voor een verbeterde samenwerking inzake harmonisatie van militaire behoeften, continuïteit van het aanbod, exportprocedures, onderzoek en technologie, omgang met geheime informatie en de behandeling van technische gegevens. Sinds de oprichting van het EDA heeft de groep haar werkzaamheden voortgezet en enkele nuttige stappen afgesproken, maar de samenwerking heeft niet tot gezamenlijke aanbestedingsprojecten geleid. Een rapport uit 2005 over de landen in de raamovereenkomst vond verrassend genoeg amper aanwijzingen van fragmentatie en duplicatie, zelfs niet bij landen met een sterke defensie-industrie. Bovendien bleek dat slechts 7% van de besproken defensietechnologieën voor alle zes de landen een gemeenschappelijke prioriteit was. Bilateraal was er wel sprake van een gemeenschappelijke vraag naar 74% van de technologieën (UK MoD, 2006:35). Dit doet de vraag rijzen of de EU-analyse van marktfragmentatie en –duplicatie wel correct was maar toont aan – en dit is wellicht belangrijker – hoe moeilijk er onderzoeks- en aanbestedingsprojecten te vinden zullen zijn waaraan alle grote wapenproducerende landen bereid zouden zijn deel te nemen.

OCCAR is een beheersagentschap voor collaboratieve aanbestedingsprogramma's inzake defensie-uitrusting. Sinds 2009 blokkeren Griekenland en Cyprus in de Raad een overeenkomst met het oog op een administratieve regeling voor samenwerking tussen het EDA en OCCAR en betreffende de uitwisseling van geheime informatie. OCCAR moest collaboratieve aanbestedingsprojecten inzake defensie-uitrusting op een veel commerciële basis beheren, gebruikmakend van beste praktijken met betrekking tot aanbestedingen uit de privésector, en als een onafhankelijk agentschap om het proces los van politieke kwesties te laten verlopen. De A400M was het eerste project dat via deze commerciële aanpak zou worden begeleid en de resultaten waren niet goed. Dit deed Britten en Fransen besluiten dat ze de duurzaamheid van hun DITB niet op het spel mochten zetten door samen te werken met partners die hen niet in hun ernstige aanpak volgden (Brits Lagerhuis, 2010; Masseret en Gautier, 2009). OCCAR is niet afgeschreven, maar door de ervaring met het A400M-project zullen belangrijke landen misschien niet meer zo makkelijk over de streep te trekken zijn om mee in grootschalige GVDB-aanbestedingsprojecten te stappen die openbaar zijn voor alle EDA-lidstaten.

4.5.2 Is de NAVO relevant?

Zoals Haine (2011) aangeeft blijft de NAVO een centrale speler in het overleg over Europese veiligheid en defensie. Hoewel de VS aarzelde in haar optreden werd de NAVO (onder leiding van Fransen en Britten) en niet de EU de belangrijkste actor tijdens de Libische operatie in 2011. Verwijzend naar de inhoud van dit rapport engageert de NAVO zich ook in samenwerkingen rond terrorismebestrijding en cyberoorlogvoering. Hier willen we kort beschrijven hoe NAVO- en EU-acties voor wat de rol van de industrie in deze domeinen en desbetreffende technologieën betreft met elkaar overlappen.

Overlapping bestaat er al zeker tussen het 'Smart Defence'-initiatief van de NAVO, dat landen in staat wil stellen om gezamenlijk apparatuur aan te kopen, en het EU-initiatief van Gent betreffende 'pooling and sharing' van militaire capaciteit. Beide initiatieven proberen de Europese militaire capaciteit te verbeteren. Maar volgens Maulny (2012) bestaat het gevaar dat de twee programma's in conflict zullen komen, tenzij duidelijke afspraken worden gemaakt over de modaliteiten van de respectieve programma's. Maulny (2012) gebruikt het voorbeeld van het poolingsysteem om bij te tanken in de lucht, waarbij de EU en de NAVO mekaar de loef afsteken.

Op het vlak van terrorismebestrijding is er tevens overlapping mogelijk tussen het NAVO-programma Defence Against Terrorism (DAT) en initiatieven van de Europese Commissie en het EDA inzake de ontwikkeling van veiligheids- en defensietechnologieën. Het DAT-programma gebruikt wetenschappelijk onderzoek en tests van technologieën voor terrorismebestrijding als basis. De NAVO en het EDA werken evenwel intensief samen zodat ze geen dubbel onderzoekswerk verrichten, en DAT is een louter militair programma. Het is toegespitst op tien domeinen waarin technologie een nuttige rol zou kunnen spelen. Voor elk domein is telkens één land verantwoordelijk.

- Civiele en militaire breedrompvliegtuigen minder kwetsbaar maken voor draagbare luchtverdedigingssystemen (MANPADs) (VK)
- Havens en schepen beschermen aan de hand van sensornetten, elektro-optische detectoren, snelle-reactie-vermogens en onbemande onderwatervaartuigen (Italië / Portugal)
- Helikopters minder kwetsbaar maken voor rocket-propelled grenades (RPG's) (Bulgarije / Griekenland)
- Geïmproviseerde explosieven (IED's) zoals auto- en bembommen bestrijden door deze te detecteren, onklaar te maken of te neutraliseren (Spanje)
- Chemische, biologische, radiologische en nucleaire (CBRN) wapens opsporen, daartegen beschermen en uitschakelen (Tsjechië).
- Technologieën voor inlichtingendiensten, verkenning, bewaking en het opsporen van doelwitten (IRSTA), om betere tools te kunnen ontwikkelen met het oog op waarschuwing voor en identificatie van terroristen en hun activiteiten (Duitsland)
- Explosievenopruiming (EOD) (Slowakije)
- Technologieën om te beschermen tegen morteraanvallen (DAMA) (Noorwegen)
- Bescherming van kritieke infrastructuur – vandaag een overkoepelend project binnen het DAT-programma, geïntegreerd in het door Portugal geleide programma voor de bescherming van havens
- niet-dodelijke capaciteiten (Canada)¹

Dit werkprogramma werd goedgekeurd in juni 2004 en mag niet overlappen met de activiteiten die de Commissie vandaag rond veiligheidsonderzoek uitwerkt, aangezien deze van civiele aard

¹ Voor meer informatie over het DAT-programma, zie http://www.nato.int/cps/en/natolive/topics_50313.htm.

moeten zijn. Maar het industriële veiligheidsbeleid van de Commissie en haar Defence Task Force trachten beide om naar de toekomst toe synergiën tussen de veiligheids- en de defensiesector tot stand te brengen. Dit betekent dat conflicten mogelijk zijn. Ook cyberbeveiliging en cyberoorlogvoering zijn domeinen waarvoor gemeenschappelijke interesse kan bestaan. Precies op dit domein zou de NAVO haar rol kunnen spelen, gesteld dat ze zou worden gebruikt als forum waar de VS en de EU technologische informatie kunnen uitwisselen over welke projecten op gebied van 'homeland security' haalbaar waren. Het Amerikaanse ministerie van Homeland Security is nu niet in de mogelijkheid om aan dergelijke uitwisselingen deel te nemen. Maar als daar verandering in zou komen, dan zou de NAVO wellicht het geschikte speelveld vormen (Commissie homeland security en exportcontroles, 2012). Daar sommige door de Europese Commissie gefinancierde onderzoeken sterk gelijken op projecten die de VS wegens hun inefficiëntie heeft stilgelegd, kan dit kostenbesparend zijn (wat erg belangrijk is in tijden van financiële crisis).

4.6 Samenvatting

Dit hoofdstuk van het rapport schetste in om te beginnen de juridische basis voor EU-optreden. Vervolgens besprak dit deel het beleid van de Commissie, vanuit het standpunt van het programma voor veiligheidsonderzoek, het optreden om de sector competitiever te maken, het zogenaamde defensiepakket en ten slotte de betrokkenheid van DG Binnenlandse Zaken in de ontwikkeling van een beleid naar analogie met de Amerikaanse 'homeland security'. Vervolgens richtte het zijn blik op het Europees Defensieagentschap. Het laatste deel ging over de relevante Europese activiteit buiten de EU, in casu de Frans-Britse defensieakkoorden, OCCAR, de Raamovereenkomst en de NAVO, met een poging om te beoordelen of zij dan wel enige betekenis hebben voor het welslagen van het EU-beleid.

Hoewel de Commissie lang de ambitie heeft gekoesterd om actief te zijn in de sector, is ze daar slechts de laatste tien jaar enigszins in geslaagd. Het is pas nu dat de eerste richtlijnen worden omgezet in nationale wetgeving. Vandaag is niet duidelijk of de lidstaten zullen toestaan dat de Commissie haar rol verder uitbreidt (hoewel dit klaarblijkelijk wel haar bedoeling is) en bestaat er onenigheid over de vraag of er al dan niet een juridische basis voorhanden is om op het vlak van nationale veiligheid nog meer initiatief te nemen. Haar acties op het vlak van interne veiligheid vallen deels binnen, deels buiten het Verdrag van Lissabon. En ook lijkt het erop dat de aandacht die de Commissie tot dusver aan bewakingstechnologieën heeft besteed juridisch zal standhouden. Blijkbaar stelt de Commissie voor zowel de defensie- als de veiligheidsmarkt dezelfde diagnose, en die is:

- Het aanbod is te gefragmenteerd. Dit vraagt om industriële consolidering en fusies in alle sectoren.
- Ook de vraag is te gefragmenteerd en zowel nationale systemen voor aanbesteding als behoeften moeten op elkaar worden afgestemd.

Vanuit deze overtuiging zet de Commissie haar acties uit. Maar volgens haar critici mag ze niet veronderstellen dat de veiligheids- en de defensiemarkt in feite inwisselbaar zijn, en moet ze naar meer genuanceerde beleidsbehoeften toewerken. Ook vinden zij dat de Commissie een fout heeft begaan door een te zeer op technologie en op de defensiesector gerichte aanpak te volgen in vergelijking met de eerder genuanceerde behoeften die gebruikers van interne veiligheid ervaren (en door de ethische vragen die omtrent haar agenda opdoken te weinig aandacht te verlenen). Dat de Commissie, die (ondanks duidelijke pogingen via het Buitengrenzenfonds) niet als klant kan

optreden, de vraag van gebruikers te hoog heeft ingeschat, wijst erop dat dergelijke interacties in het volgende kaderprogramma meer aandacht moeten krijgen, want dat onderzoek anders verloren zal gaan. Wellicht het grootste probleem in de ontwikkeling van het veiligheidsonderzoek is dat wat de Commissie heeft ondernomen om meer beleidsbevoegdheden binnen te halen een kloof heeft geslagen tussen waar de Commissie en de sector heen willen en wat lidstaten en EU-burgers bereid zijn te aanvaarden. Dit kan onbedoelde gevolgen hebben. Ook is het heel belangrijk dat ze probeert om de vraagzijde van de defensiemarkt aan de hand van aanbestedingen te hervormen op een manier dat dit niet raakt aan de EDITB.

Het Europees Defensieagentschap heeft de schier onmogelijke opdracht gekregen, de lidstaten met elk hun eigen tegenstrijdige wensen op één lijn te krijgen, zonder dat het daarvoor het vereiste budget en de steun van ook maar één belangrijke lidstaat (en steeds minder andere lidstaten) heeft. Hoewel het enkele ontegensprekelijk nuttige projecten heeft lopen, is het er zoals we konden verwachten niet in gelukt deze verschillen weg te werken. Ondanks het feit dat het moeilijk zal zijn om tot een politiek compromis te komen, vereisen de vragen over hoe tegenstellingen tussen marktgedreven en protectionistische methodes te overwinnen, en hoe belangrijke EDITB-capaciteiten te behouden nu de vraag zo beperkt is, nu dringend een antwoord. Zoals Hartley (2011) aangeeft, zijn Europese defensiebedrijven vergeleken met hun Amerikaanse tegenhangers niet bepaald concurrentieel. En het valt niet te verwachten dat, zoals sommigen optimistisch hebben gemeend, de veiligheidsindustrie en de vraag hieraan snel iets zullen veranderen.

Aan de beleids capaciteit van de EU om het concurrentievermogen van de Europese veiligheids- en defensiesector te versterken wordt vooral van buiten de EU-instellingen getornd. Hier spelen voornamelijk twee zaken. Ten eerste is er de NAVO die actiever wordt op het vlak van terrorismebestrijding. Dit houdt het risico in dat er een trans-Atlantische agenda opduikt die de Commissie in haar acties misschien zal overvleugelen of tegenwerken. Maar zoals hierboven vermeld kan dit ook nuttig zijn om geen dubbel of tevergeefs werk te leveren. Ten tweede kunnen de Frans-Britse akkoorden het startsein betekenen voor een nog verdere concentratie van de aanbestedings- en onderzoeksuitgaven en industriële macht in zowel de defensie- als de veiligheidssector, wat indruist tegen elk poging om tot regulering te komen. Hoe moeilijk dit voor diegenen die liever een EU-optreden zien plaatsvinden ook te verteren mag zijn, het is ook mogelijk dat beide landen het bij het rechte eind hebben en dit de enige manier is om met het oog op een eventuele Europese veiligheidsactie voldoende industriële, technologische en militaire capaciteiten te vrijwaren.

Ondanks deze kanttekeningen is de Commissie momenteel een hoofdrolspeler in dit veld. Maar als ze haar bevoegdheden zonder meer verder wil uitbreiden, moet ze een meer realistische inschatting maken van wat lidstaten ten tijde van een begrotingscrisis kunnen uitgeven aan veiligheid en defensie, en veel meer oog hebben voor de ethische kwesties die bij veiligheid komen kijken. Als reactie op de negatieve houding van voorstanders van een civiele EU-macht tegenover het EVDB stelde Bailes het volgende:

“Het echte probleem is niet zozeer de ‘militarisering’ van de Unie als wel een steeds meer opvallende verveiliging van haar hele identiteit en imago, die de EU als gewetensvol organisme nog niet kan erkennen, laat staan er op een volwassen manier mee omgaan, en waarop de kleinschalige, naïef aandoende avonturen van het EVDB een welkome afwisseling kunnen zijn.”
(Bailes, 2008: 119)

Dit is zeker geen foute omschrijving van de activiteiten van de Commissie, in die zin dat het net is alsof deze geen aanvaardbaar evenwicht tussen mensenrechten en veiligheid wil vinden. En dit zal

de kloof tussen wat de EU op dit domein doet en haar verklaringen betreffende het buitenlandbeleid alleen maar vergroten. Dit heeft zijn onmiddellijke gevolgen voor de exportcontroles op veiligheidstechnologieën.

5 Veiligheidstechnologieën en hun impact op exportcontroles van strategische goederen

5.1 Inleiding

De Arabische Lente deed opnieuw vragen rijzen bij de geschiktheid van de EU-regelgeving met betrekking tot wapenexportcontrole. Bromley (2012: 14-5) stelt het als volgt: *“Vooral bezwarend in het hele exportverhaal vanuit EU-lidstaten naar het Midden-Oosten en Noord-Afrika in het spoor van de opstanden in de Arabische landen was de overdracht van bewakingssoftware en andere soorten technologie om tegenstanders van het regime in het oog te houden.”*ⁱ Deze rapporten hebben beleidsmakers doen buigen over de vraag hoe deze technologieën op te volgen en te controleren zijn. In 2011, toen het Europees Parlement een poging ondernam om Verordening 428/2009 van de Raad betreffende de uitvoer van technologieën voor tweeeërlei gebruikⁱⁱ te wijzigen, is het er slechts deels in geslaagd om dergelijke technologieën mee te laten opnemen. Maar dat de in 2012 door de EU getroffen sancties tegen Syrië en Iran nu ook beperkingen zetten op de export van telecommunicatietechnologie en –apparatuur voor bewakingsdoeleinden, wijst erop dat het thema nog steeds op de politieke agenda staat. Het hernieuwde debat over de controle van veiligheidstechnologieën verplicht de EU nogmaals om deze moeilijke kwestie op tafel te leggen. De gedragscode betreffende wapenuitvoer, die naderhand een gemeenschappelijk standpunt is geworden, moest initieel ook een derde lijst bevatten (naast de lijst met militaire producten en die met producten voor tweeeërlei gebruik) bestaande uit goederen bestemd voor gebruik door veiligheids- en politiediensten. Volgens Bauer (2003) leidde onenigheid over wettelijke bevoegdheid, definities en controlemethodes ertoe dat de lijst niet werd toegevoegd. In de plaats daarvan kwam er in 2005 een afgezwakte (in die zin dat er minder goederen in stonden) en specifiekere verordening, de zogenaamde folterverordening. Deze legt bepalingen vast voor sommige veiligheidstechnologieën en -producten – soms vallen deze onder de militaire of ‘dual-use’ lijst, soms onder de folterverordening – terwijl bij andere de controle enkel op nationaal niveau plaatsvindt. Maar de wettelijke situatie is niet zo duidelijk als zou kunnen. Bromley (2012) stelt dat één groep van veiligheidstechnologieën voor bewakings- en detectiedoeleinden buiten elke controle valt. Tijdens de Arabische Lente werden ze dan ook uitgevoerd en misbruikt.ⁱⁱⁱ

Hoewel Privacy International (1995) al in 1995 wees op de problematische aard van de handel in bewakingstechnologieën, hadden noch het middenveld noch wetgevers vóór de Arabische Lente

ⁱ Zie onder andere Wagner (2012a) en Timm en York (2012).

ⁱⁱ Deze omschrijft ‘producten voor tweeeërlei gebruik’ als “producten, met inbegrip van programmatuur en technologie, die zowel een civiele als een militaire bestemming kunnen hebben, met inbegrip van alle goederen die voor niet-explosieve doeleinden gebruikt kunnen worden en op enige manier bijdragen in de vervaardiging van nucleaire wapens of andere nucleaire explosiemiddelen”, Raad van de Europese Unie, Verordening 428/2009 tot instelling van een communautaire regeling voor controle op de uitvoer, de overbrenging, de tussenhandel en de doorvoer van producten voor tweeeërlei gebruik, Brussel, 5 mei 2009: artikel 2 (1)

ⁱⁱⁱ Het is niet helemaal duidelijk of dit klopt. In 2012 verklaarde de Britse regering, in een antwoord op een brief van Privacy International, Gamma International, de producent van de Finspy-bewakingssoftware, te hebben laten weten dat zij een licentie moesten hebben voor alle uitvoer buiten de EU. Het product gebruikte immers gecontroleerde cryptografie zoals voorzien in categorie 5 deel 2 van de wetgeving inzake producten voor tweeeërlei gebruik. Het heeft er alle schijn van dat dit zou gelden voor andere, gelijkaardige producten (Privacy International, 2012)

veel aandacht voor de export van bewakings- en andere veiligheidstechnologieën. Wel waren er enkele rapporten van ngo's zoals Amnesty International en de Omega Foundation die campagne hebben gevoerd rond het thema (Amnesty International en Omega, 2010; Amnesty International, 2011). Sterker nog, sommige landen, met name Duitsland, zagen niet zozeer de problemen dan wel de enorme exportmogelijkheden die de sector van veiligheidstechnologieën te bieden had (Bundesministerium für Wirtschaft und Technologie, 2010).^I Ook de Europese Commissie (2012a: 2) bleef zelfs na de Arabische Lente vinden dat er een EU-merk voor veiligheidstechnologieën moest komen, omdat: *“in de toekomst de belangrijkste markten voor veiligheidstechnologie zich niet in Europa zullen bevinden, maar in opkomende landen in Azië, Zuid-Amerika en het Midden-Oosten.”*

De mededeling inzake het beleid op het gebied van de veiligheidsindustrie wijst zelfs in de richting van meer liberalisering in plaats van handelsbeperkende maatregelen (Europese Commissie, 2012a). De tegenstrijdige visies op deze kwestie duiden erop dat een politiek akkoord vinden erg moeilijk zal worden. Verder zal deze inleiding kort ingaan op hoe en waarom controles van veiligheidstechnologieën nu weer op de politieke agenda staan.

Ordediensten hebben steeds technologieën ingezet om politieke betogingen te onderdrukken, bijvoorbeeld een waterkanon of traangas. Maar recent heeft de politiek zijn aandacht gevestigd op software gebruikt om activisten te traceren of communicatieverbindingen te verbreken. Sinds 2009 zijn verschillende protesten bedacht met de termen twitter- / facebook- / wikileaks-revoluties, vooral dan de burgeroproer in Moldavië, de Iraanse verkiezingsprotesten in 2010 en de opstanden in Tunesië en Egypte in 2010 en 2011, die deel uitmaakten van een reeks revoltes die de naam Arabische Lente hebben gekregen. De media roemden de sociale media als dé manier om intern informatie uit te wisselen en over de grenzen heen naar buiten te brengen wat er zich afspeelde, zelfs in die mate dat de onderliggende oorzaken van de protesten werden genegeerd.^{II} De media-aandacht voor het gebruik van sociale media liet echter ook zien hoe het internet werd gecensureerd, en dat de regimes, in een poging een einde te maken aan de protesten, bewakingstechnologieën inzetten om demonstranten te traceren. Zoals Wagner (2012a) nauwkeurig omschrijft, neemt de bewijslast toe waaruit blijkt hoe een groot aantal landen in het Midden-Oosten en Noord-Afrika (MENA) en elders gebruikmaakt van 'deep packet inspection technology' om het internet te censureren. Daarenboven bestaan er bewijzen dat veel landen in de regio bewakingsinfrastructuren operationeel houden (Wagner, 2012a). Beide types technologie moesten tijdens de Arabische Lente de informatie filteren die burgers te lezen kregen (bv. buitenlandse nieuwsverslagen) maar ook – en dat is zorgwekkender – helpen om social-media-activisten te identificeren en arresteren. Een onderzoek door Bloomberg voerde bewijzen aan dat sommige via deze methodes gevatte activisten waren gefolterd (Elgin, Silver en Zschiegner, 2011).

Veel van deze technologie en de technische expertise om ze te onderhouden was door ondernemingen uit de VS en de EU uitgevoerd naar de MENA-regio. Het Bloomberg-onderzoek noemde volgende EU-bedrijven: Nokia Siemens Networks (Finland), Ericsson AB (Zweden), ETI A/S (Denemarken), AdaptiveMobile Security Ltd (Ierland), Creativity Software Ltd (VK), Amesys (Frankrijk), Qosomos SA (Frankrijk), Trovicor GmbH (Duitsland), Ultimaco Software AG (Duitsland) en Area SpA (Italië) (Elgin, Silver en Zschiegner, 2011). Wagner (2012) duidt ook de activiteiten van

^I Duitsland koos voor veiligheidstechnologieën als een van de vier domeinen waarop een in januari 2012 gestart steunprogramma voor KMO's met het oog op de uitbreiding van de exportmarkt zich moest richten: Auslandsmarkterschließung für kleine und mittlere Unternehmen – officieel document geraadpleegd op 21 juli 2012 op het volgende adres: <http://www.bmwi.de/DE/Themen/Aussenwirtschaft/Aussenwirtschaftsfoerderung/aussenwirtschaftsfoerderungsinstrumente,did=193980.html>

^{II} Andere, meer analytische bronnen hebben benadrukt dat we de bijdrage van sociale media niet mogen overschatten (Comninos, 2011; Morozov, 2011).

het Franse Wanadoo in Tunesië en Gamma International (VK) in Egypte aan als problematisch. In een rapport beschuldigde de New York Times Gamma International er eveneens van, de bewakingssoftware 'Finspy' te hebben verkocht. Deze software werd in Bahrein, Brunei en Turkmenistan (Perlroth, 2012) ingezet om activisten te monitoren. Uit recent door Wikileaks gepubliceerde documenten bleek ook dat het Italiaanse Finmeccanica tot 2012 communicatietechnologieën verkocht aan de Syrische politie (Clark, 2012). Naarmate de negatieve pers toenam, kwamen er in de lidstaten en in het Europees Parlement discussies op gang over hoe en of de export van dergelijke technologieën moest worden gereguleerd. Door zijn voorgeschiedenis richtte het hernieuwde debat over de vraag of en hoe de export van veiligheidstechnologieën moet worden gecontroleerd zich vooral op bewakingstechnologieën.

Onder de huidige omstandigheden is het nuttig dat we de discussie over veiligheidstechnologieën in deel 3 van dit rapport er terug bijnemen. Het rapport gaf al aan dat militaire en veiligheidsproducten steeds meer vertrekken van dezelfde generische technologieën, vooral dan ICT-technologieën, die reeds een brede toepassing kennen in civiele sectoren. Dit doet de grenzen van zowel kenniscreatie als de toepassing van de technologieën vervagen, niet enkel tussen militaire en niet-militaire veiligheidsproducten, maar ook ten opzichte van de ruimere innovaties in civiele en commerciële technologieën (James, 2009b). Het stelt nieuwe uitdagingen aan het non-proliferatiebeleid en aan het ontwerp van efficiënte controlesystemen voor materiële en immateriële export. In feite is dit een klassiek voorbeeld van hoe moeilijk het is de uitvoer van producten voor tweeërlei gebruik te reguleren,¹ met dat verschil dat deze groep van technologieën en producten nog complexer is. Immers, de definitie van 'voor tweeërlei gebruik' is er niet noodzakelijk op van toepassing, want ze kunnen worden ingezet om mensenrechten te schenden en interne repressie te organiseren, zonder dat daarbij noodzakelijk een strijdmacht is betrokken. Als laatste punt heeft de Commissie, zoals Edler en James (2012) vermelden, met opzet en in haar eigen belang geen eenduidige omschrijving gegeven van wat veiligheidsonderzoek en de veiligheidsbedrijven en -technologieën precies inhouden. Deze dubbelzinnigheid maakt het moeilijk om voor veiligheidstechnologieën een precieze afbakening te maken in de lijsten voor exportcontroles die al bestaan voor militaire goederen en goederen voor tweeërlei gebruik. Er is al op gewezen dat veiligheidstechnologieën en -producten deels onder drie afzonderlijke EU-stelsels vallen, namelijk het gemeenschappelijk standpunt over wapenuitvoer, de verordening betreffende goederen voor tweeërlei gebruik en de folterverordening. En dan zijn er nog de nationale controles. Alle drie bleken toen we dit schreven ter herziening voor te liggen. Het rapport zal elk van deze stelsels onderzoeken, aangeven op welke veiligheidstechnologieën ze van toepassing zijn en wat de voor- en nadelen zijn, en de mogelijke voorgestelde hervormingen bespreken. Ook zal het nagaan of sancties, embargo's of vrijwillige codes op initiatief van de sector hun nut kunnen hebben. Tenslotte bespreekt het de stelling dat we zulke exporten beter kunnen faciliteren in plaats van ze te controleren, steek houdt. We bestuderen dan vooral de externe aspecten van de interne-veiligheidsstrategie in de EU.² Het volgende deel van dit debat begint echter met een beschrijving hoe het Europese en recentelijk het EU-standpunt over de controle van strategische goederen is geëvolueerd, van de verschillende manieren waarop het debat vorm kan krijgen en een verwijzing naar de opkomende trends die mogelijk een impact zullen hebben op de discussie over de controle van veiligheidstechnologieën.

¹ Hoewel Wagner (2012a: 7) aangeeft dat "typische technologieën voor censurering en bewaking worden verkocht als systemen en doorgaans geen meerdere, overlappende doeleinden hebben. De basis hardware kan in theorie dan wel meerdere verschillende taken uitvoeren, de systemen zelf worden normaal gezien gebouwd en onderhouden voor één specifiek doel: individuele mensenrechten inperken."

² De Amerikaanse Commissie binnenlandse veiligheid en exportcontroles (2012) oordeelt bijvoorbeeld dat Amerikaanse exportcontroles op 'homeland security'-technologieën het ministerie van Homeland Security beletten om internationale samenwerking aan te gaan.

5.2 De controle van strategische goederen: de contouren van het debat

Alhoewel de synergiën tussen defensie- en veiligheidstechnologieën vaak overdreven worden (IRIS et al, 2010), valt het omwille van de gelijkenissen te begrijpen dat beleidsmakers die de uitvoer van veiligheidstechnologieën aan banden willen leggen daarvoor het kader inzake export van defensiemateriaal en vooral dan de wetgeving rond producten voor tweëerlei gebruik willen gebruiken. Misschien loont het op dit punt de moeite stil te staan bij de mogelijke redeneringen die achter wapenexportcontrole zitten en te bekijken hoe ze gelden voor veiligheidstechnologieën en – producten. Regeringen hebben het om volgende redenen nodig geacht, de uitvoer van wapens te beperken:

1. Non-proliferatie van bepaalde types technologie – hier denken we vooral aan controles op de export van technologieën die dienen als platform voor nucleaire, biologische en chemische (NBC) wapens, maar eveneens bepaalde types rakettechnologieën. De proliferatie van dergelijke technologieën wordt algemeen als een gevaar voor de mondiale veiligheid en stabiliteit beschouwd.
2. Strategische superioriteit behouden – landen kunnen de export verbieden van technologieën die hen in staat stellen hun concurrenten strategisch voor te blijven.
3. Controle over ‘hun’ defensiebedrijven behouden – bekommernissen over de continuïteit van het aanbod kunnen landen belangrijke defensiebedrijven doen verbieden, elders uitgebreide activiteiten op te zetten. Zo blijven zij meester over dat bedrijf en dus over de defensieleveringen.
4. Schendingen van mensenrechten of escalatie van conflictsituaties voorkomen – landen kunnen wapenexporten om ethische redenen verbieden, bv. wanneer zij vermoeden dat het land van bestemming de uitrusting gaat gebruiken om mensenrechten te schenden. Ook zijn zij misschien van oordeel dat wapenexporten de escalatie van een regionaal conflict zouden inluiden.

Realistisch gesproken kunnen bij veiligheidsproducten enkel mensenrechten in het gedrang komen. Anderzijds zijn regeringen mogelijk voorstander van wapenexporten om volgende redenen:

- Invloed najagen of behouden – regeringen kunnen wapenexporten toestaan naar regio's of landen waar zij hun strategische invloed wensen te vergroten of behouden.
- Financieel – wapenexporten leveren de uitvoerende staat doorgaans aardige winsten op (hoewel dit in het geval van exportsubsidies een twijfelachtige redenering is)
- Nationale wapenprogramma's onderhouden – aanzienlijke exporten maken eigen wapenprogramma's betaalbaarder dankzij de schaalvergroting.

In haar mededeling betreffende het beleid inzake de veiligheidsindustrie vermeldt de Commissie (Europese Commissie, 2012a) al deze argumenten impliciet of expliciet om te pleiten voor de export van veiligheidsproducten. Dit suggereert dat de EU moeilijk van de noodzaak van exportcontroles op veiligheidstechnologie zal te overtuigen zijn.

Eveneens moeten we ons afvragen of wapenexportcontroles efficiënt zijn en makkelijk toepasbaar op veiligheidstechnologieën. Cooper (2006) betoogt dat wapencontroleregimes om de proliferatie van sleuteltechnologieën (vooral NBC-technologieën) tegen te gaan al aanzienlijk in efficiëntie verschillen van controles op conventionele wapens, die naar zijn aanvoelen grotendeels symbolisch

zijn. Het eerste type controles is behoorlijk succesvol omwille van drie factoren. Cooper (2006: 119) stelt dat ten eerste *“aan de instap relatief grote technologische hindernissen verbonden zijn”* in combinatie met *“beperkte beschikbaarheid van sleutelmaterialen”*, ten tweede dat de stelsels strenge disciplinaire maatregelen kunnen opleggen, en ten derde dat ze kunnen terugvallen op een *“krachtige (en bijna universele) norm tegen NBC-proliferatie”*. Exportcontroleregimes voor conventionele wapens ontbreekt het daarentegen vaak aan politieke bereidheid om strategische en commerciële belangen opzij te schuiven. Bovendien maakt de steeds globalere aard van de defensiesector het moeilijk om nationaal te controleren. Ten slotte hebben het groeiende belang van technologieën voor tweeërlei gebruik in defensie-uitrusting en het bestaan van pervasieve *“geglocaliseerde illegale wapennetwerken”* de kracht van bestaande controles op de overdracht van conventionele wapens aanzienlijk vermindert, omdat proliferatie onder deze omstandigheden heel wat moeilijker is te voorkomen is (Cooper, 2006: 118). Met name het gemeenschappelijk standpunt van de EU over de uitvoer van conventionele wapens heeft kritiek gekregen omdat het de export van conventionele wapens naar problematische landen van bestemming niet kon voorkomen. Exportcontroles op producten voor tweeërlei gebruik worden ook, voor conventionele wapens tenminste, als ongeschikt beschouwd. Alle aandacht is immers naar de stopzetting van nucleaire proliferatie uitgegaan.

Wat zegt dit ons over de kans op slagen van een regime bedoeld om de uitvoer van veiligheidstechnologieën te controleren? Laat ons eerst kijken naar de factoren waarop het succes van de NBC-regimes is gestoeld. Moeten instappers grote technologische hindernissen overwinnen of beschikken over moeilijk te verkrijgen materialen? Bij veiligheidsuitrusting (en veel conventioneel militair materieel) is dit steeds minder het geval. De expertise is ook niet alleen bij de EU en haar bondgenoten terug te vinden. Dit beperkt de EU onmiddellijk in haar capaciteit om de proliferatie van veiligheidsuitrusting in te perken, vooral als er geen sprake hoeft te zijn van complexe systeemintegraties. Ten tweede is, net als bij de uitvoer van conventionele wapens, de internationale strafmaat voor landen die nalaten een regeling in verband met producten voor tweeërlei gebruik en sancties op te leggen niet bepaald zwaar (Cooper, 2006). Ten derde bestaat er geen universele of vergaande norm tegen de uitvoer van veiligheidsuitrusting. De globale logica van de ‘War on Terror’ impliceert namelijk dat dergelijke exports wenselijk kunnen zijn.

Ten slotte moeten we bekijken hoe het debat rond de controle van strategische goederen momenteel vorm krijgt. Cornish (1995) wijst erop dat Europa niet altijd eenduidig redeneert in het toelaten of verbieden van wapenverkoop, maar zich eerder door de toestand van de internationale betrekkingen op het gegeven moment laat leiden. Tijdens de Koude Oorlog gingen wapenexporten uit West-Europa doorgaans hand in hand met het ideaal van ondersteuning aan het gedachtegoed en de invloed van het Westen, terwijl de verkoop werd tegengehouden naar die landen die andere doelen nastreefden. Maar daarna verdween het politieke voorbehoud, wat kort een zo goed als vrije wapenmarkt deed ontstaan (Cornish, 1995). Economische overwegingen kwamen in de plaats van bezorgdheid over het machtsverwicht. Ook kunnen we stellen dat politici en ngo's in de jaren '90 algemene controles op conventionele wapens minder aandacht verleenden, en zich eerder inspanden voor een non-proliferatie van nucleaire, biologische en chemische wapens en een stopzetting van de handel in wat we pariawapens zijn gaan noemen, zoals clusterbommen en landmijnen. Naar aanleiding echter van een reeks schandalen in de jaren '90 vond de EU de politieke bereidheid om een systeem van wapenexportcontroles overeen te komen, dat zou rekening houden met de mensenrechtensituatie in het land van bestemming. De gedragscode deed, zoals Bailes aanduidde, her en der druk ontstaan om via jaarverslagen en wederzijdse controle tot meer consistentie en transparantie tussen EU-lidstaten te komen. Geen race to the bottom dus; het leek er zelfs op dat een nieuw tijdperk van verantwoordelijkheid was

aangebroken.^I Toen Frankrijk in 2008 haar aloud verzet (in ruil voor goedkeuring van de richtlijn betreffende intracommunautaire overdrachten van defensiegerelateerde producten) liet varen en de gedragscode een wettelijk bindend gemeenschappelijk standpunt werd, betrad de EU nieuw terrein. Maar het gemeenschappelijk standpunt is, zoals Poitevin (2011) en Depauw (2010) aangeven, eigenlijk een ontgoocheling gebleken in de manier waarop dit tot dusver werd uitgevoerd. Lidstaten brengen te laat en onvoldoende verslag uit, het standpunt wordt niet overal geïmplementeerd (zeer problematisch gezien de richtlijn betreffende intracommunautaire overdrachten) en de schandalen zijn niet van de baan. Meer nog, er zijn tekenen dat één belangrijk land, Duitsland, probeert om wapenexportcontroles via de NAVO te versoepelen. Duitse media meldden dat Duitsland tijdens de top in Chicago van 2012 opriep tot een overeenkomst over een lijst met daarin voor de NAVO-partners strategisch belangrijke landen, die wel wapens zouden mogen aankopen, zelfs als de mensenrechtensituatie daar ondermaats zou zijn (Steinmann en Dierks, 2012). Volgens de Financial Times Deutschland ging het daarbij onder andere over de leden van de Samenwerkingsraad van de Arabische Golfstaten. Hoewel andere NAVO-lidstaten maar koeltjes hadden gereageerd op het initiatief, geeft dit aan dat Duitsland haar eigen restrictieve aanpak inzake wapenexportcontroles geheel heeft herzien. Ook kan dit mogelijk problemen opleveren voor ngo's die pleiten om het gemeenschappelijk standpunt van de EU te verbeteren.

Deze gewijzigde houdingen naar de export van conventionele wapens toe zetten zich ook door in hoe het initiële debat over de controle van veiligheidstechnologieën vorm krijgt. De eerste overlegondes, met name in het Europees Parlement over een mogelijke aanpassing aan de regeling voor producten voor tweërlei gebruik in 2011^{II} en de mediaverslaggeving over de Arabische Lente, spitsten zich toe op bewakings- en detectietechnologieën. Daaruit bleek telkens dat de politieke wil in sommige kampen ontbrak. Ofschoon er hier en daar wel steun is, vooral dan in Nederland (de Nederlandse minister van Buitenlandse Zaken was voorstander van exportcontroles bijvoorbeeld voor technologieën die gegevens op het internet filteren) en tot op zekere hoogte in het VK, lobbyde de Duitse regering zwaar tegen de opname van striktere maatregelen voor telecommunicatietechnologieën in de herziene wetgeving inzake producten voor tweërlei gebruik. In 2010 verklaarde de toenmalige Duitse minister van Economie Rainer Brüderle openlijk dat hij civiele veiligheid als een toekomstmarkt voor de Duitse industrie zag en dat we de sector geen wettelijke belemmeringen mochten opleggen.^{III} Ondanks het toenemende bewijs dat door de EU en Duitsland naar repressieve regimes uitgevoerde bewakingstechnologieën daar worden misbruikt,^{IV} is ook zijn opvolger Rösler allerminst bereid om van deze lijn af te wijken (Schumann, 2011). In diezelfde zin zwakte Zweden in 2011 sancties tegen Syrië af door te weigeren twee Syrische telecommunicatiebedrijven met commerciële banden met het Zweedse Ericsson op de sanctielijst te laten opnemen (Brunnstrom en Ringstrom, 2011). De discussie over veiligheidstechnologieën speelt zich ook af tegen de achtergrond van een Commissie die probeert om controles op producten voor tweërlei gebruik te versoepelen, iets wat in het desbetreffende punt aan bod zal komen.

De EU kan in dit dossier als internationale actor blijkbaar niet zo eenduidig normatief of deugdelijk optreden – d.w.z., de uitvoer van veiligheidstechnologieën omwille van de mensenrechten tegenhouden – als het verleden inzake de uitvoer van conventionele wapens. Dit laat beleidsruimte

^I Hoewel Frankrijk, Duitsland en het VK elk jaar nog regelmatig opdoken in de top vijf van wapenexporterende landen.

^{II} Deze worden in detail besproken in het punt over producten voor tweërlei gebruik.

^{III} De positie van Duitsland is veelzeggend omdat de Duitse federale dienst voor exportcontrole (BAFA) van de EU de opdracht heeft gekregen, projecten uit te voeren met het oog op een ruimere internationale samenwerking inzake controles op producten voor tweërlei gebruik. Een overzicht van hun activiteiten is hier terug te vinden: http://www.eu-outreach.info/eu_outreach/

^{IV} Zie 'Security made in Germany' voor details over de meer controversiële Duitse exporten: <http://www.german-foreign-policy.com/en/fulltext/57919?PHPSESSID=snktg8f7sg5f55goenjb9lol4>

voor verschillende opvattingen, bijvoorbeeld dat de EU een handelsmacht of een opkomende veiligheidsprovider kan zijn. Door zich te concentreren op bewakingstechnologieën hebben klokkenluider-ngo's (en mensenrechten-ngo's) het debat kunnen sturen, en niet diegenen die gespecialiseerd zijn in de wapenhandel (wellicht ging hun energie naar de onderhandelingen over het wapenhandelsverdrag van de VN). De aanhoudende economische malaise in de meeste EU-lidstaten brengt een akkoord rond controles ook niet dichterbij. Het is bovendien niet de eerste keer dat de EU het niet eens raakt. Denken we maar aan de controlelijst met goederen bestemd voor gebruik door veiligheids- en politiediensten die er nooit is gekomen. Zoals tabel 1 aangeeft is het realistisch genomen ook niet wenselijk om alle veiligheidstechnologieën voor exportdoeleinden te controleren. Alle landen moeten investeren in de bescherming van kritieke infrastructuur. En de wereldwijde onderlinge afhankelijkheid maakt het bijvoorbeeld wenselijk dat zij allen hun luchthavens kunnen uitrusten met de geschikte passagiers- en bagagecontroleapparatuur. Globale interdependentie houdt in dat 'homeland security' niet mogelijk is zonder internationale samenwerking en, indien nodig, gedeelde technologieën (Commissie homeland security en exportcontroles, 2012). Exportcontroles kunnen ook andere ongewenste gevolgen hebben voor de mensenrechten: wanneer door een ruimere definitie van goederen voor tweërlei gebruik ook alle mogelijke probleemgevallen in aanmerking komen, kunnen hieruit humanitaire crisissen ontstaan, zoals bleek toen de VS het concept tijdens de VN-sancties tegen Irak tussen 1990 en 2003 misbruikte (Gordon, 2010). In plaats van alle veiligheidstechnologieën te willen controleren lijkt het dan ook opportuun dat we hieronder nadenken over de manier waarop we bestaande en potentiële controlestelsels kunnen wijzigen of verbeteren. Kunnen we zo de mazen dichten of deze stelsels voor de meest problematische technologieën doen gelden?

5.3 Bestaande en potentiële controleregimes

Het debat over de exportcontrole bij bepaalde types veiligheidsuitrusting heeft in een eerste fase zijn focus op de EU-regeling voor producten voor tweërlei gebruik gelegd. Wellicht is dit het stelsel dat in deze omstandigheden het meest aan bod zal komen. Toen het in 2011 is bijgewerkt, heeft dit tot enige vooruitgang geleid. Bovendien loopt het overleg over de regeling en wordt deze voortdurend herzien. Maar zoals eerder uiteengezet leidt de classificatie van deze technologieën en producten als 'voor tweërlei gebruik' onder de huidige wetgeving tot problemen. Het is dus mogelijk dat een andersoortig regelgevend kader beter geschikt is. Ook is het reeds duidelijk dat niet iedereen gelukkig is dat de regeling voor producten voor tweërlei gebruik dienstdoet als regelgevend kader. Terwijl deze sectie een nauwkeurige blik werpt op hoe men tegenover de regeling voor producten voor tweërlei gebruik staat, bespreekt het ook het belang van het gemeenschappelijk standpunt over wapenuitvoer, de folterverordening, sancties en embargo's en door de industrie aangestuurde zelfregulerende kaders.

5.3.1 EU-verordening inzake producten voor tweërlei gebruik

'Voor tweërlei gebruik' zijn technologieën en goederen die voor zowel civiele als militaire doeleinden inzetbaar zijn. De EU heeft een regeling afgesproken voor controle op de uitvoer, de overdracht, de tussenhandel en de doorvoer van producten voor tweërlei gebruik (Verordening 428/2009 van de Raad, gewijzigd in 2010, 2011 en 2012). Onder de regeling mogen gecontroleerde producten het grondgebied van de EU niet zonder vergunning verlaten. De handel in producten voor tweërlei gebruik is overal binnen de EU toegestaan, met uitzondering van die producten die in bijlage 4 staan. Er bestaan vier types uitvoervergunningen: communautaire algemene uitvoervergunningen, nationale algemene uitvoervergunningen, globale vergunningen en

individuele vergunningen. De EU-lijst van gecontroleerde goederen baseert zich op de lijst die de internationale exportcontroleregimes – de Australiëgroep (biologische en chemische wapens), de Groep van nucleaire exportlanden (nucleaire wapens), het Wassenaar Arrangement (conventionele wapens) en het Missile Technology Control Regime (onbemande lanceersystemen voor massavernietigingswapens) – hebben goedgekeurd om de proliferatie van bepaalde types wapens tegen te gaan. Twee aspecten van de regeling verdienen meer analyse: de procedure voor het samenstellen van deze lijsten en de EU-tenuitvoerleggingsprocedures. Omdat de EU-lijsten een geconsolideerde lijst vormen, moeten we zeker onderzoeken hoe wordt beslist wat op de lijst komt en ervan verdwijnt. Vervolgens bespreekt dit deel van het rapport de tenuitvoerlegging en de pogingen om door de implementatiewijze te veranderen enkele problemen aan te pakken die zich met exporten naar de MENA-regio hebben voorgedaan.

Het Wassenaar Arrangement vormt de voor dit rapport belangrijkste regeling, ondanks dat sommige types onbemande luchtvaartuigen (en daaraan verbonden technologieën) en bepaalde sensortechnologieën onder het MCTR vallen. Het Wassenaar Arrangement wordt vaak vergeten in verband met de regeling voor producten voor tweërlei gebruik omdat de politieke prioriteit reeds enige tijd bij de preventie van massavernietigingswapens lag en niet de proliferatie van conventionele wapens (Wetter, 2009). Volgende criteria bepalen de opname (of schrapping) van goederen in of van de Wassenaar-lijsten:

“Goederen en technologieën voor tweërlei gebruik die controle vereisen zijn de belangrijke of sleutelonderdelen om militaire capaciteiten nationaal te ontwikkelen, produceren, gebruiken of uit te breiden. Om de producten voor tweërlei gebruik te selecteren moeten ze op volgende criteria worden beoordeeld:

- *Verkrijgbaarheid in andere dan de deelnemende landen.*
- *De mogelijkheid om de export van goederen efficiënt te controleren.*
- *De mogelijkheid om het product duidelijk en objectief te specificeren*
- *Gecontroleerd door een andere regeling.”* (Wassenaar Arrangement, 2005)

Onmiddellijk blijkt waar de eerder aangehaalde problemen zitten om veiligheidstechnologieën als groep te controleren. Het concept is niet eenduidig, de technologieën zijn grotendeels gebaseerd op overal verkrijgbare generische technologieën en zorgen niet noodzakelijk voor meer militaire capaciteit. Evans (2008) merkt op dat bij het Wassenaar Arrangement in de beslissingen over opname in of schrapping van de lijst de spanning speelt tussen diegenen die technologieën voor tweërlei gebruik moeilijk te controleren vinden, en diegenen die ze als een nieuwe, uit te baten markt beschouwen die dus geen controle behoeft. Deelnemende landen stemmen er mee in exportcontroles te doen op alle producten in de lijst, maar zij zijn het die beslissen of ze al dan niet een vergunning verlenen. Modaliteiten om informatie te delen moeten daarbij tot meer transparantie leiden. De Wassenaar-lijsten met producten voor tweërlei gebruik bestaan uit volgende categorieën:¹

- Categorie 1 Speciale materialen en aanverwante uitrusting
- Categorie 2 Materiaalbewerking
- Categorie 3 Elektronica

¹ Het Akkoord van Wassenaar bevat ook de munitielijst, die equivalent is aan de gemeenschappelijke EU-lijst van militaire goederen en twee bijlagen – de gevoelige en de zeer gevoelige lijst. Deze bijlagen vormen deelcategorieën van de hoofdcategorieën vallen en omvatten technologieën waarover een consensus bestaat datze kritiek zijn en waarbij intensievere informatiedeling inzake vergunningsbeslissingen vereist is. In het geval van de zeer gevoelige lijst spreken deelnemende landen af om uiterst waakzaam te zijn.

- Categorie 4 Computers
- Categorie 5 - deel 1 Telecommunicatieapparatuur
- Categorie 5 - deel 2 "Informatiebeveiliging"
- Categorie 6 Sensoren en "lasers"
- Categorie 7 Navigatie en vliegtuigelektronica
- Categorie 8 Zeewezen en schepen
- Categorie 9 Ruimtevaart en voortstuwing

Het spreekt voor zich dat slechts een klein percentage van de producten die mogelijk onder deze categorieën vallen, wordt gecontroleerd – meestal zouden zij de criteria voor opname in de lijst niet halen. Niettemin komen in de lijst enkele veiligheidstechnologieën voor die de EAVO daarin heeft gezet, zoals hyperspectrale en multispectrale sensoren, bepaalde encryptietechnologieën en een groot deel van de technologieën en materialen gebruikt in de productie van grotere onbemande luchtvaartuigen. Volgens Wagner (2012b) zouden, als de EU met de Wassenaar-partners meewerkte, meer technologieën op de lijst terecht kunnen komen. Wellicht klopt dit, ondanks het feit dat de criteria het moeilijk maken om zulke technologieën te laten opnemen. Bovendien is het toegestaan om naast de EU-lijsten nog extra technologieën nationaal te controleren.^I

Pogingen binnen de EU om de uitvoering van de regeling voor producten voor tweërlei gebruik vlotter te laten verlopen, hebben zich in het Europees Parlement geconcentreerd. Sinds de inwerkingtreding van het Verdrag van Lissabon worden updates van de lijsten, communautaire algemene uitvoervergunningen en eventuele doorlichtingen van de verordening aan de co-decisieprocedure onderworpen. Toen in 2011 rapporten melding maakten van misbruik van bewakings- en detectietechnologieën tijdens de Arabische Lente, probeerden sommige leden van het Europees Parlement^{II} van het bijwerken van de verordening gebruik te maken om in het Commissievoorstel tekst op te nemen waardoor de controles op deze technologieën strenger zouden worden. Jörg Leichtfried, de rapporteur voor de Commissie internationale handel, stelde naar aanleiding van het Commissievoorstel uit 2010 tot wijziging van de wetgeving voor producten voor tweërlei gebruik enkele amendementen voor, sommige inhoudelijk en andere om het Europees Parlement een beter overzicht te bieden over de regeling voor producten voor tweërlei gebruik^{III}. Een van deze voorstellen was erg belangrijk voor de bewakingstechnologieën en werd goedgekeurd door de Raad. De algemene uitvoervergunning van de EU voor telecommunicatieapparatuur werd in die zin aangepast dat de uitvoer niet werd toegestaan indien de uitvoerder wist dat de apparatuur kon worden gebruikt voor (of hiervoor door de lidstaat gewaarschuwd was):

“doeleinden die gepaard gaan met schendingen van de mensenrechten, de democratische beginselen of de vrijheid van meningsuiting zoals omschreven in het Handvest van de grondrechten van de Europese Unie, waarbij gebruik wordt gemaakt van onderscheppingstechnieken en digitale gegevenstransferapparatuur voor het afluisteren van mobiele telefoons en het meelesen van tekstberichten en van gerichte bewaking van het internetgebruik (bijvoorbeeld met behulp van controlecentra en legale interceptiegateways);” (Verordening 1232/2011 bijlage IIe deel 3 1(1)(d))

^I Artikel 8 van Verordening 428/2009 van de Raad laat lidstaten toe, unilateraal om redenen van openbare veiligheid of uit mensenrechtenoverwegingen een verbod in te stellen op producten die niet op de lijst voorkomen. Frankrijk, Duitsland, Letland en het VK hebben deze maatregel benut. Details zijn na te lezen in het Publicatieblad van 6 maart 2012.

^{II} Zeer actief waren de Nederlandse parlementsleden Marietje Schaake en Lambert van Nistelrooij, Jörg Leichtfried uit Oostenrijk en Vital Moreira uit Portugal.

^{III} Een voorstel tot een algemene uitvoervergunning haalde het evenmin. Een volledig overzicht van de wijzigingen is terug te vinden op: <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2011-0028&language=NL>

Hoewel de algemene uitvoervergunning niet van toepassing is op deze landen waar de Arabische Lente zich afspeelde, is dit wel het geval voor landen als Rusland en China, waarvan geweten is dat ze zulke praktijken toepassen. Ze schept ook een nuttig precedent voor verdere veranderingen. Leichtfried zegt verrast te zijn geweest over de tegenstand die sommige van zijn andere amendementen opriepen.¹

In juni 2011 publiceerde de Commissie een Groenboek inzake de hervorming van de regeling voor goederen voor tweërlei gebruik en startte ze een raadpleging op. Het Groenboek neigt naar meer harmonisatie en algemene uitvoervergunningen op EU- en niet op nationaal niveau. Bedrijven uit landen die catch-all clausules strikter interpreteren zouden in het nadeel zijn. Algemeen genomen hanteert de Commissie een aanpak die meer liberalisering in plaats van inperking voorstaat. In hun conclusies hebben zowel het VK als Duitsland zich uitgesproken tegen meer harmonisatie, omdat dit volgens die landen onnodig was. Volgens de Gemeinsame Konferenz Kirche und Entwicklung (GKKE) groep (2012), die elk jaar een rapport over het Duitse wapenexportbeleid produceert, was van alle maatregelen in het Groenboek de Duitse regering enkel enthousiast over de versnelde aanpassingsprocedure voor de verordening. Daardoor zou het Europees Parlement immers minder gelegenheid krijgen om de wetgeving aan te passen. Nederland is evenmin overtuigd van het nut van ingrijpende veranderingen en een uitbreiding van de algemene EU-uitvoervergunningen, maar zou wel achter de invoering van een catch-all clause op EU-niveau staan om de tenuitvoerlegging geharmoniseerd te laten verlopen (Bleker, 2011).

Tijdens de raadpleging zijn verschillende voorstellen naar voren gebracht die, mits goedkeuring, zouden bijdragen tot verscherpte exportcontroles op veiligheidstechnologieën. In zijn conclusie stelde het VK voor om de definitie van militair eindgebruik in artikel 4(2) van Verordening (EG) 428/2009 van de Raad als volgt te wijzigen: *“bedoeld voor militaire, paramilitaire, veiligheids- of politiediensten op een bestemming waartegen een wapenembargo heerst of naar een entiteit die in hun naam instaat voor de aankoop, de productie, het onderhoud, de reparatie of de bediening.”* Hun motivatie luidt dat de huidige controle te eng is. Als juridisch advies voeren zij daarbij aan dat de huidige formulering geen uitvoer kan voorkomen van volledige producten die als dusdanig te gebruiken zijn. *“We zouden bijvoorbeeld de uitvoer kunnen voorkomen van een product dat niet op de lijst staat en moet dienen als onderdeel in een militair voertuig, maar niet de uitvoer van een volledig civiel voertuig bestemd voor strijdkrachten of binnenlandse veiligheidsdiensten van het land van bestemming, zelfs niet indien er tegen dat land een wapenembargo geldt. Evenmin is duidelijk of de controle van het militair eindgebruik ons in staat stelt, de uitvoer te voorkomen van een product dat niet op de lijst staat en voor militaire doeleinden aanpassing vereist in het land van bestemming of op een tussenbestemming”* (Brits Lagerhuis, 2012). Dergelijk amendement zou militair eindgebruik dan ook uitbreiden naar gebruik door binnenlandse veiligheidsdiensten, wat nuttig zou zijn. Vranckx, Slijper en Isbister (2011) doen een voorstel dat in dezelfde richting wijst, nl. dat een product dat niet op de lijst staat en moet worden omgebouwd met het oog op militair of veiligheidsgebruik ook onder de verordening zou moeten vallen indien het land of het bedrijf daarvan op de hoogte is. Uit een recent geval blijkt echter dat dit moeilijk te beoordelen is. Motoren van het Duitse 3W Modellmotoren zijn blijkbaar zonder medeweten van het bedrijf door dealers doorverkocht aan Wit-Rusland, waar ze dienen om spionagedrones aan te drijven. En dit terwijl er sinds 2011 een EU-embargo van kracht is dat de verkoop verbiedt van technologieën die inzetbaar zijn bij interne repressie. Bromley (2012) is voorstander om in het kader van de regeling voor producten voor tweërlei gebruik of herzieningen van het gemeenschappelijk standpunt nieuwe controles in te voeren op de uitvoer van bewakingstechnologieën. Al deze suggesties zouden ruimte kunnen bieden voor actie rond de uitvoer van bepaalde types

¹ De opmerkingen van Leichtfried tijdens 2012 zijn hier terug te vinden: <http://www.europarl.europa.eu/ep-live/nl/committees/video?event=20120208-1630-COMMITTEE-AFET>

veiligheidstechnologieën. Het blijven echter suggesties die in sommige gevallen niet stroken met de Commissievoorstellen.

5.3.2 Gemeenschappelijk standpunt inzake wapenuitvoer

Sinds 2008 heeft de EU een gemeenschappelijk standpunt met daarin alle regels betreffende de controle op de uitvoer van militaire technologie en goederen in de hele EU. Dit is de opvolger van de gedragscode betreffende wapenuitvoer, die dateert van 1998. De harmonisatie van het beleid inzake wapenexportcontroles, die gedurende de laatste vijftien jaar tot stand kwam, richtte zich niet enkel op het vastleggen van voor de hele EU geldende minimumnormen, maar beoogde ook meer uitwisseling van gegevens en transparantie tussen de lidstaten. Het gemeenschappelijk standpunt is, in tegenstelling tot de gedragscode, wettelijk bindend. Goederen in de gemeenschappelijke EU-lijst van militaire goederen¹ zijn in geval van export vergunningsplichtig. Vergunningsbeslissingen moeten worden gebaseerd op de acht criteria in tabel 5.1.¹¹

Tabel 6 Criteria van het gemeenschappelijk standpunt

Criterium	Omschrijving
1	Naleving van de internationale verplichtingen en verbintenissen van de lidstaten, in het bijzonder de door de VN-Veiligheidsraad of de Europese Unie aangenomen sancties, overeenkomsten ter zake van non-proliferatie en andere onderwerpen, alsmede andere internationale verplichtingen
2	Eerbiediging van de rechten van de mens in het land van bestemming
3	Interne situatie van het land van eindbestemming ten gevolge van spanningen of gewapende conflicten
4	Handhaving van vrede, veiligheid en stabiliteit in de regio
5	Nationale veiligheid van de lidstaten, van de gebieden waarvan een van de lidstaten de buitenlandse betrekkingen behartigt, alsmede van bevriende landen of bondgenoten
6	Gedrag van het land dat militaire goederen of technologie koopt, jegens de internationale gemeenschap, met name de houding van dat land tegenover terrorisme, de aard van zijn bondgenootschappen en de eerbiediging van het internationale recht
7	Gevaar dat de militaire goederen of technologie in het kopende land een andere bestemming krijgen of onder ongewenste voorwaarden opnieuw worden uitgevoerd
8	Compatibiliteit van de uitvoer van militaire goederen of technologie met de technische en economische capaciteit van het ontvangende land, rekening houdend met de wenselijkheid dat de staten aan hun legitieme behoeften inzake veiligheid en defensie voldoen met zo gering mogelijke aanwending van menselijk en economisch potentieel voor bewapening

Bron: Cooper (2012: 11)

Lidstaten moeten elke gedurende de afgelopen drie jaar geweigerde vergunning voor dezelfde apparatuur in overweging nemen en over hun vergunningsbeslissingen een jaarverslag opmaken. Het gemeenschappelijk standpunt wordt gezien als een verbetering tegenover de gedragscode omdat dit wettelijk bindend is maar daarnaast maatregelen omvat inzake tussenhandel, doorvoertransacties en immateriële technologieoverdrachten. Hoewel het gemeenschappelijk

¹ De gemeenschappelijke lijst van militaire goederen is te vinden op: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:069:0019:0051:NL:PDF>

¹¹ Artikel 12 van Verordening 428/2009 (regeling voor producten voor tweeterlei gebruik) stelt dat vergunningsbeslissingen inzake de uitvoer van producten voor tweeterlei gebruik ook deze criteria in acht moeten nemen.

standpunt geldt voor militaire en niet voor veiligheidstechnologieën (tenzij opgenomen in de lijst met producten voor tweërlei gebruik) is het om verschillende redenen interessant.

Een eerste reden is artikel 6, dat duidelijk maakt dat de bepalingen niet enkel van toepassing zijn in het geval van militaire eindgebruikers maar evenzeer bij uitvoer naar binnenlandse veiligheidsdiensten en vergelijkbare entiteiten.

Onverminderd Verordening (EG) nr. 1334/2000 van de Raad gelden de criteria in artikel 2 van dit gemeenschappelijk standpunt en de raadplegingsprocedure van artikel 4 ook voor lidstaten met betrekking tot goederen en technologie voor tweërlei gebruik als vermeld in bijlage I bij Verordening (EG) nr. 1334/2000 wanneer er ernstige redenen zijn om aan te nemen dat de eindgebruikers van dergelijke goederen en technologie de strijdkrachten, de binnenlandse veiligheidsdienst of vergelijkbare eenheden in het ontvangende land zijn. Referenties in dit gemeenschappelijk standpunt naar militaire goederen of technologie worden geacht ook betrekking te hebben op dergelijke goederen en technologie.” (Raad van de Europese Unie, 2008c)

Ten tweede komt een klein aantal technologieën die in tabel 1 als veiligheidstechnologieën staan aangeduid ook voor in de gemeenschappelijke lijst van militaire goederen, onder het voorbehoud dat deze daar enkel betrekking op heeft als de technologieën specifiek zijn ontworpen of aangepast voor militair gebruik. De meest voor de hand liggende voorbeelden zijn onbemande luchtvaartuigen en bepaalde types CBRN-apparatuur. Indien de Commissie (2012a) haar plannen hard maakt om, zoals aangekondigd in haar mededeling betreffende het beleid inzake de veiligheidssector, hybride militaire en veiligheidsnormen voor bepaalde producttypes op te stellen, zullen deze vermoedelijk ook gelden voor producten met civiele gebruiksdoeleinden. Op een zelfde manier zouden de onderzoeksactiviteiten die het EDA en de Commissie onder een kadersamenwerking gemeenschappelijk ontwikkelen vergelijkbare resultaten kunnen opleveren.

Ten derde, en misschien vanzelfsprekend, belet geen enkele bepaling in het gemeenschappelijk standpunt de lidstaten om striktere controles in te voeren. Zo heeft het VK aan haar nationale lijst van militaire goederen enkele producten toegevoegd die ze als veiligheids-, paramilitaire en politiegoederen omschrijft.¹ Als er geen consensus op EU-niveau wordt bereikt, is dit een piste die betrokken lidstaten kunnen volgen.

Zoals voorzien in het initiële besluit ondergaat het gemeenschappelijk standpunt ook een toetsingsproces. Dit moet niet noodzakelijk tot herzieningen leiden, hoewel volgens Bromley

¹ Het VK heeft bijvoorbeeld volgende producten toegevoegd aan haar lijst met militaire goederen: “Andere veiligheids- en paramilitaire politieproducten, met name:

- a. Geluidsapparaten die door de fabrikant of de leverancier worden omschreven als geschikt voor oproerbeheersing, en speciaal daarvoor ontworpen onderdelen;
- b. Schilden voor oproerbeheersing en kogelbestendige schilden, alsmede speciaal hiervoor ontworpen onderdelen;
- c. Kluisters ontworpen voor het in hun bewegingen beperken van mensen, waarvan de totale afmeting, met inbegrip van de ketting, gemeten van de buitenzijde van één boei tot de buitenzijde van de andere, indien gesloten, tussen 240mm en 280mm bedraagt;
- d. Stroomgordels die speciaal zijn ontworpen voor het in hun bewegingen beperken van mensen door toediening van elektrische schokken met een nullastspanning van maximaal 10.000 volt;
- e. Waterwerpers en speciaal ontworpen of speciaal aangepaste onderdelen daarvoor;
- f. Anti-oproervoertuigen die speciaal zijn ontworpen of aangepast om door middel van stroomstoten indringers af te weren, en onderdelen die daarvoor speciaal zijn ontworpen of aangepast;
- g. Geweren voor het afvuren van schokpijltjes met een nullastspanning van maximaal 10.000 volt;
- h. Onderdelen die speciaal ontworpen of aangepast zijn voor draagbare toestellen die zijn ontworpen of aangepast ten behoeve van oproerbeheersing of zelfbescherming door toediening van elektrische schokken (met inbegrip van stroomstokken, stroomschilden, verdovingsgeweren en geweren voor het afvuren van schokpijltjes).” (BIS, 2012)

(2012) wel enkele punten op de agenda terecht zijn gekomen. Oorzaak daarvoor is dat sommige EU-lidstaten hun posities op die van het voorgestelde wapenhandelsverdrag van de VN hebben afgestemd, zoals uitgebreide overlegmechanismen voor problematische bestemmingen; hoe gegevens voor het EU-jaarverslag moeten worden ingediend; de nationale tenuitvoerlegging van controles op doorvoer, overlading en tussenhandel op nationaal niveau; hoe de COARM werkt; welke informatie moet worden gedeeld over geweigerde vergunningen en het gebruik van globale en algemene vergunningen. Veel hervormingsvoorstellen uit de ngo-wereld delen deze bezorgdheden en hameren vooral op de nood aan een meer uniforme tenuitvoerlegging en grotere transparantie inzake goedkeuring en weigering van vergunningen. Depauw (2010) wijst er bijvoorbeeld op dat nu de richtlijn inzake intracommunautaire handel er is, het niet duidelijk is hoe landen kunnen voorkomen dat militair materieel initieel verkocht aan andere lidstaten opnieuw wordt uitgevoerd, indien zij het daarmee niet eens zijn. Indien landen de criteria op verschillende wijze toepassen, bestaat het gevaar dat men elkaars beleid ondermijnt. Ook stelden analisten zich, naar aanleiding van de Arabische Lente, vragen bij de robuustheid van EU-wapenexportprocedures. Ze stelden voor een nieuw criterium toe te voegen waardoor slecht bestuur echt als risicofactor zou worden beschouwd. Verder raadden ze aan om een lijst samen te stellen van verdachte landen en de mogelijkheid te creëren tot een bijzondere regeling nadat een embargo is opgeheven (Vranckx, Slijper en Isbister, 2011; Bromley, 2012). Het mag hierbij dan misschien niet over veiligheidstechnologieën gaan, de regelingen houden wel met elkaar verband en wijzigingen in één stelsel kunnen nuttige precedents scheppen in andere debatten.

De EU zou er ook voor kunnen pleiten, bepaalde technologieën aan de Wassenaar-lijsten toe te voegen. Voor wat het type bewakingstechnologieën betreft dat tijdens de Arabische Lente werd gebruikt, kan munitielijst 11a (c) *“Elektronische systemen of apparatuur ontworpen voor ofwel het observeren en volgen van het elektromagnetisch spectrum voor militaire inlichtingen of veiligheidsdoeleinden, ofwel het tegengaan van dergelijke observatie- en volgactiviteiten;”* mogelijk een handig beginpunt zijn om het overleg van start te laten gaan. Binnen de EU-context, waar de Commissie en sommige lidstaten vrezen dat wetgeving op dit domein nadelige gevolgen zou hebben voor EU-bedrijven, zal er misschien meer enthousiasme zijn over het toevoegen van sommige technologieën aan de Wassenaar-regeling.

5.3.3 De EU-folterverordening

Zoals we al vermeldde, is het niet gelukt om een lijst met goederen bestemd voor gebruik door veiligheids- en politiediensten aan de gedragscode betreffende wapenuitvoer toe te voegen. Wel was iedereen bereid een Commissievoorstel te aanvaarden om de uitvoer te regelen van producten die bruikbaar zijn tijdens folteringen of andere wrede, onmenselijke en ontorende behandelingen. Dit lag in het verlengde van richtsnoeren voor een EU-beleid ten aanzien van derde landen die zich schuldig maken aan foltering, goedgekeurd in 2001. Deze richtsnoeren creëerden geen juridische verplichtingen maar waren eerder een manier voor de EU om zich politiek achter de wereldwijde campagne tegen folterpraktijken te scharen. De eerste toetsingen (Raad van de EU, 2008a) gaven aan dat de richtsnoeren niet het verwachte omvattende effect hadden gesorteerd maar leidden onder andere wel tot de goedkeuring van EG-verordening 1236/2005, die algemeen bekendstaat als de folterverordening. De verordening verbood de handel in een aantal goederen die gebruikt worden om mensen in bedwang te houden of te executeren, en voerde controles in op de uitvoer van andere producten die kunnen worden gebruikt voor foltering. Het zijn twee korte lijsten, maar toch is dit een goed voorbeeld van een beslissing om de uitvoer van bepaalde veiligheidsgesegunde producten aan banden te leggen, zelfs al bestaat er geen verband met

militaire activiteiten. Daarom is het ook voor dit rapport interessant. De werkingssfeer van de verordening wordt hieronder beschreven. Daarna komen de sterke en zwakke punten aan bod.

De verordening, die werd herzien in 2011, verbiedt de in- en uitvoer van volgende in bijlage 2 genoemde producten:

1. De volgende goederen, ontworpen met het oog op de executie van mensen:

- 1.1. Galgen en guillotines
- 1.2. Elektrische stoelen voor de executie van mensen
- 1.3. Hermetisch gesloten kluizen, bijvoorbeeld van staal en glas, ontworpen met het oog op de executie van mensen door toediening van een dodelijk gas of een dodelijke stof
- 1.4. Systemen voor het automatisch injecteren van verdovende middelen die ontworpen zijn voor de executie van mensen door toediening van een dodelijke chemische stof

2. De volgende goederen, ontworpen om mensen in bedwang te houden:

- 2.1. Elektrische schokapparaten die bedoeld zijn om door een gefixeerde persoon op het lichaam te worden gedragen, zoals gordels, mouwen en handboeien die zijn ontworpen om mensen in bedwang te houden door toediening van elektrische schokken met een nullastspanning van meer dan 10000 V

3. De volgende draagbare toestellen die zijn ontworpen ten behoeve van oproerbeheersing:

- 3.1. Knuppels of stokken van metaal of een ander materiaal, met een schacht die is voorzien van metalen spijkers

De redenering achter het uitvoerverbod op deze producten is dat ze enkel en alleen inzetbaar zijn voor foltering en onmenselijke, wrede of ontorende behandelingen. Ngo's hebben op deze basis tijdens de herziening in 2011 knuppels met spijkers en stokken in de verordening kunnen doen opnemen (Amnesty International en Omega Foundation, 2010). Bijlage 3 bevat een lijst met specifieke producten onder volgende punten:

- Goederen ontworpen om mensen in bedwang te houden:
- Draagbare toestellen die zijn ontworpen ten behoeve van oproerbeheersing of zelfbescherming
- Draagbare apparatuur voor de verspreiding van stoffen die mensen tijdelijk kunnen uitschakelen, ten behoeve van oproerbeheersing of zelfbescherming, en aanverwante stoffen
- Producten die zouden kunnen worden gebruikt voor de executie van mensen door middel van een dodelijke injectie.

Enkel vergunningsinstanties mogen voor deze producten per specifiek geval een uitvoervergunning uitreiken, mits overleg over de kansen dat het land van bestemming deze gaat misbruiken. Indien een lidstaat de voorgaande drie jaar een vergunning heeft geweigerd, moet een andere lidstaat zich daar in haar beslissing aan houden. De meeste lidstaten maken deze informatie niet publiek, maar op basis van zes landen die dit wel deden, wijzen Amnesty International en Omega (2010) erop dat zowel Tsjechië als Duitsland tussen 2006 en 2008 veiligheidsuitrusting inzetbaar bij foltering hebben geleverd aan landen waarvan bekend is dat er schendingen van mensenrechten plaatsvinden. Dit zijn gekende problemen met de verordening. Naast de gebrekkige transparantie kampt de verordening met de moeilijkheden die telkens bij controles op basis van een lijst opduiken. Een ngo beschrijft het als volgt in haar rapport:

“Systemen op basis van een lijst scheppen duidelijkheid voor uitvoerders en invoerders, maar kennen wel enkele inherente nadelen, zoals:

- *Geen controle van bepaalde producten die wel binnen de beoogde werkingssfeer van de overeenkomst vallen maar niet specifiek op de controlelijsten worden vermeld;*
- *De vaak lange periode tussen productie, levering en ingebruikname van pas ontworpen apparatuur, en de vereiste tijd om deze op een lijst te laten verschijnen;*
- *De mogelijkheid voor leveranciers om controles te ontwijken gewoon door hun producten een nieuwe naam of specificatie te geven.” (Amnesty International en Omega Foundation, 2010: 28)*

Sinds 2008 al pleit het VK voor de invoering van een catch-all clause over feindgebruik voor foltering op EU-niveau, waardoor lidstaten vergunningen kunnen verstrekken en zodoende elk product verbieden dat om te folteren kan worden gebruikt. De briefwisseling die de Britse regering en Catherine Ashton in 2011 onderhielden en in 2012 werd gepubliceerd door de Britse parlementaire commissies inzake wapenexportcontroles laat uitschijnen dat het bereik van de wetgeving wordt herbekeken (Brits Lagerhuis, 2012 – schriftelijk bewijs 142). Maar vooral in het VK drukken ngo's en het parlement er steeds meer op dat landen die in dezelfde richting denken dergelijke maatregelen unilateraal zouden nemen, omdat zij menen dat er vanuit de EU onvoldoende steun komt.^I De folterverordening mag dan haar nadelen hebben, ze schept wel een precedent in de beperking van niet-militaire, veiligheidsgerelateerde goederen op EU-niveau en kan dienen als model om een verbod te stellen op 'single use' technologieën die uitsluitend dienen voor repressie, en die Wagner (2012b) als de slechtste van de slechtste technologieën bestempelt.

5.3.4 Sancties en embargo's

Sinds eind 2011 is de EU steeds meer specifieke clausules aan haar sancties en embargo's gaan toevoegen, zodat deze ook van toepassing worden op bewakingstechnologieën. In december 2011 keurde de Raad van de Europese Unie bijkomende sancties goed, die moesten voorkomen dat “apparatuur en software om internetcommunicatie en telefoongesprekken te kunnen opvolgen” (17985/11) Syrië binnen zou geraken. Toen ook bleek dat Iran dergelijke technologieën gebruikte als onderdrukkingsmiddel, breidde de EU op 23 maart 2012 haar sancties tegen het land uit door goedkeuring van Verordening 264/2012 van de Raad, die de verkoop, levering, overdracht of uitvoer naar Iran verbiedt van apparatuur en technologie die kan worden gebruikt voor het toezicht op en de interceptie van internetcommunicatie en telefoongesprekken. Hierbij hoort ook het verstrekken van technische bijstand. Het Amerikaanse Witte Huis ging in april 2012 nog een stap verder door gerichte financiële sancties aan te kondigen tegen bedrijven die nog bewakingstechnologieën aan Iran en Syrië zouden verkopen.^{II} Het is vrijwel zeker dat de aanhoudende druk van de media en het parlement voor deze ommekeer heeft gezorgd. Bieden sancties een afdoend antwoord voor dit probleem? Volgens Wagner (2012b) beschouwen we ze best als een kortetermijnoplossing, die ervoor zorgt dat regimes die zich actief schuldig maken aan interne repressie geen toegang meer krijgen tot de ergste soort bewakingstechnologieën. Doorgaans is er sneller een akkoord over een sanctie dan over een wijziging aan een multilateraal

^I Als reactie op druk vanuit ngo's en media is het VK in 2011 begonnen met het uitvoeren van unilaterale controles op de levering aan de VS van verdovende middelen die kunnen helpen bij de uitvoering van de doodstraf, en eerder al op zogenaamde sting sticks en elektrischeschokapparaten (Brits Lagerhuis, 2012).

^{II} Het uitvoeringsbevel van het Witte Huis van 23 april 2012 is te raadplegen op: http://content.govdelivery.com/attachments/USTREAS/2012/04/23/file_attachments/108232/2012iransyria.eo.rel.pdf

exportcontroleregime. Maar de grijze zones tussen aanvaardbare en onaanvaardbare technologieën maken dat dergelijke sancties niet waterdicht zijn en moeilijk te handhaven. Nog een zwak element is dat men meestal pas gaat optreden wanneer de media, politici en ngo's voldoende ijver aan de dag leggen om misbruiken bloot te leggen. Bepaalde wantoestanden met grote nieuwsaarde krijgen zo onevenredig veel aandacht, terwijl andere, die even erg zijn, onopgemerkt voorbijgaan. Had men de Arabische Lente en de protesten in Iran niet verkocht als een revolutie van de sociale media, zou er dan ook zoveel aandacht zijn uitgegaan naar de uitvoer van bewakingstechnologie? Dit kan ook betekenen dat sommige landen worden gevisieerd, wat tot inconsistentie leidt. Verslaggevers Zonder Grenzen (2012) noemde bijvoorbeeld Vietnam (samen met Syrië en Iran) als een van de twaalf 'vijanden van het internet'. Dit hield de EU echter niet tegen om in juni 2012 een partnerschaps- en samenwerkingsovereenkomst met het land af te sluiten en zo de relaties aan te halen. Met een landenspecifiek in plaats van een algemeen verbod wordt het tevens moeilijk om de wederuitvoer uit derde landen te voorkomen.

5.3.5 Vrijwillige codes op initiatief van de sector

Hoewel bedrijven die wapens exporteren naar ongeschikte landen van bestemming veel negatieve publiciteit krijgen, lijken deze, zolang zij wettelijk en met de steun van de regering handel kunnen drijven, niet meteen wakker te liggen van de publieke imagoschade die voortvloeit uit hun associatie met schendingen van mensenrechten. Uiteindelijk leveren zijn aan overheden, niet aan het grote publiek. Bedrijven met niet-gouvernementele klanten nemen de reputatie van hun merken veel ernstiger. Beschuldigingen in 2011 tegen de Britse krant 'News of the World' dat deze illegaal de gsm-berichten had afgeluisterd van een vermoord schoolmeisje zetten bijvoorbeeld een erg succesvolle sociale-mediacampagne in gang, die andere bedrijven dwong om zich terug te trekken als adverteerders. Israel (2009) stelt dat ICT-ondernemingen erg kwetsbaar zijn voor reputatieschade omdat zij vooral dankzij een sterk merk en hun menselijk kapitaal kunnen overleven. Met dit in het achterhoofd en wetende dat de sector overheidsinterventie wil vermijden, is het geen verrassing dat verschillende stakeholders, met de steun van overheden, initiatieven hebben genomen betreffende ICT en mensenrechten, vergelijkbaar met het Kimberleyproces inzake conflictdiamanten,. Ook bieden zij een antwoord op de VN-richtsnoeren inzake het bedrijfsleven en mensenrechten die in 2011 werden bevestigd door de VN-Raad voor de mensenrechten.

De inspanning met misschien de meeste visibiliteit is het Global Network Initiative (GNI). Dit ging van start in 2008 nadat drie vooraanstaande ICT-bedrijven (Microsoft, Yahoo en Google), mensenrechtenonderzoekers, academici en investeerders twee jaar hadden samengewerkt om tot een gezamenlijke aanpak te komen. Het initiatief wilde reageren op de kritiek dat ICT-bedrijven met name in China de vrijheid op het internet zouden inperken, alsook op het feit dat het Amerikaanse congres van plan leek wetgeving uit te vaardigen over deze thema's (Israel, 2009). Wanneer een bedrijf lid wordt van het GNI, onderschrijft het de beginselen ervan, en laat het onafhankelijk beoordelen of het deze ook naleeft. Het GNI-initiatief heeft echter kritiek moeten incasseren van Amnesty International, dat bij de gesprekken aanwezig was maar niet is toegetreden omdat het de regeling te zwak vond, en van commentatoren uit de bedrijfswereld die erop wijzen dat geen enkel ander ICT-bedrijf er mee is ingestapt omdat het zich dan aan te zware verplichtingen zou onderwerpen (Downes, 2011). Daarnaast zijn (enkele vooral Europese) telecommunicatiebedrijven een industriële dialoog aangegaan rond kwesties van privacy en vrijheid van meningsuiting. Ten slotte is er de Europese Commissie, die als reactie op de problematiek inzake ICT en repressie tijdens de Arabische Lente een 'No Disconnect'-strategie ontwikkelt met volgende vier doelstellingen:

1. **“Technische instrumenten ontwikkelen en verstrekken met het oog op meer privacy en veiligheid voor mensen die onder niet-democratische regimes ICT gebruiken.**
2. **Activisten opleiden in en bewust maken van de mogelijkheden en risico's van ICT.** Met name activisten bijstaan zodat ze optimaal gebruikmaken van instrumenten zoals sociale netwerken en blogs, en hen tegelijk bewust maken van de bewakingsrisico's wanneer ze via ICT communiceren.
3. **Kwaliteitsvolle informatie verzamelen over de toestand "in het veld"** om het niveau van bewaking en censuur op een bepaald tijdstip op een bepaalde plaats te kunnen opvolgen.
4. **Samenwerking.** Een praktische manier ontwikkelen om te zorgen dat alle betrokkenen informatie over hun activiteiten kunnen delen en multilaterale actie kunnen bevorderen, en een samenwerking over de regio's heen opzetten ter bescherming van de mensenrechten.” (EU-persbericht, 2011)

In de werkzaamheden die het Institute for Human Rights and Business rond zelfregulerende normering inzake het respect voor mensenrechten aan betrokkenen uit de ICT-sector verricht in naam van de Commissie, ziet Wagner (2012b) een voorbeeld dat deze aanpak kan illustreren.

Hoewel maatschappelijk verantwoord ondernemen aanbeveling verdient en bedrijven die allerhande veiligheidstechnologieën (niet enkel ICT-gerelateerd) exporteren zoveel mogelijk aansturing inzake mensenrechten moeten krijgen, zullen deze initiatieven, ten gevolge van de onduidelijke bestaande wetgeving inzake exportcontroles, wellicht niet volstaan. Volgens Wagner (2012b) moet men deze initiatieven vooral beschouwen als nuttige stappen die hand in hand met wetgevende initiatieven kunnen gaan. Imago schade is te herstellen. Men kan deze bijvoorbeeld beperken met filialen die mogelijk problematische transacties voor hun rekening nemen. Zonder een juridische stok achter de deur en meer transparantie over de uitvoer zullen er wellicht meer schandalen volgen.

5.4 Is controle nodig? De externe aspecten van de EU-interne veiligheidsstrategie

De EU-interne veiligheidsstrategie stelt het volgende:

“Het concept interne veiligheid heeft geen zin zonder externe dimensie, want interne veiligheid wordt grotendeels bepaald door externe veiligheid. Zowel bilaterale als multilaterale internationale samenwerking door de EU en haar lidstaten is essentieel om de veiligheid te verzekeren, de rechten van de burgers te beschermen en hun veiligheid en de eerbiediging van hun rechten buiten de EU-grenzen te bevorderen.” (Raad van de Europese Unie, 2010: 16).

Deze stelling erkent impliciet de verwevenheid van de huidige mondiale veiligheid. Als men de veiligheid van de internationale burgerluchtvaart bijvoorbeeld wil garanderen, is het duidelijk beter om, in plaats van vluchten uit landen met een eventuele terreurdreiging te verbieden, ervoor te zorgen dat het land geavanceerde screeningstechnologie voor passagiers en bagage kan aankopen. Dezelfde logica is van toepassing op heel wat samenwerkingsverbanden met derde landen in de strijd tegen terrorisme, migratie en internationale misdaad; wil de EU haar beleidsdoelstellingen

halen, dan moet ze technologie gaan delen. Maar waarbij de doelstellingen van de interne veiligheidsstrategie en daarmee ook die van het programma van Stockholm afhangen van overeenkomsten met derde landen, kan het, zoals Monar aangeeft, *“moeilijk zijn zulke overeenkomsten te onderhandelen, aangezien derde landen vaak niet voldoen aan wat de EU inzake eerbiediging van de grondrechten, juridische procedures en gegevensbescherming verwacht.”* (Monar, 2010: 32)

Deze spanning ligt aan de grondslag van de moeilijkheden waarmee de EU kampt om de uitvoer van veiligheidstechnologieën te beheersen. Het EU-nabuuerschapsbeleid drijft deze nog verder op met haar nadruk op stabiliteit in de buurlanden van de EU, ten koste van de bevordering van de democratie (Youngs, 2002). De EU heeft dus al moeten onderhandelen met actoren die het niet te nauw nemen met de mensenrechten, en zal dit nog regelmatig moeten blijven doen. Ten slotte wordt typisch aangenomen, aansluitend op de algemene opstelling van de EU inzake vrije handel, en voor zover de EU en haar lidstaten een gemeenschappelijk beleid voor de veiligheidssector voeren, dat in deze sector het exportpotentieel groot is (Schumann, 2011; Europese Commissie 2012a).

Laat ons aan de hand van een voorbeeld dieper ingaan op deze netelige kwesties. Samenwerken rond terrorismebestrijding met derde landen die slecht scoren op het vlak van mensenrechten gaat altijd gepaard met een moeilijke zoektocht naar een evenwicht tussen de hoop op veiligheid en de wens om mensenrechten te bevorderen. Het Actieplan EU-Egypte uit 2010 streefde bijvoorbeeld naar een samenwerking tussen de EU en Egypte ter bestrijding *“van het gebruik van internet voor terroristische doeleinden”* en voorzag dat de EU steun zou verlenen aan de opbouw van *“technologische capaciteiten bij wetshandhavingsinstanties”* (Europese Commissie, 2010: 31). Maar dit kan niet zonder het internet te filteren en te blokkeren. Bovendien was het algemeen geweten dat Egypte de communicatiemediën in het oog hield om de vrijheid van meningsuiting te onderdrukken (Wagner, 2012b). In dit geval is niet duidelijk of wat de EU voor wat mensenrechten en terrorismebestrijding betreft nastreeft, te verenigen valt.

Ook heeft de Europese Commissie (2012b) cybercriminaliteit als een belangrijk veiligheidsprobleem omschreven. Ze beschouwt het als de ultieme grensoverschrijdende misdaad, wat de behoefte aan internationale partners duidelijk maakt. De voorstellen die de Commissie de afgelopen twee decennia heeft geformuleerd om de EU beleidsmatig beter te wapenen tegen terroristische radicalisering of het online delen van kinderporno waren vaak afhankelijk van filterpraktijken of dwongen internetproviders, de browsegeschiedenis van hun abonnees te delen. Deze technologieën zijn in de EU zelf verkrijgbaar en in gebruik.¹ Willen we cybermisdaad met succes aanpakken, dan moeten ook derde landen toegang krijgen tot dergelijke technologie. Dit zou de uitvoer van dergelijke veiligheidstechnologie kunnen rechtvaardigen, maar tegelijk zijn het nu precies die systemen geweest die tijdens de Arabische Lente gebruikt zijn om activisten op te sporen en waarover zoveel controverse is ontstaan (Valentino-Devries et al, 2011).

Een ander voorbeeld is grensbeheer. Het eigen grensbeheersplan van de EU, EUROSUR en het initiatief inzake slimme grenzen veronderstellen een massale inzet van bewakingstechnologieën zoals onbemande luchtvaartuigen om de Middellandse Zee te bewaken. Het eigen grensbeheersplan van de EU, EUROSUR en het initiatief inzake slimme grenzen veronderstellen een massale inzet van bewakingstechnologieën zoals onbemande luchtvaartuigen om de Middellandse Zee te bewaken. De initiatieven raakten in een stroomversnelling door de ‘grenscrisis’ als gevolg van de Arabische Lente, toen veel mensen door de conflicten hun toevlucht zochten in de EU. Het

¹ Een uitspraak door het Hof van Justitie in 2011 verbood het gebruik van algemene internetfilters. Meer gerichte filterpraktijken vinden echter nog steeds plaats.

is niet louter de bedoeling om migratie- en visummisbruik veel strikter op te sporen, maar ook bufferzones te creëren waar de migratiestroom buiten de grenzen van de EU kan worden beheerd. Dit beleid is intrinsiek afhankelijk van de samenwerking met derde landen, en van het delen van persoonlijke gegevens over migranten, en het aan hen beschikbaar stellen van migratie in kaart te brengen. Hayes en Vermeulen (2012) laten zich in hun rapport heel kritisch uit over de voorstellen voor EUROSUR en het initiatief inzake slimme grenzen. Zij voeren aan dat de plannen niet stroken met de Universele Verklaring van de Rechten van de Mens. De EU-samenwerkingsakkoorden met derde landen houden immers in dat iemand niet zonder toestemming mag vertrekken, waarmee hem of haar het recht op asiel wordt ontnomen. Daarnaast is het een twijfelachtige manier om ontwikkelingshulp te gebruiken. Vranckx, Slijper en Isbister (2011) wijzen er tevens op dat dit alles zijn invloed heeft op de daarmee samenhangende beslissingen voor uitvoervergunningen. Voor spelers als EADS is de levering van gesofisticeerde en geïntegreerde grensbewakingssystemen belangrijk geworden. Zo sleepte dit bedrijf een opdracht in de wacht voor de uitbouw van een dergelijk systeem in Saoedi-Arabië, waarbij het voorzien is dat de Duitse politie een ondersteunende opleiding voorziet. Blijkbaar zou het redelijk makkelijk zijn om voor zulke systemen een uitvoervergunning te krijgen. Een relatief klein percentage van de technologie is immers vergunningsplichtig en niet veel ervan is voor militair gebruik. Vranckx, Slijper en Isbister (2011: 34) betogen dat exportvergunningen voor *“grenscontrole technologie door veel van de vergunnende landen worden aanzien als een bijdrage aan hun pogingen om migratie en de instroom van vluchtelingen te controleren”* en daarmee een manier om het Europees Agentschap voor de samenwerking aan de buitengrenzen, Frontex, in zijn werk bij te staan. Dit betekent dat bezorgdheden omtrent mensenrechten, zoals de behandeling van migranten en vluchtelingen in het land van ontvangst, misschien een mindere rol zullen spelen in de vergunningsbeslissing. Dit zijn geen dilemma's waarmee enkel de EU worstelt. Ook de VS heeft het moeilijk om, met het oog op haar 'homeland security'-doelstellingen, een vergelijk te vinden tussen de noodzaak om internationaal samen te werken en technologie te delen, en haar voorkeur voor een streng exportcontrolesysteem (Commissie binnenlandse veiligheid en exportcontroles, 2012).

5.5 Samenvatting

In dit gedeelte is gebleken dat het moeilijk zal zijn, exportcontroles op veiligheidstechnologieën in te voeren, zelfs nu de Arabische Lente het misbruik van bewakings- en detectietechnologieën duidelijk heeft aangetoond. We hebben kunnen zien dat veiligheidstechnologie geen eenduidig concept is en heel lastig te classificeren, en dat ze vaak uitgebouwd worden op overal verkrijgbare generische technologieën. Bovendien is in sommige gevallen geen controle nodig. Verder werd er betoogd dat regeringen en de EU enkel als mensenrechten in het spel waren bereid zouden zijn om beperkingen of een verbod op het gebruik ervan in te voeren. Er werd op gewezen dat het debat vorm kreeg op een geheel andere manier dan bij de discussies over wapenexport het geval was, en dat dit het moeilijker zou maken om die kaders als wetgevende basis te hanteren.

Vervolgens besprak dit gedeelte de bestaande reikwijdte en het potentieel om controles aan te passen of er nieuwe in te voeren in de volgende kaders:

- EU-regeling voor producten voor tweërlei gebruik
- Gemeenschappelijk standpunt inzake wapenuitvoer
- Folterverordening
- Sancties / embargo's
- Door de sector aangevoerde initiatieven

Omdat de juridische bepalingen rond de controle op veiligheidstechnologieën ontegensprekelijk fragmentarisch en onduidelijk zijn, dient er zich geen eenvoudige oplossing aan. De Arabische Lente heeft vooral het gebrek aan controle op de uitvoer van bewakingstechnologieën blootgelegd. Maar omdat in het verleden nooit een akkoord heeft bestaan rond exportcontroles op politie-uitrusting, worden repressieproducten zoals waterkannonnen en elektroshock-wapens enkel gecontroleerd als een lidstaat beslist om dit nationaal te doen. Sancties vormen een efficiënte oplossing op korte termijn, maar de regeling voor producten voor tweërlei gebruik vormt op middellange termijn wellicht de beste basis om exporten te controleren. De folterverordening bood een precedent voor de verordening die de export en import van, wat Wagner (2012b) omschrijft als, 'single-use' producten die alleen dienen voor repressie verbiedt.

Als laatste punt besprak dit deel van het rapport de externe vereisten van het EU-interne veiligheidsbeleid, vooral dan inzake transnationale misdaad, terrorismebestrijding en grensbeheer. Deze zijn maar realiseerbaar mits samenwerking en het delen van technologieën met derde landen. Sommige van deze landen presteren slecht op het vlak van mensenrechten. De vereiste technologie zijn net die bewakings- en detectieapparaten die heel eenvoudig te misbruiken zijn. Dit betekent dat de EU, door de export van veiligheidstechnologieën te controleren, misschien niet in staat zal zijn om sommige van haar plannen inzake interne veiligheid ten uitvoer te brengen (of dit een slechte zaak is, is een andere vraag).

6 Conclusies

Zoals Edler en James (2012) stelden, heeft de Europese Commissie als beleidsondernemer een nieuw EU-beleidsdomein rond de veiligheidssector en technologische ontwikkeling geopend. In een eerste fase had ze geen duidelijk mandaat en onvoldoende steun van zowel de sector als de lidstaten. De gesprekken die voor dit rapport werden gevoerd, toonden aan dat het programma voor veiligheidsonderzoek in veel opzichten een succes was, maar dat de acties van de Commissie nog steeds geen volledige steun genoten van alle betrokken actoren. Edler en James (2012) hebben aangevoerd dat het niet-bereiken van een akkoord over defensieonderzoek in het financieringsprogramma Horizon 2020 het bewijs is dat de Commissie beperkt is in haar capaciteit om haar rol verder uit te breiden. Bovendien is de bewering van de Commissie dat er niet echt een onderscheid bestaat tussen de veiligheids- en de defensiesector en desbetreffende technologieën en gebruikersbehoeften door verschillende rapporten (waaronder het onderhavige) in vraag gesteld. Ze vonden dat vooral de gebruikersbehoeften nog duidelijk van elkaar verschillen. De technologieën en sectoren van veiligheid en defensie (ofwel interne en externe veiligheid) zijn echter ontegenzegglijk met elkaar verbonden, niet in het minst door de EU-beleidsacties die deze grens hebben willen doen vervagen. Eén onderbelicht verband is de kwestie van de exportcontroles: de Arabische Lente heeft bevolking en politiek doen inzien dat de controles op de EU-uitvoer van veiligheidstechnologieën ontoereikend zijn.

Het rapport heeft bij aanvang volgende onderzoeksvragen gesteld:

- Hoe is het veiligheidsconcept veranderd in de periode na de Koude Oorlog? En hoe heeft de EU dit begrepen?
- Wat is de veiligheidsmarkt? Welke parameters zijn bepalend voor haar technologieën en geven vraag en aanbod vorm? Kunnen deze worden gedifferentieerd van de meer gevestigde defensietechnologieën, bedrijven en klanten / gebruikers?
- Welke beleidsinitiatieven neemt Europa op dit vlak en wat stuurt ze aan? Hoe beïnvloeden zij de markt? Wie zijn de beleidsondernemers – de Europese instellingen of de lidstaten? Bestaat er samenhang tussen de verschillende beleidsdoelstellingen? Is het bevorderlijk of gevaarlijk om defensie en veiligheid in elkaar te laten opgaan? Welke impact hebben kwesties gerelateerd aan veiligheidsindustrie en –technologie op andere EU-beleidsdomeinen?
- Ten slotte is er analyse vereist naar de plaats die veiligheidstechnologieën in het strategische exportcontrolesysteem innemen. Zijn de bestaande stelsels voorzien op veiligheidstechnologieën? Moeten veiligheidstechnologieën worden gecontroleerd? Wat zijn de ethische vraagstukken?

In wat volgt, overlopen we hoe elk hoofdstuk deze vragen heeft beantwoord.

Als antwoord op de eerste groep vragen kunnen we niet ontkennen dat het veiligheidsconcept verandert na het einde van de Koude Oorlog. Beleidsmakers hebben zich mee in een academisch debat over het veiligheidsconcept ingeschreven, en de definitie van veiligheidsbedreigingen beperkt zich niet langer tot externe militaire bedreigingen. In deze context is de opkomst van het concept ‘homeland security’ heel belangrijk geweest. Dit Amerikaans begrip heeft ingang gevonden in de hele EU, maar dan vooral in de agenda van de Europese Commissie. Door het ontstaan van de ‘homeland security’-idee vond de Commissie klaarblijkelijk nog een weg om zich toegang te verschaffen tot het veiligheids- en defensiedomein, dat de lidstaten liefst verder

intergouvernementeel behandelden. Dit heeft een ongewone beleidsdynamiek op gang gebracht waarbij de Commissie er belang bij had de nadruk te leggen op de mate van grensvervaging tussen interne en externe veiligheidsbehoeften, leveranciers en technologieën.

De Commissie heeft ervoor gekozen de veiligheidsmarkt behoorlijk eng te definiëren en zich te richten op bepaalde types producten die volgens haar aantrekkelijk zijn voor overheidsklanten. Dit is uitgemond in beleidsmaatregelen die volgens critici voorrang geven aan defensiebedrijven boven niet-defensieleveranciers. Het rapport vroeg zich af of er nog een onderscheid bestond tussen defensie- en veiligheidstechnologieën, bedrijven en klanten. Beide types technologieën vertrekken van dezelfde generische civiele technologieën en er is sprake van een zekere overlapping, hoewel dit mogelijk overdreven is. Bovendien erkent zelfs de Europese Commissie (2012a) nu dat onderzoeksondernemingen en producenten van defensie- en veiligheidstechnologieën niet identiek zijn. De Commissie had verwacht dat er een veiligheidsmarkt zou ontstaan die – en dit was in het voordeel geweest van de defensiebedrijven – op de defensiemarkt zou lijken. Deze markt is er echter nog niet, en vandaag zijn ook niet-defensiebedrijven actief op de veiligheidsmarkt, met name in domeinen zoals telecommunicatie en bewaking. Bovendien zien niet alle defensiebedrijven veiligheid als de meest veelbelovende markt om naar te diversifiëren, terwijl andere niet onmiddellijk bereid zijn om concrete stappen te zetten. Ten derde meldde het rapport dat militaire en civiele veiligheidsopdrachten (en dus behoeften) op sommige punten overlappen. Maar weinig wees erop dat er een overkoepelende overheidsklant zou opstaan (zelfs niet in de vorm van één nationale, civiele veiligheidsklant). De redenen hiervoor waren dat behoeften en verwachtingen verschilden, en dat civiele klanten niet geneigd waren om het militaire aankoopmodel – omwille van de inefficiëntie ervan – te hanteren. Een laatste punt ging erover dat welbekende mislukkingen van grootschalige veiligheidsprojecten in zowel de VS als het VK andere landen konden doen aarzelen om in zulke grote projecten te stappen, zeker nu deze volop in de overheidsuitgaven moeten snijden. De vraagzijde was daarmee niet zo sterk als de Commissie had verwacht.

Onderdeel 4 omschreef de huidige beleidsinitiatieven in Europa voor de veiligheids- en de defensiesector. Met uitzondering van de Frans-Britse akkoorden lagen deze in handen van de EU-instellingen. Uit de beoordeling kwam naar voren dat het EDA niet voluit kon werken omdat het onvoldoende financiering en steun kreeg om de zo goed als onmogelijke hervorming van de EDITB tot een goed einde te brengen. En dit terwijl de Commissie beleidsmatig het midden leek te willen houden tussen enerzijds de handel in defensie- en veiligheidsuitrusting intern en extern liberaliseren, en anderzijds actieve beleidsmaatregelen introduceren om de sector steun te bieden. Het rapport vond evenwel dat, omdat de Commissie niet als klant kon optreden, zij de sector niet zo efficiënt kon beheren als zij misschien wilde. De Commissie is maar beperkt in staat om een tegenwicht te bieden aan de beperkte vraag naar veiligheidstechnologieën in de lidstaten. Dat de Commissie concrete stappen wilde zetten in de beleidsontwikkeling bleek uit hoe actief zij waren op een aantal beleidsdomeinen. Neem nu de grenscontroles: deze konden, in een poging om de vraag op te krikken, in verband worden gebracht met veiligheids- en defensietechnologieën. Tevens viel het op dat het beleid inzake interne veiligheid een richting leek uit te gaan die moeilijk te rijmen was met de prominente plaats die mensenrechten in het buitenlands beleid van de EU kregen. Ook schat de Commissie het enthousiasme voor veiligheidstechnologieën bij lidstaten en EU-burgers misschien te positief in. Deze problemen betekenen dat de Commissie in haar plannen voor de industriële veiligheidssector wellicht meer dan verwacht rekening moet houden met de wereldwijde exportmarkt.

Ten slotte stelde het rapport dat veiligheidstechnologieën en exportcontroles op de politieke agenda waren verschenen nadat de media hadden bericht over hoe bewakings- en

detectietechnologieën tijdens de Arabische Lente waren misbruikt. De opkomst van deze op afstand bediende technologieën is duidelijk het belangrijkste aspect van de nieuwe veiligheidstechnologieën. Het is namelijk in deze technologieën dat de mogelijke grensvervaging tussen interne en externe veiligheid of tussen veiligheid en defensie zich het sterkst zal doorzetten. Het is ook de groep technologieën die doorslaggevend is voor de groei van de 'homeland security'-staat. Dit stelt het interne beleid voor heel wat ethische dilemma's. Het rapport heeft echter enkel die voor de externe betrekkingen van de EU behandeld.

Omdat de interne veiligheid, via de externe dimensie van de ruimte van vrijheid, veiligheid en recht, een onvermijdelijk extern aspect kent, kan het beleid van de EU (bijvoorbeeld op vlak van grenscontroles) enkel succesvol zijn wanneer veiligheidstechnologieën naar buurlanden worden uitgevoerd. Volgens het rapport leidt dit onvermijdelijk tot het moeilijke ethische vraagstuk hoe een evenwicht te vinden tussen mogelijk misbruik en beleidsefficiëntie. Deze ethische dilemma's kwamen duidelijk tot uiting tijdens de Arabische Lente. Daar maakten regimes die betogers wilden onderdrukken misbruik van door Europese exporteurs verkochte bewakingstechnologieën.

Daar waar het de exportcontroles voor veiligheidstechnologieën besprak, stelde het rapport dat in deze kwestie maar moeilijk een EU-consensus te vinden zou zijn. Sommige lidstaten zitten op dezelfde lijn als de Commissie dat veiligheidstechnologieën een groeiende exportmarkt moeten zijn voor Europese bedrijven. Anderen zien de exportcontroles liever uitgebreid. Dit is een aloude tegenstelling tussen voor- en tegenstanders van controles op politie-uitrusting die kan worden ingezet voor repressie en als middel om mensenrechten te schenden. Omwille van deze tegenstelling zijn dergelijke producten niet opgenomen in de gedragscode inzake wapenexport en is de folterverordening in plaats daarvan van een kortere lijst vertrokken. Het rapport merkte wel op dat lidstaten wettelijk enkele mogelijkheden hebben om unilateraal actie te ondernemen, iets wat sommigen ook hadden hebben. De kwestie wordt nog complexer doordat we niet alle technologieën die de EAVO (2006) veiligheidstechnologieën heeft genoemd als één groep kunnen beschouwen. Sommige staan al op lijsten met militaire producten of met producten voor tweërlei gebruik. Bij anderen is misbruik weinig waarschijnlijk. De kloof is het grootst bij op afstand bediende of bewakings- en detectietechnologieën.

Het rapport besprak volgende alternatieven om exportcontroles ook naar deze veiligheidstechnologieën uit te breiden:

- EU-regeling voor producten voor tweërlei gebruik
- Gemeenschappelijk standpunt inzake wapenuitvoer
- Folterverordening
- Sancties / embargo's
- Door de sector aangevoerde initiatieven

Het besloot dat het regime voor tweërlei gebruik op middellange termijn de beste basis biedt om ook veiligheidstechnologieën aan controle te onderwerpen, niettegenstaande dat deze nieuwe groep op-afstand-bediende technologieën ook weer duidelijk maken in welke mate het dual-use regime, inclusief de definitie van dual-use, een complexe aangelegenheid is. Daarnaast voerde het aan dat de folterregeling een model aanreikte om de export te verbieden van bepaalde bewakingstechnologieën die volgens Wagner (2012b) alleen konden worden gebruikt voor repressie. Het rapport oordeelde dat sancties en door de sector aangevoerde initiatieven waarschijnlijk niet de kracht hadden om oplossingen op lange termijn aan te bieden.

We mogen dus besluiten dat, in weerwil van het uitgangspunt van de Commissie, de veiligheids- en de defensiesector, technologieën en behoeften niet inwisselbaar zijn. Dankzij haar ondernemingszin heeft de Commissie snel een nieuw beleidsdomein kunnen openen, maar de Commissie en de lidstaten verschillen van mening betreffende het soort technologieën waaraan nood is, en – potentieel belangrijker – welke soort technologieën aanvaardbaar zijn. De toestand in de VS is vergelijkbaar, en we kunnen maar hopen dat er trans-Atlantisch lessen worden getrokken, om zo geen schaarse middelen te verspillen. De Arabische Lente heeft de EU er ook aan herinnerd dat haar exportcontroleregime niet geheel waterdicht is. Een van de probleemgebieden hierbij is de controle op bepaalde types veiligheidstechnologieën. Hoewel de externe behoeften van het EU-beleidsdomein interne veiligheid zonder twijfel belangrijk zijn, mogen verstandige beleidsmakers de ethische vragen die dit beleidsdomein opwerpt niet onbeantwoord laten.

7 Literatuurlijst

Akkermann, Mark (2012) Militarisering van Security Inventarisatie Nederlandse bedrijven, Amsterdam, Campagne tegen Wapenhandel, november 2012: te vinden op http://stopwapenhandel.org/sites/stopwapenhandel.org/files/cybersecurity_final.pdf (geraadpleegd op 14 november 2012)

Amnesty International (2011), Arms for Internal Security: Will they be covered by an Arms trade Treaty?, Londen, Amnesty International

Amnesty International en Omega Research Foundation (2010), From Words to Deeds: making the EU Ban on the Trade in 'Tools of Torture' a Reality, Londen, Amnesty International

Archick, Kristin (2011) US-EU Cooperation against Terrorism, CRS Report for Congress RS22030, Congressional Research Service, Washington

ASD-Europe (2011) Facts and Figures 2010, te vinden op: http://www.asd-europe.org/site/fileadmin/images/publications_thumbs/FF2010.pdf

Auswärtiges Amt (2012) Deutsch-Französische Erklärung: Für eine stärkere europäische Sicherheit und Verteidigung, Parijs, 6 februari 2012
<http://www.auswaertigesamt.de/cae/servlet/contentblob/608180/publicationFile/164316/120206-D-F-Sicherheitserklaerung.pdf>

Ayoob, Mohammed (1997) 'Defining Security: A Subaltern Realist Perspective', in Keith Krause en Michael Williams (eds.) *Critical Security Studies: Concepts and Cases*, UCL Press, Londen: 121-147

Baldwin, David (1997) The Concept of Security, *Review of International Studies*, 23(1997): 5-26

Bailes, Alyson (2008), 'The EU and a 'Better World': What Role for the European Security and Defence Policy?', *International Affairs*, 84(1): 115-30

Bailes, Alyson (2004), 'Preface', in Sybille Bauer en Mark Bromley, *The European Union Code of conduct on Arms Exports*, SIPRI Beleidsnota nr. 8, Stockholm: SIPRI

Bauer, Sibylle (2003) The EU Code of conduct on Arms Exports-Enhancing the Accountability of Arms Export Policies?, *European Security*, 12(3/4): 129-48

Beidel, Eric (2011) Homeland Security Market Vibrant despite Budget Concerns, *National Defense*, september 2011:
<http://www.nationaldefensemagazine.org/archive/2011/September/Pages/HomelandSecurityMarket%E2%80%98Vibrant%E2%80%99DespiteBudgetConcerns.aspx>

Bellavita, Christopher (2008) Changing Homeland Security: What is Homeland Security?, *Homeland Security Affairs*, 4(2): 1-30

Bigo, Didier (2002) Security and Immigration: Toward a Critique of the Governmentality of Unease, *Alternatives*, 27(1): 63-92.

Bigo, Didier en Julien Jeandesboz, (2010), *The EU and the European security industry questioning the 'public-private dialogue'*, INEX Policy Brief no. 5/februari 2010.

BIS (Department for Business, Innovation and Skills), (2012) *UK Strategic Export control Lists: The consolidated list of strategic military and dual-use items that require export authorisation*, Londen, augustus 2012, te vinden op: <http://www.bis.gov.uk/assets/biscore/eco/docs/control-lists/12-1014-uk-strategic-export-control-list-consolidated.pdf> (geraadpleegd op 13 augustus 2012)

Bleker, Henk (2011) *Kabinetsreactie Groenboek exportcontrole dual-usegoederen*, Ministerie van Economische Zaken, Landbouw en Innovatie, Den Haag, 20 september 2011

Bossong, Raphael (2008) The Action Plan on Combating Terrorism: A Flawed Instrument of EU Security Governance, *Journal of Common Market Studies*, 46(1): 27-48

Briani, Valerio en Nicolo Sartori (2011) Transatlantic Industrial Policies in the Security Sector, in *EU-US Security Strategies: Comparative Scenarios and Recommendations*, Issue 3: 156-66 Te vinden op: http://csis.org/files/publication/110614_Conley_EUUSSecurity_WEB.pdf

Brits ministerie van Defensie (2006), *Defence Technology Strategy*, Londen: http://www.mod.uk/NR/rdonlyres/27787990-42BD-4883-95C0-48BB72BC982/0/dts_complete.pdf

Brits ministerie van Defensie (2012) *National Security through Technology: Technology, Equipment and Support for UK Defence and Security*, Cm 8278, The Stationery Office, Londen, februari 2012

Britse parlementaire commissie voor defensie (2010) *Defence equipment*, Sixth Report of Parliamentary Session 2009-10, Londen, Brits Lagerhuis

Britse parlementaire commissies inzake wapenexportcontroles (2012), *Commissies inzake wapenexportcontroles - First Joint Report Scrutiny of Arms Exports 2012*, Londen, Brits Lagerhuis

Bromley, Mark (2012) *The review of the EU common position on arms exports: prospects for strengthened controls*, Non-Proliferation Papers No. 7 januari 2012, EU Non-Proliferation Consortium, Te vinden op: <http://www.sipri.org/research/disarmament/eu-consortium/publications/publications/non-proliferation-paper-7> (geraadpleegd op 7 mei 2012)

Brunnstrom, David en Anna Ringstrom, (2011) Sweden blocked an effort by other EU states to add two telecoms firms in Syria with commercial links to Swedish firm Ericsson to an EU sanctions list this week, EU diplomats said, Reuters, 2 december 2011, te vinden op: <http://www.reuters.com/article/2011/12/02/us-eu-syria-sweden-idUSTRE7B120J20111202> (geraadpleegd op 7 mei 2012)

Bundesministerium für Wirtschaft und Technologie (2010), *Zukunftsmarkt zivile Sicherheit: Industriepolitische Konzeption des Bundesministeriums für Wirtschaft und Technologie*, Berlin, november 2010

Buzan, Barry (1991) *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Lynne Rienner, Boulder

Buzan, Barry, Ole Wæver en Jaap de Wilde, (1998) *Security: A New Framework for Analysis*, Lynne Rienner, Boulder

Chandler, David (2008) Human Security: The Dog that didn't Bark, *Security Dialogue*, 39(4): 427-38

Chick, Claire (2011) *2011 Franco-British Council Annual Defence Conference Report*, Franse ambassade, Londen 31 maart 2011

Clark, Liat (2012), Wikileaks' Syria files will be 'embarrassing' for Syria and the West, *Wired*, 5 juli 2012 Te vinden op; <http://www.wired.co.uk/news/archive/2012-07/05/wikileaks-syria-files> (geraadpleegd op 16 juli 2012)

Coats, R Morris, Gökhan Karahan en Robert Tollison (2006) Terrorism and Pork Barrel Spending, *Public Choice*, 128(1): 275-87

Cohen, Dara et al (2006) Crisis Bureaucracy: Homeland Security and the Political Design of Legal Mandates, *Stanford Law Review*, 59(3): 673-760

Colvin, Michael (1998) European armaments restructuring and the role of WEU: Report submitted on behalf of the Defence Committee to the WEU Assembly, *Document 1623*, Parijs, 9 november 1998

Committee on Homeland Security and Export controls, (2012) *Export control Challenges Associated with Securing the Homeland*. Washington, DC, The National Academies Press

Comninos, Alex (2011) *Twitter revolutions and cyber crackdowns: User-generated content and social networking in the Arab spring and beyond*, Association for Progressive Communications, te vinden op: http://www.apc.org/en/system/files/AlexComninos_MobileInternet.pdf (geraadpleegd op 21 juli 2012)

Cooper, Neil (2012) *The Arms trade Treaty in the Context of Post-Cold War Conventional arms trade Regulation*, 10 juli 2012, Te vinden op: <http://www.caat.org.uk/issues/att/att-neil-cooper.pdf> (geraadpleegd op 13 augustus 2012)

Cooper, Neil (2006) What's the point of arms transfer controls?, *Contemporary Security Policy*, 27(1): 118-37

Cornish, Paul (1995) *The Arms trade and Europe*, Chatham House Papers, Londen, Royal Institute of International Affairs

Craig, Paul (2010) *The Lisbon Treaty: Law, Politics and Treaty*, Oxford, OUP

Curtis, Polly (2011), Government faces legal action by US firm over e-border system, *Guardian*, Londen, 25 augustus 2011: <http://www.guardian.co.uk/uk/2011/aug/25/government-legal-action-e-border>

De Pauw, Sara (2010) *Het gemeenschappelijk standpunt over wapenuitvoer in het licht van een ontluikende Europese defensiemarkt*, Achtergrondnota, Brussel, Vlaams Vredesinstituut.

Downes, Larry (2011) Why no one will join the Global Network Initiative, *Forbes*, 30 maart 2011, te vinden op: <http://www.forbes.com/sites/larrydownes/2011/03/30/why-no-one-will-join-the-global-network-initiative/> (geraadpleegd op 3 augustus 2012)

Dunne, J Paul (1995) The Defense Industrial Base, in Hartley, Keith en Todd Sandler, (Eds.), *Handbook of Defense Economics*, Oxford, Elsevier: 399-430

Ecorys et al, (2009) Document ENTR/06/054, Study on the Competitiveness of the EU Security Industry, Onderzoek ten behoeve van het DG Ondernemingen en industrie binnen de Raamovereenkomst voor het uitvoeren van sectorale concurrentiestudies, Brussel, DG Ondernemingen en industrie, 15 november 2009

Edler, Jakob en Andrew James (2012) Understanding the Emergence of STI policies in the EU: *the Genesis of EU Security Research and the Role of the EU Commission as Policy Entrepreneur*, Manchester Business School Working Paper No. 630, Manchester, juni 2012

Edwards, Jay (2011) The EU Defence and Security Procurement Directive: A Step Towards Affordability?, *International Security Programme Paper ISP PP 2011/05*, Londen, Chatham House

Eguren Secades, Santiago (2011) Openness in the European Defence Market and Company Competitiveness, in Bailes, Alyson en Depauw, Sara (Eds.) *De Europese defensiemarkt: een kwestie van efficiëntie en verantwoordelijkheid*, Brussel, Vlaams Vredesinstituut: 29-36

Elgin, Ben, Vernon Silver, en Hermann Zschiegner, (2011) *Wired For Repression*. Bloomberg, Te vinden op <http://www.bloomberg.com/data-visualization/wired-for-repression/> (geraadpleegd op 16 juli 2012)

EAVO (2006) *Meeting the Challenge: the European Security Research Agenda*, rapport van de Europese Adviesraad voor veiligheidsonderzoek, september 2006, Luxemburg, Bureau voor Officiële Publicaties van de Europese Gemeenschappen

Euractiv (2006) Critical Infrastructure, <http://www.euractiv.com/en/security/critical-infrastructure/article-140597>

European Organisation for Security (2011) Security Market Evaluation and Recommendations for Funding Future EU Security Activities, maart 2011, te vinden op; <http://www.eos-eu.com/LinkClick.aspx?fileticket=y0rpzCaYh7o=&tabid=318>

Europees Defensieagentschap, (2007) *A Strategy for the European Defence Technological and Industrial Base*, Brussel: Europees Defensieagentschap, mei 2007

Europese Commissie (2012a) *Beleid op het gebied van de veiligheidsindustrie: Actieplan voor een innovatieve en concurrerende veiligheidsindustrie*, COM (2012) 417 definitief, Brussel, 26 juli 2012

Europese Commissie (2012b) *De aanpak van criminaliteit in het digitale tijdperk – Oprichting van een Europees Centrum voor de bestrijding van cybercriminaliteit*, COM(2012) 140 definitief, Brussel, 28 maart 2012

Europese Commissie, (2011) *De totstandbrenging van een open en veilig Europa: de begroting voor binnenlandse zaken 2014-2020*, COM (2011) 749 definitief, Brussel, 15 november 2011

Europese Commissie (2010) Actieplan EU-Egypte, te vinden op: http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146097.pdf (geraadpleegd op 13 augustus 2012)

Europese Commissie (2009) *Een Europese agenda voor onderzoek en innovatie op het gebied van veiligheid – Initieel standpunt van de Commissie over de belangrijkste bevindingen en aanbevelingen van het ESRIF*, COM (2009) 691 definitief, Brussel, 21 december 2009

Europese Commissie (2008) *Onderzoek naar de mogelijkheden tot instelling van een Europees grensbewakingssysteem (EUROSUR)*, COM (2008) 68 definitief, Brussel, 13 februari 2008

Europese Commissie (2007) *Een strategie voor een sterkere en meer concurrerende Europese defensie-industrie*, COM (2007) 764 definitief, Brussel, 5 december 2007

Europese Commissie (2006) *Interpretatieve mededeling over de toepassing van artikel 296 van het Verdrag voor overheidsopdrachten op defensiegebied*, COM (2006) 779 definitief, Brussel, 7 december 2006.

Europese Commissie (2004a) *Veiligheidsonderzoek: de volgende stappen*, COM (2004) 590 definitief, Brussel, 7 september 2004

Europese Commissie, (2004b), *Groenboek: overheidsopdrachten op defensiegebied*, Document COM (2004) 608 definitief, Brussel, 29 september 2004

Europese Commissie (2003a) *Europese defensie - Industriële en marktvraagstukken - Naar een EU-beleid voor defensiematerieel*, COM (2003) 113, Brussel, 11 maart 2003.

Europese Commissie (2003b) *Een samenhangend kader voor de lucht- en ruimtevaartindustrie: een antwoord op het STAR 21-verslag*, COM (2003) 600 definitief, Brussel, 13 oktober 2003.

Europese Commissie, (1997), *Tenuitvoerlegging van de strategie van de Unie inzake de defensie-industrie*, COM 97/583, december 1997, Brussel

Europese Commissie, (1996), *Uitdagingen voor de Europese defensie-industrie: een bijdrage voor actie op Europees niveau*, COM 96/10, januari 1996, Brussel

Europese Raad, (2003) *Een veiliger Europa in een betere wereld* Brussel: Europese Unie

Evans, Samuel, (2009), *Technological ambiguity & the Wassenaar Arrangement*, DPhil. Thesis, University of Oxford

Flechtner, Stephanie (2006) European Security and Defense Policy: Between 'Offensive Defense' and 'Human Security', *Internationale Politik und Gesellschaft*, 4/2006: 157-73

Gemeinsame Konferenz Kirche und Entwicklung (2012) *Rüstungsexportbericht 2011 der GKKE*, januari 2012, Bonn/Berlijn

Gordon, Joy (2010) *Invisible War: The United States and the Iraq Sanctions*, Harvard, Harvard University Press

Haine, Jean Yves, (2011) The Failure of a European Strategic Culture – EUFOR CHAD: The Last of its Kind?, *Contemporary Security Policy*, 32:3, 582-603

Hale, Julian (2011) EU to Establish Defense Policy Task Force, *Defense News*, 7 november 2011 <http://www.defensenews.com/article/20111107/DEFSECT04/111070302/EU-Establish-Defense-Policy-Task-Force>

Hallsworth, Simon en John Lea (2011) Reconstructing Leviathan: Emerging contours of the security state, *Theoretical Criminology*, 15 (2): 141-157

Hartley, Keith (2011), Creating a European Defence Industrial Base, *Security Challenges*, 7(3): 95-111.

Hayes, Ben en Mathias Vermeulen (2012) *Borderline: The EU's New Border Surveillance Initiatives: Assessing the Costs and Fundamental Rights Implications of EUROSUR and the "Smart Borders" Proposals*, Berlijn en Brussel, Heinrich Böll Stiftung

Hayes, Ben (2010) 'Full Spectrum Dominance' as European Union security policy: On the trail of the 'NeoConOpticon', in Kevin Haggerty en Minas Samaras (Eds) *Surveillance and Democracy*, Routledge, Abingdon: 148-70

Hayes, Ben (2009), NeoConOption: The EU Security-Industrial Complex, Transnational Institute, Amsterdam (<http://www.statewatch.org/analyses/neoconopticon-report.pdf>)

Hayes, Ben (2006), Arming Big Brother; the EU's Security Research Programme, Statewatch-TNI Report: <http://www.statewatch.org/analyses/bigbrother.pdf>

ICISS (2001) The Responsibility to Protect: Report of the International Commission on Intervention and State Sovereignty, International Development Research Council, Ottawa

International Institute for Strategic Studies (IISS), (2012) *The Military Balance 2012*, Londen, Routledge

IRIS, Instituto Affari Internazionali en University of Manchester, (2010) Study on the Industrial Implications of the Blurring of Dividing Lines between Security and Defence Eindverslag juni 2010 http://ec.europa.eu/enterprise/sectors/defence/files/new_defsec_final_report_en.pdf

Israel, Brian (2009) "Make Money Without Doing Evil?" Caught Between Authoritarian Regulations in Emerging Markets and a Global Law of Human Rights, U.S. ICTs Face a Twofold Quandary, *Berkeley Technology Law Journal*, 24(1): 617-55

James, Andrew (2009a), Defence and Security R&D in Europe: SANDERA Background Report: www.sandera.net

James, Andrew (2009b) Introduction and Synthesis Paper, www.sandera.net

Jeandesboz, Julien en Francesco Ragazzi, (2010), *Review of Security Measures in the Research Framework Programme*, Onderzoek voor de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken van het Europees Parlement, Europees Parlement, Brussel <http://www.statewatch.org/news/2010/nov/ep-review-security-research-programme.pdf>

Katzenstein, Peter (1997), Introduction, in Katzenstein, Peter (Ed.), *The Culture of National Security: Norms and Identity in World Politics*, Columbia University Press, New York: 1-32

Kempin, Ronja, Jocelyn Mawdsley en Stefan Steinicke (2012) *Entente Cordiale: Eine erste Bilanz französisch-britischer Zusammenarbeit in der Sicherheits- und Verteidigungspolitik*, Deutsche Gesellschaft für Auswärtige Politik, Berlijn

Kington, Tom (2011) Anglo-French Deal Upsets Neighbors: Germans, Italians Warn of '2-Tier Europe', *Defense News*, 13.6.2011, te vinden op: <http://www.defensenews.com/article/20110613/DEFFEAT04/106130301/Anglo-French-Deal-Upsets-Neighbors> (geraadpleegd op 23 juli 2012).

Lodge, Juliet (2004) EU Homeland Security: Citizens or Suspects? *Journal of European Integration*, 26(3): 253-79

Marti Sempere, Carlos (2011) The European Security Industry: A Research Agenda, *Defence and Peace Economics*, 22 (2): 245-64

Masseret, Jean-Pierre en Jacques Gautier, (2009) 'L'Airbus militaire A400m sur le «chemin critique» de l'Europe de la défense', Rapport d'information, No. 205, *Sénat français*, februari 2009

Masson, Hélène en Lucia Marta (2011), The Security Market in the EU and United States: Features and Trends, in *EU-US Security Strategies: Comparative Scenarios and Recommendations*, Issue 3: 111-26 Te vinden op: http://csis.org/files/publication/110614_Conley_EUUSecurity_WEB.pdf

Maulny, Jean-Pierre (2012) *The Franco-British Treaty, the European Union's 'Pooling and sharing' and NATO's 'Smart Defence': How can the different initiatives in terms of pooling capabilities be coordinated?* Parijs, IRIS

Mawdsley, Jocelyn (2011) Towards a Merger of the European Defence and Security Markets?, in Bailes, Alyson en Depauw, Sara (Eds.) *De Europese defensiemarkt: een kwestie van efficiëntie en verantwoordelijkheid*, Brussel, Vlaams Vredesinstituut: 11-19

Mawdsley, Jocelyn (2008a) European Union Armaments Policy: Options For Small States?, *European Security*, 17 (2-3): 367-86

Mawdsley, Jocelyn (2008b) L'industria europea degli armamenti nel contesto dell'integrazione europea: alcune contraddizioni" in Chiara Bonaiuti e Achille Lodovisi (Eds.), *Industria militare e difesa europea: rischi e prospettive*, Annuario La Pira Armi e Disarmo n. 3, Milano, Jaca Books: 75-82

Mawdsley, Jocelyn (2004) The Commission Moves into Defence Research, *European Security Review* 2004, (22), 6-8.

Mérand, Frédéric (2008) *European Defence Policy: Beyond the Nation State*, Oxford University Press, Oxford

Merritt, Giles (2004), Industrial Aspects of European Defence and Concrete Measures, in von Wogau, Karl (Ed.), *The Path to European Defence*, Antwerpen, Maklu-Publishers: 215-40

Molas-Gallart, Jordi (1999), Measuring Defence R&D: A Note on Problems and Shortcomings, *Scientometrics*, 45(1): 3-16

Monar, Jörg (2010) The EU's Externalisation of Internal Security Objectives: Perspectives after Lisbon and Stockholm, *The International Spectator*, 45(2): 23 -39

Morag, Nadav (2011) Does Homeland Security Exist Outside the United States?, *Homeland Security Affairs*, 7(september): 1-5

Morozov, Evgeny (2011) *The Net Delusion: The Dark Side of Internet Freedom*, New York, Public Affairs

Mörth, Ulrika en Malena Britz (2004) 'European Integration as Organizing: The Case of Armaments', *Journal of Common Market Studies*, 42(5): 957-73

Mörth, Ulrika, (2000), 'Competing Frames in the European Commission - the Case of the Defence Industry and Equipment Issue', *Journal of European Public Policy*, 7(2): 173-89

Mueller, John en Mark Stewart (2012) The Terrorism Delusion: America's Overwrought Response to September 11, *International Security*, 37(1): 87-110

Nielsen, Nikolaj (2012a) EU-funded consortium unveils border-control robot, *EUObserver*, 10 mei 2012: <http://euobserver.com/22/116223> (geraadpleegd op 10 mei 2012)

Nielsen, Nikolaj (2012b) EU components used in Belarus spy drones says NGO, *EUObserver*, 10 september 2012: <http://euobserver.com/foreign/117489> (geraadpleegd op 20 september 2012)

Pawlak, Patryk (2009) Made in the USA? The influence of the USA on the EU's Data Protection Regime, Centre for European Policy Studies, Brussel

Perlroth, Nicole (2012) Software Meant to Fight Crime Is Used to Spy on Dissidents, *New York Times*, 30 augustus 2012

Persbericht van de Europese Unie (2011) Digital Agenda: Karl-Theodor zu Guttenberg invited by Kroes to promote internet freedom globally, te vinden op: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1525&format=HTML&aged=0&language=EN&guiLanguage=en> (geraadpleegd op 13 augustus 2012)

Poitevin, Cedric (2011) Een Europees exportcontrole regime: een kwestie van efficiëntie en verantwoordelijkheid, in Bailes, Alyson en Depauw, Sara (Eds.) *De Europese defensiemarkt: een kwestie van efficiëntie en verantwoordelijkheid*, Brussel, Vlaams Vredesinstituut: 47-52

Privacy International (2012) British government admits it has already started controlling exports of Gamma International's FinSpy, Persbericht 10 september 2012, te vinden op: <https://www.privacyinternational.org/press-releases/british-government-admits-it-has-already-started-controlling-exports-of-gamma> (geraadpleegd op 21 september 2012)

Privacy International (1995) *Big Brother Incorporated 1995*, Londen, Privacy International: te vinden op: <https://www.privacyinternational.org/reports/big-brother-incorporated-1995> (geraadpleegd op 13 juni 2012)

Raad van de Europese Unie (2010) *Interneveiligheidsstrategie voor de Europese Unie: Naar een Europees veiligheidsmodel*, Brussel, 23 februari 2010, 5842/2/10

Raad van de Europese Unie (2008a), Uitvoering van de EU-richtsnoeren inzake foltering en andere wrede, onmenselijke of ontterende behandeling of bestraffing - Stand van zaken en nieuwe uitvoeringsmaatregelen, *nota 8407/1/08 van het secretariaat-generaal van het Politiek en Veiligheidscomité*, Brussel, 18 april 2008

Raad van de Europese Unie (2008b) De identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuur als Europese kritieke infrastructuur en de beoordeling van de

noodzaak de bescherming van dergelijke infrastructuren te verbeteren, *Richtlijn 2008/114/EG van de Raad*, Brussel, 8 december 2008

Raad van de Europese Unie (2008c) *Gemeenschappelijk Standpunt 2008/944/GBVB van de Raad van 8 december 2008 tot vaststelling van gemeenschappelijke voorschriften voor de controle op de uitvoer van militaire goederen en technologie*, Brussel, 8 december 2008

Rees, Wyn en Richard Aldrich (2005) Contending Cultures of Counterterrorism: Transatlantic Divergence or Convergence?, *International Affairs*, 81(5): 905-23

Relya, Harold (2002) Homeland Security and Information, *Government Information Quarterly*, 19(2002): 213-23

Schmitt, Burkard et al, (2005), *Defence procurement in the European Union: The current debate*, Report of an EUISS Task Force, Parijs, mei 2005

Schumann, Harald (2011) Die Schnüffel-Industrie unterstützt autoritäre Staaten, *Der Tagesspiegel*, 29 oktober 2011

Slijper, Frank, (2005), *The Emerging EU Military-Industrial Complex: Arms industry Lobbying in Brussels*, TNI Briefing Series 2005/1, Amsterdam, The Transnational Institute

Stankiewicz, Rikard et al (2009), Knowledge Dynamics Scoping Paper, www.sandera.net

Steinmann, Thomas en Benjamin Dierks (2012) Deutschland will NATO für Panzerverkäufe einspannen, *Financial Times Deutschland*, 31 juli 2012

Taylor, Trevor (1997) Arms Procurement, in Howorth, Jolyon en Anand Menon (Eds.) *The European Union and National Defense Policy*, Londen, Routledge: pp.121-40

Thorleuchter, Dirk en Dirk van den Poel (2011) Semantic Technology Classification - A Defence and Security Case Study, *2011 International Conference Proceedings on Uncertainty Reasoning and Knowledge Engineering*: te vinden op:
<http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06007833>

Tigner, Brooks (2003a) EU moves to directly fund research, *Defense News*, 6 januari 2003

Tigner, Brooks (2003b) EU to shift research funds into defense: move mixes national, EU money for global security, *Defense News*, 5 mei 2003

Timm, Trevor en Jillian York (2012) Surveillance Inc: How Western Tech Firms Are Helping Arab Dictators, *The Atlantic*, 6 maart 2012,
<http://www.theatlantic.com/international/archive/2012/03/surveillance-inc-how-western-tech-firms-are-helping-arab-dictators/254008/>

Trybus, Martin (2000) On the application of the EC Treaty to Armaments, *European Law Review*. 25(6): 663-68

Ullman, Richard (1983) 'Redefining Security', *International Security*, 8(1): 129-153.

United Nations Development Programme (1993) *Human Development Report 1993: People's Participation*, te vinden op: <http://hdr.undp.org/en/reports/global/hdr1993/>

United States Commission on National Security in the 21st Century (2000) *Seeking a National Strategy: A Concept for Preserving Security and Promoting Freedom*: te vinden op <http://www.au.af.mil/au/awc/awcgate/nssg/>

Valentino-Devries, Jennifer et al. (2011) Document Trove Exposes Surveillance Methods, *Wall Street Journal*, 19 november 2011

Verslaggevers Zonder Grenzen (2012) *Beset by Online Surveillance and Content Filtering Netizens fight on*, Parijs, 29 maart 2012, te vinden op: <http://en.rsrf.org/beset-by-online-surveillance-and-13-03-2012,42061.html> (geraadpleegd op 5 augustus 2012)

Vranckx, An, Frank Slijper en Roy Isbister (2011) *Lessons from MENA: Appraising EU Transfers of Military and Security Equipment to the Middle East and North Africa: a Contribution to the Review of the Common Position*, Gent, Academia Press

Wagner, Ben (2012a) *Exporting Censorship and Surveillance Technology*, HIVOS-rapport januari 2012, Humanistisch Instituut voor Ontwikkelingsamenwerking (HIVOS), Den Haag, Geraadpleegd op 28 april 2012: <http://www.hivos.nl/eng/Hivos-Knowledge-Programme/Themes/Digital-Natives-with-a-Cause/Publications/Exporting-Censorship-and-Surveillance-Technology>

Wagner, Ben (2012b) *After the Arab Spring New Paths for Human Rights and the Internet in European Foreign Policy*, directoraat-generaal Extern Beleid van het Europees Parlement Briefing Paper EXPO/B/DROI/2011/28, juli 2012, Brussel

Wassenaar Agreement (2005) *Criteria for the Selection of Dual-use items*, Te vinden op http://www.wassenaar.org/controllists/2005/Criteria_as_updated_at_the_December_2005_PLM.pdf (geraadpleegd op 13 augustus 2012)

Wetter, Anna (2009) *Enforcing European Union Law on Exports of Dual-Use Goods*, SIPRI Onderzoeksrapport 24, Oxford, OUP

Wolfers, Arnold (1952) National Security as an Ambiguous Symbol, *Political Quarterly*, 67 (december): 481-502

Youngs, Richard, (2002) *The European Union and the Promotion of Democracy: Europe's Mediterranean and Asian Policies*, Oxford, OUP

COLOFON

Auteur:

Jocelyn Mawdsley

Projectbegeleiding Vlaams Vredesinstituut:

Sara Depauw

Uitgever:

Tomas Baum (Leuvenseweg 86, 1000 Brussel)

Brussel, 22 februari 2013

ISBN 9789078864561

Disclaimer

Hoewel door het Vlaams Vredesinstituut uiterste zorgvuldigheid werd betracht bij de redactie van dit rapport, kan het niet aansprakelijk worden geacht of gesteld voor mogelijke fouten of onvolledigheden. Tevens wordt geen enkele vorm van aansprakelijkheid aanvaard voor enig gebruik dat een lezer van dit rapport maakt.

Het Vlaams Vredesinstituut werd bij decreet opgericht door het Vlaams Parlement als onafhankelijk instituut voor vredesonderzoek. Het Vredesinstituut voert wetenschappelijk onderzoek uit, documenteert relevante informatiebronnen, en informeert en adviseert het Vlaams Parlement en het brede publiek inzake vredesvraagstukken.

Vlaams Vredesinstituut

Leuvenseweg 86

1000 Brussel

tel. +32 2 552 45 91

vredesinstituut@vlaamsparlement.be

www.vlaamsvredesinstituut.eu