

Per Eriksson, 08-473 30 01
Per.Eriksson@VINNOVA.se

Datum
2005-01-31
Projektnr

Diariernr
2004-00968
Ert diariernr
N2004/2869/ITFoU

Regeringskansliet
Näringsdepartementet
Jakobsgatan 26
103 33 STOCKHOLM


Redovisning av regeringsuppdrag avseende en nationell strategi för säkerhetsforskning

VINNOVA har haft ett regeringsuppdrag att tillsammans med Krisberedskapsmyndigheten, Försvarmakten, Försvarets materielverk och Totalförsvarets forskningsinstitut utarbeta ett gemensamt förslag till en nationell strategi för säkerhetsforskning. Till arbetet har även knutits Förvarshögskolan och Svenskt Näringsliv.

VINNOVA överlämnar härmed ett gemensamt förslag till en nationell strategi för säkerhetsforskning *Kunskap för säkerhets skull*.

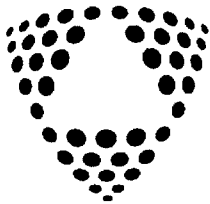
Samtliga medverkande myndigheterna har i särskilda skrivelser bekräftat att de ställer sig bakom förslaget. Även Förvarshögskolan och Svenskt Näringsliv ställer sig bakom förslaget. Se bilagor.

Beslut i detta ärende har fattats av undertecknad efter föredragning av avdelningschef Eva Lindencrona. Närvarande vid beslutet var även tf avdelningschef Gunnel Dreborg och handläggare Torbjörn Fångström.


Per Eriksson

Bilagor:

Nationell strategi för säkerhetsforskning *Kunskap för säkerhets skull* inkl bilagor.
Brev från Krisberedskapsmyndigheten
Brev från Försvarmakten
Brev från Försvarets materielverk
Brev från Totalförsvarets forskningsinstitut
Brev från Förvarshögskolan
Brev från Svenskt Näringsliv



**KRISBEREDSKAPS
MYNDIGHETEN**

Proj. nr.
VERKET FÖR INNOVATIONSSYSTEM
Ank. 2005 -01- 2 7
D/Dnr. 2004 - 00968

Sid 1(1)

0091/2005

2005-01-25

Stab

Generaldirektör Per Eriksson
VINNOVA
101 58 STOCKHOLM

Gemensamt förslag till en nationell strategi för säkerhetsforskning

VINNOVA har haft ett regeringsuppdrag att tillsammans med Krisberedskapsmyndigheten, Försvarsmakten, Försvarets materielverk, och Totalförsvarets forskningsinstitut utarbeta ett gemensamt förslag till en nationell strategi för säkerhetsforskning.

Krisberedskapsmyndigheten har deltagit i arbetet och stöder de förslag som redovisas i rapporten *Kunskap för säkerhets skull*, som kommer att överlämnas till regeringen under januari 2005.



Fredrik Hasael
stabschef

Box 599
101 31 Stockholm

Tel 08-593 710 00
Fax 08-593 710 01

kbm@krisberedskaps
myndigheten.se

www.krisberedskaps
myndigheten.se

Besöksadresser
Kungsgatan 53,
Stockholm

Hågesta, Sollefteå



Proj. nr.
VERKET FÖR INNOVATIONSSYSTEM
Ank. 2005 -01- 2 6
D/Dnr. 2004 - 00968

Sändlista

Ert tjänsteställe, handläggare

GD

Vårt tjänsteställe, handläggare

STRA UTVS, kk C Ramstedt

Ert datum

Vårt föregående datum

Er beteckning

Vår föregående beteckning

Gemensamt förslag till en nationell strategi för säkerhetsforskning

VINNOVA har haft ett regeringsuppdrag att tillsammans med Krisberedskapsmyndigheten, Försvarmakten, Försvarets materielverk och Totalförsvarets forskningsinstitut utarbeta ett gemensamt förslag till en nationell strategi för säkerhetsforskning.

Försvarmakten har deltagit i arbetet och står bakom strategin *Kunskap för säkerhets skull* så som den kommer att överlämnas till regeringen under januari 2005.

Claes-Göran Fant
Chef för Strategiledningen

Michael Moore

Sändlista

VINNOVA

Inom högkvarteret

PLANS PLAN
UTVS SK
KRI STAB
GRO PLAN
MUST Utv

(CR)

FMV

YTTRANDE

Datum
2005-01-26FMV beteckning
GD21000:10906/2005Utgåva nr
1

Sida 1(2)

Generaldirektör Per Eriksson
Vinnova
101 58 Stockholm

Proj. nr. VERKET FÖR INNOVATIONSSYSTEM
Ank. 2005 -01- 2 8
D/Dnr. 2004 - 00968

Er referens
GD Per Eriksson
FMV tjänsteställe, handläggare
VO FoT, Magnus Levin, 08-782 50 18Ert datum
2005-01-21
FMV föreg. datumEr beteckning
Kunskap för säkerhets
FMV föreg. beteckningYTTRANDE ÖVER STRATEGI FÖR SÄKERHETS ForskningSvar före
2005-01-31

VINNOVA har haft ett regeringsuppdrag att tillsammans med Krisberedskapsmyndigheten, Försvarsmakten, Försvarets materielverk och Totalförsvarets forskningsinstitut utarbeta ett gemensamt förslag till en nationell strategi för säkerhetsforskning.

Försvarets Materielverk har deltagit i arbetet och stödjer de förslag som redovisas i rapporten *Kunskap för säkerhets skull*, som kommer att överlämnas till regeringen under januari 2005.

FMV vill särskilt framhålla rapportens förslag i Förslagsområde 4. "Skapa innovationskraft för säkerhet", i vilket en gemensam funktion för upphandling av forskning och teknikutveckling för säkerhetsändamål efterlyses. FMV har lång erfarenhet av standardisering, kravdefinition, upphandling och utveckling av tekniska system som till sitt innehåll mycket liknar de system som skulle kunna bli resultatet av ett forsknings- och utvecklingsprogram inom säkerhetsområdet. Detta gör FMV till en effektiv aktör för att snabbt realisera rapportens förslag avseende område 4.

FMV vill i synnerhet också framhålla myndighetens status som anmält organ för certifiering av IT-säkerhetsprodukter eftersom sådana kan tänkas utgöra viktiga delar i tekniska lösningar för avvärijande av säkerhetshot.

FÖRSVARETS MATERIELVERK

Anette Wik
Tjfr GD

M:\FoT\Civil samverkan\Vinnova\Säkerhetsforskning-yttrande-050128.doc

Försvarets materielverkPostadress
115 88 StockholmBesöksadress
Banérgatan 62
(T-Kariaplan)Telefon
08 - 782 40 00Telefax
08 - 667 57 99Internet
www.fmv.se
e-mail: registrator@fmv.se

FMV



YTTRANDE

2005-01-26

GD21000:10906/2005

Utgåva nr 1

Sida 2(2)

Sändlista inom FMV

- VL
- OP VL Prod
- OP VL Komm
- OP VL Resurs
- Planeringssamordning
- TOPS
- VO StraMtrl
- VO Mark
- VO Flyg o Rymd
- VO Sjö
- VO Led
- VO FoT
- VO Log
- VO VoV
- HEL SystO
- HEL SystT
- HEL Marknad
- Arkiv

Proj. nr.
VERKET FÖR INNOVATIONSSYSTEM
Ank. 2005 -01- 2 5
D/Dnr. 2004-00968

Generaldirektör Per Eriksson
VINNOVA
101 58 STOCKHOLM

Er referens

Vår handläggare

Gemensamt förslag till en nationell strategi för säkerhetsforskning

VINNOVA har haft ett regeringsuppdrag att tillsammans med Krisberedskapsmyndigheten, Försvarsmakten, Försvarets materielverk och Totalförsvarets forskningsinstitut utarbeta ett gemensamt förslag till strategi för säkerhetsforskning.

Totalförsvarets forskningsinstitut har deltagit i arbetet och stöder de förslag som redovisas i Rapporten *Kunskap för säkerhets skull* som kommer att överlämnas till regeringen under januari 2005.

Totalförsvarets Forskningsinstitut



Madelene Sandström
Generaldirektör



Proj. nr. VERKET FÖR INNOVATIONSSYSTEM Ank. 2005 -01- 2 7 D/Dnr. 2004 -00968
--

Generaldirektör Per Eriksson
VINNOVA
101 58 Stockholm

Ert tjänsteställe, handläggare

Ert datum

Er beteckning

Vårt tjänsteställe, handläggare

MTI, professor Stefan Axberg, 08-788 9374

Vårt föregående datum

Vår föregående beteckning

Gemensamt förslag till en nationell strategi för säkerhetsforskning

VINNOVA har haft ett regeringsuppdrag att tillsammans med Krisberedskapsmyndigheten, Försvarmakten, Försvarets materielverk och Totalförsvarets forskningsinstitut utarbeta ett gemensamt förslag till en nationell strategi för säkerhetsforskning.

I arbetet med regeringsuppdraget har, förutom ovan nämnda myndigheter, även Försvarshögskolan och Svenskt Näringsliv ingått.

Försvarshögskolan stöder de förslag som redovisas i rapporten *Kunskap för säkerhets skull*, som kommer att överlämnas till regeringen under januari 2005.

Henrik Landerholm
Rektor och chef för Försvarshögskolan

()

Postadress	Besöksadress	Telefon	Telefax
Box 278 05 115 93 Stockholm	Valhallavägen 117 Sehlstedtgatan 9	08-788 75 00	08-788 94 27
Box 389 831 25 Östersund 651 80 Karlstad	Genvägen 35 Våxnäsgatan 10	063-55 70 00 054-10 40 20	063-55 86 85 054 10 40 21

Vinnova
GD Per Eriksson
101 58 Stockholm

, 2005-01-28

Kunskap för säkerhets skull – förslag till en nationell strategi för säkerhetsforskning

Svenskt Näringsliv och dess medlemsorganisationer är angelägna om att Sverige har kvalificerad forskning inom strategiska områden. Detta skapar förutsättningar för att trygga näringslivets konkurrenskraft och Sveriges välfärd. Målmedvetna satsningar på att utveckla kunskaper inom framtidsområden för svenskt näringsliv är också en investering med hög avkastning i ekonomisk tillväxt.

Säkerhet och forskning om säkerhet och riskhantering är områden som blir allt viktigare för både företag och medborgare. Det handlar om allt från att skydda intrång i företagets affärshemligheter till skydd för den personliga integriteten. Vi anser därför att det är av stor vikt att vi ökar vår forskningskompetens inom området och att detta görs vid universitet, högskolor och institut i nära samarbete med näringslivet. All erfarenhet visar att sådant samspel också är avgörande för att utveckla forskning av världsklass. Forskning som utförs i samverkan stimulerar utveckling av ny kunskap, metoder och verktyg för forskare och företagare.

Svenskt Näringsliv anser att den föreslagna strategin för säkerhetsforskning är ett viktigt område för både näringsliv och medborgare och vi vill redan på detta tidiga stadium uttrycka vårt principiella stöd till detta initiativ

Med vänlig hälsning

Ulla-Britt Fräjdin-Hellqvist
Avd.chef SME och kompetensförsörjning

Jan Persson
Avd.chef Juridik och säkerhet

Kunskap för säkerhets skull

Förslag till en nationell strategi för säkerhetsforskning

VINNOVA
Krisberedskapsmyndigheten
Försvarmakten
Försvarets materielverk
Totalförsvarets forskningsinstitut

Försvvarshögskolan
Svenskt Näringsliv

31 januari 2005

Innehåll

Sammanfattning.....	1
En angelägen satsning	1
Vision och strategi för nationell säkerhetsforskning	1
1. Tilldela ansvar för samordning av säkerhetsforskning.....	2
2. Inrätta nationellt FoU-program inför PASR/ESRP	2
3. Underlätta deltagandet i amerikanska säkerhetsforskningsprogram.....	3
4. Skapa innovationskraft för säkerhet	3
Fortsatt arbete i det korta perspektivet	4
Ett gemensamt förslag till en nationell strategi för säkerhetsforskning	5
Säkerhet och innovation.....	5
Uppdraget.....	5
Arbetsgruppens deltagare	6
Dialog med referensgrupp	6
Arbetsgruppens arbete	6
Att förstå säkerhet.....	8
Ett vidgat säkerhetsbegrepp.....	8
En nationell säkerhetsstrategi	9
Den europeiska unionens säkerhetsstrategi	10
Etik, integritet och respekt för mänskliga rättigheter	11
Innovationskraft för Sverige och Europa	12
Innovativa Sverige	12
Säkerhetsforskningsprogram.....	13
Behov av säkerhetsforskning.....	13
Den europeiska unionens säkerhetsforskningsprogram	13
Amerikanska säkerhetsforskningsprogram	15
Svensk säkerhetsindustri	18
Svensk säkerhetsindustri	18
Marknadspotential.....	20
Vision och mål för en nationell strategi	21
Arbete mot 2010	21
Vision för strategin.....	21
Mål för strategin	21
Strategins förslag.....	22
1. Tilldela ansvar för samordning av säkerhetsforskning.....	23
Styrning av säkerhetsforskning	23
1.1. Ansvar för samordning av säkerhetsforskning	23
1.2. Finansiering av strategin.....	25
2. Inrätta nationellt FoU-program inför PASR/ESRP	26
2.1. Nationellt program för säkerhetsforskning.....	26
3. Underlätta deltagandet i amerikanska säkerhetsforskningsprogram.....	29
Utveckla förmåga att skapa framgångsrika ansökningar.....	29
3.1. Förstärka säkerhetskompetens vid ambassaden i Washington D.C.	29
3.2. Deltagande i amerikanska säkerhetsforskningsprogram	30
4. Skapa innovationskraft för säkerhet	32
Utveckla svensk säkerhetsindustri.....	32
4.1. Utvecklande av beställarkompetens	32

4.2. Ansvar för gemensamma tekniska krav och standarder.....	32
4.3. Skapa starka forsknings- och innovationsmiljöer.....	33
4.4. Identifiera hinder för säkerhetslösningar	34
Fortsatt arbete i det korta perspektivet	35
Snabbt agerande.....	35
Fortsatt arbete för arbetsgruppen.....	35
Referenser	36
Europeiska unionen.....	36
Svenskt bakgrundsunderlag.....	36
Amerikanska säkerhetsforskningsprogram	37
Övrigt.....	37

Sammanfattning

En angelägen satsning

Händelser i vår omvärld, med naturkatastrofer och internationell terrorism, har satt frågan om det vidgade säkerhetsbegreppet i fokus. Kunskap genom forskning och utveckling är central för att kunna möta dessa hot. Vi behöver kunskap för säkerhets skull.

Arbetsgruppen anser att det är angeläget att så snart som möjligt skapa ny kunskap och ett effektivt innovationssystem för säkerhetsområdet för att positionera Sverige i de framväxande europeiska och amerikanska säkerhetsforskningsprogrammen. Därmed kan vår gemensamma säkerhet stärkas samtidigt som forskningen ger ett väsentligt bidrag till innovation, konkurrenskraft och tillväxt.

Tidpunkten är gynnsam eftersom både EU och USA för närvarande gör omfattande satsningar inom ett nytt område där svenska aktörer har möjlighet att söka anslag. En studie av vilka aktiviteter inom säkerhetsforskningsområdet som pågår i andra europeiska länder visar att Sverige ligger relativt sett långt framme i sitt förberedelsearbete.

Arbetsgruppen bedömer att förutsättningarna för att skapa ett starkt nationellt innovationssystem inom säkerhetsområdet är goda. Sverige har starka forskningsmiljöer inom dessa områden. Sverige har en stark tradition av komplexa systemlösningar, vilket dessutom underlättas av en väl utvecklad infrastruktur (e-tele-IT) för implementering av dessa systemlösningar. Flera av de svenska industriella

styrkeområdena ligger centralt inom säkerhetsområdet.

Det finns exempelvis värdefulla kompetenser i det svenska försvarssystemet som kan vara av betydelse för säkerhetsforskningen. Dessa kompetenser kan bidra till ett konkurrenskraftigt svenskt innovationssystem för säkerhetsområdet samtidigt som totalförsvaret ges möjlighet att dra nytta av civila säkerhetslösningar.

Vision och strategi för nationell säkerhetsforskning

Arbetsgruppen har väglett av följande antagna vision:

Vision för en nationell strategi

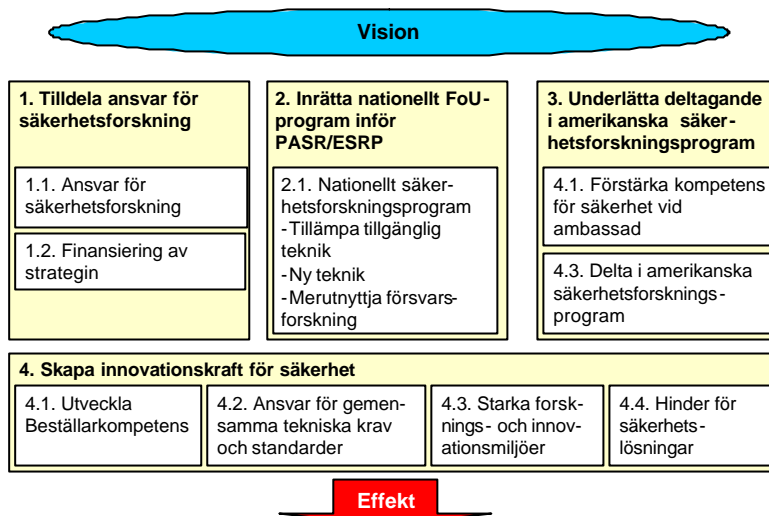
Fram till år 2010 ger svensk forskning och industri väsentliga bidrag till ökad säkerhet i Sverige och omvärlden och bidrar samtidigt till hållbar tillväxt. Svensk forskning och industri samverkar i internationella nätverk och är världsledande inom några områden.

För att realisera denna vision föreslår arbetsgruppen en strategi bestående av fyra huvudsakliga förslagsområden:

1. Tilldela ansvar för samordning av säkerhetsforskning;
2. Inrätta nationellt FoU-program inför PASR/ESRP;
3. Underlätta deltagandet i amerikanska säkerhetsforskningsprogram;
4. Skapa innovationskraft för säkerhet.

Därutöver föreslår arbetsgruppen åtgärder på kort sikt tills dess att de föreslagna åtgärderna har implementerats.

Strategins förslagsområden



1. Tilldela ansvar för samordning av säkerhetsforskning

Arbetsgruppen konstaterar att det inte finns någon samlande funktion för säkerhet och säkerhetsforskning i Sverige. Idag är ansvaret fördelat över flera politikområden och aktörer. Ett samlat grepp kring säkerhetsforskningen skulle stärka möjligheterna till att skapa både säkerhet och innovationskraft.

Den föreslagna strategin kommer att kräva resurser för att implementeras. Den föreslagna strategin som helhet kräver på sikt offentliga satsningar i storleksordningen 150-200 miljoner kronor årligen för att nå uppsatta mål.

Arbetsgruppen föreslår därför att

- Krisberedskapsmyndigheten ges ansvar för samordning av säkerhetsforskning.*
- Krisberedskapsmyndigheten ges de resurser som krävs för att finansiera ett nationellt säkerhetsforskningsprogram. Därutöver behövs särskild finansiering för övriga strategiförslag.*

2. Inrätta nationellt FoU-program inför PASR/ESRP

Den främsta utgångspunkten för strategin har varit ett framgångsrikt svenskt deltagande i säkerhetsforskningsprogram inom ramen för EU. För att åstadkomma detta föreslår arbetsgruppen ett nationellt säkerhetsforskningsprogram.

Arbetsgruppen konstaterar att nationella forskningsprogram visat sig ge goda förutsättningar för svenska aktörer att delta i sådana program. Arbetsgruppen redovisar möjliga inriktningar för ett sådant säkerhetsforskningsprogram.

Arbetsgruppen föreslår därför att

- ett nationellt säkerhetsforskningsprogram inrättas för en period av fyra år med start 2005. Arbetsgruppen föreslår att VINNOVA ansvarar för genomförande av detta forskningsprogram, i samråd med och finansierat av Krisberedskapsmyndigheten.*

3. Underlätta deltagandet i amerikanska säkerhetsforskningsprogram

Den största marknaden för säkerhetslösningar finns i USA. Där finns också ett program för säkerhetsforskning. Ett nationellt forskningsprogram kan ge förutsättningar för att delta i sådana. Det är dock svårt att etablera sig som en betydelsefull aktör på den amerikanska marknaden.

Särskilda instrument kan behöva inrättas för att underlätta för svenska aktörer, myndigheter, forskningsutförare och näringsliv.

Arbetsgruppen föreslår därför att

- en kompetens inom säkerhetsområdet knyts till den svenska ambassaden i Washington D.C. för att förstärka förutsättningarna för svenska myndigheter, universitet, högskolor, institut och företag att delta i amerikanska säkerhetsforskningsprogram.

- förutsättningarna för deltagande i amerikanska säkerhetsforskningsprogram och möjligheter att finna affärsmöjligheter förstärks genom att det tecknas ett Memorandum of Understanding mellan Sverige och USA för säkerhetsforskningssamverkan och att resurser avsätts för att genomföra denna samverkan.

4. Skapa innovationskraft för säkerhet

Det föreslagna nationella säkerhetsforskningsprogrammet är huvudsakligen inriktat för att ge förutsättningar för deltagande i europeiska och amerikanska säkerhetsforskningsprogram.

Därutöver kan programmet ge värdefulla bidrag till att utveckla innovation och tillväxt i samhället. Det krävs särskilda satsningar för att skapa innovationskraft för säkerhet för att den framväxande säkerhetssektorn inom näringsliv, forskningsväsende samt forskningsinstitut ska kunna ge maximal nytta.

Sådana satsningar bör involvera svenska aktörer på bredd, och speciellt de som företräder behovsperspektivet.

Arbetsgruppen föreslår därför att

- Krisberedskapsmyndigheten ges ansvar för att stödja utvecklingen av beställarkompetens avseende säkerhetslösningar för de myndigheter som enligt förordningen (2002:472) har ett särskilt ansvar för framtida krishantering.

- Krisberedskapsmyndigheten ges i uppdrag att, i samverkan med berörda myndigheter, ansvara för att

- stödja utvecklingen av gemensamma tekniska krav för säkerhetsområdet*
- identifiera, initiera och stödja utveckling av nödvändiga standarder*
- koordinera och stödja deltagande i internationellt standardiseringsarbete.*

- svenska intressenter gemensamt skapar starka forsknings- och innovationsmiljöer till stöd för innovation av säkerhetslösningar och successivt öppnar upp dessa för internationell samverkan.

- regeringen uppdrar till Krisberedskapsmyndigheten att utreda behov av nya sammanhållande samhällsfunktioner samt att ge rekommendationer på hur eventuella hinder för säkerhetslösningar kan åtgärdas eller elimineras.

Fortsatt arbete i det korta perspektivet

Det har ovan betonats vikten av att snabbt initiera de åtgärder som föreslås i strategin. Arbetsgruppen anser att deras arbete ska fortsätta under en övergångsperiod, till dess att nödvändiga åtgärder är vidtagna, så att det skapas kontinuitet.

Det finns ett antal åtgärder som på kort sikt skulle vara värdefulla för att förbereda implementeringen av förslagen.

Arbetsgruppen föreslår därför att

- den interimistiskt ska fortsätta sitt arbete med att utveckla för säkerhetsområdet prioriterade frågor intill slutet av 2005.

Ett gemensamt förslag till en nationell strategi för säkerhetsforskning

Säkerhet och innovation

Skydd av samhället är av största vikt för alla demokratier. Utmaningen är att skapa säkerhet för samhället och dess medborgare. Samtidigt måste risken för intrång i den personliga integriteten minimeras.

Terrorattackerna i New York/Washington D.C. 2001 och Madrid 2004 samt omfattande naturkatastrofer såsom tsunamin i Sydostasien 2004 har gjort detta alltmer påtagligt.

Synen på säkerhet har också vidgats sedan det kalla krigets slut. Säkerhet är mer än avsaknad av militära konflikter mellan nationer och är inte heller begränsad till det egna territoriet. Den breddade hotbilden och ökade sårbarheten medför ett ökat kunskapsbehov.

Mot bakgrund av detta har den europeiska kommissionen tagit initiativ till att driva säkerhetsforskning inom ramen för EU. Säkerhetsfrågor och säkerhetsforskning är även prioriterade i USA.

Förutom att generera teknologiska och operativa förmågor som hanterar de möjliga hoten utgör teknikutveckling även en egen drivkraft för säkerhetsforskningen. Teknikförsörjning, industriell innovationskraft, och konkurrenskraft är viktiga för att skapa tillväxt i samhället och att skapa industriella tillämpningar.

Uppdraget

Regeringen har därför givit i uppdrag till ett antal myndigheter, under ledning av VINNOVA, att utarbeta ett gemensamt förslag till en nationell strategi för säkerhetsforskning.¹

”VINNOVA skall inrätta en arbetsgrupp bestående av VINNOVA (ordförande), Krisberedskapsmyndigheten, Försvarmakten, Försvarets materielverk och Totalförsvarets forskningsinstitut (sekretariatfunktion) vars syfte är att utarbeta ett gemensamt förslag till en nationell strategi för säkerhetsforskning. Arbetsgruppen skall även samverka med andra berörda myndigheter, industrier samt universitet och högskolor, inklusive Förvarshögskolan. Arbetsgruppen skall löpande informera Regeringskansliet (Näringsdepartementet) om arbetet samt inkomma med en delrapport den 30 augusti 2004 och den 31 december 2004 inkomma med ett förslag till nationell strategi för säkerhetsforskning. Strategin skall ta sin utgångspunkt i innehållet i kommissionens meddelande KOM (2004) 72 final ”On the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security research, Towards a programme to advance European security through Research and Technology”, men i tillämpliga delar anpassas till svenska förhållanden.”

¹ Uppdraget givet via ändring i regleringsbrev till de i uppdraget ingående myndigheterna daterat den 15 april 2004.

Arbetsgruppens deltagare

De ingående myndigheterna och deras utpekade representanter har varit:

- Direktör Dr Eva Lindencrona, VINNOVA (ordf.)
- T.f. avdelningschef Gunnel Dreborg, VINNOVA
- Senior advisor Dr Peter Stern, Krisberedskapsmyndigheten
- Kommendörkapten Christer Ramstedt, Försvarsmakten
- Chief Scientist Dr Gunnar Hult, Försvarets materielverk²
- Avdelningschef Martin Rantzer, Totalförsvarets forskningsinstitut³

Professor Stefan Axberg, Försvarshögskolan, och direktör Svante Bergh, som representant från Svenskt Näringsliv, har båda adjungerats till arbetsgruppen.

Arbetsgruppen har haft ett sekretariat bestående av Forskare Stefan Törnqvist, Totalförsvarets forskningsinstitut, och Dr Torbjörn Fängström, VINNOVA.

Dialog med referensgrupp

Som stöd för arbetsgruppens arbete tillsatte regeringskansliet en referensgrupp bestående av representanter från näringsdepartementet, utbildningsdepartementet, försvarsdepartementet, justitiedepartementet och utrikesdepartementet.

Arbetsgruppen har kontinuerligt avrapporterat sitt arbete till referensgruppen.

² Gunnar Hult har vid enstaka tillfällen ersatts av Christer Olausson.

³ Martin Rantzer har vid enstaka tillfällen ersatts av laborator E Anders Eriksson.

Arbetsgruppens arbete

Arbetsgruppen har genomfört sexton ordinarie möten och därutöver genomfört ett antal aktiviteter och studier.

Aktiviteter och studierna har genomförts för att belysa nödvändiga aspekter av säkerhetsforskningsområdet, samt att ge information om de huvudsakliga aktörerna i ett svenskt innovationssystem⁴ för säkerhet, näringsliv, myndigheter och forskningsutförare.

Den 19 augusti genomförde arbetsgruppen en hearing med representanter från företag inom svenskt näringsliv med intresse för säkerhetsforskning.⁵

Arbetsgruppen överlämnade, i enlighet med uppdraget, en skriftlig delrapport till regeringskansliet den 31 augusti 2004.

För att få information om behovet från användare och ansvariga myndigheter kontaktade arbetsgruppen ordförandena i alla samverkansområden i det svenska krishanteringssystemet. Arbetsbelastningen hos de inblandade myndigheterna i ett pågående riskanalysarbete medförde dessvärre att de inte kunde återrapportera i tillräcklig omfattning så att någon komplett analys skulle vara möjlig. Arbetsgruppen konstaterar dock att det pågående riskanalysarbetet slutrapporteras under våren 2005 och kan i ett senare skede ligga till grund för en analys, även om arbetsgruppen för sitt arbete inte kunde utnyttja detta underlag.

⁴ ”Begreppet innovationssystem rymmer flera olika dimensioner och kan avse olika nivåer. Ett nationellt innovationssystem kan beskrivas i termer av samverkan mellan viktiga aktörer och komponenter, till exempel universitet, högskolor, institut, stora och små företag, riskkapital och regelverk. Staten spelar en viktig roll i nationella innovationssystem. Staten tillhandahåller i stor utsträckning regelverk, infrastruktur, sammanhållande organ samt utbildnings- och forskningsorganisationer”. Regeringskansliet (2004), sid 21

⁵ Dokumentationen återfinns i bilaga.

För att belysa intresset hos svenska forskningsutförare att genomföra säkerhetsforskning genomfördes genom VINNOVA en Expression of Interest (EoI) sänd till universitet, högskolor och forskningsinstitut. Det tycks finnas ett stort intresse från forskningsutförare att bedriva säkerhetsforskning, dock kan konstateras att svarsunderlaget inte är fullständigt, bl.a. saknas svar från flera universitet och vissa respondenter har lämnat efterfrågade gemensamma svar och i andra fall har institutioner vid universitet själva lämnat svar. Underlaget kommer därför att behöva kompletteras innan en fullständig analys kan genomföras.

Som en fallstudie genomfördes en funktionsanalys av det svenska innovationssystemet för sensorteknik av examensarbetare vid Chalmers tekniska högskola.⁶

Arbetsgruppen har också sökt att belysa den internationella dimensionen av säkerhetsforskningen. En studie genomfördes för att se hur andra och jämförbara länder inom den europeiska unionen förbereder sig inför europeiska kommissionens säkerhetsforskningsprogram.⁷

I oktober 2004 genomförde arbetsgruppen även en studieresa till USA för att bland annat besöka Department of Homeland Security.⁸

Arbetsgruppen slutrapporterade enligt uppdraget i januari 2005 efter medgivande av en månads förlängning.

⁶ Examensarbetarna var Eugenia Perez Vico och Gustav Oltander. Fallstudien finns sammanfattat i ett senare kapitel och den fulla studien återfinns i bilaga.

⁷ Studien genomfördes av Dr Mathias Kirsten från Fraunhofer Institut, under tiden för studien placerad vid VINNOVA. Studien återfinns i bilaga.

⁸ Det fulla programmet för resan återfinns i bilaga.

Att förstå säkerhet

Ett vidgat säkerhetsbegrepp

En strategi för säkerhetsforskning kan inte utvecklas utan en god förståelse av ett vidgat säkerhetsbegrepp. Avgränsningar mot andra säkerhetsområden krävs liksom en konceptuell förståelse av vad säkerhet innebär.

I uppdraget till arbetsgruppen anges att arbetet med den nationella strategin ska nära följa arbetet i EU:s förberedande åtgärd för ett kommande europeiskt säkerhetsforskningsprogram. Den europeiska kommissionen har för denna åtgärd avsiktligt valt att inte definiera eller skarpt avgränsa säkerhetsbegreppet varför arbetsgruppen heller inte gör någon sådan skarp definition.

Arbetsgruppen bedömer dessutom att en skarp avgränsning eller en definition av säkerhetsbegreppet i detta läge skulle kunna försvåra för kommande samspel mellan nationellt säkerhetsforskningsprogram och det kommande europeiska säkerhetsforskningsprogrammet.

Arbetsgruppen har därför valt att för strategins behov karakterisera säkerhetsbegreppet med utgångspunkt från två aspekter; med utgångspunkt från *hotets ursprung* och *graden av påverkan på samhällsfunktioner*.

Hotets ursprung

Den första aspekten är att hoten har sitt ursprung i ett medvetet mänskligt agerande hos en enskild individ eller en grupp av individer, d.v.s. utgör antagonistiska hot. Exempel kan vara terroristattacker, spridning av mjältbrandsbakterier, informationsmanipulering, organiserad brottslighet, m.m.

Icke-antagonistiska hot utgörs å andra sidan av slumpvis inträffade händelser, eller av icke avsiktliga handlingar. Exempel kan vara naturkatastrofer, smitta och omfattande tekniska störningar orsakade av oförutsebara brister eller fel.

Graden av påverkan på samhällsfunktioner

Säkerhet kan omfatta en stor bredd av olika typer av säkerhet, säkerhet för individen, för den enskildes närmiljö, för infrastruktur, samhället och vårt sätt att leva. Dessa utgör grundläggande värden (såsom skyddet av och respekten för mänskliga rättigheter) och funktioner i samhället som är hotade och som vi därmed vill skydda oberoende av vilka hot och risker mot säkerheten som finns.

Arbetsgruppen konstaterar att säkerhetsbegreppet därmed spänner över ett mycket brett område. Även om alla typer av hot är relevanta har arbetsgruppen valt att fokusera på de hot som innebär en signifikant påverkan på samhällsfunktioner.

Security och safety

Den säkerhetsforskning som utgör fokus för denna strategi syftar därmed till att i första hand hantera antagonistiska hot som innebär en signifikant påverkan på samhällsfunktioner. Detta motsvarar det engelska begreppet *security*.

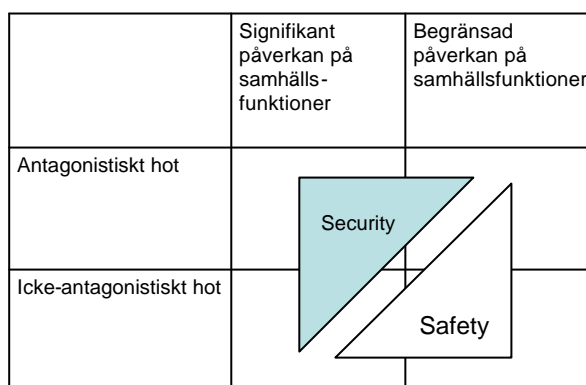
Icke-antagonistiska hot med begränsad påverkan på samhällsfunktioner utgör inte ett primärt fokus för denna säkerhetsforskningsstrategi. Med ett engelskt begrepp kan dessa betecknas som *safety*.

Även om strategins fokus kan sägas ligga på *security* snarare än *safety* är skiljelinjen mellan dessa båda begrepp inte skarp.

Arbetsgruppen bedömer att en stor del av de säkerhetslösningar som utarbetats för antagonistiska hot med signifikant påverkan på samhällsfunktioner kan vara relevanta även för andra hot eller ge upphov till kompletterande säkerhetslösningar för sådana hot. Inte minst gäller detta för

verksamhet vars syfte är att minimera verkan av ett realiserat hot. En förbättrad situationsmedvetenhet och kris hantering bidrar till att minska mänskligt lidande och materiell förödelse såväl efter ett terrorangrepp som efter stora naturkatastrofer.

Security och safety



Det kan även finnas växelverkan mellan olika typer av hot. Därför kan hot som är icke-antagonistiska eller som innebär en begränsad påverkan på samhällets funktioner ändå utgöra föremål för den forskning som den föreslagna strategin syftar till. Ett hot som på individnivå kan anses som safety kan för samhället vara ett security-problem. Ett exempel kan vara stenkastning mot pendeltåg. Förutom att man åsamkar potentiell skada på resenärer kan det få stora effekter på samhällets förmåga att fungera då ett viktigt transportnät inte kan lösa sin uppgift.

Avgränsningar

Arbetsgruppen har valt att bortse från särskilda typer av hot, såsom angrepp från nationalstater, samt i andra änden av hot-skalan vardagsnära hot och olyckshändelser.

En nationell säkerhetsstrategi

De hot som en nation utsätts för är ofta komplexa, okända, sammansatta och samvarierar ofta. De flesta hotsituationer som kan uppstå omfattas av särskilda regler. I Sverige är militär verksamhet definierad i successiva försvarsbeslut. På samma sätt har hanteringen av kriminalitet, olyckor och annat reglerats i styrning av polis, rättsväsende och kriminalvård, samt räddningstjänst.

Sedan 2002 finns i Sverige ett krishanteringssystem med ett antal ingående myndigheter med ansvar för fredstida krishantering. Krisberedskapsmyndigheten, KBM, samordnar arbetet med att utveckla krisberedskapen i det svenska samhället. Tillsammans med kommuner, landsting, myndigheter, näringsliv och organisationer minskar myndigheten samhällets sårbarhet och förbättrar förmågan att hantera kriser.

Det saknas emellertid en övergripande strategi för säkerhet. En sådan strategi skulle kunna syfta till att värna samhällets grundläggande värden såsom demokrati, mänskliga rättigheter, trygghet, frihet, tolerans, pluralism och rättssäkerhet.

Försvarsberedningen arbetar med en samlad strategi för att stärka samhällets förmåga inför framtida hot och risker. Försvarsberedningen lämnar sommaren 2005 sin syn på behovet inför den proposition som regeringen planerar att lägga i höst. En sådan strategi kan påverka vidareutvecklingen av den här föreslagna nationella strategin för säkerhetsforskning.

Den europeiska unionens säkerhetsstrategi

Den europeiska unionen har tagit intryck av det förändrade säkerhetsläget i omvärlden. En bärande tanke i unionens framväxande säkerhetsarbete är att säkerhet är en global utmaning för alla länder, som därmed också bäst hanteras på ett gemensamt sätt.

I december 2003 antog europeiska rådet en europeisk säkerhetsstrategi – ”Ett säkert Europa i en bättre värld”.⁹ Den är ett inriktningsdokument för EU:s arbete inom den gemensamma utrikes- och säkerhetspolitiken (GUSP), inklusive den europeiska säkerhets- och försvarspolitikerna (ESFP), samt även det framväxande krisberedskaps- och säkerhetssamarbetet.

Säkerhetsstrategin tar sin utgångspunkt i att Europa står inför en rad hot mot dess säkerhet. Ett ökat ömsesidigt beroende mellan staterna ökar dessutom sårbarheten.

Dessa hot är i de flesta fallen gemensamma. Man konstaterar att storskaliga invasioner knappast är troliga i ett kort-siktigt perspektiv, men att hoten istället består av ett eller flera samverkande hot i form av:

- Terrorism
- Spridning av massförstörelsevapen
- Regionala konflikter
- Sönderfallande stater
- Organiserad brottslighet

Den europeiska säkerhetsstrategin anger också några riktlinjer för hur dessa hot bäst kan hanteras. Grundtesen är att det är medlemsstaterna som bär det huvudsakliga ansvaret för sin egen säkerhet. Emellertid är konsekvensen av att utmaningarna är gemensamma också att de effektivast hanteras med gemensamma åtgärder där medlemsländernas individuella åtgärder koordineras och kanaliseras.

Tidigare har den första skyddslinjen varit vid Europas gränser, eller snarare vid de nationella gränserna. EU erkänner nu att den främsta försvarslinjen för att garantera Europas säkerhet nu lika gärna kan ligga utanför Europas gränser.

Unionens inre hot¹⁰

Den europeiska unionens inre krishanteringsarbete¹¹ täcker ett stort antal politikområden och sektorer, exempelvis transportsäkerhet, räddningstjänst, livsmedels-säkerhet, smittskydd, etc. Verksamheten har bedrivits fragmenterat utan någon högre grad av samordning.

⁹ Europeiska rådet (2003)

¹⁰ För en översikt över den europeiska unionens arbete med inre hot och krishantering, se Totalförsvarets forskningsinstitut (2004) och KBM (2004)

¹¹ Den europeiska unionens yttre säkerhets- och krishanteringsarbete sker genom ESFP.

Detta håller idag på att förändras. Exempel är den deklaration och det konkreta handlingsprogram som framtoqs efter terrorattentatet i Madrid 2004, ett CBRN-program¹² och ett solidaritetsprogram för terroristhot.

I förslaget till fördrag för den europeiska unionen finns också exempel på detta i solidaritetsklausulen om att bistå varandra med hjälp vid såväl antagonistiska som icke-antagonistiska hot.

Än så länge har samarbetet huvudsakligen gällt rättsligt och polisiärt samarbete (framförallt mot terrorism). Krishanteringsaspekter har tidigare inte varit så framträdande, vilket dock håller på att förändras.

Etik, integritet och respekt för mänskliga rättigheter

Säkerhet är en angelägenhet inom många olika samhällssektorer, och därmed spelar flera olika slags etiska aspekter in. Oftast brukar man anse att ansvaret för säkerheten i en viss verksamhet följer med ansvaret för verksamheten i stort. Det finns emellertid många säkerhetsfrågor som inte är kopplade på ett tydligt sätt till ett verksamhetsansvar. Det finns många frågeställningar kopplade till verksamhetens ansvar för säkerhet.

Exempel på sådana frågeställningar är avvägningar mot personlig integritet, t.ex. vid personkontroll och övervakning. Ett annat exempel är avvägningar mot rätts-säkerhet. Hur väger man rätts-säkerhet mot personsäkerhet i t.ex. ärenden om avvisning av misstänkta terrorister.

Detta innebär att etik, integritet och mänskliga rättigheter är en viktig del i såväl utveckling som tillämpning av säkerhetslösningar.

¹² CBRN står för Chemical, Biological, Radiological and Nuclear (kemiska, biologiska, radiologiska och nukleära).

Innovationskraft för Sverige och Europa

Innovativa Sverige

Den svenska regeringen har identifierat tillväxtfrågor som ett nyckelområde för sin mandatperiod. I sitt arbete med tillväxt och förnyelse presenterades under hösten 2004 en långsiktig strategi för konkurrenskraft, tillväxt och innovation i form av *Innovativa Sverige – En strategi för tillväxt genom förnyelse* (Ds 2004:36 Näringsdepartementet och Utbildningsdepartementet).

Innovativa Sverige anger en inriktning på de kommande årens arbete med att skapa ett starkt innovationsklimat i hela landet. Genom en rad åtgärder och genom mer samverkan mellan politikområden, forskning, näringsliv och offentlig sektor ska Sveriges innovativa förmåga stärkas. Ett gott innovationsklimat skapar förutsättningar för att kunskap och entreprenörskap ska leda till nya varor och tjänster, eller till nya sätt att producera.

Innovativa Sverige framhåller att den offentliga sektorn bör utvecklas som drivkraft för hållbar tillväxt och att den industriella och teknologiska potentialen inom försvarsområdet bör utnyttjas för civil tillämpning.

*"Det är en stor utmaning och möjlighet för Sverige att kreativt bygga vidare på den industriella och teknologiska potential som finns inom försvars- och säkerhetsområdet för civila tillämpningar. Det bör göras på ett sådant sätt att det stärker befintliga branscher och företag men också främjar framväxten av nya branscher och företag"*¹³

Det är med bl.a. detta som bakgrund som förslagen i denna strategi har utvecklats.

¹³ Regeringskansliet (2004)

Internationalisering

Sverige har ett internationellt gott rykte som kunskapsnation. Svenska företag och det svenska forskarsamhället har goda internationella nätverk. De är mycket aktiva i internationella forskningssamarbeten och är intressanta samarbetspartners i strategiska allianser för kunskapsuppbyggnad.

Inom EU:s ramprogram för FoU ligger Sverige i förhållande till folkmängd bland de främsta beträffande grader av deltagande liksom när det gäller återflödet av ekonomiska medel från ramprogrammet.

Samverkan mellan näringsliv och offentlig verksamhet

Innovativa Sverige identifierar den långsiktiga och strategiska samverkan mellan näringsliv och offentliga verksamheter som avgörande för framväxten av kunskapsbaserade verksamheter i Sverige.

Goda förutsättningar för kunskapsbaserad ekonomi

Regeringen menar i sin strategi att få länder har så goda förutsättningar som Sverige att komma till sin rätt i sin kunskapsbaserade ekonomi och dra nytta av internationaliseringen.

Sverige har i en internationell jämförelse hög kompetens och konkurrenskraft inom många näringsgrenar. Sverige har, enligt OECD, den högsta andelen av arbetskraften i kunskapsintensiva arbeten.¹⁴

¹⁴ Regeringskansliet (2004), sid 4

Säkerhetsforskningsprogram

Behov av säkerhetsforskning

I dagens samhälle råder osäkerhet om vilka hot eller risker som kan komma att behöva hanteras, när det kan behöva göras och vad som är effektivaste motmedel. Osäkerheten innefattar även konsekvenserna av de hot och risker som kan drabba samhället.

De hot som står framför oss innebär att det finns ett stort, och inom vissa områden växande, kunskapsbehov avseende både hoten och möjligheter att kunna hantera och möta dem. Forskning kan hjälpa oss att fylla detta kunskapsbehov och stödja utvecklingen av säkerhetslösningar.

Förslaget till en nationell strategi har utgått från säkerhetsforskningsprogram inom den europeiska unionen och i USA.

Den europeiska unionens säkerhetsforskningsprogram

Den europeiska unionens säkerhetsforskningsprogram har sin bakgrund i gemensamma säkerhetshot samt behovet att stärka den europeiska industriella och teknologiska förmågan.

*"...To achieve these objectives, Europe must take advantage of its technological strengths. This requires state-of-the-art industries, a strong knowledge infrastructure, appropriate funding and an optimal use of resources."*¹⁵

Forskning och teknikutveckling anges som ett nyckelområde och framgångsfaktor när det gäller att garantera Europas säkerhet. Forskningen för säkerhetsändamål uppges dock ha ett antal brister. För det första uppges militär och civil forskning i alltför hög grad vara skilda från varandra, både på

nationell och europeisk nivå. För det andra anses att ett europeiskt ramverk för säkerhetsforskning saknas vilket är en konsekvens av att det internationella samarbetet inom säkerhetsområdet överhuvudtaget är svagt utvecklat. Avsaknaden av en koordinering mellan nationella och europeiska ansträngningar förvärras av de begränsade investeringarna i forskning inom området.¹⁶

Inom ramen för den europeiska unionen har den europeiska kommissionen lanserat idén om ett säkerhetsforskningsprogram från 2007 med början i en förberedande åtgärd för åren 2004-2006.

European Security Research Program (ESRP)

Det europeiska säkerhetsforskningsprogrammet (European Security Research Programme, ESRP) föreslås av kommissionen att påbörjas 2007.

Som stöd för utvecklande av ett säkerhetsprogram har kommissionen haft en särskild referensgrupp till hjälp, den s.k. Group of Personalities. Referensgruppen presenterade under våren 2004 sin slutrapport med förslag på inriktning för ett europeiskt säkerhetsprogram samt på kort sikt även med den förberedande åtgärden.¹⁷

Den europeiska referensgruppen påtalar tydligt behovet av att ha en förmågebaserad inriktning av säkerhetsforskningen. Forskningen ska direkt svara mot operativa behov, i närtid eller längre fram i tiden. Referensgruppen poängterar att det är svårt

¹⁵ Europeiska kommissionen (2004). Research for a Secure Europe

¹⁶ Europeiska kommissionen (2004). Research for a Secure Europe, sid 14

¹⁷ Gruppen stöddes av en annan grupp av s.k. sherpas som gjorde större delen av det konkreta arbetet. Europeiska kommissionen (2004) Research for a secure Europe

att förutse hotutvecklingen och därmed vilka behov man kan komma att få, samt att området, till skillnad från det militära, inte bara har en användare i sina respektive nationella system utan en lång rad olika aktörer.

Principer för EU:s säkerhetsforskningssamarbete:¹⁸

- Deltagande av alla medlemsstater
- Effektiv samordning mellan nationella och europeiska ansträngningar
- Systematisk analys av säkerhetsrelaterade förmågebehov
- Tillräcklig finansiering
- Maximal exploatering av potentiella synergier mellan försvars- säkerhets och civila system
- Tillse att särskilda juridiska villkor och finansieringsinstrument finns för säkerhetsområdet
- Skapa institutionella instrument som är effektiva och flexibla nog för att kombinera medlemsstaternas ansträngningar och Gemenskapens, samt att involvera andra parter med ömsesidig nytta

Till detta kommer att medan det på det militära området finns en begynnande process för att identifiera och hantera gemensamma förmågebrister så saknas detta på säkerhetsområdet.¹⁹ Erfarenheterna från försvarsområdet ska tas tillvara och öka synergieffekterna mellan försvarsforskning och säkerhetsforskning.

ESRP är föreslaget som en del av det sjunde ramprogrammet. Man vill att ESRP ska ha en egen budget, egna regler om deltagande med mera. Ett slutligt ställningstagande rörande ESRP beräknas vara klart våren 2005. Budgeten har föreslagit uppgå till över 1 miljard euro årligen.

Förberedande åtgärd för säkerhetsforskning (PASR)

Som en inledande verksamhet för det kommande säkerhetsforskningsprogrammet har den europeiska kommissionen reserverat budgetmedel genom ett budgettekniskt instrument för att lansera kommande policyinitiativ, en s.k. förberedande åtgärd (Preparatory Action on the enhancement of the European industrial potential in the field of Security research, PASR).

Den förberedande åtgärden för säkerhetsforskning beslutades av kommissionen under 2004²⁰ baserat på ett meddelande om förbättrande av den europeiska industrins potential för säkerhetsforskning²¹.

Det förberedande säkerhetsprogrammet är treårigt från 2004 till 2006. Det omfattar forskningsverksamheter som ska stödja den europeiska säkerhetsförmågan samt i övrigt ge inriktning för det tilltänkta fullskaliga säkerhetsforskningsprogrammet. Under programmets tre år beräknas omfattningen uppgå till 65 miljoner euro.

Prioriterade områden inom PASR

- Förbättrad lägesuppfattning
- Optimerad säkerhet och skydd av nätverksbaserade system
- Skydd mot terrorism (inklusive bioterrorism och insatser med biologiska, kemiska eller andra ämnen)
- Förbättra krishanteringsförmåga
- Interoperabilitet och integrerade system för information och kommunikation

Den första utlysningen genomfördes under 2004 och omfattade 15 miljoner euro. Sverige har varit framgångsrikt i ansökningarna.

¹⁸ Europeiska kommissionen (2004). Research for a Secure Europe, sid 14

¹⁹ Europeiska kommissionen (2004). Research for a Secure Europe, sid 16-17

²⁰ Kommissionens beslut (2004/213/EC) .

²¹ Kommissionens meddelade KOM (2004) 72 slutlig.

Svenska aktörer bör fortsätta att bygga vidare på den erfarenheten som en handfull aktörer nu har. En erfarenhet har varit att industrins medverkan behöver förstärkas.

Kommissionen har inför kommande utlysningar annonserat följande:

- Utannonseringen under 2005 ska börja tidigare under året
- Förmågeperspektivet ska behållas
- Uppmuntra medverkan från slutanvändare
- De prioriterade områdena för PASR 2004 behålls
- Uppmuntra förslag på områdena human factors, etiska och sociala värden
- Undvik duplicering
- Betona synergieffekter med pågående arbeten inom FP6²², PASR eller andra program
- Fokus på säkerhetslösningar och inte på tekniska lösningar

En andra utlysning av PASR öppnar i början av 2005.

Andra säkerhetsforskningsrelevanta inom EU

Inom den europeiska unionen finns andra verksamheter av relevans för säkerhetsområdet, även om säkerhetsforskningsprogrammet med all säkerhet kommer att bli det mest väsentliga framöver.

Exempelvis bedriver kommissionens direktorat för energi och transport programmet ”Security in Energy and Transport” där både användare och experter/forskare bidrar. Inom generaldirektoratet för informations samhället bedrivs även verksamhet för tillit och säkerhet i informations och kommunikationsteknologi (ICT for Trust and Security).

²² EU:s sjätte ramforskningsprogram

Amerikanska säkerhetsforskningsprogram

De samlade amerikanska satsningarna på säkerhetsforskning omfattar för budgetåret 2005 ca 4 miljarder USD, huvudsakligen inom Department of Health and Human Services och Department of Homeland Security.

Andra finansiärer är National Science Foundation (NSF) liksom jordbruks- och försvarsdepartementet med egna säkerhetsforskningsprogram.²³

Department of Health and Human Services

Inom Department of Health and Human Services (HHS) bedrivs forskning till skydd för människors hälsa. Den delen som är till gagn för säkerhetsforskningen utgör den största enskilda anslagsposten för säkerhetsforskning i USA, 1,7 miljarder USD för 2005. Det enskilt största anslagsposten går till NIAID. Man använder inom HHS inga nya mekanismer för säkerhetsforskning utan använder etablerade finansieringsmekanismer.

Verksamheten inom HHS bedrivs huvudsakligen inom Centers for Disease Control and Prevention (CDC) samt National Institutes of Health (NIH).

CDC är ansvarig för mer användarnära kunskap såsom övervakning och detektion av smittsamma substanser samt medicinsk och biologisk kunskap vid beredskapsplanering och operativa insatser.

²³ Information från American Association for the Advancement of Science (AAAS), se www.aaas.org/spp/rd

Verksamheten inom NIH är mer forskningsnära, och frågor som är relevanta för säkerhetsområdet är:²⁴

- Förhindra spridning av smittsamma sjukdomar
- Förhindra att nödvändig medicinsk kunskap inte utnyttjas för illegitima syften (biosecurity)

Ett av de största programmen inom HHS är *Project BioShield* med syfte att tillgodose behovet av medicin och vaccin vid en eventuell attack med massförstörelsevapen med biologiska och/eller kemiska substanser framförallt mjältbrand och smittkoppor.²⁵

NIH ger också anslag till universitet och högskolor och forskningsinstitut, även internationella sådana, samt finansierar stipendier och forskarutbyten.

Department of Homeland Security

Det amerikanska säkerhetsdepartementet (Department of Homeland Security, DHS) bedriver egna forsknings- och tekniksatsningar med uppgift att ta fram framtida säkerhetslösningar.

DHS Science & Technology Mission

Conduct, stimulate, and enable research, test, evaluation and timely transition of homeland security capabilities to federal, state and local operational end-users.

Ett vetenskaps- och teknologidirektorat leder DHS verksamhet inom detta område i enlighet med följande uppgifter:

- Tillsammans med användarna identifiera behov;
- Underlätta innovation för säkerhet;
- Säkerställa en nationell bas för forsknings- och teknikkunnande för

säkerhetslösningar, bl.a. i universitet och högskolor;

- Göra egna studier och analyser;
- Koordinera med andra departement och myndigheter;
- Etablera internationella samarbeten;
- Initiera "rapid prototyping".
- Etablera standarder som motsvarar säkerhetsbehoven

Forskningsamarbete betonas av DHS, framförallt i fyra dimensioner: privat sektor, universitet och forskningsinstitut, lokal nivå och delstater, samt andra myndigheter och internationellt samarbete.

Säkerhetsdepartementets forskningsprogram är i detta skede tydligt inriktat på att snabbt leverera lösningar.

Department of Homeland Security har för 2005 en budget på 1,24 miljarder USD för forskningsändamål - en ökning på nästan 20 procent från 2004.²⁶ En stor del av DHS forskningsprogram är riktat mot skydd mot massförstörelsevapen och smittspridning.

En del av DHS finansiering av säkerhetsforskning sker genom Homeland Security Advanced Research Projects Agency (HSARPA), vilken modellerat sitt namn på sin militära motsvarighet²⁷, men detta till trots delvis agerar annorlunda. HSARPA:s budget är ca 350 miljoner USD.

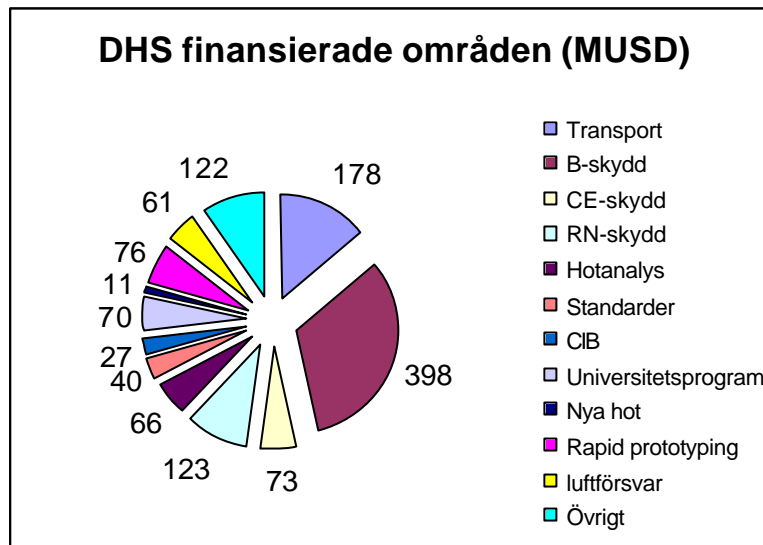
Finansieringen stödjer olika typer av verksamhet. DHS finansierar federala och nationella laboratorier. Därefter finansieras universitetsprogram via stipendier och kompetenscentra (Centers of excellence).

²⁴ Verksamheten inom NIH bedrivs huvudsakligen inom National Institute of Allergy and Infectious Diseases (NIAID).

²⁵ Se National Academy of Sciences, National Research Council (2003).

²⁶ Information från American Association for the Advancement of Science (AAAS), se www.aaas.org/spp/rd

²⁷ Defence Advanced Research Projects Agency (DARPA)



Amerikanska federala forskningsprogram ska enligt lag innehålla särskild finansiering till små och medelstora företag till förmån för innovation, s.k. Small Business Innovations Research, SBIR. Detta ska motsvara 2,5 % av den totala finansieringen. Även DHS bedriver ett sådant program.²⁸

Den största delen av forsknings- och utvecklingsmedlen vid DHS inriktas mot utveckling (66 %). En mindre del riktas mot forskning (grundforskning 5 % och tillämpad forskning 13 %). Detta innebär att man än så länge är fokuserad på tidiga resultat och att leverera lösningar.

²⁸ Mer information finns på www.hsarpasbir.com.

Svensk säkerhetsindustri

Svensk säkerhetsindustri

Den internationella hotbilden har ökat samhällets behov av skydd. Det har medfört att en civil säkerhetsmarknad börjar växa fram.

En analys av svensk säkerhetsindustri har genomförts inom ramen för uppdraget till myndigheterna. Denna analys har gjorts som ett examensarbete vid Chalmers tekniska högskola och refereras i detta avsnitt.²⁹ Syftet med studien var att beskriva industristrukturen och dess dynamik, identifiera potentiell marknadstillväxt och identifiera hinder för industriell tillväxt inom en sektor med hög tillväxtpotential.

Säkerhetsindustrin definieras i analysen som den industri som har förmågan att tillhandahålla teknologi, produkter och tjänster för att motverka antagonistiska hot och skydda samhället och dess medborgare mot antagonistiska handlingar (exklusive oorganiserad brottslighet och krigshandlingar).

Svensk säkerhetsindustrisektorer

- Komplexa system och simulering
- IT-säkerhet
- Sensorteknologi
- Mobila lösningar
- Fysiska transporter
- NBC-teknologi
- Vapentechnologi

Säkerhetsindustrin har indelats i sektorer inom vilka finns såväl militära som civila kunder.

Komplexa system och simulering

Företagen i denna sektor producerar produkter och tjänster inom de tre applikationsområdena integrerad övervakning, kontrollsystem och simuleringssystem vilka underlättar samordning och beslutsfattande för skydd av samhället och dess medborgare.

Totalt finns det 19 företag inom sektorn med tillsammans knappt 7000 anställda. SAAB Aerotech Telub är det största företaget. SAAB Bofors Dynamics är ett annat stort företag. Det svenska försvaret är idag den viktigaste kunden till de större företagen men även utländska försvarsmakter är viktiga kunder.

Trenden att företagen söker civila applikationer är tydlig, enligt den genomförda studien, speciellt när det gäller nätverksbaserade lösningar. De mindre företagen, som t.ex. HiQ AB, C-ITS och CC Systems AB, arbetar mot civila svenska och utländska myndigheter.

IT-säkerhet

I denna sektor produceras produkter och tjänster som skyddar datoriserad information, system och tjänster. De tre största applikationsområdena är skydd mot virus, spam och mikroågsvapen, skydd mot intrång samt metoder för riskanalyser och säkerhetsstrategier.

Sektorn innefattar omkring 200 företag och majoriteten av dem är små. Endast 24 av företagen har fler än 20 anställda och tillsammans har dessa företag knappt 2000 anställda. De största är Proact Datasystem

²⁹ Studien är genomförd av Gustav Oltander och Eugenia Perez Vico vid Chalmers Tekniska Högskola. Den fullständiga studien finns i bilaga. Liknande undersökningar har gjorts i andra länder, se bl.a. en kanadensisk studie "Canadian Advanced Security Industry" på www.cata.ca där det också finns en databas.

och Technology Nexus. Merparten av företagen arbetar mot den civila marknaden där större företag har behov av sofistikerade säkerhetslösningar medan konsumentmarknadens behov rör säkerhetsprodukter. Myndigheter är en kundkategori med behov av samma karaktär som de större företagen.

Sensorteknologi

Sensorteknologiföretag producerar produkter och tjänster som upptäcker hot av skilda slag. Det är produkter med komponenter för upptäckt och komponenter för signalbearbetning som kvantifierar upptäckten. Teknologin har många applikationer:

- Identifiering (biometri d.v.s. avsökning av fingeravtryck, iris och ansikte) vid gränskontroll och för skydd av fysisk infrastruktur
- Screening (t.ex. metalldetektorer och röntgen) för upptäckt av vapen och farliga substanser
- Övervakning (t.ex. radar och IR) av t.ex. fysiska objekt
- Spårning (t.ex. GPS) av t.ex. gods.

Sektorn utgörs av 21 företag med totalt runt 2000 anställda och det största företaget är Ericsson Microwave Systems AB. Saab Bofors Dynamics och Biacore är andra större företag. Merparten av företagen är emellertid små som exempelvis Exensor Technology AB, Precise Biometrics och Applied Sensor. Ericsson Microwave Systems AB och SAAB Bofors Dynamics producerar huvudsakligen för den militära marknaden men söker efter civila applikationer för sina teknologier. Civila kunder som flygplatser och hamnar har ett starkt behov av förbättrade screeningtekniker. Andra civila kunder är myndigheter som kustbevakningen och tullen samt andra företag.

Mobila lösningar

Företagen i denna sektor producerar produkter och tjänster som förbättrar samhällets förmåga att handskas med antagonistiska handlingar. Applikationer återfinns inom telematik, mobila kommunikationsstationer och mjukvara för mobila lösningar. Telematiken används av fordonsindustrin i SOS Alarm, automatisk SOS-meddelande vid kollision, direktkontakt med bärgare, spårning av kapade/stulna fordon och övervakning av fordon med farlig last.

Inom sektorn finns 56 företag och antalet anställda uppgår till omkring 2400. Det finns sex större företag, varav Ericsson är det största. Kunderna är både militära och civila. De mindre företagen i sektor arbetar huvudsakligen mot den civila marknaden. När det gäller telematikprodukter så är fordonsindustrin den största kunden men även transportföretag är kunder, enligt analysen.

Fysiska transporter

Företagen i sektorn producerar produkter och tjänster för övervakning och transport av utrustning med applikationer inom flyg, fartyg och fordon.

Företagen uppgår till sju stycken med tillsammans drygt 6600 anställda. Saab Aerosystems, som verkar inom flygområdet, är det största företaget. Kockums applikationer rör det marina området och BAe Land Systems Hägglunds producerar fordon. De viktigaste kunderna är svenska och utländska militära myndigheter. Den kundkategori som ökar i betydelse, men som är liten idag, är civila myndigheter både i Sverige och utomlands, som t.ex. polis och kustbevakning.

NBC-teknologi

I denna sektor producerar företagen produkter och tjänster för skydd av samhället och dess medborgare mot nukleära, biologiska, kemiska³⁰ massförstörelsevapen. Applikationerna avser motmedel som t.ex. vaccin och motgift.

Studien visar att det finns fyra företag som täcker hela sektorn. De är alla små med som mest 20 anställda. Totalt finns drygt 40 anställda i sektorn. Idag är deras kunder enbart militära och civila myndigheter såsom Socialstyrelsen, polisen, landstingen och Räddningsverket. Deras efterfrågan är dock liten då de bedömer NBC-hotet som litet. Däremot bedöms den amerikanska marknaden som stor och växande.

Vapentechnologi

Företag i sektorn med säkerhetsrelevans producerar produkter och tjänster som motverkar väpnade attacker.

Enligt studien består sektorn av sju företag med drygt 2000 anställda och Saab Bofors Dynamics och Bofors Defence är de största och de är fokuserade på militära applikationer men söker efter civila applikationer för sin teknologi. Företag som enbart producerar för den civila marknaden är få och små t.ex. Dynasafe, Carl Bro AB och Aimpoint. Efter terrorattentaten i USA 2001 har den globala efterfrågan från luftfartsmyndigheter världen över ökat på säkerhetsprodukter som produceras av sektorn. Potentiella svenska civila kunder är polisen och transportföretag och generellt expanderar den civila marknaden.

Marknadspotential

Analysen av tillväxtpotentialen på sektorernas marknader visar att den kan betraktas som stark i alla sektorer. Starkast potential återfinns inom sektorerna sensor-teknologi, komplexa system och IT-säkerhet. Analysen visar även att den svenska civila säkerhetsmarknaden är liten för alla sektorer men att en tillväxtpotential finns. Civila marknader för den svenska säkerhetsindustrin återfinns framför allt i USA.

Den bedömning som görs i ovan refererat examensarbete överensstämmer med resultatet från den hearing som genomfördes med representanter från svenskt näringsliv.

Ett område som inte omfattas av examensarbetet är flyg och rymd. För beskrivning av dessa områden hänvisas till Näringsdepartementets arbete med en flyg- och rymdstrategi.³¹

³⁰ Nuclear, Biological and Chemical (NBC)

³¹ Regeringskansliet (2005)

Vision och mål för en nationell strategi

Arbete mot 2010

Arbetsgruppen har valt att sätta 2010 som tidpunkt för vision och mål för strategin. De åtgärder som föreslås leder mot målet, men kan behöva revideras om ett antal år, exempelvis efter utgången av det i strategin föreslagna säkerhetsforskningsprogrammet.

Det finns en rad skäl till varför strategin bör utvärderas efter en tid. Inledningsvis kommer åtgärderna att stärka svenska aktörers förmåga att skapa säkerhetslösningar att fokusera kring att nyttja befintlig teknik men i nya innovativa systemkopplingar. Viktigt är att som exempel nyttja synergier mellan militär och civil teknik och forskning.

De första åren handlar därför främst om tillämpad forskning och att fokus efter ett par år allt mer glider över mot teknisk och metodinriktad, något mera långsiktig verksamhet.

Den föreslagna strategin gäller dessutom under kända förutsättningar. Arbetsgruppen bedömer redan nu att regeringens kommande proposition om krishantering och civil beredskap 2005, en framväxande nationell säkerhetsstrategi, och andra processer under de närmaste åren ändrar förutsättningarna för innovation och säkerhetslösningar och därmed också för denna strategi.

Arbetsgruppen har också särskilt uppmärksammat behovet av kunskapsutveckling inom etik, integritet och mänskliga rättigheter för säkerhetsforskning.

Vision för strategin

Arbetet med att ta fram en nationell strategi för svensk säkerhetsforskning har väglett av följande antagna mål och vision.

Vision för en nationell strategi

Fram till år 2010 ger svensk forskning och industri väsentliga bidrag till ökad säkerhet i Sverige och omvärlden och bidrar samtidigt till hållbar tillväxt. Svensk forskning och industri samverkar i internationella nätverk och är världsledande inom några områden.

Mål för strategin

Visionen har resulterat i följande mål för svensk säkerhetsforskning inför år 2010:

Mål för en nationell strategi

1. Svenska företag, institut och universitet och högskolor har tagit en ledande position inom strategiskt viktiga områden inom ramen för EU:s säkerhetsforskningsprogram;
2. Tidigare och nya investeringar inom såväl civil som militär FoU har utnyttjats på ett effektivt sätt inom säkerhetsområdet;
3. Svenska produkter och tjänster ingår ofta i större internationella säkerhetslösningar;
4. Svenska företag utvecklar innovativa produkter och tjänster inom säkerhetsområdet;
5. Svenska företag gör konkurrerar framgångsrikt i USA bl a genom att svenska företag, institut och universitet och högskolor deltar i amerikanska säkerhetsforskningsprogram inom strategiskt viktiga områden.

Strategins förslag

Resultatet från visionen och målen har arbetsgruppen antagit ett gemensamt förslag till en nationell strategi för säkerhetsforskning.

Strategin omfattar fyra huvudsakliga förslagsområden:

1. Tilldela ansvar för samordning av säkerhetsforskning
2. Inrätta nationellt FoU-program inför PASR/ESRP
3. Underlätta deltagandet i amerikanska säkerhetsforskningsprogram
4. Skapa innovationskraft för säkerhet

Därutöver presenteras ett förslag på åtgärder på kort sikt. Förslagen presenteras nedan.

1. Tilldela ansvar för samordning av säkerhetsforskning

Styrning av säkerhetsforskning

Säkerhetsforskning har två huvudsakliga syften, att bidra till medborgarnas säkerhet, samt att stärka innovation, konkurrens kraft och tillväxt. I Sverige ansvarar på politisk nivå näringsdepartementet (och till politikområdenas hörande myndigheter) för det senare. Det krävs emellertid samordning mellan ett antal politikområden som listas i *Innovativa Sverige*.³² Säkerhetsbegreppet sträcker sig över ett antal politikområden samt över departements- och myndighetsgränser. För att skapa säkerhet saknas idag en samlande funktion.

Det är arbetsgruppens bedömning att säkerhetsforskningsarbetet väsentligen skulle stärkas om strategin både kunde vägledas av ett mer utvecklat och sammanhållet säkerhetstänkande inom riksdag, regering och myndigheter (exempelvis genom en säkerhetsstrategi) och av att det fanns en tydlig mottagare för säkerhetsforskningsstrategin.

På ett övergripande plan behöver Sverige skapa förståelse för hela säkerhetsområdet, inte bara för säkerhetsforskning. I detta ingår synen på säkerhet, ett vidgat säkerhetsbegrepp, och hur säkerhet avgränsas mot andra områden.

1.1. Ansvar för samordning av säkerhetsforskning

Arbetsgruppen föreslår att Krisberedskapsmyndigheten ges ansvar för samordning av säkerhetsforskning.

Varje myndighet med behov av kunskap för sitt säkerhetsarbete måste tillgodose detta behov. Dock saknas idag en samlad

bild av säkerhetsforskningen. De operativa behoven är i dag fördelade på ett stort antal statliga myndigheter (inkluderande regeringen) samt över ett flertal departement och politikområden. Därutöver hanterar kommuner och länsstyrelser sina egna behov.

En samlande funktion skulle därför behövas. Arbetsgruppen bedömer att Krisberedskapsmyndigheten vore bäst lämpad att hantera denna funktion. KBM ansvarar idag för samordning och inriktning av krisberedskapsåtgärder. Det är därför naturligt att KBM tar ett motsvarande ansvar även för säkerhetsforskning. I detta samordnande ansvar bör ej ingå att utföra någon egen säkerhetsforskning. Sådan bedrivs även fortsättningsvis av universitet och högskolor, samt forskningsinstitut, m.fl.

I ett ansvar för samordning av säkerhetsforskning ingår huvudsakligen att:

- Analysera samhällets behov av säkerhetsforskning
- Skapa samsyn bland aktörerna
- Initiera och inrikta forskning
- Förmedla resultat
- Utvärdera genomförd forskning

För det första innebär det att skapa överblick över hela säkerhetsforskningsystemet och att analysera och värdera samhällets behov av säkerhetslösningar och utifrån dessa identifiera forskningsbehov.

För säkerhetsområdet finns det ett stort antal huvudmän. Varje myndighet inom säkerhetsområdet svarar för sina egna behovskrav. Detta kan leda till samverkansproblem av teknisk art (bristande interoperabilitet).

³² Regeringskansliet (2004), sid 43

En funktion behövs därför för att genomföra analyser av behovsperspektivet för alla svenska aktörer inom säkerhetsområdet som underlag för forskningsinriktning.

För det andra ingår i ansvaret att se till att nödvändig samsyn, samverkan och samordning mellan berörda aktörer i säkerhetsforskningssystemet kommer till stånd och att rollspelet mellan dessa utvecklas. Baserat på samsynen måste myndigheter och näringsliv gemensamt skapa former och förutsättningar för att kunna förverkliga innehållet i den föreslagna strategin.

Arbetsgruppen har noterat det stora intresset från näringslivet för samverkan med myndigheter. Former bör därför etableras som medger ett samordnat agerande mellan myndigheter och näringsliv, i nationella såväl som i internationella forskningsprogram. Som ett stöd till detta skulle ett säkerhetsforskningsråd kopplat till KBM kunna övervägas med deltagande från operatörer, samverkansansvariga myndigheter, forskningsutförare och näringsliv.

Utbildningsåtgärder krävs troligen för att ge aktörerna en större samsyn, samt insyn och förståelse för varandras verksamhet, och skapa insikt om gemensamma behov.

I ett bredare synsätt på utbildning skulle kunskapen om säkra produkter och tjänster kunna utvecklas. Arbetsgruppen konstaterade under sin studieresa i USA att särskilda program finns inom Department of Homeland Security för att ge studenter som studerar mjukvaruutveckling kunskap om att skapa säkrare IT-system. Arbetsgruppen bedömer att ett sådant tänkande skulle kunna tillämpas även i Sverige för många olika områden.³³ På universitet och högskolor skulle därför säkerhetstänkande

³³ Gissningsvis gällande ett flertal teknik- och ingenjörsutbildningar, men även utbildning i stadsplanering, arkitektur, m.m.

kunna ingå som en integrerad del i utbildningar.

För det tredje ingår i ansvaret att initiera och inrikta forskning för att skapa kunskap och kompetens som leder till utveckling av nya produkter, system och infrastruktur.

För att göra detta krävs att KBM kan

- identifiera tekniska behov;
- analysera och utvärdera arbetet i samverkansområdena och föreslå områden för teknisk samordning;
- samverka med Försvarets materielverk i dess roll som teknisk kravställare.

I det svenska krishanteringssystemet har ett trettiotal myndigheter indelats i sex samverkansområden. Dessa är inte operativa, men utgör en gemensam grund för samordning och planering. KBM inriktar denna samordning och planering. Forskningsbehov inom säkerhetsområdet är ett naturligt område för samverkansområdena.

Samverkansområden i krishantering

- Transporter
- Teknisk infrastruktur
- Spridning av allvarliga smittämnen, giftiga kemikalier och radioaktiva ämnen
- Ekonomisk säkerhet
- Områdesvis samordning
- Skydd, undsättning och vård

För det fjärde krävs en förmåga att kunna värdera de resultat som framkommer och att sedan kunna förmedla dessa resultat. Värderingen bygger på en väl utvecklad analyskompetens och syftar till att se om forskningsinsatser verkligen bidragit till de utpekade målen och givit någon effekt.

Det krävs också att alla aktörer i innovationssystemet kan ta till sig resultaten och förstå hur forskningsresultat och ny teknik kan förbättra den operativa förmågan. Samtidigt krävs att forskningsutförare och näringsliv förstår säkerhetsbehov och förutsättningar för att kunna uppnå en effektiv kunskapsöverföring.

För det femte krävs en värdering av genomförd forskning. En sådan värdering ska bygga på en väl utvecklad analyskompetens och syftar till att visa om forskningsinsatser har bidragit till de utpekade målen och givit effekter i samhället.

1.2. Finansiering av strategin

Arbetsgruppen föreslår att Krisberedskapsmyndigheten ges de resurser som krävs för att finansiera ett nationellt säkerhetsforskningsprogram. Därutöver behövs särskild finansiering för övriga strategiförslag.

De åtgärder och förslag som föreslås i denna strategi kräver att resurser anslås för att genomföra dessa.

Arbetsgruppen bedömer att om inte tillräckliga resurser anslås minskar förutsättningarna för att stimulera innovation, tillväxt och konkurrenskraft i näringsliv och forskningsinstitutioner.

Sverige skulle därmed riskera att suboptimera förutsättningarna för framgångsrikt deltagande i europeiska säkerhetsforskningsprogram. Sverige kommer då visserligen fortsättningsvis delta i PASR och efterföljande ESRP men på nivåer som ligger under de eftersträvade. Eftersom arbetsgruppen bedömer att Sverige har goda förutsättningar att lyckas väl i europeiska säkerhetsforskningsprogram skulle ett gynnsamt tillfälle att göra strategiska satsningar därmed försvinna.

Den grundläggande delen av strategin är det nationella säkerhetsforskningsprogrammet. Det föreslagna säkerhetsforskningsprogrammet är fyraårigt och syftar till svenskt deltagande i slutfasen av PASR och de inledande faserna av ESRP. När ESRP väl är etablerat bedömer arbetsgruppen att det kan finnas anledning till en översyn och möjlig utvidgning av satsningar till stöd för svenskt deltagande.

Som en jämförelse har arbetsgruppen studerat den ekonomiska omfattningen av existerande nationella forskningsprogram. Det nationella flygforskningsprogrammet (NFFP) har en omfattning av 60 miljoner kronor. NFFP finansieras till hälften av staten och till hälften av näringslivet.

Det nationella säkerhetsforskningsprogrammet bör ligga på minst samma nivå, med hänsyn till de framväxande säkerhetsforskningsprogrammen i Europa såväl som i USA.

Villkoren för det nationella säkerhetsforskningsprogrammet bör dock följa villkoren i motsvarande europeiska forskningsprogram där man förväntar att en offentlig finansiering överstiger femtio procent.

Övriga delar av strategin kräver ytterligare resurser, främst för skapande av innovationskraft för säkerhet. Arbetsgruppen har inte i detalj analyserat de ekonomiska behoven för de olika delarna i strategin. Dock gör arbetsgruppen bedömningen att för den föreslagna strategin som helhet krävs på sikt offentliga satsningar i storleksordningen 150-200 miljoner kronor årligen för att nå uppsatta mål.

2. Inrätta nationellt FoU-program inför PASR/ESRP

2.1. Nationellt program för säkerhetsforskning

Arbetsgruppen föreslår att ett nationellt säkerhetsforskningsprogram inrättas för en period av fyra år med start 2005.

Arbetsgruppen föreslår att VINNOVA ansvarar för genomförande av detta forskningsprogram, i samråd med och finansierat av Krisberedskapsmyndigheten.

Möjlighet till svensk påverkan

Arbetsgruppen bedömer att ett särskilt, nationellt forskningsprogram för säkerhet krävs för att säkerställa att svensk forskning och svenskt näringsliv kan bidra till säkerhetslösningar. Detta för att öka förutsättningarna för medverkan i EU:s forskningsprogram samt i motsvarande amerikanska forskningsprogram.

En förutsättning för svenskt deltagande i internationella säkerhetsforskningsprogram är att svenska företag, universitet, högskolor och institut har en hög egen kompetens inom säkerhetsområdet. Ett nationellt säkerhetsforskningsprogram kan bidra till att stärka denna kompetens samt medverka till en fokusering mot säkerhetslösningar.

Det nationella programmet för säkerhetsforskning bör starta redan under 2005 för att skapa goda förutsättningar för svenska företag och organisationer att delta i förberedelserna inför ESRP och, om möjligt, i den sista utlysningen till PASR. Ett aktivt deltagande i PASR och ESRP utgör en viktig förutsättning för att uppnå de av arbetsgruppen föreslagna målen. Det finns likheter mellan de förutsättningar för internationell samverkan som ett nationellt säkerhetsforskningsprogram kan skapa och de förutsättningar som skapas via andra

nationella forskningsprogram. Exempelvis ger det nationella flygforskningsprogrammet förutsättningar för svenska aktörer att delta i och finansiera sin medverkan i europeiska forskningssystem.

Merutnyttjande av resultat från försvarsforskning

Försvarmakten har i sitt FoT-program ett särskilt program för samverkan med civilt drivna teknikområden. På samma sätt som Försvarmakten utnyttjar civil teknik för försvarsändamål kan säkerhetsområdet också utnyttja militär teknik. Civila lösningar bör kunna utvecklas till en lägre kostnad än motsvarande militära då kraven ofta kan sättas annorlunda. Genom att civil och militär teknik i ökande omfattning blir gemensam och militära lösningar kan nyttjas för säkerhetsrelaterade behov, öppnas möjligheterna till att nyttja resultaten från Försvarmaktens FoT-satsningar i ett bredare perspektiv och till att synergier utvecklas.

Ett nationellt säkerhetsforskningsprogram

Ett nationellt program för säkerhetsforskning bör initialt innehålla stöd för:

- Tillämpningar av redan tillgänglig teknik och forskningsresultat för säkerhetslösningar;
- Merutnyttjande av resultat från försvar till säkerhetssektorn;
- Utvecklandet av ny teknik för säkerhet.

En stor del av den teknik som kan tillämpas för säkerhetslösningar finns nämligen redan tillgänglig. Dock krävs satsningar för att skapa samverkan mellan projekt som redan pågår så att de tillsammans kan skapa de synergieffekter som krävs för att skapa effektiva och konkurrenskraftiga säkerhetslösningar.

Ny kunskap för säkerhet ska innehålla konkreta satsningar som syftar till att ta fram ny teknik, dels inom teknikområden som prioriteras inom PASR eller ESRP och dels inom teknikområden som identifierats ur behov hos svenska myndigheter och företag.

Svenska styrkeområden

Möjligheterna till svenska framgångar i europeiska säkerhetsforskningsprogram är större om insatser och åtgärder fokuseras till existerande eller framtida styrkeområden.

Sverige har en industritradition med starkt teknikkunnande. Det är viktigt att fortsatt bygga på detta inom säkerhetsområdet. För att skapa en stark position för svenska aktörer anser arbetsgruppen att det krävs en fokusering på de teknologi- och systemområden som utgör framtida tillväxt- och styrkeområden.

Dessa styrkeområden behöver identifieras och särskilda processer utvecklas för en sådan identifiering. Arbetsgruppen har sökt göra en inledande analys av svenska styrkeområden. Denna analys kan bidra till utformningen av ett nationellt säkerhetsprogram.

Analysen bygger på bidrag från arbetsgruppens medlemmar, den hearing som arbetsgruppen genomförde med företrädare för svenskt näringsliv, innovationssystemanalysen, samt den s.k. ”expression of interest” som genomfördes med universitet och högskolor, institut och andra forskningsutförare under hösten 2004.

Förutom den genomförda innovationssystemanalysen finns begränsad systematik i underlaget varför generaliserbarheten får ses som begränsad och den är inte heller uttömmande. Baserat på detta materiel ges följande förslag på svenska styrkeområden med relevans för säkerhetsområdet.

Förslag på svenska styrkeområden

- Nätverksbaserade lösningar
- Mobil och integrerad telekommunikation
- Informationsteknologi
- Informationssystem i vid bemärkelse
- Bioteknik
- Detektion av biologiska och kemiska ämnen
- Sensorer

Svenska lösningar bör vara inriktade mot högre systemnivåer, system av system och komplexa system. Det föreslagna FoU-programmet syftar inte till att finansiera fullskaliga demonstratorprogram, men programmet bör ändå ge byggstenarna och förutsättningarna för svenskt näringsliv att fortsätta utveckla mer komplexa produkter och tjänster.

Det finns i Sverige goda förutsättningar att skapa en världsledande miljö för utveckling av nätverksbaserade lösningar, inte bara för försvaret utan också för andra sektorer och tillämpningar i samhället. Därmed kan den kompetensuppbyggnad och industriella spridningseffekt som en satsning på nätverksbaserade lösningar och system möjliggör tas till vara.

Satsningar på nätverksbaserade lösningar t.ex. krisledningssystem kan åstadkomma ökad säkerhet samt effektivisera annan offentlig verksamhet såsom vård, omsorg, miljöövervakning, transporter och ”blåljusmyndigheter”. Väl utformade kan sådana satsningar alstra breda tekniska och industriella spridningseffekter till nytta för näringslivets konkurrenskraft och utveckling, och för den ekonomiska tillväxten i Sverige.

Genom IT-utvecklingen har möjligheter skapats för att utveckla nätverksbaserade lösningar för varierande ändamål. Tekniken utvecklas successivt och kommer till realisering bl.a. i utvecklingen av nätverksbaserade försvarskoncept, ofta i internationell samverkan för interoperabilitet.

Sådan utveckling bedöms även kunna appliceras i system och produkter inom säkerhetsområdet.

Sverige har genom universitet, högskolor och industri en framträdande och i viss mån ledande roll inom områdena telekommunikation och informationsteknik och kan genom fortsatt utveckling och marknadsföring bidra till effektiva säkerhetslösningar.

Utöver de ovan angivna områdena finns två viktiga områden där Sverige har en styrkeposition. Det första är analys och värdering av säkerhetssystemet, såväl vad avser hot som möjligheter. Svenska aktörer har god kompetens att göra analyser och simuleringar av hotets karaktär och möjliga konsekvenser därav. I det finns även en god kompetens för att kunna göra tekniska systemvärderingar av olika säkerhetslösningar.

Det andra området är etik, integritet och respekt för mänskliga rättigheter. Arbetsgruppen tror att svenska aktörer kan ha ett försprång genom att kunna förstå, värdera och integrera dessa värderingar i säkerhetslösningar.

3. Underlätta deltagandet i amerikanska säkerhetsforskningsprogram

Utveckla förmåga att skapa framgångsrika ansökningar

Det föreslagna nationella säkerhetsforskningsprogrammet syftar huvudsakligen till att skapa förutsättningar för deltagande i EU:s säkerhetsforskningsprogram, men även till möjligheten att delta i amerikanska säkerhetsforskningsprogram.

Möjliga samverkansområden mellan USA och Sverige³⁴

- Mikrobiologisk beredskap
- Katastrofmedicinsk planering
- Personsaneringsområdet
- Ambulansflyg
- Okända prover
- Kemiska motmedel
- Salmonellaområdet
- Kärnavfall och använt kärnbränsle
- Strålningsmedicin
- Strålskyddsområdet
- Ackrediteringsystem (för logistik i tullen)
- Krishantering och krisbeslutsfattande
- Morfologisk analys
- Krypteringsteknik
- Intelligent transportssystem
- Vägdatabaser
- Trafiksäkerhet för järnväg och tunnlar
- Dammsäkerhet
- Energisystemområdet
- Oljebekämpning
- Samverkan mellan myndigheter

Institutet för tillväxtpolitiska studier (ITPS) har studerat det amerikanska säkerhetssystemet³⁵ och särskilt samverkansmöjligheter finns mellan Sverige och USA.³⁶

³⁴ Institutet för tillväxtpolitiska studier (2004).

³⁵ Institutet för tillväxtpolitiska studier (2003). Se även National Academy of Sciences, National Research Council (2002) och University of Manchester, PREST (2004).

³⁶ Institutet för tillväxtpolitiska studier (2004)

Slutsatsen i studien är att sådana möjligheter finns och rekommendationer ges på kontaktpersoner och ingångar för att skapa dialog mellan Sverige och USA, främst för myndigheter. Intresse finns också från amerikansk sida att undersöka möjligheterna till samverkan med Sverige.

En handelsfrämjarstrategi är dessutom under utarbetande i Utrikesdepartementet och de nedan föreslagna åtgärderna stödjer ansträngningarna att stärka förmågan att skapa framgångsrika ansökningar.

3.1. Förstärka säkerhetskompetens vid ambassaden i Washington D.C.

Arbetsgruppen föreslår att en kompetens inom säkerhetsområdet knyts till den svenska ambassaden i Washington D.C. för att förstärka förutsättningarna för svenska myndigheter, universitet, högskolor, institut och företag att delta i amerikanska säkerhetsforskningsprogram.

Arbetsgruppen bedömer att kunskapsläget om de amerikanska säkerhetsforskningsprogrammen idag är dåligt utvecklad. Svenska forskningsorganisationer och svenskt näringsliv bör därför utveckla sin förmåga att skapa framgångsrika ansökningar och samverkan med USA. Detta bör ske genom att kontakter med amerikanska myndigheter och potentiella samverkansparterna etableras. Erfarenheten visar dock att det tar lång tid och mycket arbete för att skapa långsiktiga allianser.

De amerikanska programmen är också av sådan omfattning att de är svåröverskådliga varför en särskild befattning skulle kunna vara till hjälp för svenskt näringsliv och myndigheter.

En sådan befattning bör vara placerad vid ambassaden och ha ett nära samarbete med ITPS och Exportrådet. Rapportering bör ske till KBM, eftersom myndigheten föreslagits som ansvarig för säkerhetsforskning, samt till VINNOVA, såsom föreslagen ansvarig myndighet för ett nationellt säkerhetsforskningsprogram. I tillämpliga delar bör andra svenska aktörer inom säkerhetsområdet informeras.

En annan uppgift skulle vara att sprida information om svenska företags affärsmöjligheter. Exempelvis annonseras alla amerikanska federala upphandlingar på webbplatser:

- www.fedbizops.gov
- www.hsarpabaa.com
- www.hsarpasbir.com

Affärskontakter och annan information kan sökas på www.hsianet.org vilket är en intresseorganisation för säkerhetsindustri (Homeland Security Industries Association, HSIA).

En motsvarande kompetens skulle även kunna förstärka den svenska representationen i Bryssel. Arbetet med att formulera projektansökningar väntas intensifieras och allt mer av verksamheten kommer att fokuseras till Bryssel vilket kommer att behöva stärka svensk förmåga där.

Arbetsgruppen bedömer att kunskapen om uppbyggnaden av EU:s säkerhetsforskningsprogram är begränsat spridd inom Sverige. Ett framgångsrikt deltagande kräver att potentiella aktörer skaffar sig relevant information för att bättre kunna placera sig. Inom ramen för arbetsgruppens arbete genomförde VINNOVA i oktober 2004 ett erfarenhetsutbyte mellan de svenska aktörer som deltog i den första

utlysningen. Erfarenhetsutbytet var mycket uppskattat och fyllde också ett stort informationsbehov.

Detta informationsbehov finns även inom myndigheter. En samlad syn på vad som sker inom säkerhetsområdet i EU skulle bättre kunna förbereda regeringskansli och myndigheter för en svensk syn.

3.2. Deltagande i amerikanska säkerhetsforskningsprogram

Arbetsgruppen föreslår att förutsättningarna för deltagande i amerikanska säkerhetsforskningsprogram och möjligheter att finna affärsmöjligheter förstärks genom att det tecknas ett Memorandum of Understanding mellan Sverige och USA för säkerhetsforskningssamverkan och att resurser avsätts för att genomföra denna samverkan.

Sverige har behov av att öka kontaktytorna mot USA när det gäller säkerhetsforskningsprogram och stödja förutsättningarna för svenska företag och myndigheter att finna affärsmöjligheter i USA.

Inom försvarsområdet finns sedan många år flera Memoranda of Understanding (MoU) med USA avseende försvarsmateriel- och försvarsforskningssamarbete. Avtalen skrivs på regeringsnivå och samverkan sker på myndighetsnivå. De möjliggör kontakter, informationsutbyte och projektsamverkan mellan de bägge länderna, inte bara mellan myndigheter utan också mellan företag (även om dessa inte är fördragsslutande part).³⁷

Sverige har idag inte motsvarande möjligheter att samverka med USA inom säkerhetsområdet på grund av att det saknas en formell struktur för samverkan inom det området.

³⁷ För en mer ingående beskrivning, se Institutet för tillväxtpolitiska studier (2004), sid 16-17

Ett liknande system som inom försvarsområdet skulle kunna användas för säkerhetsforskning. För försvarssamverkan leds samverkan av en Senior National Representative (SNR) från vart land för utpekade områden. Exempelvis skulle på säkerhetsforskningsområdet en företrädare från Department of Homeland Security kunna utgöra amerikansk SNR och en svensk SNR skulle kunna utgöras av en företrädare från den föreslagna ansvariga myndigheten för säkerhetsforskning, KBM.

Arbetsgruppen har under sin studieresa till USA uppfattat att det kan finnas ett intresse från amerikansk sida att utveckla ett sådant MoU eller motsvarande avtal med Sverige.

För närvarande pågår förhandlingar mellan Sverige och USA avseende ett övergripande forskningsavtal. Det av arbetsgruppen föreslagna avtalet skulle dock utgöra ett från detta övergripande avtal självständigt avtal.

För att svenska forskningsorganisationer och svenskt näringsliv ska bli framgångsrika och skapa tillväxt bör strävan vara att inte stanna vid informationsutbyte som nämns under MoU utan att även leda till tjänsteexport.

I arbetet med att exportera varor, tjänster och forskning till USA är det viktigt att vara interoperabel med de standarder som används inom det amerikanska försvaret och Department of Homeland Security. Det räcker dock inte bara att anpassa sig till standarderna, Sverige bör även vara aktivt i att utforma framtida standarder. Detta gör att vi både kan föra ut resultatet av svensk forskning och att svenska företag skulle få ett försteg att nå ut med ny teknik som är anpassad till dessa nya standarder.

Arbetsgruppen har under studieresan i USA förstått att konkret samarbete bygger på ömsesidig finansiering. Därför behöver en del av budgeten för säkerhetsforskningsstrategin avsättas för sådant samarbete.

4. Skapa innovationskraft för säkerhet

Utveckla svensk säkerhetsindustri

Det föreslagna nationella programmet för säkerhetsforskning syftar till att ge svenska aktörer möjlighet att delta i europeiska säkerhetsforskningsprogram, men även i amerikanska. Därutöver krävs dock ytterligare åtgärder för att ge förutsättningar för att skapa innovationskraft för säkerhet i Sverige.

För att skapa innovationskraft krävs samverkan. Samverkan bör omfatta såväl stora som små företag, högskolor, universitet, institut användare och företrädare för det politiska systemet enligt en innovations-systemmodell (trippelhelix).

4.1. Utvecklande av beställarkompetens

Arbetsgruppen föreslår att Krisberedskapsmyndigheten ges ansvar för att stödja utvecklingen av beställarkompetens avseende säkerhetslösningar för de myndigheter som enligt förordningen (2002:472) har ett särskilt ansvar för framtida krishantering.

Svenska myndigheter bör anpassa sig till de nya förutsättningarna som råder inom exempelvis EU och medverka i rollerna som pionjärer och kompetenta beställare och kravställare för utveckling av avancerade säkerhetsprodukter och säkerhetstjänster, även i internationell samverkan.

Det finns ett behov av att utveckla kompetensen för beställningar av säkerhetslösningar hos myndigheter, främst de som är företrädare inom krishanteringssystemets samverkansområden, kommuner, länsstyrelser och landsting, m.fl.

Kompetent offentlig upphandling av produkter och tjänster har visat sig vara verkningsfull för industriell utveckling och tillväxt.

4.2. Ansvar för gemensamma tekniska krav och standarder

Arbetsgruppen föreslår att Krisberedskapsmyndigheten ges i uppdrag att, i samverkan med berörda myndigheter, ansvara för att

- *stödja utvecklingen av gemensamma tekniska krav för säkerhetsområdet*
- *identifiera, initiera och stödja utveckling av nödvändiga standarder*
- *koordinera och stödja deltagande i internationellt standardiseringsarbete.*

Inom säkerhetsområdet finns ett stort antal huvudmän och det finns för säkerhetslösningar inte någon enhetlig användare, kund eller kravställare. Varje myndighet inom säkerhetsområdet svarar för sin egen upphandling och behovskrav för system och teknik. Detta leder bl.a. till problem med interoperabilitet.

För statliga myndigheter ansvarar Statskontoret för att ta fram ramavtal och ge riktlinjer för funktionskrav m.m. för olika typer av tekniska system. För försvarsområdet är Försvarsmakten den huvudsakliga kunden och Försvarets materielverk den upphandlande myndigheten för teknikutveckling. Försvarsmakten lägger dessutom forskningsuppdrag på Totalförsvarets forskningsinstitut och Försvarshögskolan.

Det finns dock inte någon för myndigheterna gemensam funktion för upphandling av forskning och teknikutveckling för säkerhetsändamål. Dessutom saknas en sådan funktion för kommuner och lands-

ting eftersom Statskontorets rekommendationer inte alltid gäller för dessa. Det är därför angeläget att det skapas en gemensam kompetens inom detta område.

En viktig förutsättning för framgångsrika svenska säkerhetslösningar är att dessa utvecklas i linje med internationella standarder, främst europeiska. En ökad grad av standardisering ökar dessutom interoperabiliteten mellan olika typer av system och samverkan över gränserna.

Sverige bör vara aktivt inom standardiseringsområdet och medverka i de fora som bedöms som särskilt viktiga, exempelvis de CEN-grupper³⁸ som startats i slutet av 2004. Europeiska kommissionen har tillsammans med CEN initierat ett arbete som ska pågå under 2005 för medborgarnas skydd och säkerhet. De standarder som föreslås bör dessutom vara öppna standarder.

Möjligheten att genom deltagande i dessa grupper kunna bidra till standardiseringsutveckling som gynnar svenska intressen genom att svenska idéer kan göra sig gällande främjar även svensk säkerhetsutveckling, inte minst avseende industriell verksamhet. Inom vissa områden kan forskning resultera i väsentliga bidrag till prestandastandardisering, som senare kan utnyttjas av standardiseringsorganisationerna.

Det är angeläget att Sverige tar initiativ och driver sådana inom valda teknikområden. Forskningen spelar här en viktig roll eftersom den kan påverka standardiseringsarbetet. Deltagande i standardiseringsarbete gynnar våra intressen genom att svenska idéer tidigt kan få genomslag.

4.3. Skapa starka forsknings- och innovationsmiljöer

Arbetsgruppen föreslår att svenska intressenter gemensamt skapar starka forsknings- och innovationsmiljöer till stöd för innovation av säkerhetslösningar och successivt öppnar upp dessa för internationell samverkan.

Nationella aktörer behöver skapa en gynnsam miljö för innovation, kommersialisering och utveckling av säkerhetslösningar som komplement till det föreslagna nationella forskningsprogrammet.

Strävan är att skapa en gynnsam miljö för innovation, kommersialisering och utveckling av säkerhetslösningar.

Starka forsknings- och innovationsmiljöer bör vara skapade kring ett trippelhelix-koncept och samla olika typer av intressenter och forskare.

Förutsättningar bör också skapas för att sådana miljöer skulle kunna samfinansieras mellan aktörerna. Arbetsgruppen menar att själva skapandet av sådana forsknings- och innovationsmiljöer inte kan finansieras inom ramen för det föreslagna nationella forskningsprogrammet utan kräver särskilda resurser. Däremot kan ansökningar till det nationella programmet ske för stöd av verksamhet.

Sådana miljöer kan vara virtuella, och arbetsgruppen anser att de med fördel kan skapas kring existerande forsknings- och innovationsgrupper och också kopplas till andra närliggande verksamheter på lokal/regional nivå eller nationell nivå. De skulle kunna etableras utifrån den typ av arenor som nu skapas i Göteborgsregionen, i Linköping genom Navet och i Stockholmsområdet genom Vetenskapsstaden.

En arena i detta sammanhang är ett kluster av forskningsprojekt sammanhållna genom olika scenarier. Ett exempel kan vara transporter genom Göteborg ut på haven.

³⁸ Comité Européen de Normalisation

Inom en arena skapas tillfällen för små och medelstora företag att delta ihop med större företag och få sin teknologi exponerad. Arenorna syftar även till att knyta till sig utländska företag och institut inom delområden och ansöka om medel från EU.

Regionala demonstratorer som exempelvis GOTSAM, VÄSTSAM och det tidigare nämnda Navet ger möjligheter att testa nya tekniklösningar med verklig kund.

Demonstratorarbetet ska även uppmuntras att ske tillsammans med internationella partners, främst europeiska, så att interoperabilitet kan påvisas.

4.4. Identifiera hinder för säkerhetslösningar

Arbetsgruppen föreslår att regeringen uppdrar till Krisberedskapsmyndigheten att utreda behov av nya sammanhållande samhällsfunktioner samt att ge rekommendationer på hur eventuella hinder för säkerhetslösningar kan åtgärdas eller elimineras.

Inom den militära sektorn finns, och utvecklas, de funktioner som behövs för att skapa ett insatsförsvaret på nätverksbaserad grund. På den civila sidan finns inte motsvarande helhetsansvar. Det kan därigenom uppstå funktionella behov där det idag saknas aktörer som fyller sådana funktioner.

Ett exempel är roaming, vilket innebär att en användare i varje situation automatiskt nyttjar det nät som ger de bästa kommunikationsförhållandena. Tekniken finns redan och sker automatiskt när utländska abonnemang nyttjas i Sverige. Roaming är emellertid inte tillåtet i Sverige med svenskt abonnemang.

Det bör utredas om t.ex. roaming skulle kunna tillåtas för att utveckla samhällets informations- och ledningsstruktur.

För att åstadkomma en sammanhållande samhällsfunktion kan exempelvis en enskild aktör få i uppdrag att ansvara för att utveckla tillämpningen av gemensamma säkerhetstjänster. Detta skulle skapa förutsättningar för samutnyttjande av information för att hantera kriser.

Fortsatt arbete i det korta perspektivet

Snabbt agerande

Det finns en risk att den svenska positionen går förlorad om det uppstår ett tidsmässigt glapp mellan färdigställandet av en nationell strategi för säkerhetsforskning och strategins genomförande.

Arbetsgruppen finner det därför angeläget att ett visst mått av verksamhet drivs under perioden direkt efter slutförandet av arbetet med förslaget till en nationell strategi för säkerhetsforskning och fram tills dess att åtgärder vidtas för att stärka svensk säkerhetsforskning.

Arbetsgruppen bedömer att det är av stor betydelse med ett aktivt och framgångsrikt svenskt deltagande i PASR i syfte att skapa en stabil och stark svensk position i det kommande ESRP som förväntas starta 2007. Detta är viktigt mot bakgrund av att Sverige har varit tidigt ute med att identifiera säkerhetsforskning som ett strategiskt viktigt område för svenskt näringsliv. Sverige har också visat sig konkurrenskraftigt i det första utlysningen inom PASR.

Fortsatt arbete för arbetsgruppen

Arbetsgruppen föreslår att den interimistiskt ska fortsätta sitt arbete med att utveckla för säkerhetsområdet prioriterade frågor intill slutet av 2005.

Arbetsgruppen kan under denna tidsperiod bereda och följa ett antal frågor som redan är eller kommer att bli relevanta för svensk säkerhetsforskning. Följande uppgifter bör ingå:

- Bevaka utvecklingen inom PASR och ESRP samt lämna stöd till svenska företag och organisationer som önskar delta i dessa;
- Erfarenhetsutbyte av svenskt deltagande i PASR 2004 inför PASR 2005;
- Bevaka amerikansk säkerhetsforskning, främst inom Department of Homeland Security samt Department of Health and Human Services;
- Tillsammans med Kungliga Ingenjörsvetenskapsakademien (IVA) utreda förutsättningarna för att genomföra och initiera en säkerhetsframsyn³⁹;
- Informera om och följa internationellt standardiseringssamarbete inom säkerhetsområdet;
- Påbörja en djupare analys av Expression of interest;
- Bereda ärenden rörande upprättande av bilaterala Memoranda of Understanding (MoU) samt utvecklande av kompetens för säkerhet vid ambassaden i Washington D.C.

³⁹ I syfte bl.a. att stärka samsyn mellan centrala aktörer inom säkerhetsområdet har IVA föreslagit ett projekt avseende säkerhetsframsyn. Kungliga Ingenjörsvetenskapsakademien (2004).

Referenser

Europeiska unionen

Europeiska kommissionen (2004). *Research for a Secure Europe. Report of the Group of Personalities in the field of Security Research*. ISBN 92-894-6611-1

Krisberedskapsmyndigheten (2004), *Säkerhet och beredskap i Europeiska unionen*, Helén Jarlsvik och Kerstin Castenfors, KBM:s temaserie 2004:3,

Europeiska kommissionens meddelande KOM (2004) 72 slutlig: *Om genomförandet av den förberedande åtgärden om förbättrande av den europeiska industrins potential för säkerhetsforskning, mot ett program för att förbättra Europas säkerhet genom forskning och teknologi*, 3 februari 2004

Europeiska kommissionens meddelande KOM (2004) 590 slutlig: *Säkerhetsforskning: Nästa steg*, 7 september 2004

Europeiska kommissionens beslut (2004/213/EG) av den 3 februari 2004, *om genomförandet av den förberedande åtgärden om förbättrande av den europeiska industrins potential för säkerhetsforskning*, publicerad i EOT nr L 67 5.3.2004, sid 18-22

Europeiska rådet (2003), *Ett säkert Europa i en bättre värld. En europeisk säkerhetsstrategi*, antagen av europeiska rådet den 12 december 2003

Totalförsvarets forskningsinstitut (2004), *Ett europeiskt krishanteringssystem och dess nationella implikationer*, Helén Jarlsvik, FOI Memo 1081, november 2004

Svenskt bakgrundsunderlag

Chalmers Tekniska Högskola (2005), *A survey of the Swedish security industry and an innovation system analysis of the Swedish security sensor industry*, Gustav Oltander och Eugenia Perez Vico (examensarbete).

Kungliga Ingenjörsvetenskapsakademien (2003), *Samverkan för tillväxt med Nätverksbaserade lösningar för försvar och samhälle*, strategirapport från Försvar och säkerhet 2003-11-25

Kungliga Ingenjörsvetenskapsakademien (2004), *Säkerhetsframsyn för Sverige i det nya Europa* (Projektskiss)

Regeringskansliet (2004), Näringsdepartementet och Utbildningsdepartementet, *Innovativa Sverige. En strategi för tillväxt genom förnyelse*, Ds 2004:36, juni 2004

Regeringskansliet (2005) Näringsdepartementet, *Flyg- och rymdindustrin – En del av Innovativa Sverige*, januari 2005

VINNOVA (2004), *Security Research in selected EU member states. How Austria, the Czech Republic, Estonia, Finland, France, Germany, Poland, The Netherlands, and the United Kingdom are preparing for the European Security Research Programmes*, Dr Mathias Kirsten

Amerikanska säkerhetsforskningsprogram

Institutet för tillväxtpolitiska studier
(2003), *Homeland Security and R&D in
the US*, Magnus Karlsson, A2003:014

Institutet för tillväxtpolitiska studier
(2004), *Samverkansmöjligheter mellan
Sverige och USA avseende forskning och
teknik inom säkerhets- och
krishanteringsområdet (homeland
security)*, Magnus Karlsson, Februari 2004

National Academy of Sciences, National
Research Council (2002), *Making the
nation safer. The role of science and
technology in countering terrorism*, 2002

National Academy of Sciences, National
Research Council (2003), *Biotechnology
research in an Age of Terrorism:
Confronting the Dual Use Dilemma*, 2003

University of Manchester, PREST (2004),
*U.S. Defence R&D Spending: An Analysis
of the Impacts*, Andrew D. James, January
2004

Övrigt

CATA Alliance (2003), *Canadian
Advanced Security Industry 2003,
Executive Summary*

Kunskap för säkerhets skull

Förslag till en nationell strategi för säkerhetsforskning

Bilagor

VINNOVA
Krisberedskapsmyndigheten
Försvarmakten
Försvarets materielverk
Totalförsvarets forskningsinstitut

Försvvarshögskolan
Svenskt Näringsliv

31 januari 2005

Innehåll

1. Dokumentation från arbetsgruppens hearing om nationell säkerhetsforskning den 19 augusti 2004 (14 sidor)

Gullers Group/Crystal Interactive Sweden

2. *A survey of the Swedish security industry and an innovation system analysis of the Swedish security sensor industry* (178 sidor)

Examensarbete från Chalmers tekniska högskola av Gustav Oltander och Eugenia Perez Vico

3. *Security Research in selected EU member states. How Austria, the Czech Republic, Estonia, Finland, France, Germany, Poland, The Netherlands, and the United Kingdom are preparing for the European Security Research Programmes* (68 sidor)

Studie genomförd av Dr Mathias Kirsten Fraunhofer-Gesellschaft/VINNOVA

4. Program för arbetsgruppens studieresa i USA (1 sida)

Bilaga 1.
Dokumentation från arbetsgruppens
hearing om nationell säkerhets-
forskning den 19 augusti 2004



Hearing om nationell strategi för säkerhetsforskning

Torsdag 19th Augusti 2004, Finlandshuset, Stockholm

Supported by: Crystal Interactive Sweden

Innehåll

1	Ge exempel på tjänster eller produkter år 2014.	3
2	Frågor till Eva Lindencrona	4
3	Var går gränsen mellan forskningens och politikens uppgifter?	4
4	Ange våra fem främsta styrkor... ..	5
5	Våra främsta styrkor	7
5.1	Teknikområden	7
5.2	Andra styrkor	8
6	Var finns den civila säkerhetsindustrins marknader i framtiden?	9
7	Vad hindrar branschen från att utvecklas. Ange de fem viktigaste?.....	10
8	Utgångspunkter för strategi.....	11
8.1	Behövs ett civilt FMV?	11
8.2	Hur utvecklar vi bättre standarder?	11
9	De tre viktigaste punkterna i nationell strategi att tänka på för arbetsgruppen.....	13

1 Ge exempel på tjänster eller produkter år 2014.

- reliable voice authentication (T7)
- Rubust mobil kommunikation med intrangsdetektering (T2)
- enkel biometrisk autentisering (T3)
- Person, kontext och positionsberoende tjänster (T2)
- arkitektur för självkonfigurerande teknisk infrastruktur (T2)
- Samverkande system för skydd av medborgaren ej övervakning av den. (T9)
- Personal Area Networks (T2)
- Modellering simulering och träning av räddningspersonal (T1)
- Säker kommunikation och access (t ex till banken) i var mans mobil (T1)
- Sensorer för individuellt bruk (T5)
- Tjänstebaserad produkt för myndighetssamarbete för (holistisk) hothantering (T8)
- Enhetlig och strukturerad produkt/program utveckling (T7)
- Säker fasttelefoni (T10)
- Integritetsskyddad samverkan i nätverk (T6)
- avancerad personlig Integritetshantering (T3)
- tjänster för att skapa "trust" i osäkra miljöer (T7)
- Ett nytt OS utan säkerhetshål (windows ??) (T6)
- Säkerhetslägesinfo i var kvinnas mobil (T1)
- Trygghetspaketet Tryggve är IKEAS nya produkt (T9)
- Säker mobiltelefoni (T10)
- Early Warning Forecast , Väderkarta över sannolika kommande hot, av alla slag. (T11)
- "Mobiltelefonen" ar forsvunnen, allt har inbyggd kommunikationsmöjlighet (T2)
- tjänster och produkter för integritetshantering (T4)
- Infrasytem-system för samverkan mot organiserad internationell brottslighet (T8)
- Produkter för personlig säkerhet (T7)
- bioterror. Bygga upp en industri som baseras på världsledande forskning Sverige inom mol.biologi och mikrobiologi (T11)
- Säkra systemkonstruktioner (T1)
- Trust via nätbaserade communities (T1)

2 Frågor till Eva Lindencrona

- Finns tankar att skapa ett nationellt säkerhetscentra i Sverige_ (T8)
- Hur mobilisera och tillhandahålla lobbying i Bryssel? (T10)
- Varför bara nischer Sverige är redan världsledande inom många områden (T2)
- Var finns pengarna_ (T8)
- Hur kommer den nationella strategin att användas? (T1)
- Kommer det att finnas svenska forskningsmedel (T6)
- Hur analyserar man utvecklingen av hotbilden generellt för samhället (T5)
- Vad inkluderas i säkerhet i detta sammanhanget? Är det allt från personlig till nationell säkerhet? (T3)
- Finns det en specifik Svensk industri (T2)
- Vem gör analysen ? (T5)
- Finns någon samlad bild av säkerhetsforskning (Projekt/bidrag) i Sverige? (T7)
- Hur ska vi få tillgång till de pengar som finns-anslås (T8)
- språkproblem_eng security`,safety istf svenska etc sandrta europisk språk har samma begrepp i säkerhet. (T4)
- Krävs motfinansiering? Hur får vi den? Ansökningspengar! (T10)
- Vi behöver en tydlig kund (T1)
- Svensk industri ags ofta internationellt (T2)
- Vi behöver två säkerhetsbegrepp (T5)
- Lobba hos handläggare och kommissionärer (T2)
- Är svenska myndigheter beredda-villiga att stödja svensk industri (T8)

3 Var går gränsen mellan forskningens och politikens uppgifter?

- kan frågeställningen förtydligas? (T9)
- Inom säkerhetsområdet måste politikerna (i alla fall) definiera balansen mellan övervakning och integritet. (T8)
- Hur hantera det kommunala perspektivet (T5)
- Politiker måste skapa förutsättningar för en fungerande forskning i Sverige (T7)
- Visst finns det forskning om metodfrågor, hot och samhällsscenarier, avvägningsfrågor etc. (T1)
- Politikerna måste definiera uppgiften / behovet för att kunna rikta forskning för metodiken och nödvändiga förmågor för att vi samtidigt ska kunna forska på tekniken (T2)
- Om forskningen förutsätter gränslöst samarbete mellan myndigheter, landsting, kommuner etc måste politikerna konfirmera att detta är möjligt och kommer att genomföras! (T8)
- Forskningen ger politikerna beslutsstöd och politikerna ger forskarna förutsättningar för forskning (T1)
- Gränsen kan inte tydligt definieras. Behoven måste definieras av företag, forskning, myndigheter och politiker tillsammans. (T3)
- Det går inte att forska på enbart metodiken först, teknikens nya möjligheter måste också beaktas (push & Pull) (T2)
- Myndigheter som motor i den offentliga upphandlingen (T6)
- Samverkan mellan myndigheter är nödvändigt för att lyckas, men måste inte någon myndighet vara totalansvarig, och vilka verktyg skall den myndigheten ha? (T9)
- Man bör försöka hitta rågången mellan det internationella perspektivet och vad som kan tänkas vara specifikt lokalt och svenskt. (T10)

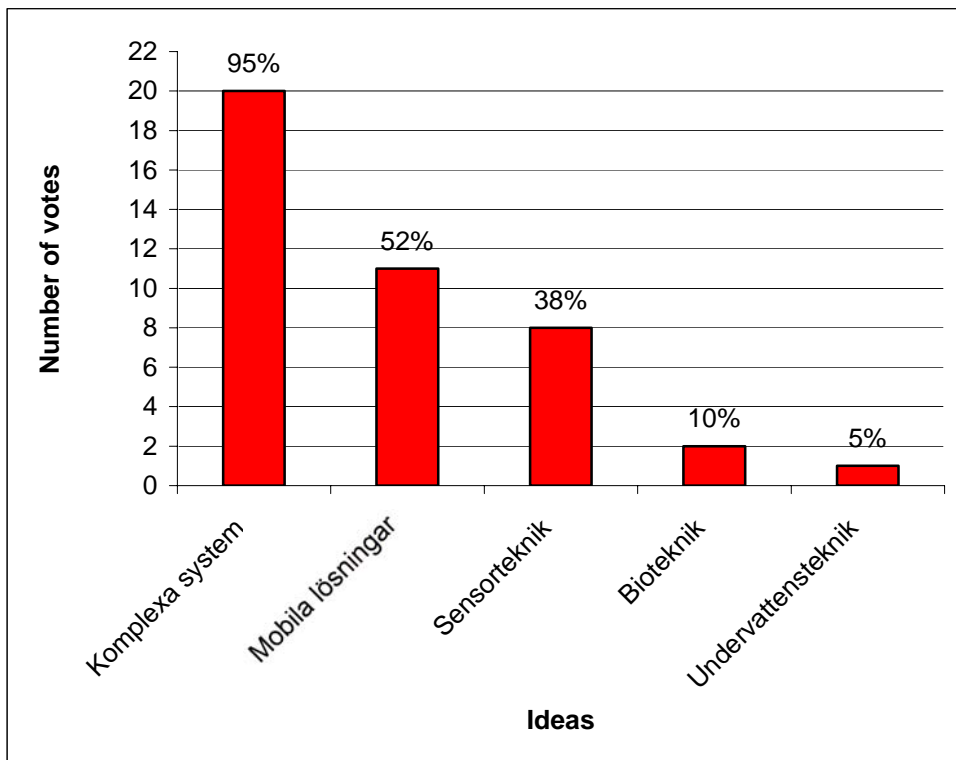
4 Ange våra fem främsta styrkor...

- Mobile communication **(T11)**
- Säker mobilkommunikation (systemdesign) **(T2)**
- Bra på systemintegration **(T7)**
- Biomedicinsk forskning för att utveckla profylax och terapi mot bioterror **(T11)**
- god förmåga hitta användarnära systemlösningar (kundfokus). anpassning till behoven **(T3)**
- klimat för prestigelöst samarbete **(T1)**
- En hög nivå på IT infrastruktur **(T10)**
- generellt hög IT-kompetens för olika typer av systemlösningar **(T3)**
- Säkerhetstänkandet i (komplexa)system **(T1)**
- Sverige intressant rollmodell för dem som strävar mot mogen infrastruktur **(T10)**
- Bra innovatörer, kostnadseffektiva lösningar (p g a lite pengar), vana vid samverkan **(T8)**
- Informationstekniskt kunnande **(T11)**
- tradition av kompetenta beställare **(T1)**
- Kostnadseffektiva (egna) lösningar för Sveriges försvar och säkerhet (behöver bli internationellt gångbar) **(T2)**
- Logistik **(T5)**
- Användarvänlighet HCI dvs människan är en del av systemet **(T7)**
- Den tidiga lagen om Extraordinära händelser och framtagning och genomförande åtgärder **(T10)**
- De flesta lösningar finns **(T8)**
- Metoder, arkitektur och teknik för IT-säkerhet **(T2)**
- behovsanpassade systemlösningar på hög nivå (arkitektur, standards,) **(T2)**
- God förmåga att driva stora projekt. Nå fram till avslut. **(T3)**
- Insikt och vana att söka samarbete pga att Sverige är en liten marknad **(T11)**
- Svenskar är snabba på att ta till sig och använda ny teknik **(T2)**
- Bra kompetens inom teknikområdet i Sverige **(T7)**
- Systemintegration, Kommunikationsteknik, Sensorteknik, Personliga nätverk, Etablerade strukturer för statistik och data **(T6)**
- (Användbarhet) Människa maskin interaktion **(T2)**
- Traditionell av prestigelöshet och konsensusbeslut **(T10)**
- Hög innovationskraft (väldigt hög på individuell nivå) **(T3)**
- Svensk Management i den Svenska modellen för säkerhetsföretag (security) med historiskt hög kompetens. Två exempel är Securitas och Assa. **(T4)**
- Säkerhetslösningar i undervattensmediet **(T1)**
- Fusion av stora datamängder **(T2)**
- Bred industristruktur **(T7)**
- trovärdiga **(T7)**
- Lagom stort land dvs. närhet mellan beslutsfattare **(T7)**
- Alliansfrihet **(T10)**
- historiskt har svenska säkerhetslösningar utvecklats och integrerats (Bilar, kärnkraft, flyg, sjöfart,...). Kan överföras till antagonistisk säkerhet. **(T2)**
- Vi har ett stort förtroende och anseende i världen **(T7)**
- Staten satsar på stor IT infrastrukturuppbyggnad vilket skapat förutsättningar för tjänste och produktutveckling Systembyggande, pga. stort land och litet befolkningsunderlag, (kostnadseffektivitet krävs) IPT, Nära samarbete mellan myndigheter, forskningsvärlden och näringsliv Små och snabba Är accepterade som internationell partner **(T9)**

- Flerhundraårig tradition av att hålla folkbokföring, koll på personnummer osv. Detta kopplat till offentlighetsprincip och principer för anonymitet. **(T11)**
- Samverkan mellan industri, institut och UoH **(T2)**
- nätverksbyggande såväl tekniskt som metodmässigt **(T2)**
- Acceptans och öppenhet för olika övnings och träningsystem **(T1)**

5 Våra främsta styrkor

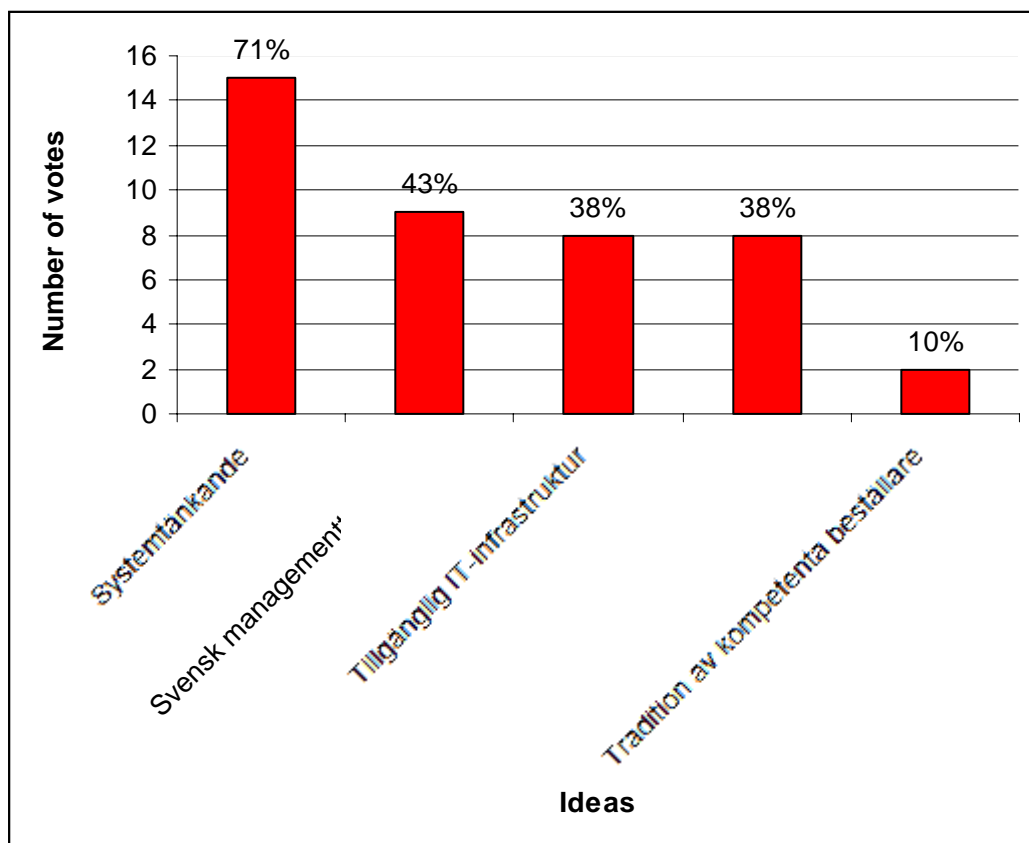
5.1 Teknikområden



Items in original order

- Undervattensteknik
- Bioteknik
- Komplexa system
- Sensorteknik
- Mobila lösningar

5.2 Andra styrkor



Items in original order

- Systemtänkande
- Tillgänglig IT-infrastruktur
- Svensk managementtradition
- Tradition av kompetenta beställare
- Teknikvänliga

6 Var finns den civila säkerhetsindustrins marknader i framtiden?

- Personliga säkerhetslösningar för att öka den personliga tryggheten **(T7)**
- Övervakningstjänster **(T7)**
- Skydd av nätverk (infrastruktur), centrala tillgångar (Energiproduktion, finanser, transportterminaler, befolkningscentra mm) **(T2)**
- Säkerhetslösningar för att värna om den personliga integriteten **(T7)**
- Ökat intresse för den europeiska marknaden **(T1)**
- Säkerhet i hemmet Omsorg och sjukvård i hemmet **(T11)**
- Personskydd, individanpassade trygghetspaket (försäkringar mm) **(T8)**
- Management och integration av säkerhetslösningar **(T7)**
- Identity theft protection **(T11)**
- regelverk kan tvinga fram nya marknader (försäkringsbolag kräver inbrottslarm för att privatpersoner ska kunna teckna hemförsäkring, finansinspektionens krav på informationssäkerhet i banker m m) **(T3)**
- Tekniska personskydd med bevakelse i den befolkningspyramid som industriländerna har framför sig. Hämta idéer från bilindustrin! **(T4)**
- Sjukvård och servicetjänster **(T7)**
- Den internationella marknaden förutsatt att kulturproblematiken kan hanteras **(T5)**
- I första hand produkter med högre tekniknivå (system eller system av system...) ger att kunden är institutioner, verk, företag e.t.c snarare än den enskilda individen **(T1)**
- Produkter för personlig säkerhet **(T11)**
- Tjänster **(T9)**
- Larm och övervakning **(T10)**
- Marknaden kommer att vara uppdelad på komponent och tjänsteleverantörer samt systemleverantör för tex. att möta framtida hemsjukvårdsbehov, säkra banktjänster etc **(T6)**
- Integritetsskyddande lösningar för telefoni, data och Internet **(T10)**
- SOS lösningar **(T10)**
- Barnsäkerhet **(T10)**
- Ökad insikt om säkerhetsbehov **(T8)**
- skydd av samhällsviktig infrastruktur (sjukvårdssystem, energi, elektronisk kommunikation m m). Den samhällsviktiga infrastrukturen är dock inget enhetligt begrepp och utgör inte en samlad kund och marknad. **(T3)**
- operatörer som erbjuder trygghetslösningar (inbrott, terrorhot, viruskydd, DOS attack/SPAM reduktion, äkthetsbevis, konfidentialitet, integritet?, oavvislighet etc) **(T2)**
- Åtgärdsanalys och genomförandeprocess (tjänst) **(T10)**
- Individ (individ, närmiljö), kommun (infrastruktur), KBM (samh. funktioner) **(T1)**

7 Vad hindrar branschen från att utvecklas. Ange de fem viktigaste?

- Stuprörstänkande i det nationella systemet (T3)
- Anslag, anslag, anslag till forskning och nya företag (T10)
- gemensam standard för samverkan mellan tjänster (T2)
- Ekonomiska resurser (T7)
- Det konstitutionella hotet (T5)
- stöd från svenska myndigheter (T2)
- Lagar och förordningar, nationellt och internationellt (T2)
- Samordning mellan myndigheter, kommuner och stat (T10)
- Bättre företagsutvecklingsklimat (T7)
- Oförmåga att anpassa sig till öppna standards (T6)
- Nationell referens (p g a bristande myndighetssamarbete) (T8)
- För lite egensatningar (av företagen) (T8)
- Tydlig problemägare och kanaler för initiativ (T10)
- Otydlig myndighetsstruktur (T1)
- Brist på politisk vision (T1)
- Europas oförmåga att snabbt driva standardisering (T5)
- Mottaglig attityd för förslag och forum för detta (T10)
- Brist på nytänkande referensupphandlingar från staten (T7)
- Insikt över olika framtida händelse scenarier (T7)
- Beställare saknas ofta Brist på standarder Oklart (fragmenterat) produktansvar för komponenter i komplexa system (T11)
- Avsaknad av kompetent beställare (T1)
- Känslan av att integriteten kränks (T6)
- oförmåga att konstruktivt hantera förändring (T2)
- Ostrukturerad och oklar behovsbild och risker. Brist på gemensam uppsättning föreställningar för företag och det offentliga. (T3)
- Otydlig behovsbild (T1)
- Brist på standarder (T1)
- för lite forskning och högskoleutbildning om säkerhets strategier (T8)
- Aktieägarnas avkastningskrav ger för kortsiktiga perspektiv. (T4)
- 1 Politisk flathet 2 Saknas Nationell strategi för säkerhetsforskning ;-)
- 3 Saknas samling, fokusering, tydlig kund med mål och resurser
- 4 Många länder lutar sig mot EU, där frågor fastnar i byråkrati
- 5 Industrin bör enas nationellt för att kunna visa styrka utåt (T9)
- Kunder och slutanvändares naivitet skapar svag efterfrågan på säkerhetslösningar (T7)
- Microsoft säljer system som inte är tillförlitliga, men de tar inget ansvar. Man kan inte stämma dem. (T11)
- Bristande samverkan mellan myndigheter (T1)
- Säkerhetsincidenter tystas ner vilket leder till bristfällig insikt om problem och hotbild. Riskmedvetenheten är låg (T7)
- för många myndigheter nationellt och internationellt hanterar samma områden (T2)
- Ett forum (T10)
- Begränsad investeringsvilja - förmåga (FoU). (T5)
- standarder för säkerhetstjänster i hemmet (medicinsk koll på distans, vattenkvalitetsmätning) (T3)
- Samlat myndighetsansvar för samhällssäkerhet saknas (T7)
- Ansvarslöshet som bottnar i en oklar juridik (ansvar för säkerhetsbrister) (T7)

- Bristande stöd för industrin i EU **(T1)**
- KBM borde gå från administrativ till operativ myndighet med militär kompetens (nuvarande försvarsmakten) inkluderad **(T8)**
- Bristande samordning i AB Sverige ger inte förutsättningar till produktvolymerna i exportsektorn och därmed dålig konkurrenskraft **(T4)**
- Höga entrybarriärer för nya bättre lösningar när de etablerade (Microsoft och andra) dominerar så starkt **(T6)**

8 Utgångspunkter för strategi

8.1 Behövs ett civilt FMV?

- Nån form av sammanhållen upphandling krävs för att den ska vara effektiv. annars blir det splittring. **(T3)**
- Upphandlingen av en gemensam upphandlingsfunktion kan vara av hela system eller genom att sätta standarder och specar som kommuner-landsting-myndigheter sedan kan använda i sin egen upphandling. **(T3)**
- Det behövs en central upphandlare. FMV? **(T5)**
- Viktigt med koppling mellan beslutsfattande och pengar (jfr TETRA-upphandling där systemet blir alldeles för dyrt för vissa aktörer). Ansvar och befogenheter ska korrespondera. **(T3)**
- Viktigt med samverkan mellan kravställare och upphandlare. **(T5)**
- EU håller på att bilda en myndighet för försvarsupphandling. Det krävs samverkan i säkerhetsfrågor med bl a öppna standarder, metoder o.d. Hur rymmer detta med en ny nationell upphandlare? Färre myndigheter för dessa frågor - JA. Nya nationella upphandlare - ej självklart **(T2)**
- ska denna upphandlingsorganisation bygga på nuvarande FMV? Ja, i så fall en utveckling mot Samhällets Upphandlingsverk. Tar uppdrag från hela samhällssektorn (sjukvård, försvar, tull, mm). Myndigheten skulle kunna sortera under ett nybildat Säkerhetsdepartement. **(T3)**
- JA! Ett Statens MaterielVerk (SMV) behövs för att industrin skall få en tydlig kompetent kund för det svenska OCH europeiska behovet av säkerhetssystem **(T1)**
- Det är både ett hot och en möjlighet. Operativa krav måste omsättas i tekniklösningar vilket är en förutsättning för att rätt produkt/tjänst upphandlas **(T5)**
- Ja, för att täcka bristande upphandlingskompetens med långsiktigt mål att förbättra beställarkompetensen tills de egna vingarna bär. **(T4)**

8.2 Hur utvecklar vi bättre standarder?

- Identifiera en aktör som äger frågan och får lite initiala medel **(T10)**
- Etablera kontakter med och lobba mot EU **(T10)**
- Samla nationella aktörer **(T10)**
- Sverige skall verka för en Europeisk och internationellstandard. Detta skall ske av myndigheten och industri i samverkan. **(T6)**
- Ställ krav på standardiserade lösningar i upphandlingar. Detta tvingar fram standardiserade produkter/processer. **(T7)**
- Att Sverige deltar aktivt i EUs kommande standardiseringsarbete och försöka påverka utvecklingen **(T8)**
- 1 Vad avser systemintegration och informationsintegration, Vidareutveckla de som finns i nya grenar / varianter, istället för att skapa nya då det tar för lång tid. 2 Säkerhet är en del av systemet och skall därför integreras i befintliga utvecklingsprocesser 3 Bättre att arbeta med ramverk och existerande standarder 4 Ansvar skall finnas kvar i etablerade organisationer 5 Framtidsutveckling av system och produkter måste vara proaktivt i standardiseringsfrågor **(T9)**
- Förbättrad samordning mellan myndigheter, stat och kommuner **(T10)**

- en global organisation som ansvarar och koordinerar standarder för juridik, metod, teknik, mm **(T11)**
- Behöver vi standarder eller produkter? **(T7)**

9 De tre viktigaste punkterna i nationell strategi att tänka på för arbetsgruppen.

- Det konstitutionella hotet!! (T5)
- Vilken hotbild ska vi skydda oss emot? (T4)
- Att verka för att höja säkerhetsnivån i industrin genom att stödja säkerhetslednings systemet (T7)
- Ag skall vara tydlig och fokuserad i sina förslag till regeringen. (T6)
- införa ISO 17799 se tidigare svar (T7)
- Tydlighet i förslagen (T10)
- Tuff tidplan (T10)
- Någon (VINNOVA? KBM?) måste tvinga ihop myndigheter, landsting, kommuner etc till nationellt (och internationellt)säkerhetsarbete. UoH och industri står redan till tjänst för att ta fram lösningar(teknik, metoder) (T8)
- Är definitionen av forskningsbehovet utgående från EU-behovet relevant för Sverige? Ex.vis. annan hotbild, mera utvecklad IT-struktur. (T7)
- Sekretessfrågorna (T4)
- Definition av säkerhetsbegreppet (T2)
- Ag skall ställa höga krav på feedback från EU ang. den presenterade strategin. (T6)
- innehållet i strategin skall stödja internationell utveckling inom området (T2)
- Identifiera linjerna med största hävstångseffekt gällande exempelvis export, produkt och tjänsteutveckling, kompetensutveckling etc. (T10)
- Vilka konkreta behov finns i Sverige_ (T8)
- 1 Tydliggör en viljeinriktning och beskriv en framtida behovsbild för samhällssäkerhet, så industrin kan inrikta sin tjänste och produktutveckling på ett bättre sätt 2 Ta till er metodfrågan, inte teknikfrågan, den löser vi i industrin (T9)
- Ekonomisksekretess (T4)
- skapa förutsättningar för att resursstark och kompetent beställarkapacitet uppstår (T11)
- Ag föreslår att man nationellt stimulerar offentlig upphandling på området. (T6)
- Deltagarna idag blir remissinstans (T9)
- internationell samverkan och svenskt stöd och hjälp till detta (T2)
- Beskriv hur den svenska säkerhetsforskningen skall finansieras. Enbart genom EU-bidrag och industri? (T7)
- Pengarna på bordet! (T8)
- finansiering (T2)
- Fokuserad behovsbild. Även om det vi planerar för kanske inte inträffar, kanske planer och beredskap är nyttiga för att hantera de händelser som faktiskt inträffar (T3)
- Ag får ej glömma innovationskraften i små och medelstora svenska företag. (T6)
- Gärna ett nyhetsbrev eller ännu hellre en hemsida som ger möjlighet till dialog. (T6)
- Industrin måste få möjlighet till att yttra sig om förslaget som arbetsgruppen tar fram (T1)
- Arbetsgruppen bör publicera sina resultat snarast, helst löpande. En hearing efter avslutat arbete bör hållas. (T10)
- Webbplats med fortlöpande info från arbetsgruppen och där man också kan mejla till arbetsgruppen för synpunkter (T8)
- förmåga till snabb återhämtning (inte bara fokus på säkerhetsutmaningar). Om en händelse inträffar ska tiden till normaltillstånd vara så kort som möjligt. (T3)
- Det borde finnas representanter (adjungerande) från näringslivet i arbetsgruppen i Vinnova. (T4)
- Uppmuntra deltagarna att förklara och förtydliga de inlämnade synpunkterna (T1)

- resursstark inhemsk beställarorganisation skapar förutsättningar för svensk forskning och industri utveckla för en global marknad **(T11)**
- Säkerhet mot terrorism (T4)

Bilaga 2.

A survey of the Swedish security industry and an innovation system analysis of the Swedish security sensor industry.

Examensarbete från Chalmers tekniska högskola av Gustav Oltander och Eugenia Perez Vico

A survey of the Swedish security industry and an innovation system analysis of the Swedish security sensor industry

Chalmers University of Technology

Vinnova

Master's Thesis

January 2005

Gustav Oltander 780308

Eugenia Perez Vico 801201

Tutor at Chalmers University of Technology:

Sven Lindmark

Tutor at Vinnova:

Lennart Norgren

Preface

Following report shows the results of a master thesis work at the department of Innovation Engineering and Management at Chalmers University of Technology in Gothenburg, Sweden. The thesis was initiated by Vinnova in August 2004 and finished in January 2005. The report was conducted in order to support Vinnova in their work with the development of a national strategy for security research. We would like to thank our tutors, PhD Sven Lindmark at the department of Innovation Engineering and Management at Chalmers University of Technology and PhD Lennart Norgren at Vinnova, for their support and guidance in the conduction of the thesis. We would also like to thank all the interviewees for their help. Further, we would like to thank Professor Staffan Jacobsson at the department of Industrial Dynamics at Chalmers University of Technology for providing us with ideas and helping us with the understanding of the functional analysis.

Gustav Oltander
Eugenia Perez Vico

2005-01-12

Gothenburg, Sweden

Summary

The threatening picture has changed, from threats related to political conflicts between nations, to terrorism and organized crimes, augmenting the need for security. At the same time, the Swedish defence industry is facing restructuring needs and in its place, a new civil industry is emerging. In the light of this, the Swedish government has appointed a project group to design a national security research strategy. Vinnova, the Swedish Agency for Innovation Systems, which is the assigner of this report, has the main responsibility in this project. In order to support Vinnova's task, this report aims at clarifying the Swedish security industry structure, identifying market growth potentials and recognizing deficient industry factors. This was achieved through the conduction of an industry survey and an innovation system analysis. In the industry survey, the Swedish security industry was divided into seven sectors, weapon technology, sensor technology, complex systems (system integration) and simulation, IT-security, mobile solutions, physical transportation and NBC technology. Sensor technology was selected as the most interesting industry sector given its perceived future market potential and perceived level of related national capability. Further, an innovation system analysis was conducted on the Swedish sensor security industry using the functional analysis framework.

The industry survey showed that although there are differences in technologies, applications, actors, regulations and trends regarding each sector, they have three factors in common. Firstly, the market potential of the general security industry is perceived as at least relatively high in all industry sectors, resulting in that companies with previously exclusively military customers are entering the emerging civil security market. Secondly, the national industry actors are prominent in almost every security industry sector and Sweden is among the leading nations in the world regarding telematics, sensor technology and complex systems. Finally, the national security market is regarded as weak by the industry actors. Also, the lack of collaboration between local and governmental authorities has been recognized as a vast hindrance for market development.

The innovation system analysis showed that a stronger guidance and coordination among governmental authorities is needed, both referring to the articulation of the demand and in the process of acquisitions of supplies. By concentrating resources on creating such guidance and coordination among authorities, the Swedish security sensor innovation system, would be improved. Also, the cultural differences between commercial companies and governmental authority decrease the innovation system efficiency. By concentrating resources on augmenting the interaction between the two, the innovation system performance can be improved. Further, the incentives for entering the sensor security market are identified abroad. By extending the existing collaboration between the DHS and the SEMA,

it would be possible to project the American incentives for market entrance directly onto the Swedish market, increasing the perceived incentives on the Swedish market. Finally, it can be stated that the recommendations presented in this report regarding functionality improvements of the specific innovation system can be favourable for the future development of the entire Swedish security industry.

Table of contents

1. Introduction.....	1
1.1. Background.....	1
1.2. Objective.....	2
1.3. Problem formulation.....	2
1.4. Outline of the report.....	2
2. Method and theory.....	4
2.1. Overall method model for the thesis	4
2.2. Method and theory for the industry survey	5
2.2.1. Identification and survey of the actors	6
2.2.2. Identification of the sectors.....	7
2.2.3. Analysis of security industry sectors.....	8
2.2.4. Evaluation of sectors	10
2.2.5. Identification of potential sector.....	11
2.3. Method and theory for the Innovation system analysis	12
2.3.1. Technology analysis	13
2.3.2. Venture capital analysis.....	14
2.3.3. Survey of educational output.....	14
2.3.4. Patent analysis	15
2.3.5. Innovation System	16
2.3.6. System structure analysis.....	20
2.3.7. Functional analysis.....	21
2.4. Overall evaluation and validation of used method and theory	26
2.4.1. Validity	26
2.4.2. Reliability	27
3. Industry survey.....	28
3.1. Definition of the security industry.....	28
3.2. Classification of the sectors.....	30
3.2.1. Review of the categorization.....	30
3.2.2. Synthesis on industry classification	33
3.2.3. Choice of industrial classification	35
3.3. The security industry sectors.....	37
3.3.1. Weapon Technology	39
3.3.2. Sensor Technology	43
3.3.3. Complex systems (system integration) and Simulation	49
3.3.4. IT-security	54
3.3.5. Mobile Solutions.....	58
3.3.6. Physical Transportation.....	63
3.3.7. NBC technology	66
3.4. Evaluation of the sectors.....	72

3.4.1.	Results from articles and reports	73
3.4.2.	Results from the interviews.....	78
3.4.3.	Results from the hearing.....	79
3.5.	Identification of a potential sector	79
4.	Innovation system analysis of the security sensor industry.....	81
4.1.	Delimitation of the innovation system	81
4.2.	System structure	82
4.3.	The nature of the security sensor industry as an innovation system	87
4.4.	Functional analysis.....	88
4.4.1.	Function 1. Knowledge development	88
4.4.2.	Function 2. Provide incentives and guide the direction of search.....	96
4.4.3.	Function 3. Promoting entrepreneurial experimentation	100
4.4.4.	Function 4. Market formation	104
4.4.5.	Function 5. Mobilization of resources	112
4.4.6.	Function 6. Legitimization	117
4.4.7.	Function 7. Creation of free utilities.....	119
4.5.	Conclusions and recommendations.....	125
4.5.1.	Summarization of system weaknesses.....	125
4.5.2.	Blockage mechanisms	126
4.5.3.	Recommendations.....	133
5.	Conclusions.....	136
6.	Suggestions for future research.....	139
	Referenses.....	140
	Appendices	149

Table of figures

Figure 2-1 The thesis objective and problem formulation	4
Figure 2-2 The methodical frame for the thesis	5
Figure 2-3 Sector mapping.....	10
Figure 2-4 Methodical frame for the innovation system analysis	13
Figure 2-5 Overall structure for the innovation system analysis	25
Figure 3-1 Vinnova's picture of potential threats and elements worth protecting.....	29
Figure 3-2 Illustration from Civita report 2004.....	31
Figure 3-3 Technological classification of the security industry, based on empirical results	34
Figure 3-4 Mission based classification of the security industry, based on empirical results	35
Figure 3-5: The sectors presented in the security concept	37
Figure 3-6 The weapon technology sector	43
Figure 3-7 The sensor technology sector	49
Figure 3-8 The Complex systems (system integration) and Simulation sector.....	54
Figure 3-9 IT-security	58
Figure 3-10 The mobile solution sector	62
Figure 3-11 The physical transportation sector.....	66
Figure 3-12 The NBC-technology sector	72
Figure 3-13 The technological trends	73
Figure 3-14 Distribution of the DHS budget for 2004 in millions of dollars.....	74
Figure 3-15 Number of sources that have acknowledged growth potential of the particular sector.	77
Figure 3-16 Future market potential of the sectors as perceived by the interviewees	78
Figure 3-17 Potential growth as according to the results from the Vinnova hearing	79
Figure 3-18 The growth potential of the Swedish security industry sectors.....	80
Figure 4-1: Overall structure for the innovation system analysis	81
Figure 4-2 The delimitation of the innovation system.	82
Figure 4-3 Technology chain analysis.....	83
Figure 4-4 Geographical distribution of commercial companies, research institutes, suppliers, university institutions and national centres of excellence.....	84
Figure 4-5 Relative amount of Swedish patents in the sensor industry 1976 to 2004	90
Figure 4-6 Relative amount of Swedish patents in the sensor industry 1999 to 2004	90
Figure 4-7 The number of sensor patents in Sweden, Israel and Germany 1976 to 2004 ..	91
Figure 4-8 Amount of sensor patents per capita for Sweden, Israel and Germany.....	91
Figure 4-9 Number of entrants per year on the Swedish sensor security industry.....	100
Figure 4-10 Number of Swedish patents related to security sensors issued to private persons	101
Figure 4-11 Factors driving the market segments.....	107
Figure 4-12 Number of graduates from sensor related educations.....	113
Figure 4-13 Venture capital investments in Europe 2001	114
Figure 4-14 Venture capitalist activity sectors in Sweden.....	115

Figure 4-15: Connection between the function weaknesses and the blockage mechanisms 127

Figure 4-16: The blockage mechanisms with corresponding recommendations 134

Table of appendices

Appendix A: Interview questions for the industry survey (in Swedish)	149
Appendix B: Interview questions for the innovation system analysis (in Swedish)	150
Appendix C: Search strings used in the patent analysis.....	152
Appendix D: Security sensor industry actors, regulations and networks	154
Appendix E: Clarification of grading of the blockage mechanism matrix.....	163
Appendix F: Top 13 private sector opportunities according to Civita Group.....	167
Appendix G: Results from the interviews concerning sector evaluation.	168

1. Introduction

In this introducing chapter, the background, objective, problem analysis together with the delimitations and definitions of the thesis, will be presented.

1.1. Background

During the last couple of years, the threatening picture has changed, from previously consisting of threats mainly related to political conflicts between nations, to current scenarios of terrorism and organized crimes. This has augmented both individual's and society's need for security. At the same time, initiatives are taken to improve the competitiveness and growth potential of the Swedish industry. In these circumstances it has been stated that Sweden should use its industrial and technological potential in the security and defence field for developing civil applications, and that this should be done in order to strengthen existing, and support growing industries and companies¹. The Swedish defence industry is facing large restructuring needs at the same time as a new civil security industry is emerging. These two are expected to merge into a new and broader security industry.

Further, a security research program is developed within the European Union, starting with the Preparatory Action on Enhancement of the European industrial potential in the field of Security Research 2004-2006, hereafter referred to as PASR. It has been stated that Swedish research has good requisites to considerably contribute to an increased security in Sweden and the rest of the world². It is important for the new emerging Swedish industry to find its place in a changing European security industry. Both the USA and the European Union are investing in the security research area and it has been declared that Swedish actors have the possibilities to apply for appropriations and act in an international context. At the same time, Sweden is seeking to develop its own resources to create a safer society and simultaneously develop the Swedish security industry and innovative power.

In the light of this, and in order to meet the growing need of knowledge to create security, the Swedish government has appointed a project group to design a national strategy for security research. This project group is coordinated by Vinnova, the Swedish Agency for Innovation Systems, also the assigner of this report. The vision of Vinnova is to design a national research policy that enables for the Swedish security industry to become world market leaders in certain security industry niches.

¹ Törnqvist.S 2004

² Törnqvist.S 2004

1.2. Objective

The objective of this report is to present an analysis of the Swedish security industry, which clarifies the industry structure, identifies market growth potential and recognizes deficient industry factors in order to create a base for the national research strategy currently developed by Vinnova. The objective of this thesis can be broken down into three main objectives;

- Clarify the Swedish security industry structure and dynamics
- Identify market growth potential
- Recognize deficient industry factors

1.3. Problem formulation

The problem formulation for this report consists of three main questions derived from the objectives, which have been further developed into sub-questions. These are;

- ***What is the overall structure and dynamics of the Swedish security industry?***
 - *How can the security industry be defined?*
 - *How is the security industry developing and growing?*
 - *How can the security industry be divided and categorized into sectors?*
 - *Which are the actors and how are they interacting?*
- ***Which security industry sector has the highest growth potential?***
 - *Are there trends concerning the growth potential of the area?*
 - *What is the growth potential of the sectors?*
- ***Which factors should the government/actors concentrate their resources on to create appropriate conditions for development of a well-functioning innovation system in the sector of the Swedish security industry that has the highest growth potential?***

1.4. Outline of the report

Firstly, in chapter 2, the method used in the thesis will be presented starting with the method for the industry survey and followed by the method of the innovation system analysis. In chapter 3, the results from the industry survey will be presented and there, a sector will be chosen for further analysis. Chapter 4 concerns the innovation system analysis of the selected sector, and chapter 5 will

present the conclusions of the thesis. Finally, chapter 6 will give suggestions for future research.

2. Method and theory

The following chapter refers to the method and theory used in order to fulfil the objectives of the thesis. In this chapter, the method model for the thesis is firstly presented, followed by the method and theory used in order to conduct the industry survey. This chapter ends with the description of method and theory applied in the innovation system analysis.

2.1. Overall method model for the thesis

The purpose of this report is to clarify the Swedish security industry structure, identify market growth potentials and recognize deficient industry factors. Because of time limitations, only one security industry sector was analysed in order to recognize deficient industry factors. Therefore, the objectives of this thesis will be fulfilled in two phases, the industry survey and the innovation system analysis. As illustrated in figure 2-1, the objectives of the thesis will be formulated into three main research questions. The industry survey will cover the first two questions, while the innovation system analysis will cover the final question of the problem formulation.

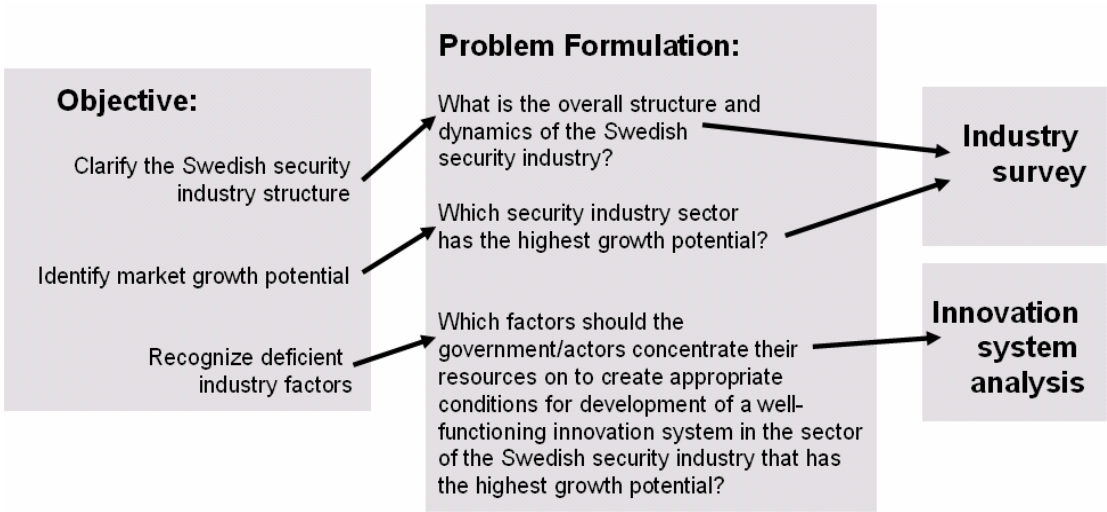


Figure 2-1 The thesis objective and problem formulation

Figure 2-2 illustrates the overall method model that this thesis is built upon and shows the two phases more directly. First, a problem analysis was conducted; which, as declared above, resulted in the problem formulation for the thesis. The industry survey was then carried out using five tools for analysis, of which four were used as data analysis tools and the fifth, the identification of a potential sector, was used for evaluation. The results from the industry survey laid the foundation for the innovation system analysis in which six tools were utilized, four

related to data analysis, and two, the system structure analysis and the functional analysis, were related to the evaluation of the innovation system. Finally, conclusions were drawn upon the results from the industry survey and the innovation system analysis.

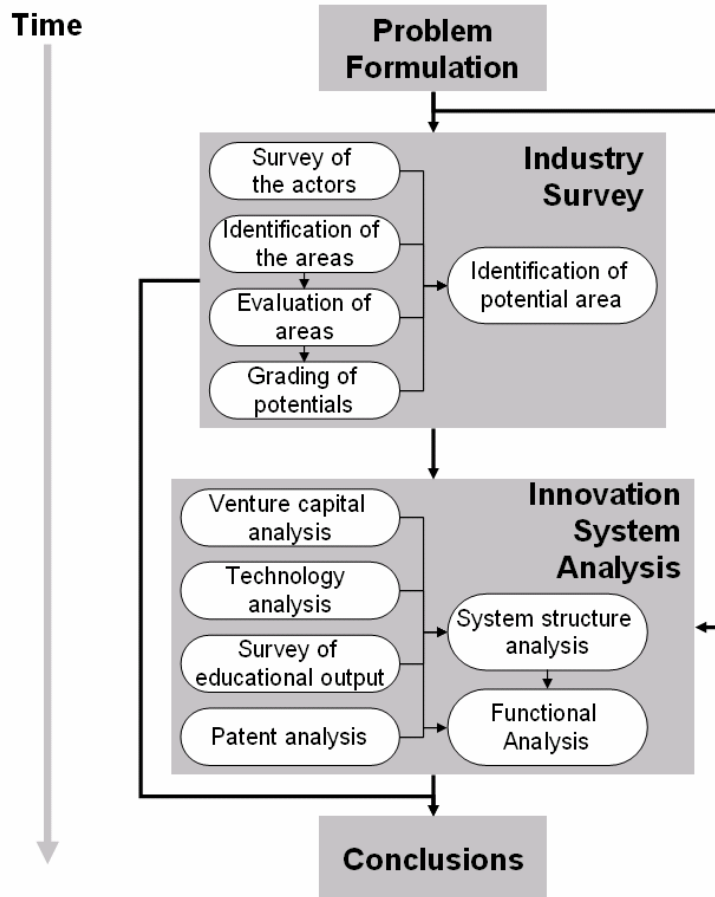


Figure 2-2 The methodical frame for the thesis

2.2. Method and theory for the industry survey

In the following section, method and theory used in the industry survey will be presented. As previously stated, the industry survey covers two main questions; what the overall picture of the Swedish security industry is and which sector of the security industry has the highest growth potential. In order to give an overall picture, the actors in the security industry were identified and surveyed. Further, the sectors in which the security industry can be divided were identified and analysed. The sectors were then evaluated and finally, following the second question in the problem formulation, one sector was identified as being the most suitable given the perceived future market potential and the perceived level of capability of the Swedish industry.

2.2.1. Identification and survey of the actors

The actors in the security industry were identified in several ways. By way of introduction, the actors were identified from the set of companies attending the hearing held by Vinnova³. Further, actors were identified from the industry association FIF and from the data sources stated below. Besides from downright utilization of search engines and databases⁴, actors were also identified by letting them name their competitors, spin-offs, partners and other actors. By doing this, a so called snowball effect was utilized for identifying new actors⁵.

Swedish owned companies or companies and firms founded in Sweden were regarded as industry actors, foreign actors in the Swedish industry were excluded. This delimitation was made since it was essential to interview people within the management group, with good insight in future company strategy. Since the timeframe for the conduction of this report was limited, no foreign companies could be interviewed, hence, this delimitation had to be made. However, few actors of relevance have been identified that do not meet these criteria. Thus, the results of this report have not been considerably affected by this delimitation.

In the survey of the actors, a number of factors were studied, like size, location, sector of activity, products and services delivered, required involvement in network and future company strategies concerning the security market. For industry actors, customer segment as well as product and technology sector were also reviewed.

Sources and data collection

To realize the identification and survey of the actors, data was collected from the Vinnova hearing⁶. Also, interviews were conducted with actors, both in person, by telephone and by mail. The main interview question structure is found in appendix A. However, these questions were alternated depending on the actor being interviewed. The internet provided information as well, since searches with Google, article searches and searches in Affärsdata and Företagsfakta were conducted. Also, a lot of information about the actors was collected from actors' homepages and annual reports.

Strengths and weaknesses in the method

³ Hearing 2004-08-19

⁴ Affärsdata, Företagsfakta and Google

⁵ Carlsson et al, 2002

⁶ Hearing 2004-08-19

Given the limited amount of time, it can be questioned if the identification and survey of the actors is complete. Due to the problem formulation, the industry survey has an inclination towards industry actors. This moved the focus of the identification of actors away from educational institutions and research institutes and it can therefore be stated that these actors are underrepresented in the industry survey. This exclusion was necessary to do given the limited amount of time and the inclination of the study towards the Swedish security industry. The second part of this report, the innovation system analysis, was more accurately conducted, and is therefore predicted to contain all actors of relevance concerning the industry sector analysed. When comparing the actors identified in the industry survey to the ones identified in the innovation system analysis, within the same industry sector, it can be declared that approximately 85 percent⁷ of the relevant industry actors have been identified in the industry survey.

2.2.2. Identification of the sectors

To be able to identify the most suitable sector for further analysis, it was necessary to divide the security industry into different sectors. Therefore, a survey on how to divide the security market was conducted in which the viewpoint on grouping into adequate sectors given by the below stated sources were considered. Based on these, and also considering the innovation system approach of the future innovation system analysis, the sectors were identified. For further description of the innovation system approach, see section 2.3.5.

As stated previously, the aim of this report is to give an accurate picture of the security industry and the possible innovation systems within it. The ability to identify possible future innovation systems depend on how the companies are grouped. Although this report will only make a deeper analysis of one sector in the Swedish security industry, providing an accurate picture of the market will help others to conduct research in other sectors not included in this report.

Sources and data collection

This identification was conducted based on information from articles, market research reports and results from preformed interviews. The main part of the articles on the subject originates from technological journals, market research reports and reports from the US Department of Homeland Security.

Strengths and weaknesses in the method

⁷ In the preliminary study 17 actors related to the sensor industry sector were identified. In the deeper analysis of the same industry sector, the innovation system analysis, four additional actors were identified. Hence 85% of the relevant actors were identified in the preliminary study.

The sources, providing the material on which the identification of the sectors is based upon, do not consider the innovation system approach. It has been stated that, in some cases, it can be difficult to identify cluster formation possibilities with standard industrial classification methods, like the one used in several of the surveyed reports⁸. Therefore, it can be argued whether the method of identifying the sectors given the innovation system approach is adequate. Even though the innovation system approach is used by the authors of this report in the process of identifying sectors, it is not the basic approach on which the surveyed sources base their identification upon. However, the method used for identification of industry sectors includes many relevant sources. The method is also appropriate since it is wide in its approach, which decreased the possibilities to overlook any sectors.

2.2.3. Analysis of security industry sectors

The first step in the analysis of the security industry sectors was to make a definition and delimitation of each sector. Also, an estimation regarding the size of each industry sector was made based on number of employees within the specific sector. This data was collected from the same sources as used for the identification and survey of the actors as described in section 2.2.1. Secondly, the actors identified in the security industry were linked to a sector based on the application and technology field in which they were active. Thirdly, the innovations system approach was used to identify the structural components that were important to consider regarding industry analysis. The innovation system approach presents three categories of structural components, actors, networks and institutions. Based on these categories, actors, customers, regulations and trends were identified in the industry survey.

Further, the actors were strategically mapped using a technique presented by Porter and referred to as structural analysis of industries⁹. The structural analysis aims at explaining differences between companies' performances and the connection between performance and strategic position. A company's strategic position is based on several dimensions. Some examples of these dimensions are listed below:

- The extent of specialization. (Customers, products and geographic markets)
- Distribution method
- Product quality
- Technological leadership
- Amount of vertical integration

⁸ Porter, M. 1998

⁹ Porter, M. 1980

By using these dimensions, a company's position can be defined. The companies that have similar strategic positions, related to the described dimensions, are regarded to be a part of the same strategic group. When company characteristics have been identified it is possible to plot the company position using a chart where the two axes represent strategic dimensions. The different companies' relative positions can then be visualized.

Porter further states that the competition within the industry is influenced by four factors.

- The interdependence between the different strategic groups, meaning to what extent different groups share the same customers.
- The amount of product diversification achieved.
- The number of groups and their relative size.
- The strategic distance between different groups within the industry.

The most unstable scenario occurs when several equally strong groups with similar strategies compete for the same customer. However, the most stable and profitable scenario takes place when a few big groups, each competing for different customers, use different strategies¹⁰.

The aim of this step was to mediate a description of each of the security industry sectors, i.e. the different actors and their customers, suppliers and partners. In this report it has also been relevant to identify existing trends in each industry sector. Therefore, the strategic analysis and strategic mapping was slightly modified to better suit the purpose of the report. The actors in each industry sector will be mapped relatively to size, customer segment and application/technology dimensions. Size of the companies is represented by the width of the ellipse based on number of employees. Customer and technology trends were visualized using arrows, which created a more dynamic picture of the industry. An exemplifying figure of the method is presented below.

¹⁰ Porter, M. 1980

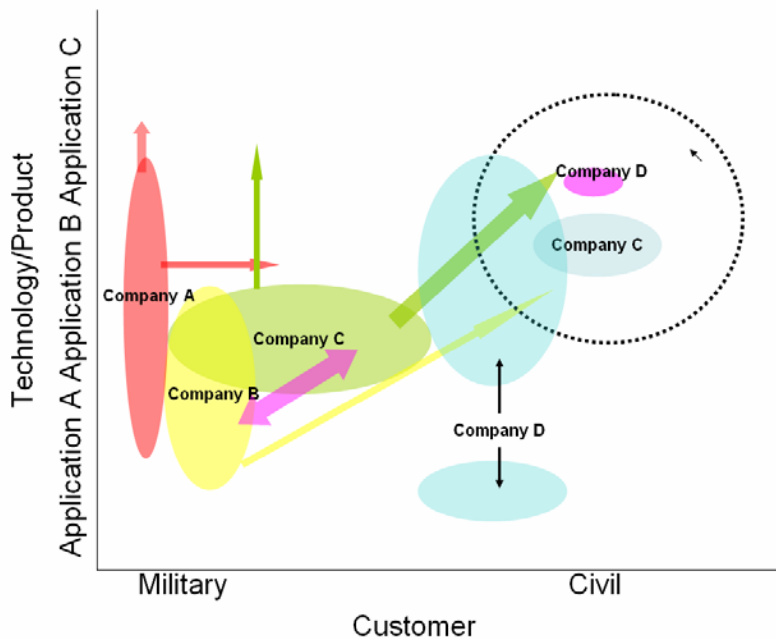


Figure 2-3 Sector mapping

The actors were arranged in the graph according to the data, regarding targeted customer segments and provided applications, that was collected as described in section 2.2.1.

Sources and data collection

In the analysis of the sectors, data was primarily collected from interviews with actors, both in person, by telephone and by mail. Also, a lot of information from the identification and survey of the actors was transferred into this step of the industry survey. Internet searches with Google and article searches were also used.

Strengths and weaknesses in the method in the method

Given the fact that the concept of the security industry is relatively new, no clear structure exists. It can therefore be argued that this obstructs the analysis of the whole industry and consequently also the analysis of each sector. However, the facts that no clear structure exist and that no similar attempts to map the industry have been identified stress the importance of conducting such mapping. Furthermore, the method correlates well with the objectives of this report, to mediate the structure and dynamics of the security industry.

2.2.4. Evaluation of sectors

To be able to identify the sector with the highest growth potential, the different sectors in the industry had to be evaluated. In this thesis, growth potential is defined with two factors, the perceived future market potential and the perceived

level of capability in the industry. For the industry to be able to grow, there has to exist a strong market potential, and to be able to take advantage of this market potential, there has to exist a high level of capability in the national industry. Therefore, these two factors will be studied in order to identify the sector of the security industry that has the highest growth potential.

Growth potential has been confirmed as a good parameter by the tutors of this thesis. Also, the vision for the Swedish security research strategy, and partly the purpose of this report, is to develop a cooperation between Swedish and international research agencies and industry actors. Further, there exists a vision to make Sweden a world market leader in at least one security business area. However, for this position to be profitable the market must show growth potential both in Sweden as well as internationally. Therefore, identifying a technology area with high growth potential is important if the vision shall be achieved.

For the purpose of sector evaluation, a self-develop model was used, where the sectors were mapped out regarding the two factors. The sectors were then located on a map with each of the factors represented on a corresponding axis, according to the results from the data sources presented below. This was made for each of the results from the three sources, namely from interviews, the hearing with Vinnova, articles and reports. Finally, the results were summed up and in a concluding map were all three results were considered.

Sources and data collection

In the application of this tool data from interviews, the hearing with Vinnova, articles and reports was used. The sectors were weighted based on these three sources, from which perceived market potential and the level of national strength were derived.

Strengths and weaknesses in the method

The major problem with this technique is obtaining objective data, given the fact that the information given during the interviews often reflects the interests of the actors. Therefore, this mapping technique only gives a perceptual picture of the evaluation of the sectors. However, the method includes many different sources which decrease the influence of the objectivity in the data. Also, the method corresponds well to this report's objectives, to find one sector where the Swedish industry can be a world leading nation.

2.2.5. Identification of potential sector

When the sector with the highest potential concerning the perceived future market potential and the perceived level of capability of the Swedish industry was

identified, two factors were considered. Firstly, conclusions were drawn based on the evaluation of the sectors. Secondly, a discussion with the project team, also the initiators of the report, led to further input on the compilation of the most potential sector.

Sources and data collection

The application of this tool was conducted primary based on the results reached using of the four above presented tools. Also, the discussion with the working team at Vinnova provided input to the process of identification.

Strengths and weaknesses in the method

Even if only a limited amount of actors were able to bring forth their opinions on the identification, these actors are among the most competent with substantial insight in the industry. Therefore, the identification of potential sector is well-founded.

2.3. Method and theory for the Innovation system analysis

In this section, method and theory for the Innovation system analysis is presented. As declared previously, the objective of this second phase of the thesis is to recognize deficient industry factors. In order to do so, the question of which functions the government and actors should concentrate their resources on to create good conditions for development of a well-functioning innovation system in the sector of the Swedish security industry that has the highest growth potential, will be answered. For this, the functional analysis described in section 2.3.7 is used, supported by the system structure analysis and the four tools concerning data analysis. The four later frameworks create a knowledgebase mainly for conducting the functional analysis, and structural analysis. The method and theory for these four functions will be presented in this section, followed by a short presentation of innovation system theory in order to give an introduction to the innovation system approach used in this thesis. Finally, the two innovation system tools, the functional analysis and the system structure analysis are presented. The following figure shows the components of the innovation system analysis and how they are related to each other.

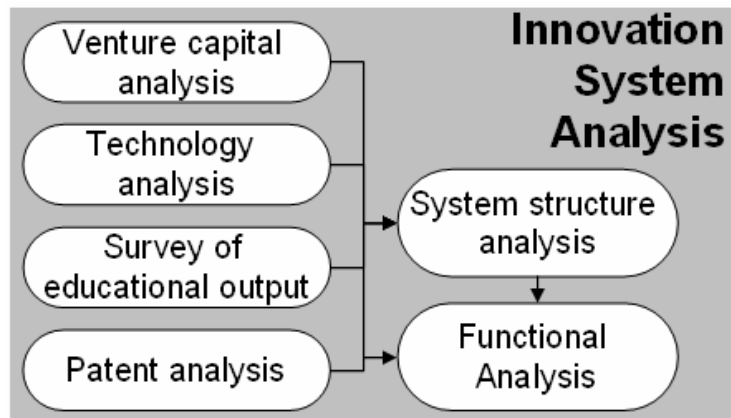


Figure 2-4 Methodical frame for the innovation system analysis

2.3.1. Technology analysis

The technology chain is a type of technology analysis method. The purpose of the technology chain is to describe the connections between technological base and market segments. The technology chain includes function, performance, application and customer advantage, which link the externalities of technological base and market segment. This framework reveals both the possibilities for technological exploitation as well as the impact of customer demand on the technology base. Generally, the technology chain analysis is based on the assumption that the company specific technological development increases its competitiveness. However, in mature industries this is not always the case. In contrary to other analytical frameworks, the technology chain analysis can easily be customized to better suit its purpose¹¹. In this report, the technology chain analysis has been slightly modified and aims at deriving technology and knowledgebase, as well as market segments from identified main functions.

Sources and data collection

The data used for conducting the technology chain analysis has been collected from various internet articles. While conducting interviews, a preliminary technology chain was presented to industry experts. Hence, industry experts have confirmed the definitions and included elements as relevant and accurate.

Strengths and weaknesses in the method

Because of the industry characteristics related to a high amount of applications and sub technologies, it has been difficult to find sources that comprehend all applications or technological aspects of the industry. However, since the relevance in the technology chain has been confirmed, it can be regarded as an accurate description of the industry. Further, this method is appropriate to use since it

¹¹ Hörstedt. F, Rickne. A, 2001

clearly presents the connection between market segments, products and knowledgebase. Such presentation is useful for defining the structure in the industry analysed.

2.3.2. Venture capital analysis

The venture capital analysis functions as an indicator of industry attractiveness related to financial investments, and investigates the venture capitalists' investment activity related to amount of resources as well as fields of investments. The analysis was conducted in four steps. Firstly, all venture capitalists active on the Swedish market were identified. Secondly, the technological fields of investment of each venture capitalist were identified. Thirdly, identified venture capitalists investing in technological fields with relevance to this report, were thoroughly examined and earlier investments of interest were identified. Finally, the venture capitalists were interviewed and asked to assess the attractiveness of the particular industry that this report concerns.

Sources and data collection

Several internet sources were used for conducting this analysis. Mainly, the home page of the Swedish Private Equity & Venture Capital Association, SVCA, was used¹². Also, every home page of the identified venture capitalists has been examined for identifying earlier and current investment projects. Some venture capitalists were interviewed and their view on the industry and its potential was revealed.

Strengths and weaknesses in the method

The limited amount of time that has been allotted to this report has inflicted limitations in number of venture capitalist that could be interviewed. Far from all venture capitalists, bearing some relevance for this report, have been interviewed. However, interviews have been conducted with the five largest firms on the national market. Even though this does not present a comprehensive picture, the interviews function as an indicator of industry assessments.

2.3.3. Survey of educational output

The survey of educational output aims at identifying trends related to the output in number of master in science graduates. By comparing national educational trends to international, a measure of the national performance can be derived. In this

¹² www.vencap.se

case, Swedish educational statistics was compared to Israeli and German statistics. Israel was chosen since they are hosting a big national security market and because they have similarities with Sweden related to size and population. Germany was chosen for their position as a very strongly industrialized country, which has cultural similarities to Sweden. Therefore, Germany presents a good criterion of comparison related to Swedish performance.

Sources and data collection

The data was collected from each country's national centre of statistics.

Strengths and weaknesses in the method

Because of the limited amount of time the survey could only include three countries. By including more countries in the survey a more accurate picture of the Swedish strength related to educational output could have been presented. Still, the method clearly reveals Sweden's performance related to one of the industrially strongest countries in Europe. Since the method was used to present a comparison of the Swedish performance, the method fulfilled this objective.

2.3.4. Patent analysis

Count of patents is one of the basic patent analysis methods. It functions as a technology activity indicator for companies or industry sectors and is of primary interest regarding competitive intelligence. If, for example, one company has more patents than its competitor in one particular technology field, it can be concluded that this company is more innovative. Therefore, the particular company can be expected to have a better position to develop new products or services based on its technological strength¹³. In the same way, counts of patents can be used for comparing competitiveness between countries. In this report, patent analysis has been conducted for establishing the Swedish strengths in technological fields related to security applications. Hence, it works as an indicator of breadth and depth of the national knowledgebase.

Sources and data collection

The patents were identified at the American States Patent and Trademark Office, USPTO. The patents in each technological field were identified by using the search strings described in appendix C. To confirm significance of the results, all national patents responding to the particular search string used, have been controlled by reviewing the title and abstract of each patent. The relevance of the search strings

¹³ Moguee. M.E, 1997

was confirmed by the fact that very few patents were identified to be divergent from the expected field of application or technology.

Strengths and weaknesses in the method

Generally, a patent analysis bears weaknesses. Firstly, cultural differences between countries affect the amount of innovations patented. For example, Japan has a tradition of using patents to a very large extent, while other countries have less intensive patenting activity¹⁴. Secondly, analysing the number of national patents does not reveal the particular importance that the patents bear, i.e. one patent can provide the same competitive advantage as a combination of several others. Therefore, only examining the number of patents might not present an accurate picture of the national knowledgebase related to specific technological fields¹⁵. Thirdly, in this report the big actors are also active in the defence industry. Military research and development often comprehend classified information. Hence, it can be argued that innovations originating from these actors will be kept a company secret instead of being patented.

Also, there are limitations derived from the vast number of patents and immaturity in the analysed market. Firstly, only one database, USPTO, has been used for identifying patents. The database covers only US patents and documents. However, in contrary to Esp@cenet which hosts worldwide patent documents, USPTO supports the complex search options necessary for conducting patent analysis related to the particular field of this report. Also, since the patent analysis conducted in this report compares the national activity between different technological fields, where no obvious differences in likelihood to seek American patents have been confirmed, the result is not considerably affected by the characteristics of the USPTO patent database. Secondly, no search string for identifying patents related to security applications could be identified. Therefore, the identification of patents related to security is a subjective evaluation given the fact that the thesis authors had to evaluate if the patented technology was applicable in a security context or not.

Still, the patent analysis presented very useful results, which were used to balance the objectivity in the results from conducted interviews. Often, the patent analysis results corresponded to the interview results. When both sources correlated, it enabled for higher accuracy in presented results.

2.3.5. Innovation System

¹⁴ Bergholtz. C, Svensson. M, 2003

¹⁵ Moge. M.E, 1997

This part will briefly review the concept of innovation system, different approaches on how to define innovation system boundaries and the dynamics of innovation systems.

In the concept of innovation system, a system approach is applied to the process of creating innovations. Hekkert et al. describe the innovation system concept as a heuristic attempt to analyse all elements, such as actors, institutions and society structures, influencing the creation of innovations¹⁶. Further, Carlsson et al. states that a system is made up of components, relationships and attributes generating, diffusing and utilizing technology¹⁷. In the case of innovation, Edquist concretizes these components, relationships and attributes in all important economic, social, political, organizational, institutional, and other factors influencing the development, diffusion, and use of innovations¹⁸.

Based on the above mentioned views of innovation system, the concept of innovation system will be defined in this thesis as follows;

An innovation system consists in a set of actors, networks and institutions that utilize create and diffuse knowledge, technology and innovations.

Delimitation of the innovation system

There are three major innovation system approaches, the National systems of innovation approach, the Technological systems approach and the Network approach. These three approaches differ when defining the components of the innovation system. The national system of innovation approach defines these components as actors, networks and institutions active within a country's physical borders¹⁹.

While the national systems of innovation emphasize the importance of geographical borders, the technology systems approach defines the system on a technology or product level. The definition of a technological system is "networks of agents interacting in a specific technology sector under a particular institutional infrastructure for the purpose of generating, diffusing and utilising technology"²⁰. This means that, in order to visualize the structure, the actors have to be grouped depending on their technology knowledgebase.

¹⁶ Hekkert. M, et al, 2004

¹⁷ Carlsson. B, et al, 2002

¹⁸ Carlsson. B, et al, 2000

¹⁹ Johnson. A, 2002

²⁰ Jacobsson S. 2004

Last, the network approach focuses on even smaller parts of the total system. These approaches can for example be used to identify existing relationship structures within a system²¹.

Further, an innovation system defined with the technology systems approach can be delimited to a specific technology, a product or application, a general-purpose technology or by a cluster of related products²².

In this report, the technology systems approach will be used and the innovation system will be delimited by a product or application. However, a national perspective will be applied given that the objective of the thesis is to be a support to the development of a national strategy for the security industry.

The development of the innovation system

The development of innovation systems can be divided into several phases of evolution. Calsson and Jacobsson identify two phases, the formative and the growth phase²³, while Hekkert et al. categorize the evolution of the innovation system in four phases, an exploration phase, a take off phase, an embedding phase and a final stabilization phase²⁴. The formative phase presented by Calsson and Jacobsson is related to the origin and early formation of the innovation. The origin of a system can be traced back to factors concerning abundance of skilled labour, unique university expertise and advantageous infrastructural conditions. The characteristics of this phase can be related to small market, diversity in the competing designs, many entrants and a high degree of uncertainties regarding technologies, markets and regulations. Also, this initial phase is characterized by the emergence of a new system in the form of an industry or an innovation system from the accumulation of many small changes in existing industries or systems. In this phase, four features for creation of a prosperous system development have been emphasized. The first one is related to institutional change and states that the creation of an innovation system requires a change in existing science and technology policy, market regulations, tax policies or standards.

The second feature is related to the market formation, also involving the development of nursing and bridging markets where improvement of price and performance of the technology can take place and where incentives for firm entry and constituency can be created. The third feature concerns the formation of technology-specific advocacy coalitions to gain ground for the new technology. To be able to create support for the specific technology in the institutional structure political networks advocating the technology must evolve. The last of the features

²¹ Johnson. A, 2002

²² Calsson. B, Jacobsson. S, 2004

²³ Calsson. B, Jacobsson. S, 2004.

²⁴ Hekkert, M et. al. 2004.

emphasized in this phase is related to the entrance of actors in the innovation system. This refers to firms, universities, and other organizations that somehow promote the new technology. In the early phase of the innovation system, these actors can play an important role referred to the process of attracting resources since a numerous actors have a greater market influence, without them it is hard to develop advocacy coalitions. This initial phase can be related to the exploration phase presented by Hekkert et al., where it is also expressed that clear directions are needed in this phase²⁵. It has also been stated that cognitive and inner core functions, like creation of knowledge and networking, are likely to dominate in this phase.

In the second, growth-related phase presented by Calsson and Jacobsson, a larger space for the growth of the innovation system has been created and it is central to fill this space. Therefore, the entry of new firm is highly essential in this phase. New entrants bring new knowledge and resources. In addition, they create so called external economies, external to firms, but internal to location. These are closer presented in the seventh function of the functional analysis referred to as the creation of free utilities. Also, new entrants strengthen the political power of the system and they may add legitimacy. Further, they create a possibility to experiment with new combinations. As the diversity grows it is highly likely that the chances for new combinations to arise also will grow. In addition, uncertainties related to markets and technologies will be reduced. In this phase, growth will occur when enough investments have been generated to initiate a change of gears and develop the system to a self-sustaining body²⁶. Hence, this phase can be related to the two phases of take-off and embedding, presented by Hekkert et al.²⁷. A take-off may be initiated by technical discontinuity, alterations in the regulatory framework or exploration of new segments or applications²⁸. Often, dominant designs appear in this phase. The take-off will start a powerful chain reaction with positive feedback loops within the system, making the process autonomous. This would be the embedding phase where there is no way back and the system becomes irreversible²⁹.

Last, the stabilization phase of Hekkert et al. is characterized by institutionalization and the system develops stable routines, infrastructure and legal framework, and becomes an established system³⁰. A typical indicator in this phase is a saturated market and for further non-incremental development, a new exploration phase is needed.

²⁵ Hekkert, M et. al. 2004

²⁶ Calsson. B, Jacobsson. S, 2004

²⁷ Hekkert, M et. al. 2004

²⁸ Calsson. B, Jacobsson. S, 2004

²⁹ Hekkert, M et. al. 2004.

³⁰ Hekkert, M et. al. 2004.

The phases described are summarized in the table below.

	Phase			
Calsson and Jacobsson (2004)	Formative phase	Growth phase		
Hekkert et al. (2004)	Exploration	Take-off phase	Embedding phase	Stabilization phase

Strength and weaknesses

Given the purpose of this report, the establishment of a national policy for enabling the creation of security innovations, the industry had to be analysed as an intra connected system, where policy changes would affect total system performance. The innovation system approach concerns the connections and relations between system components as well as their impact on the system. Therefore, the innovation system approach was considered a suitable analytical framework regarding the purpose of this report.

2.3.6. System structure analysis

After having delimited the system, the next step is to identify and analyse the structural components within the system boundaries. The structural components consist of actors, institutions and networks. Actors include commercial companies, customer and suppliers as well as research institutions, university institutions, industry organisations and public/governmental authorities³¹. Institutions consist of regulations and laws that influence the organisational structures. Networks can be either formal or informal, between industry actors or include universities and other intermediaries. The structural components influence the activities that are carried out in the innovation system. Also, the activities contribute to fulfil the functions and goals of the innovation system. These functions are more thoroughly discussed in section 2.3.7, concerning the functional analysis³².

Sources and data collection

In this framework, the sources and data collection method described in section 2.2.1 was utilized. The information related to each and every individual actor was collected in interviews, from the company homepage, and the databases Affärsdata

³¹ Jacobsson. S, 2004b

³² Carlsson. B et al, 2000

and Företagsfakta. The interview question frame for the innovation system analysis is shown in appendix B.

Strengths and weaknesses in the method

As concluded in section 2.2.1, it is almost impossible to tell if all actors, institutions and network of relevance have been identified. Depending on the industry immaturity and absence of industry organisation it has been difficult to confirm if all relevant structural components have been identified.

2.3.7. Functional analysis

The functional analysis is derived from the notion that a more dynamic view is needed to comprehend the functional mechanisms of an innovation system. In contrast to the structure analysis, which focuses on static components, the functional analysis focuses on what is actually happening in the innovation system. This focus makes it possible to break down total system performance into functional patterns, i.e. the characteristics of innovations system functions, which enables formation of clear policy goals regarding functional performance. By setting performance goals, system performance can be more easily evaluated³³.

Also, the functional analysis framework includes not only the market but also other factors influencing system performance, such as the impact of institutions and networks. The analysis enables for identification of system weaknesses, and it facilitates specification of goals of policy and key obstacles for reaching those goals. The stand point of the functional analysis is that for the system to perform well, a number of functions must be fulfilled. How these functions are fulfilled depends on the system structure, i.e. the characteristics of actors, institutions and networks which are defined by the system structure analysis. The functions that do not perform well can be targeted by policy makers to reach desirable functional patterns. Also, within each function there are factors that either decrease or increase the strength of the function. These factors can again be derived from the market, institutions or networks, and it is of special interest for policy makers to thoroughly investigate how these factors affect system performance³⁴. This report will concentrate on the factors negatively affecting the innovation system and these will be referred to as blockage mechanisms.

It should be mentioned that this analytical framework is under development. This report can be seen as one more brick in the evolution process. The exact number or definition of the functions has yet not been established, which leaves space for

³³ Carlsson.B , Jacobsson, S, 2004 and Jacobsson. S, 2004b

³⁴ Carlsson.B , Jacobsson, S, 2004 and Jacobsson. S, 2004b

improvisation when conducting the analysis. Based on the work of Carlsson and Jacobsson, (2004) and Jacobsson (2004b), the following seven functions have been identified as relevant for this analysis.

1. Knowledge development

The function describes existing knowledge within the system, related to technology application and production. The function also describes how knowledge is generated and spread throughout the innovation system. In this function the breadth and depth of the knowledgebase are evaluated, and ways to alter it to better suit current demands are identified.

2. Providing incentives and guide the direction of search

The function identifies existing incentives and drivers for actors to enter the market. Such incentives include recognition of growth potential or a strongly articulated demand. Together with standards and regulations, incentives work as guidance of the direction of search. This function evaluates the performance of existing incentives related to their ability to contribute to an increased number of new entrants. Also, it evaluates the systems ability to guide new entrants in suitable directions.

3. Promoting entrepreneurial experimentation

The function measures the number of and variety in R&D projects conducted within the innovation system. Also, it is evaluated to what extent existing companies innovate and design new applications.

4. Market formation

The function identifies drivers for market formation, i.e. identification of market drivers beyond customer demand. Also, it evaluates the characteristics of present markets, and to what extent nursing, bridging and mass markets have been formed.

5. Mobilisation of resources

The function evaluates the actors' possibilities to mobilize sufficient resources, enabling for prosperous business development. The function measures the total amount of resources within the system, related to financial capital as well as human capital and shortages of such.

6. Legitimisation

This function evaluates the legitimacy related to the industrial sector. It also identifies factors influencing the legitimacy such as factors that create acceptance and credibility for the use of the system's applications and technologies.

7. Creation of free utilities

The function identifies free utilities that have arisen from the establishment of a critical mass of actors within the system. At some point the number of actors reaches a critical mass and this critical mass self-reinforce the system by contributing to the creation of free utilities. Such utilities can take the form of specialized intermediaries and suppliers. The critical mass can also contribute to the creation of pooled-labour markets and networks as well as decrease uncertainty related to market and technology. The function evaluates the amount and strength of free utilities created within the system and is also concerned with the absence of free utilities. Often, the absence of free utilities creates uncertainty on the market and concerning the technology. Therefore, it is essential to investigate uncertainties when analysing the function since the presence of these indicates the lack of free utilities and hence, the strength or weakness of the function.

There is interdependence between the different functions. For example, increased incentives for market entry attract new entrants that in turn increase the knowledgebase, amount of resources, free utilities and strengthen the legitimacy. Increased resources, free utilities and legitimacy create even stronger incentives for market entry. This means that at some point in the evolution process, the system can produce strong feedback-loops and become self-reinforcing.

Depending on the maturity of the innovation system different functions and factors within are more or less important. As described in section 2.3.5., the innovation system could either be in a formative or growth phase. In the formative phase, it is of special importance that the functions of knowledge development, provide incentives and direction of search and market formation, are strong. In the growth phase it is critical to attract new entrants for the system to grow stronger. Therefore, the function providing incentives and guide the direction of search is of importance.

Identification and evaluation of blockage mechanisms

After analyzing the functions, the efficiency of them was evaluated by identifying system weaknesses. From these system weaknesses, the blockage mechanisms were identified by deriving the weaknesses down to the system structure of the innovation system. To further evaluate the impact on total system performance of each blockage mechanisms, a framework was developed. This framework is a

matrix that presents in what way, positively or negatively, and how strongly the identified blockage mechanisms affect each function. By this mean, the blockage mechanisms were listed in order of level of impact on total innovation system performance. Based on the results from the matrix, six blockage mechanisms, critical for innovation system growth, were identified.

Recommendations

Based on the conclusions drawn in the evaluation of the blockage mechanisms, a number of recommendations for measures against the blockage mechanisms and for enhancing future growth potential of the innovation system was presented.

The functional analysis concept

Following figure visualizes the concept that the functional analysis covers. By analyzing the system structure components through their performance in the functions describing the conduct of the innovation system, the current state of the functionality of the system can be recognized in the achieved functional pattern. The targeted functional pattern would represent the “ideal” state of the innovation system where all the functions work satisfyingly. Hence, the blockage mechanisms are the hindrances that limit the innovation system from performing ideally. By identifying functional weaknesses, the blockage mechanisms are revealed. Finally, the recommendations are based on the blockage mechanisms and applied on the components of the innovation system structure.

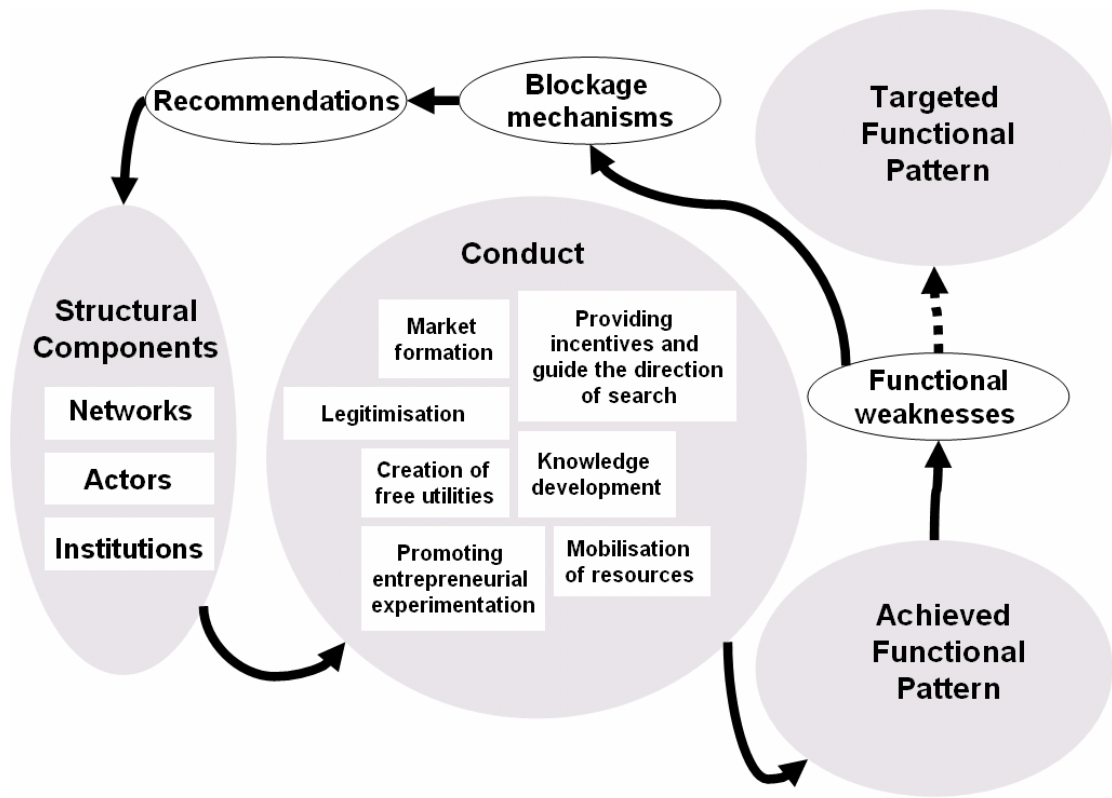


Figure 2-5 Overall structure for the innovation system analysis

Sources and data collection

In order to measure, describe and evaluate the functions and reveal blockage mechanisms, several analyses as well as interviews have been conducted. The analyses are more thoroughly discussed in section 2.3.1 through 2.3.4. The interview question frame for the innovation system analysis is shown in appendix B.

Strengths and weaknesses in the method

A major limitation is related to the evaluation of function performance. There are no clear policies for deciding each function's individual strength. The only way is to compare the particular innovation system to an identical system abroad. Since this report was given limited amount of time, it has not been possible to make this comparison. However, this problem was early on identified and measures were taken to limit its influence on the analysis. These measures were in form of comparisons of numerical data related to patents, educational output and amount of resources to international standards. Also, industry actors' assessments have given increased possibilities to evaluate the Swedish system performance. The measures taken have enabled for an accurate evaluation of the functional performance.

Regarding evaluation of blockage mechanisms, the framework used was developed by the authors of this report. However, the framework has been evaluated by experts on innovation system analysis as bearing significant relevance for this report.

Finally, the recommendations are to be viewed as guidelines for future policies. The authors of this report do not possess the political competence that would be required in order to make sharp recommendations directly useable for policy formation.

2.4. Overall evaluation and validation of used method and theory

The following sections concern the validity and reliability of the thesis.

2.4.1. Validity

This section will discuss the validity of the used method in this thesis and how well it was suited for fulfilling the purpose of this report. Firstly, concerning the internal validity, that is how well the results correspond to the real situation, the objective was to present an accurate description of the Swedish security industry structure. Since no suitable tool was identified for analysing an industry not previously defined, higher validity was achieved by using well know and highly reputable market analysis frameworks. These frameworks were altered to better suite the objectives of the report, and the alternation was approved by the tutor of this report. The final method used included all structural components sought after by the initiator of this report. This was also confirmed by the initiator. Therefore, it can be argued that the tools used for the industry survey are suitable for the purpose of this phase of the report and that they gave a correct representation of the real situation.

Concerning the choice of tools for the innovation system analysis, the main tool, the functional analysis, was provided by the initiator of this report. Further, the creators of the functional analysis suggested the data analysis tools used in the thesis. Methods used in previously preformed functional analysis were also applied in this thesis. Because the used tools have been previously used in successful terms, and were recommended by competent sources, it can be argued that the validity for them in this report is strong. However, since the method for the analysis of the innovation system was presented and not independently sought, it can be argued that perhaps a more suitable method could have been found if a more throughout search for method had been conducted.

Concerning the external validity, that is the possibility to generalize the conclusions of this thesis to other situations, the selection and amount of sources,

especially concerning interviewees, has been strictly related to the amount of time available. 46 interviews were conducted during the two phases, covering commercial, university and governmental actors, as well as networks, research institutes and customers. The validity of the study is augmented since the selected group of interviewees covers the whole spectra of the industry structure. Also, in the case of the industry survey, the fact that all the security industry sectors and all customer groups were covered in the interviews further increased the validity of the interviews. Furthermore, it is interesting to regard the reliability concerning the patent analysis. Only the USPTO database was used to conduct the patent analysis, because it is the only database currently capable of handling search strings as complex as the ones required for the conducted patent analysis. Attempts were made of using other databases, such as Esp@cenet, but it was stated that it would not be efficient considering available time. Further, the validity of the strings was confirmed by controlling a selected range of the resulting patents. By doing this, the adequacy of the strings was confirmed.

2.4.2. Reliability

Concerning reliability, this is especially interesting regarding the interviews. It can be argued that the results from the interviews somehow reflected the activities and interests of the interviewees and that this by some means creates biases in the data. However, since this is the only way of obtaining data from the commercial part of the industry, and since many of the results concurred between different actors were it was not expected, it can be argued that the data gave an accurate interpretation of the reality. Also, the same interview structure was used in all interviews. Finally, many of the interview résumés were sent back to the interviewees for confirmation of the obtained results.

3. Industry survey

This chapter concerns the results from the industry survey and starts with the definition of the security industry and classification of the sectors, followed by the presentation of each and every one of them. Further, the evaluation of the sectors is presented and this section ends with the identification of one potential sector for further analysis.

3.1. Definition of the security industry

Because this report concerns the security industry, it is of great importance to define the term of security and of the security industry.

Firstly, the new concept of security is presented in a report issued by the European Commission in the light of a number of identified key threats: Terrorism, Proliferation of Weapons of Mass Destruction (WMD), Regional Conflict, State failure and Organized Crime³⁵. This lays the foundation for the security concept used in this report. Further, Vinnova has developed a definition of the security concept in relation to the process of developing a Swedish security research strategy³⁶. This is based on the perception of security given by the European Union in connection to the work concerning the PASR. Vinnova have chosen to base their definition on antagonistic threats and acts, meaning deliberate human actions preformed by an individual, or a group of individuals. This definition is aligned with the PASR. Furthermore, Vinnova places the new security concept in between traditional police activities, for example everyday accidents and criminality, and traditional military activities, like armed attacks.

The illustration below shows the sector in which Vinnova places the new security concept, and shows the potential threats and the threatened elements worth protecting³⁷.

³⁵ Schmidt. B 2004

³⁶ Törnqvist. S 2004

³⁷ Törnqvist.S 2004

Worth protecting against antagonistic threats

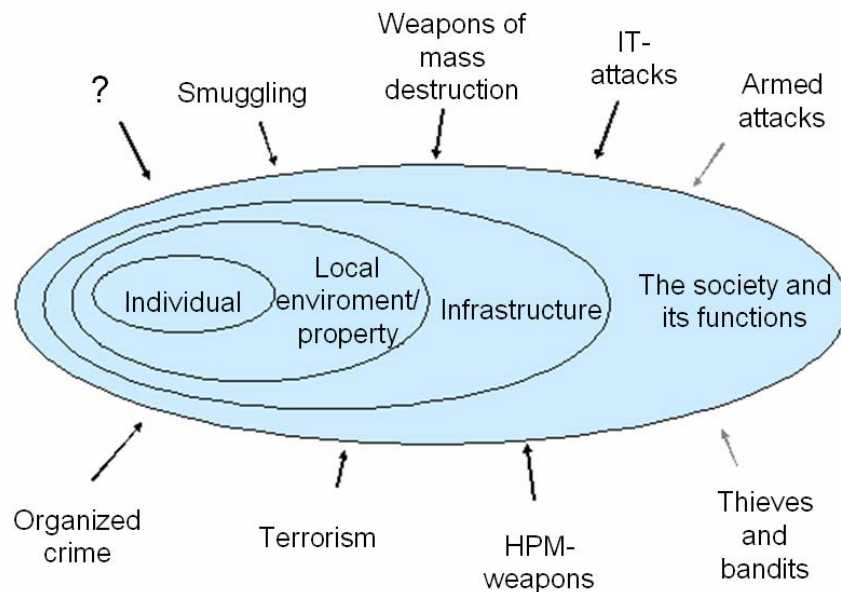


Figure 3-1 Vinnova's picture of potential threats and elements worth protecting³⁸

The Swedish emergency management agency (SEMA) officially confirms the previous described definition of the security industry. However, during an interview with Peter Stern, senior advisor at SEMA, another definition was presented. Stern mentions that the definition of the security industry must be observed from a wider point of view. All measures and methods that work to secure the society are part of the security industry. It is too narrow to define the security industry after threat and protection against antagonistic acts. The vision of the security industry should be not only to protect civil inhabitants from antagonistic acts, but to secure the entire society from a greater field of threats. Any company or actor able to supply this service or product should be regarded as part of the security industry³⁹.

Although it is interesting to use a broad approach on the security concept this would not be practical from an analytical point of view since the area of analysis would be too broad to cover and delimit. Since Vinnova is the initiator of this report, and since the majority of the actors interviewed⁴⁰ agree with Vinnova on the definition, it is of great interest to consider their definition when stating one for this particular report. Therefore this report's definition of the industry is:

³⁸ Törnqvist.S 2004

³⁹ Interview, Stern.P SEMA, 2004-09-03

⁴⁰ TeliaSonera, Ericsson Microwave, SAAB bofors Dynamics, Volvo Technology etc.

The industry, capable of providing technology, products and services in order to manage antagonistic threats and protect the society and its inhabitants against antagonistic acts, excluding unorganized crime and armed attacks.

3.2 Classification of the sectors

This section concerns the classification of the sectors based on different types of classifications and identifications found in the analysed data. As mentioned in the theory, the sources used were articles, market reports and results from the interviews and the Vinnova hearing.

3.2.1. Review of the categorization

The following section concerns the categorization presented in articles and market reports, by organizations and during interviews and the Vinnova hearing.

Categorization in articles and market reports

When reviewing the articles, two major grouping methodologies appear, one based on technology and applications and the other one on mission areas. Several articles⁴¹ divide the industry into sectors based on the different technologies used in each sector. The Civitas Group has done several analyses concerning the security industry. They use the following classification of industry sectors⁴².

- Sensor technology
- Identification and authentication technologies
- Screening technologies
- Surveillance technologies
- Tracking technologies
- Data analysis technologies
- Cyber security technologies

However, some actors have chosen to divide the market after mission sectors. The Homeland Security department has chosen to break down the market into six strategic mission sectors as follows:⁴³

- Border and transportation security
- Protecting critical infrastructure and key assets
- Emergency preparedness and response

⁴¹ For example the ones by O,Gara Company, Civitas Group. OECD

⁴² Internet, Civitas Group 2004

⁴³ Internet, Civitas Group 2004b

- Defending against catastrophic threats
- Domestic counterterrorism
- Intelligence and warning

This classification method does not consider technology when grouping the market. Hence, the same technological solution can be used in two different sectors. An example is sensor technology that can be applied in both border- and transportation security and in protecting critical infrastructures and key assets⁴⁴.

The Civitas group classification is based on the architecture of the Department of Homeland Security (DHS), and shows mission based sectors in which the private sector can play an active role⁴⁵. Because DHS is a vast actor, the architecture of their organization can symbolize the architecture of the security industry. The following figure shows where the private sector can be involved in the security industry.

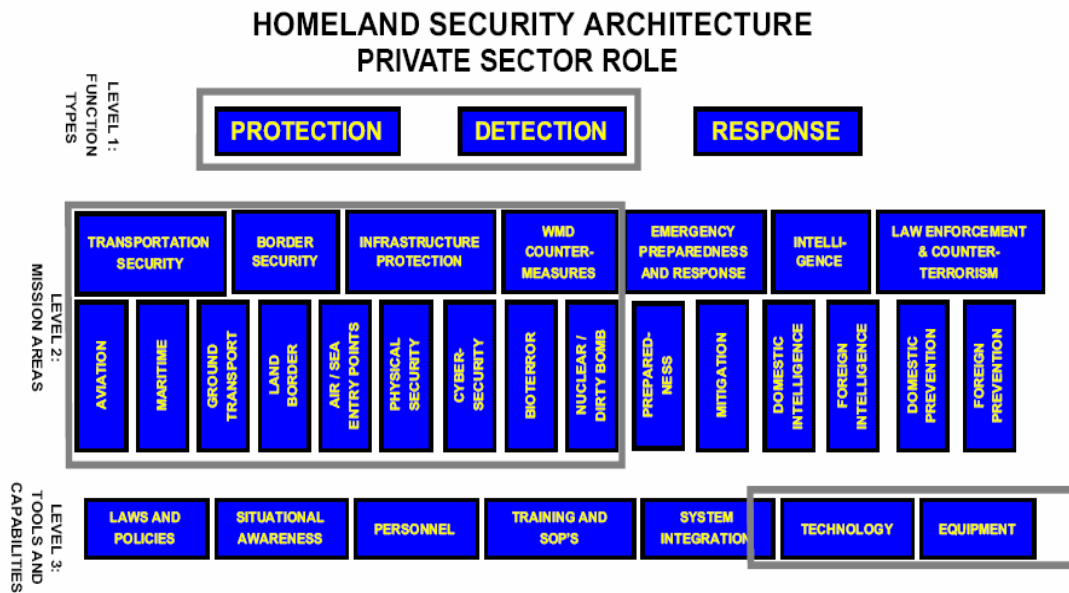


Figure 3-2 Illustration from Civita report 2004⁴⁶.

According to figure 3-2, the private sector's role, marked by the squares in the figure, is to provide technology and equipment to protect and detect threats in the transportation- and border security, as well as infrastructure protection and counter measure sectors. Studying the figure, possible grouping methods could either be influenced by company's function type (protection or detection), by mission sectors or by tools and capabilities. For a narrower grouping, a combination of two or all three levels could be used.

⁴⁴ Internet, Civitas Group 2004

⁴⁵ Internet, Civitas Group 2004

⁴⁶ Internet, Civitas Group 2004

Categorization by organizations

The Swedish equivalence to the DHS, The Swedish Emergency Management Agency, SEMA, divides their organization into six mission, or coordination sectors. These are⁴⁷:

- Technical infrastructure
- Transport
- Spreading of dangerous infectious matter, toxic chemicals and radioactive matter
- Economic security
- Co-ordination, interaction and information by sector
- Protection, rescue and care.

Another point of view that provides an aspect of the classification is the division of the business activity area of the Swedish Defence Research Agency, hereafter referred to as FOI. Their organization consists of ten divisions of which two are support functions for the research conducted, and one, Defence Analysis, is analytically oriented. The seven remaining are technologically oriented and presented as follows⁴⁸:

- Combat simulation
- Systems technology
- Command and control systems
- Weapons and protection
- NBC Defence
- Aeronautics
- Sensor technology

Further, this report originates from an identified need for Europe to use its technological strengths to build the capabilities enabling increased security in times of peace. This need is articulated in the PASR. The European Union identifies five sectors in which research shall be conducted to increase security within the European Unions physical borders⁴⁹. These five sectors are:

- *Improving situation awareness*, (surveillance of physical borders as well as surveillance and tracking of goods by using sensor technology)

⁴⁷http://www.krisberedskapsmyndigheten.se/english/documents/facts/planning_for_societys_emergency_management.pdf 2004-09-14

⁴⁸ www.foi.se

⁴⁹ Commission communication, 2004

- *Optimising security and protection of networked systems*, (Develop standards for assessing threats to critical networked infrastructures as well as develop protection and detection capabilities)
- *Protecting against bio- and chemical terrorism*, (Develop technology for detection and identification and containment of threatening substances as well as development of models of large scale dispersion.
- *Enhancing crisis management*, (Development of shared information management tools for increasing efficiency in emergency situations)
- *Achieving interoperability and integrated systems for information and communication*.

These above described sectors could also represent a somewhat broader classification of the security industry and the different activities within it.

Categorizations made during interviews and the Vinnova hearing

Results from the interviews with industry actors showed that few are aware of how to classify the industry. However, there are some examples of classification given during the interview sessions and other conventions with the industry. During the Vinnova hearing⁵⁰, a discussion about the principal technological strengths of the Swedish security industry took place. This discussion resulted in a classification, related to technology, into the following sectors.

- Under water technology
- Biotechnics
- Complex systems
- Sensor technology
- Mobile solutions

However, this only shows a classification of the sectors in which the Swedish security industry has its strength and do not cover the entire industry. Other technological sectors, not in this case referred to as Swedish strengths, were left unmentioned.

3.2.2. Synthesis on industry classification

The empirical review presented two major ways to group the companies in the security market. These were classified after technology (or application), or after

⁵⁰ Hearing, 2004-08-19

mission sector. The technology sectors identified in the empirical review are presented in figure 3-3. The marked sectors on the right represent a summarization of the technology sectors presented in this section.

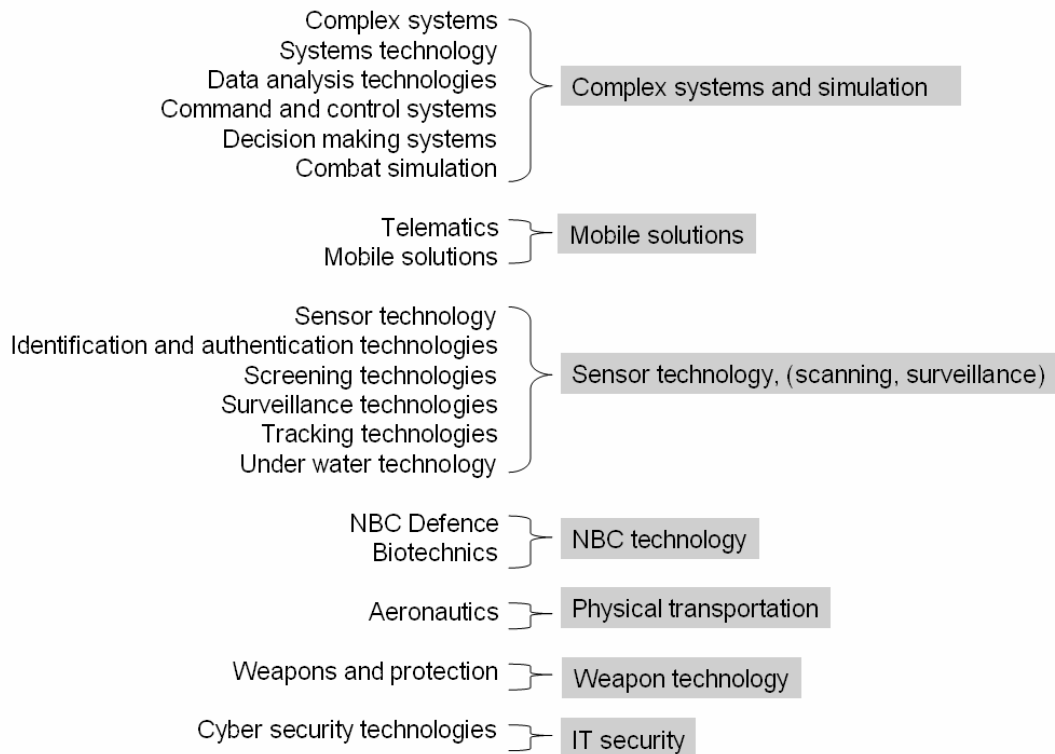


Figure 3-3 Technological classification of the security industry, based on empirical results

In the same way, the mission sectors can be summarized as shown in the following figure.



Figure 3-4 Mission based classification of the security industry, based on empirical results

3.2.3. Choice of industrial classification

When deciding on how to group the industry, it is important to consider the purpose of the innovation system analysis⁵¹. This report's purpose is to contribute to the development of a Swedish security research strategy. Regarding the companies active in this industry, a vast majority is operating in technologically intense fields of activity. Therefore, it can be argued that these companies conduct research in their specific technology field. Hence, it is of great importance to use the technological bases as a fundamental point of view when classifying the industry.

Secondly, this report makes use of the concept of innovation systems, and the goal of an innovation system is to create innovations through the establishment of flows of resources, information and knowledge⁵². However, for the flow of these three factors to be meaningful it has to be related to the particular companies' main interests. A great majority of the companies in the industry are technologically intense and are therefore highly interested in their technological field. Hence, it can be argued that any other grouping than by technology or application would

⁵¹ Interview Jacobsson 2004, and Edquist. C, 2004

⁵² Lecture innovation systems, 2004

counteract with the purpose of this report. Also, the technology and application grouping approach facilitates the conduction of the analysis.

Several articles and security market researches have used above stated approach when grouping the actors, which further confirms the legitimacy of the this decision. Also, literature describing innovation systems have used this approach to set the system boundaries.

Thus, in this report, the security industry is divided into the following eight technological sectors.

- Complex systems (system integration) and Simulation
- Mobile solutions
- Sensor technology, (scanning, surveillance)
- NBC technology, (counter measures to NBC weapons, vaccines and remedies)
- Physical transportation and surveillance
- Weapon technologies
- IT security

These sectors are a summarization of all sectors presented figure 3-3. Therefore, it can be argued that no important sector has been excluded. Also, this report later identifies companies in each sector, active in the security industry, meaning that no sector is superfluous.

To reveal how the different sectors are functioning in the context of security, the following figure was developed, showing the different sectors' characteristics as applications. The threat is menacing the society and the applications that are in direct relation to the threat are the ones related to NBC technology, sensor technology, weapon technology and IT-security. These applications can detect the threat, as in the case with sensor technology applications or counteract to the threat, as with weapon technology. In the case of the applications related to IT-security and NBC technology, both detection and counteraction is covered. Further, the concept of simulation, i.e. training and creation of scenarios, is more method related. Hence, it appears in the area in between the society and the threat. Physical transportation is the application linking the society to the threat by carrying forward the applications in direct relation to the threat, namely to NBC technology, sensor technology, weapon technology and IT-security applications. Further, mobile solutions is concerned with the links between the elements of the model, representing the need for communication. Complex systems and system integration is also concerned with this activity, though the application covers more that that since it also includes integration of systems. Hence, the applications of complex systems and system integration are represented by a wide area covering the whole space between the society and the threat,

indicating the integration aspect of the applications. The application of physical infrastructure and transportation are considered to be a national part of the existing infrastructure. Hence, they are not directly related to security and therefore not included in the security industry.

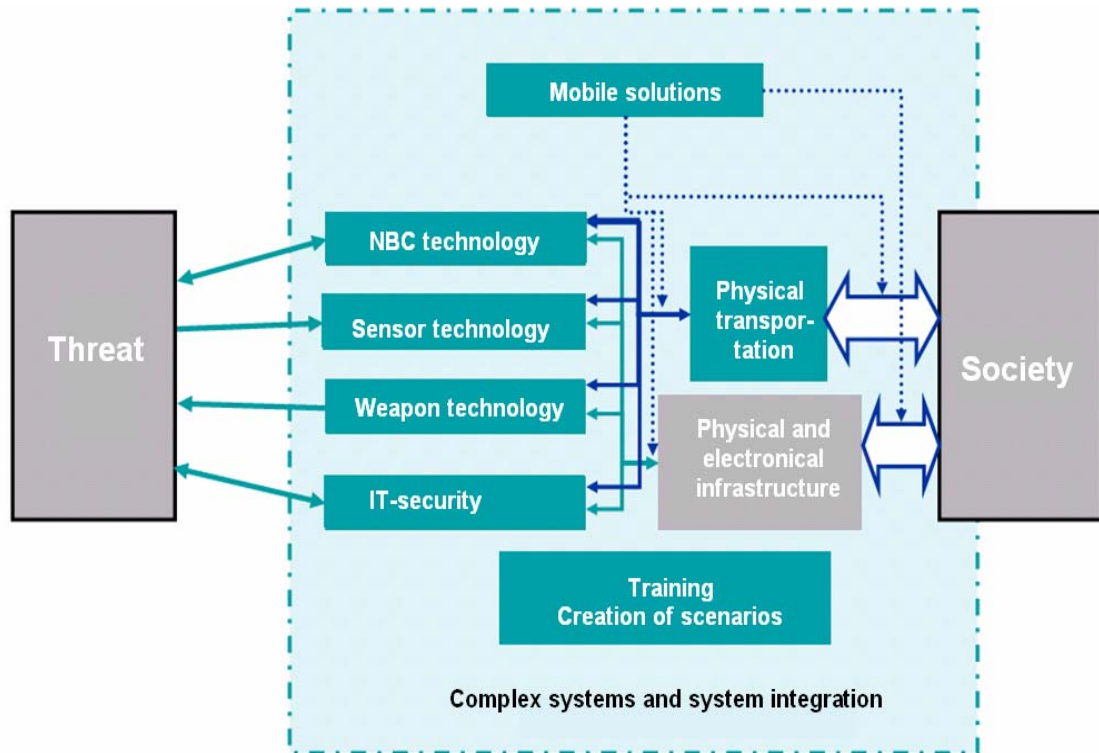


Figure 3-5: The sectors presented in the security concept

3.3. The security industry sectors

In the following subchapter, the sectors of the Swedish security industry identified in the previous chapter will be briefly presented in order to give an overall picture of the Swedish security industry. This chapter will lay the foundation for a selection of a sector for further analysis. The aspects on the sectors presented here are, the industry definition, technology and application, actors, customers, related regulations and trends, possibilities and hindrances for the sector and strength of the Swedish industry. Finally, the section will be concluded by visually mapping the actors and related industry trends.

The subsections are information dense and the main characteristics of the industry are therefore summarized in the following table.

	Weapon Technology	Sensor Technology	Complex Systems and simulation	IT-security	Mobile Solutions	Physical Transportation	NBC- Technology
Number of actors	8	21	19	24	12	7	5
Number of employees	2050	2000	6875	2000	2400	6645	210
Technology and applications	Countermeasures Anti-terrorist weapons Consulting	Tracking Under water Surveillance Screening Identification Sensor systems	Command and control Simulation Surveillance and Information	Protection Identification Strategy/Policy	Telematics Mobile-solution- software Mobile communication- stations	Naval technology Land vehicle technology Aeronautical and aviation technology	Biological Chemical Nuclear Radiological
Customers	Defence Police Transportation Large events	Defence Airports Seaports Governments authorities Civil companies	Defence Civil agencies Larger companies	Defence Private sector Civil companies Government authorities	Defence Truck industry Nations Government authorities	Defence Government authorities	Defence Governmental authorities
Regulations	Ådalen ISP	ISP EU-regulations on increased safety in harbours and airports.	Data protection- act Ådalen ISP	ISO-standards	Existing cell- phone and network technologies standards	ISP Swedish maritime safety inspection Swedish aviation safety inspection	BTWC CWC NSG ISP
Trends	More civil applications and customers.	Sensor systems Automatic systems More civil applications and customers.	Larger systems, Higher- complexity	Perceived strong future threat. Increased need for protection. Market consolidation	Fewer investments More cooperation Need for encryption	Stealth technology. Dual-use vehicles Unmanned vehicles	Project Biofield Higher security consciousness
Possibilities and hindrances	The Ådalen regulation	Lack of standards and coordination and integrity discussion.	NBD Incompetence among agencies Lack of standard	Unrealized threat	Decreased legitimacy	Ådalen ISP Lack of coordination	Lack of engagement among authorities
Industry strengths	Strong national industry	Strong national industry	Very strong national industry	Moderate	Strong national industry	Very strong national industry	Moderate

3.3.1. Weapon Technology

The following section concerns the sector related to weapon technology and applications.

Definition of the sector

“The industry capable of providing technologies and products in the form of weapons or neutralizers of weapons as well as providing services for reducing the impact of armed attacks, in order to protect the society and its inhabitants against antagonistic acts.”

Technology and Applications

Mainly, the weapon technology industry as defined in this section includes activities related to anti-terrorist weapons, countermeasures and consulting activities. This section will more thoroughly describe the included technologies and applications.

Countermeasures come in many forms. Currently, the aviation industry is the largest application area for countermeasures. Today, there exist several different technologies for protecting aircrafts from missile attacks. Laser technology seems to be the dominating technology. This aircraft protection technology combines sensor technology for identifying the missile and uses low power lasers to mislead it⁵³. It is also possible to release diversification targets from the aircraft in order to mislead missiles, which is a technology developed by Saab Technology⁵⁴. Another application area of countermeasures concerns protection of strategic buildings and sport or other big events. During the 2004 summer Olympics in Athens, the city was constantly protected by air to surface missiles. Such protection system consists of a detection or sensor system integrated with a weapon system⁵⁵.

In the weapon technology industry, development of urban-war weapons is an important field regarding protection against antagonistic acts. Earlier, war was fought on the battlefield. Today, a probable scenario is urban-war where enemies and civilians are mixed together. This calls for new and more precise weapons. Today, it is possible to use weapons with very concentrated firing power. Such weapons increase the ability to avoid civil casualties, which also makes them suitable as anti terrorist weapons⁵⁶.

⁵³ Pröckl. E, 2004

⁵⁴ Pröckl. E, 2004b

⁵⁵ Interview Hans Rehnberg, Saab Bofors Dynamics, 2004-09-15

⁵⁶ Interview Hans Rehnberg, Saab Bofors Dynamics, 2004-09-15

Regarding consultant services, several actors active in the weapon technology industry produce and develop weapons for military purpose. Hence, they possess a profound know-how in weapon technology. This know-how can be reversed engineered and used to protect and preserve instead of attack. Such know-how can be implemented when reinforcing buildings or when conducting vulnerability analysis⁵⁷.

Actors

There are a total of seven Swedish companies active in the industry⁵⁸. There are 2050 employees in the weapon technology industry. Saab Bofors Dynamics and Bofors Defence are the two big actors. Saab Bofors Dynamics is recognized for its development of precision engagement weapons. Bofors Defence develops, among other things, air defence missiles and smart ammunition⁵⁹ manufactured for today's modern warfare. Also, FOI is to be regarded as an actor.

Customers

Currently, all the sectors in the security industry have both civil and military customers. Concerning the military customers, the Swedish material administrator, FMV, is the purchasing agency. Since 9/11 international airports have stronger needs for upgraded security products including explosion containments. Furthermore, airports are not only concerned about detection of explosives. Also, procedures for handling the situation that follows when a bomb is detected are requested. Furthermore, police authorities and transportation companies are potential customers of explosion containments⁶⁰.

Regarding protection of civil aircrafts, the Department of Homeland Security is by far the major customer. The DHS invests 675 million Swedish crowns in the development of civil aircraft protection technology⁶¹.

Regarding countermeasures like ground-to-air missiles, defence agencies are the customers. However, in Sweden this can create some problems if the technology is to be used for civil purposes. This specific problem, related to the Ådalen regulation.

Regulations concerning the sector

⁵⁷ Interview Hans Rehnberg, Saab Bofors Dynamics, 2004-09-15

⁵⁸ Företagsfakta

⁵⁹ A form of high precision weapon.

⁶⁰ <http://www.dynasafe.de/explosion-containment-airport-security.html>

⁶¹ Pröckl. E, 2004

In Sweden, the weapon technology industry is indirectly affected by several regulations. The act of Ådalen, restricts any military involvement in civil or police matters. This means that the military is not authorized to prevent or hinder antagonistic threats or organized crimes⁶². However, the regulation is being debated. A proposal to allow military influence in civil matters has been suggested. If this proposal is to be accepted, it can affect the weapon technology industry positively. The know-how of using these weapons exists in the military, and it would be a waste of knowledge not to use these resources when dealing with antagonistic threats⁶³. Another implication of such decision would be the possibility of using the so called network based defence, hereafter referred to as the NBD,⁶⁴ for dealing with threats to society that does not originate from armed attack by other countries. As a result, the NBD would achieve a greater application area.

The Swedish agency, the National Inspectorate of strategic products, hereafter referred to as ISP, affects the sector with mainly two regulations. The first one concerns the trade, production and export of military equipment. Also, the agency limits the possibilities of exporting military products of dual use, i.e. products and technology that are possible to use both in civil and military contexts. Therefore, the weapon technology industry can be limited by this regulation⁶⁵. On an international level the European Union has several regulations that play a similar role.

Trends concerning the sector

In modern defence, the number of personnel and weapons is not the critical factor. Instead, efficiency related to resources and system integration as well as coordination is emphasized⁶⁶. Also, the weapon technology industry has to seek new market opportunities, since the defence customer's demand is decreasing. Still, regarding the national market, the act from Ådalen can restrict the growth potential of the civil market⁶⁷.

Generally, the civil market is growing and more civil applications are emerging. As mentioned previously, new high precision weapons are being developed for acts in urban environments and ground-to-air missiles for protecting large events⁶⁸.

⁶² http://www.aff.a.se/vf014_21.htm

⁶³ Interview Hans Rehnberg, Saab Bofors Dynamics, 2004-09-15

⁶⁴ A system that integrates defence functions and resources and works both as a surveillance and an information system and a command and control system.

⁶⁵ Interview Hans Rehnberg, Saab Bofors Dynamics, 2004-09-15

⁶⁶ Försvarsindustrin en del av säkerhetenolitiken, utgiven av sveriges försvarsindustriförening

⁶⁷ Interview Hans Rehnberg, Saab Bofors Dynamics, 2004-09-15

⁶⁸ Interview Hans Rehnberg, Saab Bofors Dynamics, 2004-09-15.

Possibilities and hindrances for the sector

Currently, the act of Ådalen and the act regulating export of dual-use products impose the greatest hindrances for development. Weapon applications, as defined in this section, ought to be handled by highly trained personnel, currently found in the military. Also, the act of Ådalen restricts military involvement in civil matters. This fact limits the civil security market for such applications. However, these regulations might be changing providing a more suitable business environment for market development.

Strengths of the Swedish industry in the sector

Swedish defence industry is characterized by very high technology competence. Few countries can develop the same kind of high quality technology defence products as Sweden. JAS-Gripen may be the strongest proof of this, but Sweden also has an advanced position in smart ammunition and anti-tank weapons⁶⁹.

Mapping the sector

Each circle represents a company and the size of the circle is related to the size of the company. The arrows symbolize trends in customer and technology areas. The thickness of the arrow symbolizes how strong the trend is.

⁶⁹ Försvarsindustrin en del av säkerhekenolitiken, utgiven av sveriges försvarsindustriförening

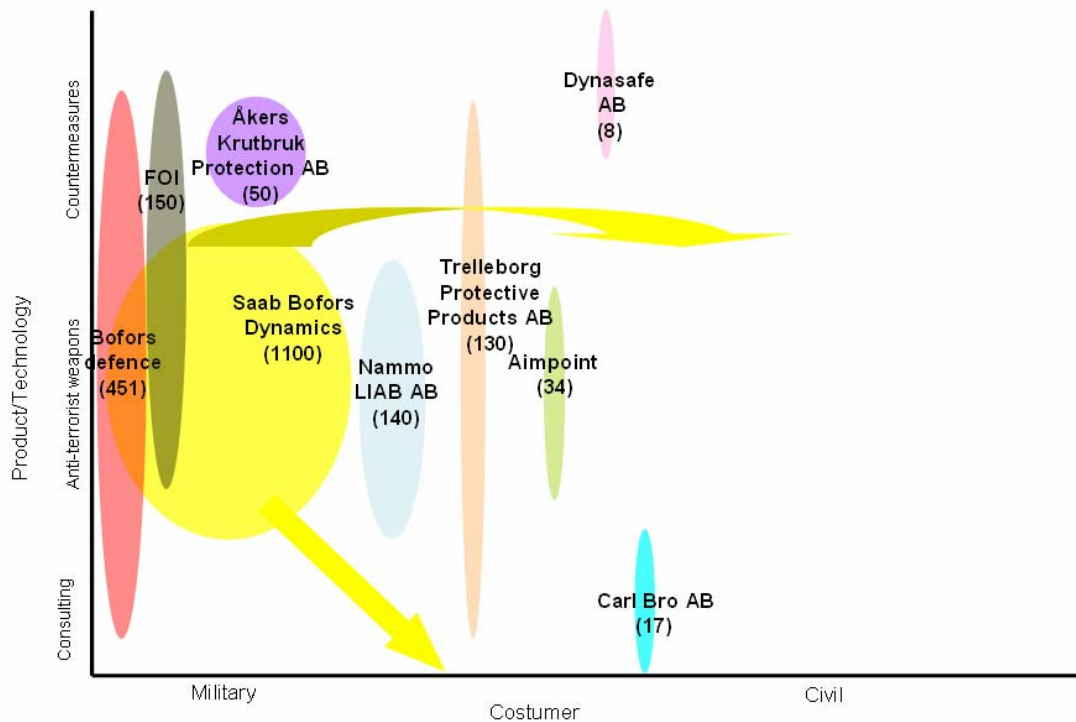


Figure 3-6 The weapon technology sector

Figure 3-6 illustrates the previously mentioned national industry sector dominance of Bofors Defence and Saab Bofors Dynamics. Also it illustrates the acknowledgements made by Saab Bofors Dynamics regarding predicted market potential of the civil security market, represented by the arrows.

3.3.2. Sensor Technology

This section concerns the security industry sector related to sensor technology and applications.

Definition of the sector

“The industry, capable of providing applications for detection of antagonistic threats, consisting of elements for detection and elements for signal processing that clearly quantify the detection.”

Technologies and Applications

There are several technological and application sub-areas included in the sensor industry sector. These are identification- and authentication-, screening-, surveillance-, tracking- and under water technologies and applications.

Identification and authentication technologies include fingerprint scanning, iris scanning and face scanning technologies, also referred to as biometrics. Considerable research efforts are taking place in this particular field of technology. Border control and security as well as protecting physical infrastructure are two major mission areas where this technology can increase security⁷⁰.

Screening technology mainly includes metal detector-, bomb sniffing- and x-ray technologies⁷¹. Newly developed technologies, like terahertz screening, are also categorized as screening technologies. These technologies facilitate detection of weapons and malicious substances. Airport and seaport security as well as protection of strategic buildings are typical application areas⁷².

Radar and IR technologies are the most well known surveillance technologies. Surveillance technologies can early on detect potential threats. Integrated with other technologies, they can create an invisible barrier around strategically important physical assets. They can also work together with ground-to-air missile defence to protect big events, as for example the Olympic Games⁷³.

The tracking technologies are GPS, RFID, bar-coding and WI-FI. These technologies can contribute to safety by enabling tracking of goods as they move through the supply chain⁷⁴.

Finally, under water applications consist of under water sensors enabling detection of intruders. Its application area is mainly harbours, which today lack an existing system for harbour entrance protection.

Actors

In Sweden there are four strong actors involved in sensor technology. These four are Ericsson Microwave, SAAB Bofors Dynamics, Biacore and FOI Sensor Systems.

Today, Ericsson Microwave's business area related to sensor technology is mainly aviation radar systems and surface surveillance systems⁷⁵. Further, SAAB Bofors Dynamics develops synthetic aperture radar, (SAR). Other business areas within SAAB Bofors dynamics related to sensor technology are IR-technology and under water sensor technology⁷⁶. Also, Biacore is the largest national actor referred to

⁷⁰ Interview, Jan Erik Dimming, Gunnebo, 2004-09-08

⁷¹ Internet, Civitas Group 2004

⁷² Interview Johan Tellander, Scancon Security 2004-09-03

⁷³ Interview Hans Rehnberg, Saab Bofors Dynamics, 2004-09-15

⁷⁴ Internet, Civitas Group 2004

⁷⁵ Interview Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

⁷⁶ <http://www.saab.se/dynamics/node4054.asp>

biosensors, and has several applications for enhancing security. Furthermore, FOI Sensor System is prominent in several technological fields related to sensor development.

Currently there are approximately 21 companies active in the Swedish security sensor industry⁷⁷. The total number of employees in this industry sector is about 2000.⁷⁸ 75 percent are employed at Ericsson Microwave (1500). FOI, SAAB Bofors Dynamics and Biacore are hosting approximately 150 to 200 employees each.

Customers

Like in all the sectors of the security industry, the customers of the sensor industry sector can mainly be classified as military or civil customers. Concerning military customers, the Swedish defence has traditionally played an important role as a strong and competent customer. Also, the development of the NBD, has increased the military needs for sensor applications.

Regarding civil customers, air and seaports have strong needs for improved screening technologies. Up until now, it has not been possible to detect non-metallic weapons, explosives and other dangerous substances. However, sniffing technologies are currently used for this purpose at several international airports, as for example Heathrow. The electronic sniffer senses a passenger carrying explosives, narcotics or other band substances. Further, there are additional sensor technologies increasing airport security like the new terahertz sensor technology, which enables seeing through passenger's clothes without exposing them to radiation⁷⁹.

An additional big group of customers are government authorities. The Swedish coastguard is looking for new advanced technologies for detection of border exceeding criminality. Also, they have a strong need for more sophisticated surveillance techniques. The Swedish custom has acknowledged the importance of intensified security in order to fulfil the USA-initiated regulations concerning a safe flow of goods through seaports to end destination. This means that the Swedish custom could also be seen as a customer to the security industry.

Finally, there are several minor customers. Sensor technology can be useful in many situations where an increased security is sought after. Fingerprint technology is for example installed at several company offices⁸⁰. Also, sport events and concerts can use sensor technology to increase security.

⁷⁷ www.foretagsfakta.se.

⁷⁸ It is hard to estimate how many from Saab and Ericsson actually involved in sensor technology.

⁷⁹ Pröckl. E, 2004c

⁸⁰ Interview Dimming Janerik, Gunnebo, 2004-09-08

Regulations concerning the sector

Since 9/11, Euro control, together with the aviation industry, has addressed several security implications affecting the sensor industry. Also, there are several existing standards specifying which security products shall be available at international airports. Such standards enhance the legitimacy and the development possibilities for security sensor applications.

As mentioned above, the European Union has decided to implement a regulation concerning the security at seaports. It specifies what security measures that have to be implemented at seaports in order to be declared as safe. Important parameters among the new rules are implementing goods control, conducting security analysis and security plan of action⁸¹. A new regulation is being developed and is to be implemented in 2006. It advocates extended security including underwater protection⁸².

Further, as in the case with weapon technology, the sector of sensor industry is affected by the regulation of the ISP, since security sensors often fall under the category of dual use or strategic products.

Trends concerning the sector

Like in many of the other security industry sectors, the large defence industry actors have identified the potential of the security industry and are repositioning themselves. Ericsson Microwave is clearly repositioning their activities, cutting down on products and technology for military purpose and expanding the civil applications. SAAB Bofors Dynamics, as well as Ericsson Microwave, is strongly connected to the military industry. Also, Saab Bofors Dynamics has experienced the military cut downs and are now looking for new customers. Saab Bofors Dynamics has identified the most probable civil customer segments⁸³, and has started to analyze each area to identify future growth potential. These areas are protection of national infrastructure and strategic buildings, protection of civil aircrafts and civil ships and protection of big events.

FOI is also looking for new customers although not in the same extent as Ericsson Microwave and SAAB Bofors Dynamics. In order to improve efficiency in the productification of FOI research material, they seek to improve their connection to the Swedish civil industry.

⁸¹ www.swedfreight.se/forstasidan/om_isps.doc

⁸² Interview Kajrud, Katrin; Göteborgs hamn AB; 2004-09-09

⁸³ Interview Rehnberg, Hans; Saab Bofors Dynamics AB; 2004-09-15

Regarding technological trends, there is a main trend in the sensor industry regarding targeted application areas. The trend is clearly pointing towards the transformation of military technology into civil applications. For example, the underwater sensor technology was developed to hinder Russian submarines from violating Swedish coastal areas. This called for a sensor that could operate in shallow waters. Today, the threat from Russia has considerably declined, and new application areas have emerged. Such an area is seaport security, where no underwater protection currently exists⁸⁴. This trend is also confirmed by leading actors⁸⁵.

Further, FOI implies that less research is conducted on component level and more on a system level. FOI predicts that the next generation sensors will be complex sensor systems⁸⁶. Today, many sensors work as autonomous systems. But as FOI implies, the trend is pointing towards an integration of several sensors into one big system.

Regarding the biometrics technology, it seems to be a probable area for potential growth during the next coming years. The technology has already been implemented at international airports. Furthermore, a new passport developed for the European Union membership countries will be released in 2005. This new passport will be provided with programmed data chip containing the passport owner's face contour⁸⁷, augmenting the demand for biometrical sensor solutions.

Possibilities and hindrance for sector development

Both Ericsson Microwave and SAAB Bofors Dynamics state that the local and government authorities will be important future customers. A common opinion within the sensor technology industry is that the lack of coordination among authorities is a big hindrance for industry development. The sensor industry needs large resources for research and development, and it seems impossible to create the amount of resources needed when the authorities act on their own⁸⁸. Further, it has been mentioned that many of the civil agencies do not understand the new and changing threat and the possibilities given by the technology to cope with it. Many of the companies perceive inertia among the agencies concerning this issue⁸⁹.

⁸⁴ Interview Eriksson, Anders; FOI; 2004-09-13

⁸⁵ Interview, Rehnberg, Hans; Saab Bofors Dynamics AB; 2004-09-15, Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02, and Eriksson, Anders; FOI; 2004-09-13

⁸⁶ Interview Eriksson, Anders; FOI; 2004-09-13

⁸⁷ Pröckl, E, 2004c

⁸⁸ Interview Rehnberg, Hans; Saab Bofors Dynamics AB; 2004-09-15 and Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

⁸⁹ Interview Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

However, in some areas there is extensive collaboration between authorities. For example, there exists an official cooperation between international airports concerning security procedures and products⁹⁰. Eurocontrol demands increased and better security procedures and products. Such regulations coordinate the customer, and create interesting fields for company investments. This enhances the possibilities for increased market development. Almost every actor interviewed makes inquiries about increased coordination between of government authorities. While this inquiry is identified in every area within the security industry, it is not considered to be a specific industry sector issue.

Secondly, it can be argued that surveillance and tracking technologies violates personal integrity. Today, technology to survey the entire USA exists, but very few would like to see that implemented. The problem is to define when the technology favours the public and when it is violating personal integrity. It is possible to imagine a scenario where the public is in favour of surveillance technology, but where social changes quickly turn the technology into something that it was not intended for. Therefore, personal integrity is an important issue to discuss. Since 9/11 the threat seems more realistic, but will the public still be in favour of surveillance in ten years time, and if not what will happen to all surveillance technology installed?⁹¹

Strength of the Swedish industry in the sector

Sweden is prominent in several sensor technologies, especially related to radar applications. For example, Ericsson Microwave is world leading concerning numerous radar applications⁹². Also, Saab Bofors Dynamics and FOI are officially acknowledged as very competent sensor actors. This fact is confirmed by Saab Bofors Dynamic's leading position in European sensor development projects⁹³. Furthermore, Sweden hosts a relatively large number of biosensor actors. Even if these actors are relative small in size, they possess very high technological competence⁹⁴.

Mapping the sector

Figure 3-7 concludes the industry sector. The actors in the sensor industry are mapped below.

⁹⁰ Interview Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

⁹¹ Interview Dimming, Janerik; Gunnebo AB; 2004-09-08

⁹² Interview Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

⁹³ Interview Eriksson, Anders; FOI; 2004-09-13

sensor, Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22

⁹⁴ interview, Holmberg, Per and Karlsson, Magnus; Applied Sensor Sweden AB; 2004-10-19, Månsson, Per; Biosensor Applications Sweden AB; 2004-10-13

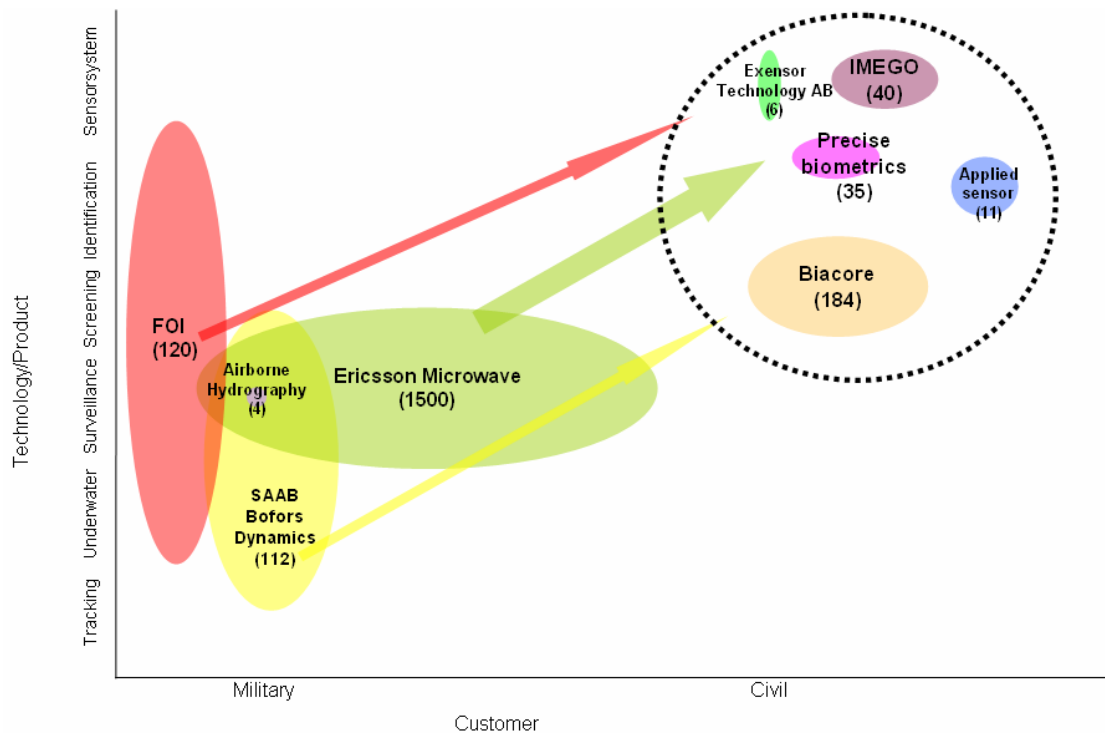


Figure 3-7 The sensor technology sector

As previously described, in the past few years, military resources have been constantly cut down. Therefore, the main actors in the sensor technology industry seek new customer groups. Ericsson Microwave is clearly repositioning their activities, cutting down on products and technology for military purpose and expanding in civil applications. Also, Ericsson Microwave predicts that the next generation sensors will be sensor systems⁹⁵. Hence, these trends direct Ericsson Microwave towards the segment represented by the dotted circle. Further, FOI has identified the trends concerning sensor applications and customer segments and is moving in the same direction as Ericsson Microwave.

If the predictions from Ericsson, SAAB and FOI are correct, a big group of companies will compete in the upper right hand corner of figure 3-7, where sensor systems are supplied to civil authorities and companies.

3.3.3. Complex systems (system integration) and Simulation

The following section concerns the security industry sector related to complex systems (system integration) and simulation.

⁹⁵ Interview Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

Definition of the sector

“The industry, capable of providing technology, products and services to facilitate the co-ordination and decision-making as well as the learning in order to protect the society and its inhabitants against antagonistic acts and their consequences.”

Technology and applications

The main technology concerning simulation is naturally computer science and programming. On the other hand, complex systems and system integration is a highly multifaceted area, and concerning complex systems, it refers more to the method of integrating elements than to a certain kind of technology. In this case it can be related to physical compatibility and integration between components, but also to the connection between information systems. Hence, the technology scope related to this concept is broad. IT and several forms of programming have frequently been mentioned as supporting technologies in these types of systems.

Concerning applications, three types have been identified. These are integrated surveillance and information systems, command and control systems and simulation systems. The main focus today is on the NBD. This type of system is both a surveillance and an information system and a command and control system. The simulation systems have mainly two functions, partly as decision-making systems and in simulations for training. Also, simulation systems can be used for scenarios analysis.

Actors

A total number of 19 producing actors are active in this industry sector. The largest actor in number of employees is Saab Aerotech telub with a workforce of 2350. The following actor referring to size is Saab Bofors Dynamics with 1181 employees. In total, the sector employs 6875 people. However, it is hard to classify which actors that belong to this sector given the somehow diffuse field covered.

Customers

As mentioned previously, the NBD is dominating the present scene in the sector, resulting in a pronounced cooperation among many companies. In this case, the Swedish defence is the customer and Saab, IBM and Ericsson are the main suppliers. In order to realize the project, Saab Ericsson NBD Innovation AB, was created⁹⁶. Other concerned actors are hoping to be a part of this project in the future.

⁹⁶ Interview Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

Furthermore, international defence agencies constitute essential customers, together with other national and international civil agencies. Larger companies and other critical functions for the society are also potential customers as they demand integrated surveillance systems and emergency and security management plans. An example is the Swedish rescue service agency. Also, the Swedish national defence demands systems for training and simulation.

Regulations concerning the sector

Due to the broad field of sub-technologies and the diffuseness of the concepts of integration and systems, it is difficult to identify specific technology based regulations. However, the Data Protection Act somewhat impacts the sector. There are also regulations concerning the information sharing among authorities and organizations, which limit the possibilities of integration of information and therefore obstruct the development of the sector. Also, the earlier mentioned Ådalen-regulation influences the performance of the sector since the regulation limits the integration between civil and military systems⁹⁷. For the companies with a military background active in the area, the previously mentioned agency ISP is a strong regulating force on the market⁹⁸.

Trends concerning the sector

Currently, there is a clear trend towards increased integration regarding all kinds of systems. An example is the integration of sensor systems with command and control systems⁹⁹. The development of component is changing from application oriented towards integration oriented, where the primal quality of the component is the ability to be integrated in a system¹⁰⁰. The systems are becoming larger and more complex, which puts a greater focus on securing the system itself¹⁰¹.

There is also a trend in the sector towards finding new civil applications, especially when it comes to network based solutions. Once again, the problem regarding this is regulations concerning authorities and their information and material sharing¹⁰².

Another trend is the higher level of autonomy in the systems when more of the integrating and information-handling functions, traditionally controlled by humans, are being substituted by technology¹⁰³.

⁹⁷ Interview Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

⁹⁸ <http://www.isp.se/nyaengelska/indexeng.htm> 04-09-17

⁹⁹ Interview with Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

¹⁰⁰ Interview with Eriksson, Anders; FOI; 2004-09-13

¹⁰¹ Interview with Rehnberg, Hans; Saab Bofors Dynamics AB; 2004-09-15

¹⁰² Interview with Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

¹⁰³ Interview with Rehnberg, Hans; Saab Bofors Dynamics AB; 2004-09-15

Possibilities and hindrances for the sector

Firstly, the organization in the sector is perceived as shattered. Further, another limitation related to the industry development is that the national market is considered to be too small and insufficient to function as a starting market¹⁰⁴. The decrease in resources that has characterized the Swedish defence market the last couple of years is also influencing this sector, as the strong and competent customer is fading. As described in the previous section, actors in the market perceive a lack of insight in the security concept among civil authorities, which makes it difficult to detect the need of the civil market.

Secondly, another identified hindrance is a perceived lack of knowledge in the method of using available technologies among governmental agencies. It is a somehow common opinion among companies that authorities, especially local authorities, lack the ability of utilizing technology¹⁰⁵.

Finally, it is also mentioned that the lack of standards is hindering the development of the industry sector. This is the case not only regarding the technology, but also in the purchasing process where the huge amount of disconnected authorities and their limited economical resources affect the smoothness of the process¹⁰⁶. Many companies demand a clearer customer and perceive a weakness in the will of national authorities to do something about the matter¹⁰⁷. This inquires greater cooperation among local authorities in order to give them purchasing power. A good example of integration found abroad is the US Department of Homeland Security which integrated a great amount of authorities¹⁰⁸.

Strength of the Swedish industry in the sector

In general, Sweden is a leading nation concerning IT, which is an often used technology in system integration considering information networks. Besides, the concept of system integration is regarded as one of Sweden's technical strengths¹⁰⁹. The deregulation of the national defence market has led to an increase in export among the companies in the sector. This has strengthened the role of the Swedish companies as international actors¹¹⁰. This is quite characteristic in this sector given

¹⁰⁴ Interview with Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02 Tor Ehlersson, Ericsson Microwave, 04-09-02

¹⁰⁵ Interview Friberg, Nicklas; C-ITS AB; 2004-09-06

¹⁰⁶ Interview Rehnberg, Hans; Saab Bofors Dynamics AB; 2004-09-15

¹⁰⁷ Interview Friberg, Nicklas; C-ITS AB; 2004-09-06

¹⁰⁸ Interview Rehnberg, Hans; Saab Bofors Dynamics AB; 2004-09-15

¹⁰⁹ Hearing, 04-09-19

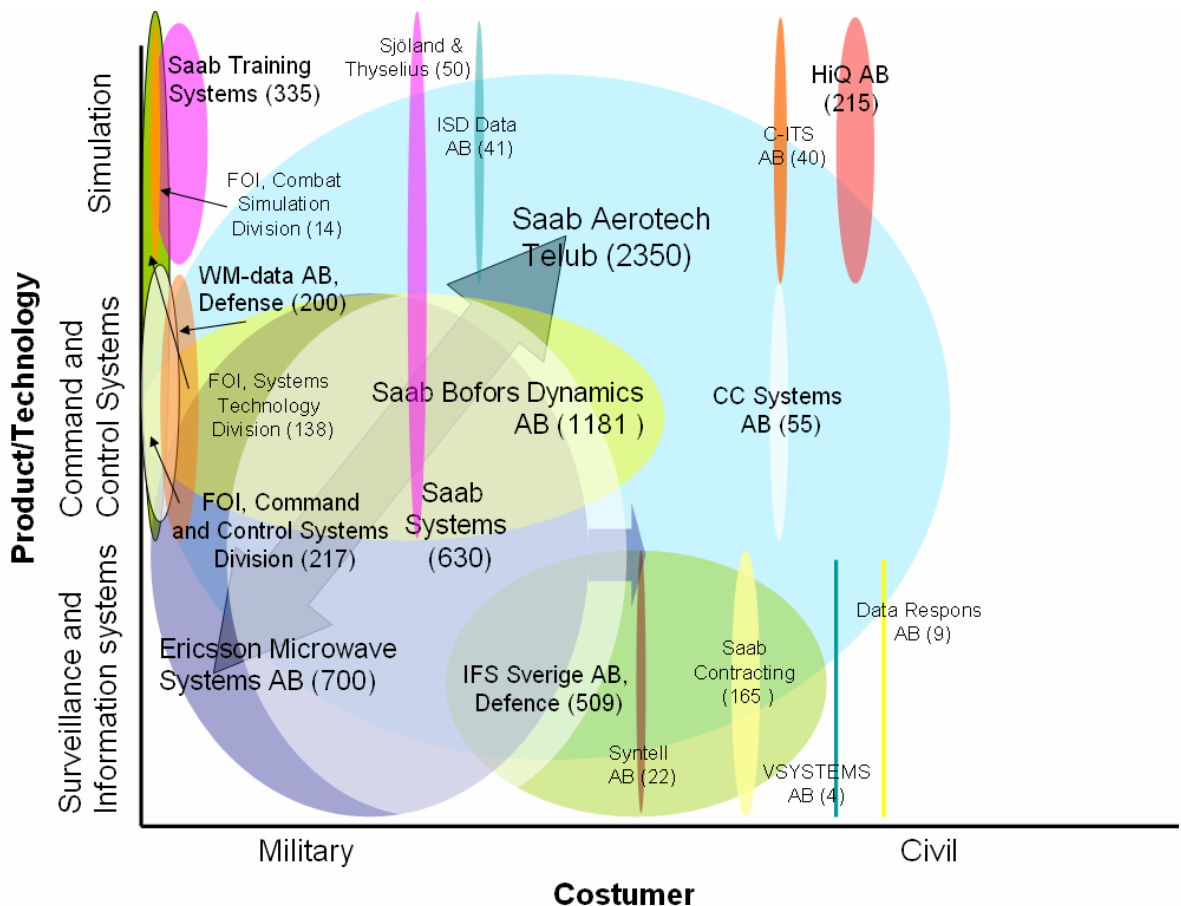
¹¹⁰ Svensk försvarsindustri, 2004

the facts that many of the active companies come from a purely defence-oriented background.

Mapping the sector

The following illustration shows the mapping of the companies. As shown in figure 3-8, Saab Aerotech Telub constitutes the biggest actor, covering all the technology and application fields of the sector. The cooperation between this company and Ericsson Microwave Systems related to the NBD is illustrated by the big double-arrow. Ericsson Microwave Systems has previously had an exclusive defence orientation concerning customers. However, this is changing, illustrated by the arrow pointing towards the civil customer segment. Worth commenting is also the rather intense concentration of companies in the upper left corner of the map.

Often, there are close relations among the companies in the sector and they frequently interact as consumer-supplier, as well as joint-venture-partners in purchasing processes. Often, the customer's needs require cooperation among the companies¹¹¹.



¹¹¹ Interview with Tor Ehlersson, Ericsson Microwave, 04-09-02

3.3.4. IT-security

This section is concerned with the sector of the security industry related to IT-security.

Definition of the sector

“The industry capable of providing technology, products and services to protect computerized information, systems and services against antagonistic acts”.

Technology and applications

There are mainly three different fields of applications related to IT-security. The first one, referred to as protection, includes applications protecting against viruses, spam and high power microwave weapons. The second set of applications, called identification, concerns system protection against intruders. The last one concerns methods, enabling for risk analysis and development of IT-security strategies and is referred to as strategy/policy¹¹².

Protection against virus and spam is achieved by installing anti virus programs or firewalls. These products and technologies are often used to solve customer specific problems¹¹³. Another form of protection is the one related to high power microwave, HPM-weapons. These are weapons that destroy IT-systems by generating a powerful electromagnetic wave¹¹⁴.

Concerning larger systems, intrusion protection is an important issue. By using identification technology it is possible to hinder intruders from breaking into information technology systems¹¹⁵. Identification technology consists of either personal electronic codes or of fingerprint and other biometric applications. It is also possible to protect the system from intruders by using products with built-in security. Examples of such products are, Secured messaging, Digital identity, and Digital signature¹¹⁶. However, for larger systems, it is often not enough to solely use security applications as the only protection against antagonistic acts. Large systems need continuous security methods, including security analysis and security policies¹¹⁷.

¹¹² Interview Axelsson, Björn; IT-företagen; 2004-09-19

¹¹³ Interview Axelsson, Björn; IT-företagen; 2004-09-19

¹¹⁴ <http://www.eme.se/> 2004-09-15

¹¹⁵ Interview Axelsson, Björn; IT-företagen; 2004-09-19

¹¹⁶ <http://www.nexus.se/sweden/files/Arsredov2003.pdf>

¹¹⁷ Interview Axelsson, Björn; IT-företagen; 2004-09-19 and <http://www.nexus.se/sweden/files/Arsredov2003.pdf>

Actors

In the Swedish IT-security industry there are approximately over 200 companies. However, the majority of them are relatively small. 24 companies have more than 20 employees¹¹⁸. The largest companies are, Proact Datasystem, and Technology Nexus. Also parts of TeliaSonera are related to IT-security and are to be regarded as a main actor¹¹⁹. The total number of employees among the 24 largest companies is close to 2000¹²⁰. About 40 percent of the employees are employed in some of the three largest companies presented above. The Swedish Computer association and the IT-security council are the two main industry associations active in this area.

Customers

Generally, it is hard to divide this sector related to civil and military customer segments. In fact, everyone with a computer and access to internet is a customer. However, the solutions for these customers differ. In the private sector, big and middle sized companies have strong needs for more sophisticated security solutions. In the consumer market, the biggest need is related to technological security products and less importance is placed on security strategy and policy¹²¹. There is also a strong relation between the type of threat and the potential customer. The threat stretches from information warfare, where the government is targeted, to recreational hacking, which mainly affects private persons¹²². The private sector market is estimated to be four times as big as the government sector¹²³.

Regulations concerning the sector

There exist several ISO standards regarding maintenance and management of information security. One example is the ISO/IEC 17799:2000 that provides recommendations for information security management on how to provide a satisfactory IT-security¹²⁴.

Trends concerning the sector

¹¹⁸ [WWW.foretagsfakta](#), search string, datasäkerhet, IT-säkerhet

¹¹⁹ Interview Björkman, Conny; TeliaSonera AB; 2004-09-07

¹²⁰ [WWW.foretagsfakta](#), search string, datasäkerhet, IT-säkerhet

¹²¹ Interview Axelsson, Björn; IT-företagen; 2004-09-19

¹²² <http://courses.washington.edu/i498aa/slides/15>

¹²³ Internet, Civitas Group 2004

¹²⁴ <http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html>

The risk of a terrorist cyber attack is not fully understood. Still, it is a fact that terrorist are becoming more technically competent, which makes the threat even more potential¹²⁵.

Internationally, there are trends towards increased needs for identification and autentification technologies and products. Among others, TeliaSonera recognizes a need for computer integrated biometrics applications, which would enable for improved possibilities for identifying network users. There is also an international trend towards that more competent customers are approaching. In Sweden the IT-security customers have not taken the threat for real. Hence, they have not been willing to invest in IT-security. However, this is changing. Currently, it is possible to identify trends showing that the potential customers have started to understand the seriousness of the threat¹²⁶.

In Sweden, there are mainly three trends identified related to future technological needs and methods. Today, the great amount of spam and viruses on the internet is an immense problem. This problem is also likely to persist in coming years. Therefore, there exists a strong need for improved viruses and spam programs, both derived from the private- and government sector¹²⁷. Secondly, as the IT-security policies and strategies in the private and public sector are implemented, there will exist a need for tools enabling for inspection of functionality of implemented strategies and policies. Finally, in the future the mobile security has to be improved. This can be done using technology for encryption of information in mobile networks. Today, it is not recommended or safe to communicate classified information via mobile communication networks. Improved security in this area would result in a safer information flow. The private sector has also recognized the need for this type of security in order to increase business efficiency¹²⁸.

Furthermore, there is a trend towards market consolidation and strong collaborations. This year Dimension AB was consolidated with Proact AB¹²⁹. Another common trend is the extensive networking with US companies within the industry. Both Nexus and Cygate have Cisco as a premium partner¹³⁰. TeliaSonera and Nexus are partners with Microsoft, and TeliaSonera regards Microsoft as an indispensable partner. Because of Microsoft's dominating market position, it is very hard to develop IT-security solutions without insight in Microsoft's activities¹³¹.

¹²⁵ Internet, Civitas Group 2004

¹²⁶ Interview Björkman, Conny;TeliaSonera AB; 2004-09-07 and Piazza.P 2003

¹²⁷ Interview Axelsson, Björn; IT-företagen; 2004-09-19

¹²⁸ Interview Axelsson, Björn; IT-företagen; 2004-09-19

¹²⁹ www.dimension.se

¹³⁰ www.nexus.se, and www.cygate.se, 2004-09-03

¹³¹ Interview Björkman, Conny;TeliaSonera AB; 2004-09-07

Finally, it can be mentioned that several IT-security networks are currently forming. These networks will host several of the large national actors, and aims at introducing IT-security issues to top management levels¹³².

Possibilities and hindrances for the sector

One large identified hindrance is that customers do not realize the impact of the IT-related threat. Many intrusions in companies' computer networks remain unnoticed. There is a need in the market for a simulation tool that shows the financial effects of IT-related crimes. Such tool could both show which actors or areas that need increased protection, and which that do not. Too much security when not needed results in inertia in every day business activities. Therefore, such a simulation tool would strengthen the IT-security business, because it would be possible to show on increased customer efficiency¹³³.

Strength of the Swedish industry in the sector

Thanks to the early existing telecommunication infrastructure, Sweden is internationally a leading country in the IT-industry. Sweden has several prominent companies in the field and is expected to remain among the leading nations related to this technological field¹³⁴. However, even if Sweden is overall strong regarding IT, it has not been possible to confirm that this is also the case regarding IT-security applications. Also, there is a tendency that the industry development in Sweden is slowing down, and other OECD-countries are approaching. Still, Sweden is a very strong country in the mobile security industry¹³⁵. Also, several companies active in authentication and encryption have very promising solutions, which are applicable in IT-security contexts.

Mapping the sector

The map presented in figure 3-9 summarizes this section.

¹³² Interview Axelsson, Björn; IT-företagen; 2004-09-19

¹³³ Interview Björkman, Conny; TeliaSonera AB; 2004-09-07

¹³⁴ http://www.itforetagen.se/pdf/Sverige_20_Visionsdel_030701.pdf, 2004-08-26

¹³⁵ Bergin, E., 2003

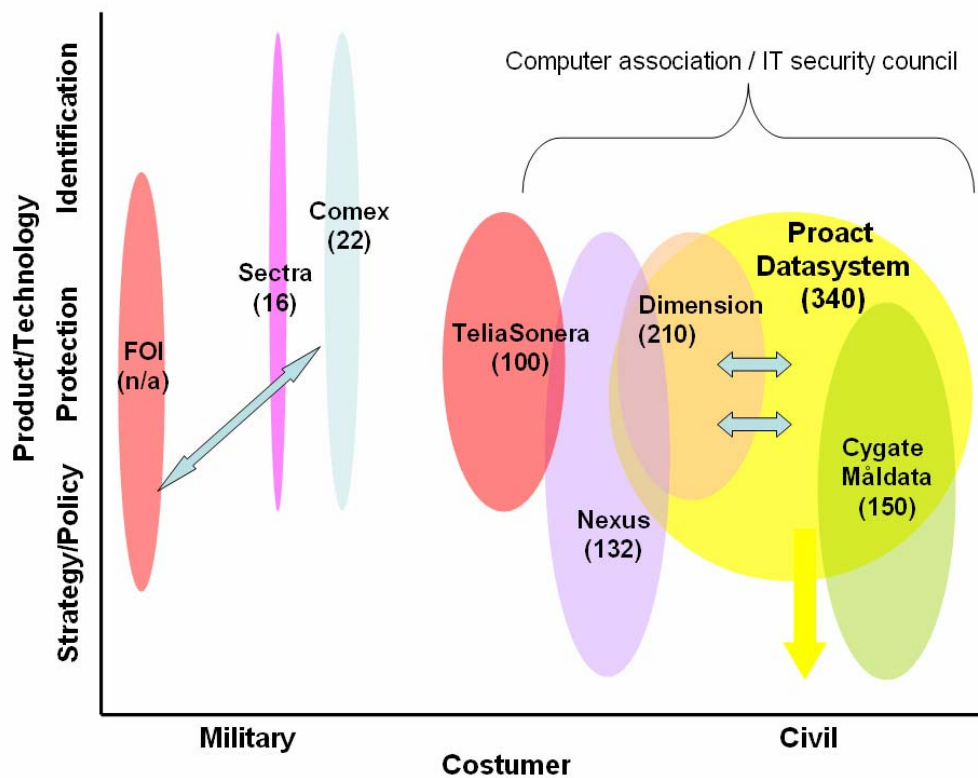


Figure 3-9 IT-security

The map concludes that very few companies offer identification or authentication technologies in order to prevent intruders from entering networks. This can have its explanation in that the technology is still very young and under development. However, Comex is an exception. The company offers advanced fingerprint technology for preventing unauthorized access to company networks¹³⁶.

It was earlier described that it exists a need for secured mobile communication. Sectra is a company that provides this kind of solutions. They have installed stationary encryption devices for mobile communication for the military¹³⁷.

3.3.5. Mobile Solutions

Definition of the sector

“The industry capable of providing technology, products and services related to mobile communication to better equip the society and its inhabitants in events of antagonistic acts.”

¹³⁶ http://www.comex.se/itsakerhet_tilltradeskydd.asp, 2004-09-02

¹³⁷ <http://www.sectra.se/security/>, 2004-09-06

Technology and Applications

In this industry sector it is hard to define which mobile products and solutions should be included. For example, a simple mobile phone can have very high security significance if handled for distress calls¹³⁸. However, the product is not designed for a security purpose, and therefore not included as such in this report. The same argument can be used for mobile positioning systems. Since this report will also discuss the industrial sector of complex systems, the mobile solutions industry analysis has limited to telematics, mobile communication stations and mobile solution software.

Telematics is a combination of data technology and telecommunication technology, and can be divided into four groups, vehicle areas, parent area network, home area network and local area network¹³⁹. But, it can also be divided according to the services provided by the technology as security, productivity, mobility, and comfort service areas¹⁴⁰. In Sweden, telematics is often related to the motor vehicle industry, which is the largest application area today. Regarding this industry telematics can be divided after five application areas. These are safety, maintenance, navigation, efficiency and information¹⁴¹. This report is off course focusing on the safety applications. The safety applications available today are SOS-alarm button installed in cars, automatic SOS-notification in case of collisions and direct connection to towing services. Telematics can also be used when help is needed for example in case of truck-hijackings¹⁴². Furthermore, telematics can enable for tracking particular vehicles, carrying dangerous goods, which further increases security.

Secondly, mobile solutions can also consist of mobile communication systems, as for example mobile GSM stations. These stations enable for establishment of communication networks when such is not available. The application area for this kind of technology could for example be when some part of society is attacked and existing network is destroyed. Another technology within this field of technology is WLAN which enables for the establishment of ad-hoc communication networks. Such network can be used among a group of people situated out of range of the stationary communication network¹⁴³.

Finally, software for mobile applications can be designed for security purposes and is therefore included in this report. The software facilitates information handling

¹³⁸ Interview, Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

¹³⁹ Interview, Oderland, Ingvar; Ericsson Microwave Systems AB; 2004-10-15

¹⁴⁰ <http://www.ad.se/index.php?serv=foretagsfakta>

¹⁴¹ Internet, Henriksson.O et al, 2003.

¹⁴² Interview, Rosenqvist, Mats; Volvo Technology AB; 2004-09-06

¹⁴³ Interview Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

via mobile communication networks. Software and encryption techniques are also an important issue for efficient mobile solutions¹⁴⁴.

Actors

In the mobile solutions industry, as defined in this section, there are six major actors on the Swedish market. Ericsson is the dominant actor in both telematics and mobile communication solutions. Ericsson Automotive is part of the Telematic valley cluster, a cluster formation in Gothenburg. The cluster involves 56 member companies, including Saab Automobile, Telia Mobile, Vodafone, Volvo Car Corporation, Volvo Global Trucks and Vägverket¹⁴⁵. The number of large companies involved can be regarded as an indicator of the industry potential. Because a majority of the companies involved in the industry are part of larger corporations, it is hard to appreciate the total number employed given the difficulty in identifying the number of employees that are active in concerned sector within the companies. Still, approximately 1000 people work with telematics in the Telematic valley¹⁴⁶. The total size of the entire mobile solution industry is estimated to be 2400 employees.

Customers

Regarding telematics, the customers are found in the car and truck industry. Both SAAB and Volvo are investing in telematic services. Today, Volvo offers this technology on their new premium class models. There are around 600 users of this service in Sweden today¹⁴⁷. Individual logistic companies can also be regarded as customers. Today, there is a strong need in the logistic industry for this kind of application. In Europe a truck is hijacked or stolen every second minute. This means immense losses for the logistic companies as well as traumatic situations for drivers. Therefore, there is a need for well functioning telematic systems¹⁴⁸.

Customers for mobile communications systems are firstly nations and big organisations. Both the UN and the USA have shown interest in buying the mobile GSM stations that Ericsson is producing¹⁴⁹.

Regarding ad-hoc communication systems, the potential customer would be government authorities that, in time of crisis or in situations where no

¹⁴⁴ Interview Axelsson, Björn; IT-företagen; 2004-09-19

¹⁴⁵ <http://www.ad.se/index.php?serv=foretagsfakta>

¹⁴⁶ Internet, Ryberg, J, 2002

¹⁴⁷ Internet, Ryberg, J, 2002

¹⁴⁸ Interview, Rosenqvist, Mats; Volvo Technology AB; 2004-09-06

¹⁴⁹ Interview, Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

telecommunication network is available, need to communicate within an enclosed group.

Regulations concerning the sector

The European Union wants to prevent telematic automobile services from being tied to country specific standards. Therefore, it exist a European Union project, which aims at establishing a platform for telematics. Volvo, BMW and Fiat are part of the group responsible for European standards development.

Generally, regarding mobile solutions the development is off course strongly tied to the communication network technology as well as to the cell phone technology. Hence, these two technologies are regulating the development of mobile solution applications.

Trends concerning the sector

Three years ago, telematics were predicted to boom on the market. But since, the market development has ceased. Companies like Volvo Technology consider telematics as field with future possibilities, but where few investments are currently made¹⁵⁰. Furthermore, the industry is now focused on developing solutions instead of individual applications. Therefore, trends towards cooperation between system integrators, operators, and telecommunication companies have started to emerge¹⁵¹.

Related to security, tracking of goods is an important issue. Today, telematic technology combined with satellite navigation technology can provide a system for increased goods surveillance. Still, the problem is to develop the complete service and solution including the administration of it. It also has to be decided if such application can be economically feasible¹⁵².

In order for mobile solutions to be more efficient, mobile security has to be improved. This can be done using technology for encoding. However, this kind of technology is difficult to administrate. Today, it is not recommended or safe to communicate classified information via mobile communication networks. In order for mobile solutions to be a possible application in bank or hospital environments, this problem has to be solved¹⁵³.

Possibilities and hindrance for the sector

¹⁵⁰ Interview, Rosenqvist , Mats; Volvo Technology AB; 2004-09-06

¹⁵¹ <http://www.ad.se/index.php?serv=foretagsfakta>

¹⁵² Interview, Rosenqvist , Mats; Volvo Technology AB; 2004-09-06

¹⁵³ Interview Axelsson, Björn; IT-företagen; 2004-09-19

Regarding telematics, the largest hinder for development can be derived from the fact that the technology has not been as prominent as was expected. This has led to decreased legitimacy, which in turn can restrict industry development.

Strength of the Swedish industry in the sector

Internationally, Sweden is the leading country in telematics research and development. Japan and Korea are following¹⁵⁴. In the Nordic countries Sectra is the market leader in safe telecommunications. It is also a respected company in Europe, and has delivered safe communication devices to the national defence of Germany, Check republic, the Netherlands, as well as to the central organisation of NATO and the US European Command. Thus, Sectra is one of the leading companies in Europe¹⁵⁵. Also, Ericsson is, if not the only, the leading company in mobile communication networks.

Mapping the actors

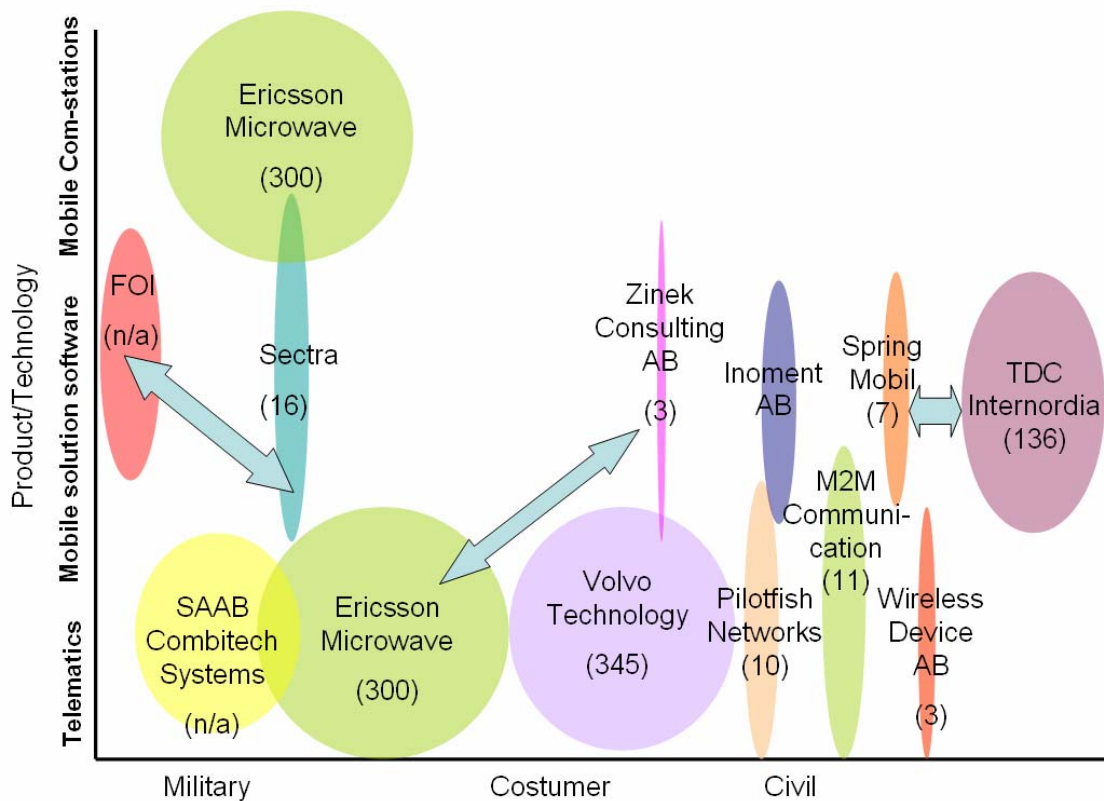


Figure 3-10 The mobile solution sector

Sectra seems to be an interesting company. It works with military customers both in Northern as well as in the rest of Europe. It also works closely with FOI for

¹⁵⁴ Interview, Greg Geiselhart,; telematic valley; 2004-10-20.

¹⁵⁵ Internet, Sectra årsredovisning 03/04

competence building in the area. SEMA, the Swedish emergency management agency, has also started to use Sectra's communication system for enhancing communication security. Also, Sectra wants to be part of the NBD¹⁵⁶.

Ericsson Microwave and Volvo Technology are both a part of the Telematic Valley. However, their attitude towards telematics is somewhat sceptical¹⁵⁷. The telematics industry has not seen the expected market rise. Therefore, new strategies are formed and it is possible to see a consolidation in the industry in coming years.

3.3.6. Physical Transportation

This section is concerned with the sector of the security industry related to physical transportation.

Definition of the sector

“The industry capable of providing technology, products and services for surveillance and transportation of physical equipment in order to protect the society and its inhabitants against antagonistic acts.”

Technology and applications

This sector consists of three main technology areas, namely aeronautical and aviation technology, naval technology and land vehicle technology. Starting with aeronautical and aviation technology, this area brings forward applications in form of aircrafts and helicopters. Naval technology results in applications like ships and submarines, and land vehicle technology is concerned with land vehicles for detection of, and rescue from occurred antagonistic acts. Also, they provide transportation for people and goods in counteraction operations.

Actors

This sector consists of seven companies with a total sum of 6645 employees. This makes the sector the second biggest one in the security industry concerning number of employees. The absolute majority of the employees, 4160 persons, are engaged by Saab Aerospace, a company active in the field of aviation. It should be mentioned that this actor is mainly concerned with civil applications not directly related to the security industry. Kockums, a traditional naval defence supplier, is the second biggest company with 1209 employees. Alvis Hägglunds, active in the

¹⁵⁶ Internet, Sectra årsredovisning 03/04

¹⁵⁷ Interview, Rosenqvist, Mats; Volvo Technology AB; 2004-09-06 and Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

area of land vehicles, is similar in size, with 1003 employees. It should be mentioned that the main actor in this sector

Customers

Like in many of the previous sectors, the Swedish national defence, through FMV, is the most important customer, although its role is decreasing. Other customers, increasing in importance, are international defence agencies and in particular the US defence agency. Also, the Swedish police and the Swedish coastguard make up an interesting and possible increasing customer group¹⁵⁸. A clear increasing customer group is international civil governmental agencies, especially in the USA.

Regulations concerning the sector

Although all actors are seeking new civil applications, they are currently mainly active in the military market. Therefore, also in this sector, the agency ISP¹⁵⁹ is a strong regulating force on the market. Further, the Swedish Maritime Safety Inspection establishes norms and regulations for the naval area, like the Swedish Aviation Safety Inspection does for the aeronautical area.

Trends concerning the sector

A trend is detected when it comes to applying Stealth technology on vehicles, ships and aircrafts. Both Kockums and Alvis Hägglunds have applied this technology in their products¹⁶⁰. Further, forthcoming products from Saab are the Unmanned Aerial Vehicles (UAVs) that are developed for surveillance and combat missions for both military and civil use. This is an example of the trend towards higher degrees of autonomy in the products. Also, new potential markets are spotted in the civil area. Examples of these are applications for combat in a possible urban terrorist scenario, where aircrafts and tanks could be used by civil authorities in order to ward off an attack¹⁶¹.

The sector is greatly dominated by conventional defence industries. There is a strong concern among these companies regarding the decrease in orders from the Swedish National Defence. It is strongly argued that the Swedish national defence is a very competent customer, and has partly helped to develop the actors in the sector into what they are today. However, the Swedish National Defence is disappearing as a main customer¹⁶² and the traditional defence companies in the sector are seeking new applications in the civil area, still the defence customer is

¹⁵⁸ Interview, Nilsson John, Kockums AB, 04-09-15

¹⁵⁹ <http://www.isp.se/nyaengelska/indexeng.htm> 04-09-17

¹⁶⁰ Interview, Nilsson John, Kockums AB, 04-09-15

¹⁶¹ Interview, Hörnström, Nils; Alvis Hägglunds AB; 2004-09-07

¹⁶² Interview, Nilsson John, Kockums AB, 04-09-15

dominating. At the same time, they are expecting the new potential customer in the form of the Swedish civil security authorities to give direction to future areas of application. The traditional defence actors are clearly aware of the changes in the market and the importance of finding new markets¹⁶³.

Possibilities and hindrances for the sector

A commonly spoken problem in this sector, like in the whole security industry, is the lack of integration between authorities, especially in the maritime area where the navy and the Swedish coast guard only have limited cooperation, even though they have similar needs¹⁶⁴. The consequences of this have been discussed in earlier presented sectors. The perception is that the technological level is high in the Swedish industry, but that there is inertia among authorities, based on old policies and perceptions¹⁶⁵.

Further, the main problem in the industry lies in the fading of the main customer. The Swedish defence has been a driving force in the development of the technology for the sector. Many of the companies in the area are used to a strong customer that points the way for them as suppliers. When that role is weakening and no new strong customer appears, the natural result is big uncertainty.

Strength of the Swedish industry in the sector

The Swedish industry has a strong international position regarding aeronautical technology, with SAAB up front¹⁶⁶. The role of the traditional Swedish defence industry concerning the aeronautical area has had a great importance for the industries national development of the technology base, giving the whole area a prominent international position. This is also the case referring to naval technology, although not leading to the same success as in the first case.

Mapping the sector

In the following illustration, all the seven commercial actors in the sector have been mapped out. It can be seen that no crossovers referring to the technology and application areas occur, i.e. the companies are strictly active in only one area. This can possibly be derived from the fact that the areas differs relatively concerning technology. An exception is Saab and Kockums that have continuous contacts with FOI in their corresponding areas. Further, it can be concluded that the main orientation in the field has been towards the defence customer segment. However, a trend has been detected in that companies are orienting towards the civil area.

¹⁶³ Svensk försvarsindustri, 2004

¹⁶⁴ Interview, Nilsson John, Kockums AB, 04-09-15

¹⁶⁵ Interview, Nilsson John, Kockums AB, 04-09-15

¹⁶⁶ Svensk försvarsindustri, 2004

This is especially the case referring to Kockums and Alvis Hägglunds, illustrated by the corresponding arrows. Also, it is important to remark the clear orientation of the biggest actor Saab Aerospace towards the civil market.

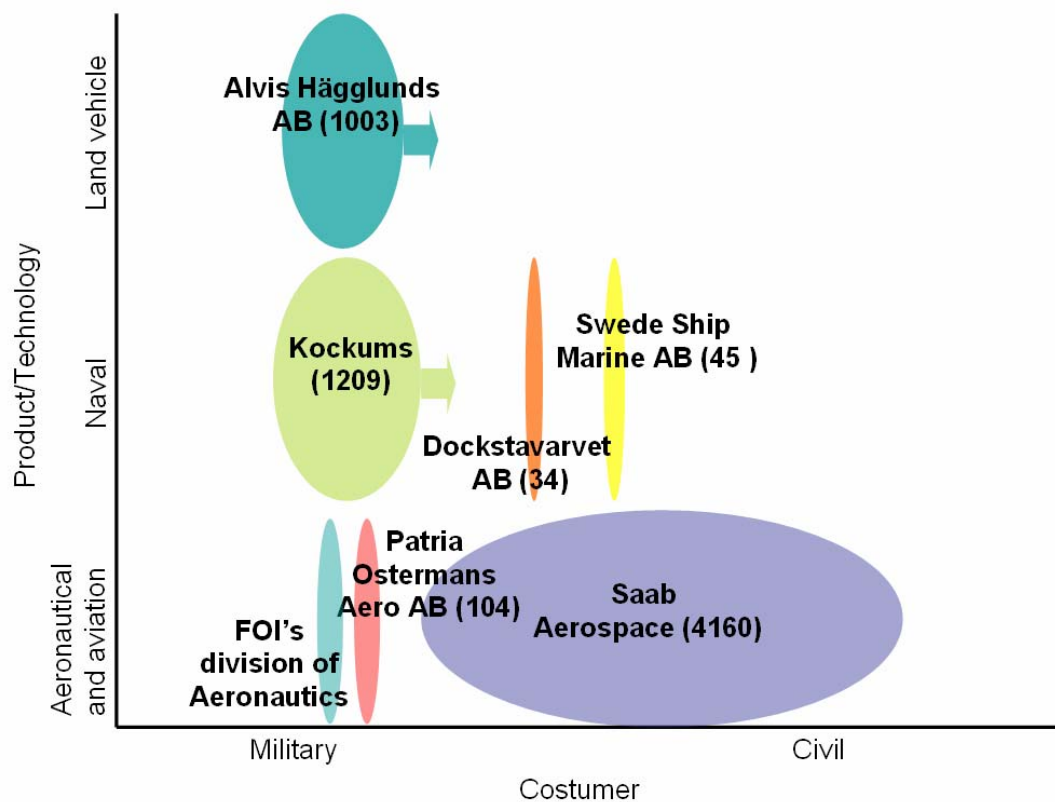


Figure 3-11 The physical transportation sector

3.3.7. NBC technology

This section concerns the sector of the security industry related to NBC-technology.

Definition of the sector

“The industry, capable of providing technology, products and services in order to protect the society and its inhabitants against antagonistic use of weapons of mass destruction including biological, chemical, nuclear and radiological technology.”

This sector covers biological, chemical, nuclear and radiological technology, also referred to as NBC technology or NBCR technology. Also, the expression “weapons of mass destruction” is often related to NBC weapons¹⁶⁷.

Technology and applications

¹⁶⁷ Internet, Krisberedskapsmyndighetens NBC-strategi 2004

The aspects of physically protecting, detecting and transporting NBC weapons are covered by other sectors. This area will only concern the technology behind the weapons and their direct countermeasures, like vaccines, antidotes and chemical neutralizers.

Regarding applications concerning protection against NBC weapons, little is achieved in the field of direct countermeasures. Today, many of the applications are related to physical protection and prevention of spreading of agents. One specific example is Filtrator, a Swedish actor that produces several types of filters against NBC agents¹⁶⁸. Dynasafe is another national actor that produces equipment for destruction and containment of biological and chemical weapons¹⁶⁹.

To understand the fields of technology covered by this sector, a closer description of each technological field will be presented.

Biological weapons are pathogenic micro organisms that are purposely spread to damage other organisms. To be a potential weapon, the micro organisms has to be able to produce in sufficient numbers, survive in the environment and be able to spread properly. Today, it is possible to use genetic engineering to create potential biological agents that are hard to detect and treat. Biological agents that are potential in terrorism related situations can be divided into four categories based on the ease of transmission and mortality rate¹⁷⁰. Listed as category A (high-priority agents) are anthrax, botulinum toxin, plague, smallpox, tularaemia and viral hemorrhagic fevers¹⁷¹. Countermeasures are vaccines and antidotes against these agents, such as the vaccine to prevent and the antibiotics to treat anthrax and the antitoxin that reduces the impact of botulinum toxin¹⁷². The Swedish company Innate Pharmaceuticals, active in Project BioShield, is developing an antidote based on innate immunity to protect against plague¹⁷³. Further, the Swedish actor Alpha Helix has developed a method that improves the quality and speed of the PCR (Polymerase Chain Reaction) process, cutting down the duration of the DNA/RNA analysis and facilitating the detection of a number of biological agents.

Chemical weapons include every chemical that through its chemical impact on the life process results in death, temporal reduction of functions or permanent damages on humans¹⁷⁴. The chemical agents, of which the absolute majority are gases or ultra fine dust, are divided into five main categories; nerve agents like VX, soman,

¹⁶⁸ www.filtrator.se, 2004-09-14

¹⁶⁹ Interview Ohlson, Johnny; Dynasafe AB; 2004-08-30

¹⁷⁰ <http://www.bt.cdc.gov/agent/agentlist-category.asp#a> 04-09-16

¹⁷¹ <http://www.foxnews.com/story/0,2933,76887,00.html>, 04-09-16

¹⁷² <http://www.bt.cdc.gov/Agent/Agentlist.asp> 04-09-16

¹⁷³ Interview Rosell, Sune; Innate Pharmaceuticals AB; 2004-08-27

¹⁷⁴ Internet, Hansson.O et al, 2002

tabun and sarin, blood agents like arsine and cyanide, blister agents/vesicants like mustard gas, choking/lung/pulmonary agents like ammonia, and riot control agents/tear gases. Concerning antidotes for chemical agents, these are of course related to the form of agent. In the case of nerve agents, atropine is the classic antidote but oximes are also used to restore muscle control. A specific application is the auto-injector containing a combination of atropine and an oxime¹⁷⁵. In other cases as in riot control agents/tear gases and mustard gas, no antidote exists.

Examples of nuclear weapons are atomic bombs and hydrogen bombs. The treatment is determined by the type of radioactive isotopes to which the victim is exposed. There is no antidote against the impact of nuclear weapons, the treatment is symptomatic and the main issue is to prevent the radioactive material resulting from an attack to spread any further¹⁷⁶.

Radiological weapons mostly consist of so called dirt bombs and are the most accessible device for spreading radioactive material. A dirt bomb combines radioactive material, radioactive waste in most of the cases, with a conventional explosive¹⁷⁷. Like nuclear weapons they spread radioactive material and the treatment is therefore similar to the one used for nuclear weapon attacks. Much of the countermeasures consist in decontamination of areas by depositing. Since the dirt bombs are relatively easy to create, terrorist actions involving these kinds of bombs are of major concern.

Actors

Only five companies were identified on the Swedish industry. These are the FOI division of NBC Defence¹⁷⁸, which has 168 employees¹⁷⁹, Alpha Helix AB with 20 employees¹⁸⁰, Innate Pharmaceuticals AB, that employs 6 persons¹⁸¹, Filtrator AB with 6 employees¹⁸² and Dynasafe AB, that employs 10¹⁸³. Hence, there is a total of 210 active employees in the sector, resulting in that NBC technology is the smallest of the sectors in the security industry.

Also, there are a lot of governmental and university actors highly relevant to this sector regarding research and development. The governmental actors have a relatively high level of coordination, based on international and national

¹⁷⁵ <http://www.foxnews.com/story/0,2933,76864,00.html> 04-09-16

¹⁷⁶ <http://www.foxnews.com/story/0,2933,76879,00.html> 04-09-16

¹⁷⁷ <http://www.foxnews.com/story/0,2933,76873,00.html> 04-09-16

¹⁷⁸ This is not a commercial company in proper terms but they provide services in the area to above stated, as well as to other, customers.

¹⁷⁹ Internet, Swedish Defence Research Agency Annual Report 2003

¹⁸⁰ www.foretagsfakta.se 04-09-16

¹⁸¹ Interview Rosell, Sune; Innate Pharmaceuticals AB; 2004-08-27

¹⁸² www.foretagsfakta.se 04-09-16

¹⁸³ www.foretagsfakta.se 04-09-16

conditions and instructions. The Institute for Infectious Disease Control, the SEMA and many of the actors described as customers fall under this group. One result of these projects of cooperation is the creation of the Knowledge Centers in the B-, C-, and N- and R-areas respectively¹⁸⁴. The B- Knowledge Centre is closely active around the P4-laboratory at the Institute for Infectious Disease Control in Solna. Research on biological terrorism takes place here, among research in other areas. The R-, N- Knowledge Centre is situated at the cancer centre at Karolinska Institutet and the N- Knowledge Centre is based on a network between FOI, Karolinska Institutet and the Swedish Poison Information Centre.

Customers

At present state, the groups of customers in question are purely government authorities. In Sweden, this group would be represented by the Swedish National Board of Health and Welfare, the Swedish Police, the county councils, the county administrative board, the Swedish Rescue Services Agency, SRSA, the National Food Administration and the Swedish National Defence. However, the Swedish civil authorities are not acting particularly on the matter, mainly because they perceive the present threat on the Swedish society to be relatively low¹⁸⁵. Internationally the market is highly dominated by the US, especially concerning Project BioShield.

Regulations concerning the sector

A number of Swedish agencies regulate the use, sales and research in these areas. Some of them regulate the whole scene concerning the area of NBC-technology, like the Swedish National Board of Health and Welfare, while others are related to a specific branch of the sector. An example of the last-mentioned is The Swedish Chemicals Inspectorate that regulates the use of chemicals. Also, other examples are the three major international organizations that control each area in the sector, the Biological and Toxin Weapons Convention, BTWC, the Chemical Weapons Convention, CWC, and the Nuclear Suppliers Group, NSG¹⁸⁶. A national authority in the chemical sub-area is the ISP¹⁸⁷ as a nationalized authority under the CWC. Regarding the biological sub-area, the Swedish Medical Products Agency's regulates the market of medical products and the Swedish Radiation Protection Authority, SSI, regulates the use of radioactive agents. On a European level the European Union have several regulations in the NBC field. FOI's division of NBC Defence has another interesting role concerning regulations. They work together

¹⁸⁴ <http://www.sos.se/hs/beredska/cbrn.htm> 04-09-17

¹⁸⁵ Internet, Krisberedskapsmyndigheten NBC-strategi 2004

¹⁸⁶ <http://www.regeringen.se/sb/d/3795/a/23209/m/wai> 2004-09-20

¹⁸⁷ <http://www.isp.se/nyaengelska/indexeng.htm> 04-09-17

with corresponding authorities in other countries and presents material to the Ministry for Foreign Affairs that influence international regulations on the area¹⁸⁸.

Trends concerning the sector

The general importance of the sector has grown drastically during the last decade, and continues to grow nationally as well as internationally¹⁸⁹. The international market is regarded as stronger than the national. The creation of Project BioShield has greatly increased the interest in the area of bio-terrorism. The project is creating an extensive stockpile of medical countermeasures, and additional diagnostic tests, drugs and vaccines are under development¹⁹⁰. Also, the project greatly encourages companies to develop new bio-terrorism countermeasures by offering economic incentives. An important part of the potential and future of the market lies in the hands of government agencies in their role as customers¹⁹¹. The insufficient activity among the Swedish, and to some extent also the European authorities, create a weak market. However, the American market, with project BioShield up front, is offering a big opportunity for companies in the sector. Although the interest among authorities in Sweden is growing¹⁹², an antagonistic attack with a NBC weapon is not considered to be a potential or probable threat against the Swedish society¹⁹³. However, the changed threatening picture is definitely increasing the need for technology against NBC weapons. At the same time, the threat from antagonistic use of NBC technology is a relatively new concept in weapon technology and new threats tend to become huge sources of fear. The impact of an NBC attack is relatively unknown among the public, comparing to the use of conventional weapons. Therefore, it can be argued that the fear is disproportionate compared to the real threat¹⁹⁴.

Possibilities and hindrances for the sector

The main area of concern for companies in the market is to engage affected authorities¹⁹⁵ and to coordinate the technical knowledge in the area. The above mentioned regulating authorities also limit the activity of the company, although they are generally seen as positive and necessary actors.

Strength of the Swedish industry in the sector

¹⁸⁸ Internet, NBC håller koll på farlig forskning, 2003,

¹⁸⁹ Interview Rosell, Sune; Innate Pharmaceuticals AB; 2004-08-27

¹⁹⁰ Internet, Project BioShield, 2003

¹⁹¹ Åkesson.B, 2004

²¹⁴ Interview Rosell, Sune; Innate Pharmaceuticals AB; 2004-08-27

²¹⁵ Internet, Krisberedskapsmyndigheten NBC-strategi 2004

¹⁹⁴ Internet, Hansson.O et al, 2002

¹⁹⁵ Åkesson.B, 2004

Although few Swedish companies are active in the industry, Swedish research, especially concerning biological and chemical weapons, is in the front edge internationally¹⁹⁶. Sweden has a weak national market with few customers. It can be argued that this fact limits the possibilities of development of the Swedish actors and can be a possible explanation to the relatively low number of national actors.

Mapping the sector

Today, the industry is relatively divided in two groups formed by the government actors and commercial actors. When it comes to cooperation between the two groups, little is achieved. The governmental actors have a relatively good collaboration when it comes to research, but the gap between them and the commercial actors is wide, especially in the biotech field¹⁹⁷. However, Filtrator and Dynasafe have relatively good contacts with authorities as customers, though the situation is different when it comes to research.

The illustration below shows the companies in the sector and where they are situated in the industry considering types of customers and technology. This study has not revealed any relevant relation between the companies.

It is also worth mentioning that both FOI and Dynasafe are moving towards the civil area of the customer field, as illustrated by the arrows on the corresponding actors.

¹⁹⁶ Åkesson.B, 2004

¹⁹⁷ Interview Rosell, Sune; Innate Pharmaceuticals AB; 2004-08-27

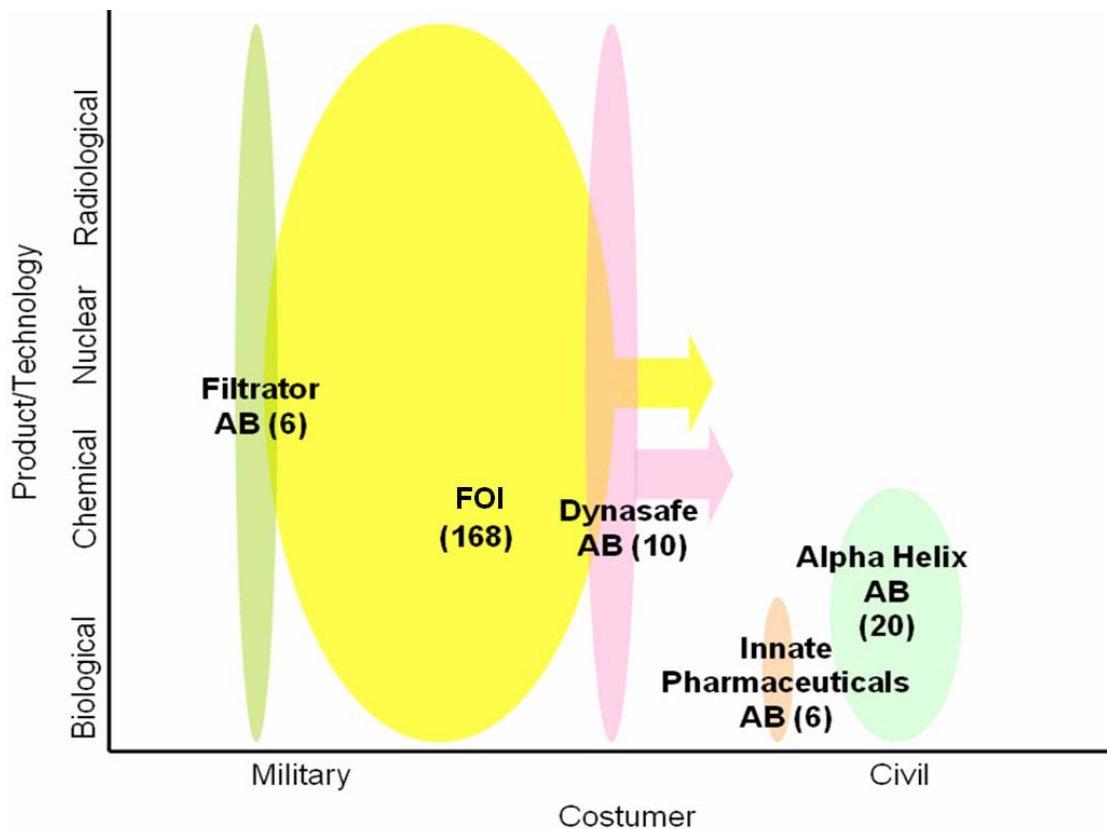


Figure 3-12 The NBC-technology sector

3.4. Evaluation of the sectors

This subchapter aims at identifying a sector with the highest growth potential. This area will later be the one in which the innovation system analysis is conducted. Firstly, different trends referring to future industry sector potential, found in articles as well as reports, are described. Secondly, the results from the interviews and Vinnova hearing are presented, revealing both perceived future market potential and perceived level of capability. The trends are then summarized and relevance and potential impact of the trends are discussed. Finally, one sector is to be chosen for further analysis.

The final choice will be based on identified growth potential of the industry sectors. Growth potential has been confirmed as a good parameter by Vinnova, and is also a parameter aligned with the purpose of this report. Partly, the purpose of this report is to function as a support in the development of a Swedish security research strategy, which would enable Sweden to become among the world market leaders in at least one security industry sector. However, for this position to be profitable, the market must show international growth potential, and it has to exist a national capability related to the specific industry sector. Therefore, identifying a sector with high growth potential, as well as high perceived level of capability is important if this purpose shall be achieved.

3.4.1. Results from articles and reports

Concerning the security market, many of the trends identified originate from the USA. The American security market constitutes over 50 percent of the world market. Therefore, it is of great interest that Swedish companies recognise these trends and act thereafter. The importance of establishing close connection with the USA has been acknowledged by several main actors in the Swedish security industry¹⁹⁸.

Technology and application trends

It is possible to identify technological application trends related to the development of security applications. The Civita Group has recognized three different generations of applications according to figure 3-13 below.

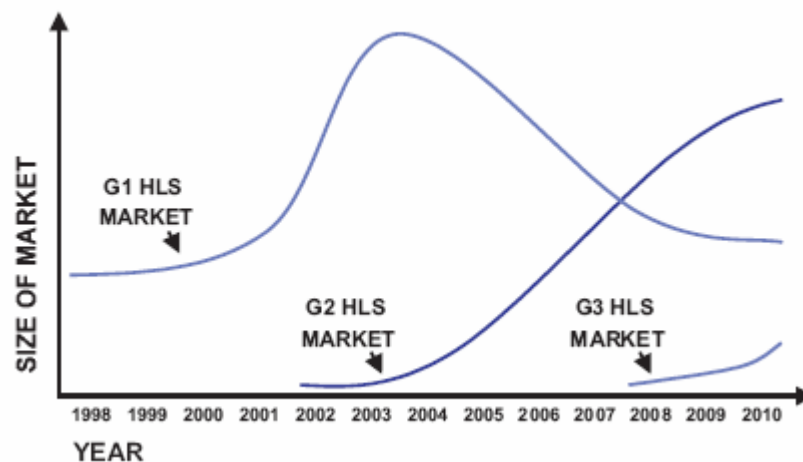


Figure 3-13 The technological trends¹⁹⁹

The first generation of security applications, referred to as G1 in figure 3-13, is available on the market today. This generation includes all technology and security products available directly after 9/11. Metal detectors, fingerprint technology, radiation detection technology and electronic access controls are all part of the first generation's technologies and applications. The second generation's applications, referred to as G2 in figure 3-13, are based on technologies that were researched on but not available on the market prior to 9/11. Such applications include biometric sensors, terahertz sensor technology and complex sensor systems. These products are also supposed to be designed to facilitate integration of products into larger systems. The third generation's applications, G3, will not be introduced on the

¹⁹⁹ Figure taken from <http://www.civitasgroup.com/reports/20040627.pdf>

market until 2008-2009. It is hard to give example of potential third generation technology²⁰⁰. Consequently, the highest future market potential is likely to appear among the second generation security technology mentioned previously.

Generally during the past years, the security market has been experiencing several consolidations. Also, it exists a trend towards solution-based pull market. According to the Civita Group it is this particular shift towards a solution based market that is the most noticeable trend and also a characteristic for the whole security industry. Generally, solution based products require several forms of applications integrated into one product. Therefore, companies with broad application areas are better suited for obtaining market shares. Also, this trend increases the importance of complementary service agreements with customers and other channel actors. Furthermore, this means that the formation of standards is very important for future revenue, since compatibility comes in focus²⁰¹.

Future growth potential

This chapter will identify growth potential by examining the Department of Homeland Security's budget for 2004 and the budget request for 2005. Trends will also be identified by examining several market research reports, conducted by leading US market research companies.

When examining the 2004 year's budget, most of the resources are directed to following areas:

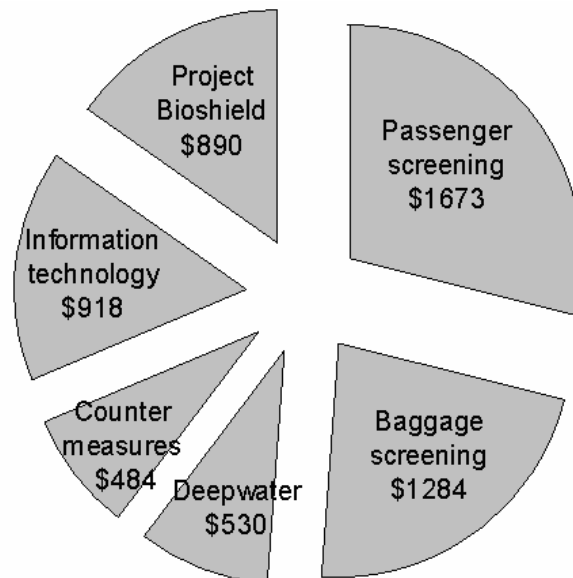


Figure 3-14 Distribution of the DHS budget for 2004 in millions of dollars

²⁰⁰ Internet, Civita Group, 2004

²⁰¹ Internet, Civita Group, 2004

These identified areas can be related to the different technological and application sectors previously described in section 3.1.2. For example, passenger and baggage screening are a part of the sensor industry sector. Counter measures can be derived to weapon technology sector. Information technology is part of complex systems and IT-security, and Project BioShield can be derived to the NBC technology sector.

When examining the areas more closely, it is possible to identify more trends. The Civitas Group has examined the Department of Homeland Security's budget for 2005 which reveals that aviation security will be awarded \$890 millions next year. About \$400 millions will be used for increased and enhanced explosive detection systems. \$85 millions will be directed to cargo screening technologies and \$61 millions will be used for protection of civil aircrafts from surface-to-air missiles²⁰². The 2005 year's budget also includes \$340 millions intended for the US-Visit Program. Most of the budget will be spent on biometric products and technologies in order to improve surveillance of visitors and immigrants. Radiation detection together with bio surveillance equipment and technologies will be allotted \$128 million. These resources will be spent on purchasing sensor technologies for scanning and detection.

It is somewhat unclear if the overall budget has increased or decreased compared to 2004. The Civita Group states that the budget has declined by 1 percent compared to 2004. The decrease can mainly be related to fewer resources for aviation and border security where very large fixed investments were realized just after the incidents on 9/11²⁰³. However, other sources state that the 2005 year's budget has increased with 9.3 percent compared to 2004²⁰⁴. The difference could be derived to the fact that the Civita Group is only comparing the parts of the budgets that are to be invested in the private sector.

To summarize, when examining the budget, it can be argued that screening products and technologies are allotted very large resources. Screening technology is part of the sensor technology sector. Two other large posts identified in the budget are Project BioShield and information technology. Hence, these resources are intended for the NBC-technology sector and IT-security sector, which further stresses their importance and future market potential.

The Freedonia Group has presented a study which identifies sectors on the security market that are likely to see substantial growth in coming years. The report reveals that chemical sensors, including gas- and bio sensors are predicted to see an 8.5 percent growth per year through 2008. Optical sensors and bio sensors are

²⁰² Internet, Civita Group, 2004b

²⁰³ Internet, Civita Group, 2004b

²⁰⁴ www.homelanddefensestocks.com//companies/HomelandDefense/News/homeland, 2004-09-16

predicted to grow the fastest, while medical diagnostic sensors will offer the most profitable market opportunities. Information security is predicted a 19 percent annually growth through the year 2008. Concerning information security, consulting activities are predicted to lead gains followed by encryption hardware and biometric access controls. Biometrics and electronic access control systems are predicted a 10 percent growth per year. Biometrics systems, including finger print, facial scanning and iris scanning technologies, are identified as the most probable field to experience the highest growth in coming years²⁰⁵. A common trend among the areas described as potential high growth areas are that they all include biometrics. It can therefore be argued that biometric has many application areas and are to be regarded as a potential high growth technology. This technological field is part of the sensor industry sector, which further establishes the potential of this particular sector.

According to Civita Group, data analysis technologies, in this report classified as complex systems technology, are expected to see the highest growth of all technological areas in coming years. Data analysis technology facilitates and enables decision making out of collected information. Domestic and foreign intelligence as well as border security are the two markets where the highest market growth regarding data analysis technologies are predicted to take place²⁰⁶.

O'gara company is a homeland security investment firm. It identifies the expected growth sectors within the market to be cargo-screening technology and tracking and authentication technologies. The sectors with the least growth potential are law enforcement and intelligence training and identification systems for national and population segments²⁰⁷.

The Civitas group have identified the top thirteen private sector opportunities, listed in appendix F. Given these business opportunities, the most likely firms to succeed on the security market are companies active in:²⁰⁸

- Biosensor technology
- Radiation detection and technology
- Intelligent surveillance system
- Biometrics
- Countermeasures to respond bio-terror attack

Conclusion

²⁰⁵ <http://www.fredoniagroup.com/pdf/1792web.pdf>, 2004-09-16

²⁰⁶ Internet, Civita Group, 2004

²⁰⁷ www. Govexec.com, 2004-08-23

²⁰⁸ Internet, Civitas Group ,2004b

In this section it has been shown that in the DHS-budget almost \$2.5 billion dollars are designated for different screening applications and technologies. Since the screening technology is part of the sensor technology sector, it makes this sector appear as an important area with high growth possibilities. Other large posts in the DHS budget have been designated for IT-security and large amount of resources will be spent on Project BioShield. Also, the market research reports have shown that biometrics is a technology that has a vast field of application areas and is furthermore part of the second generation of emerging technologies presented in figure 3-13. Biometrics is also included in the sensor technology sector, making this area look even more interesting regarding future industry development and possibilities.

Other interesting areas are Data analysis technologies referred to as complex systems. This technology was considered by the Civita Group to have the largest growth potential of all technological sectors. Also, O'gara company and Freedonia Group confirmed the market potential of sensor technology. Furthermore, Freedonia Group acknowledged IT-security as a field that is probable to expect considerable market growth in coming years.

By summarizing the presented opinions on future growth potential of the different sectors, following graph can be derived.

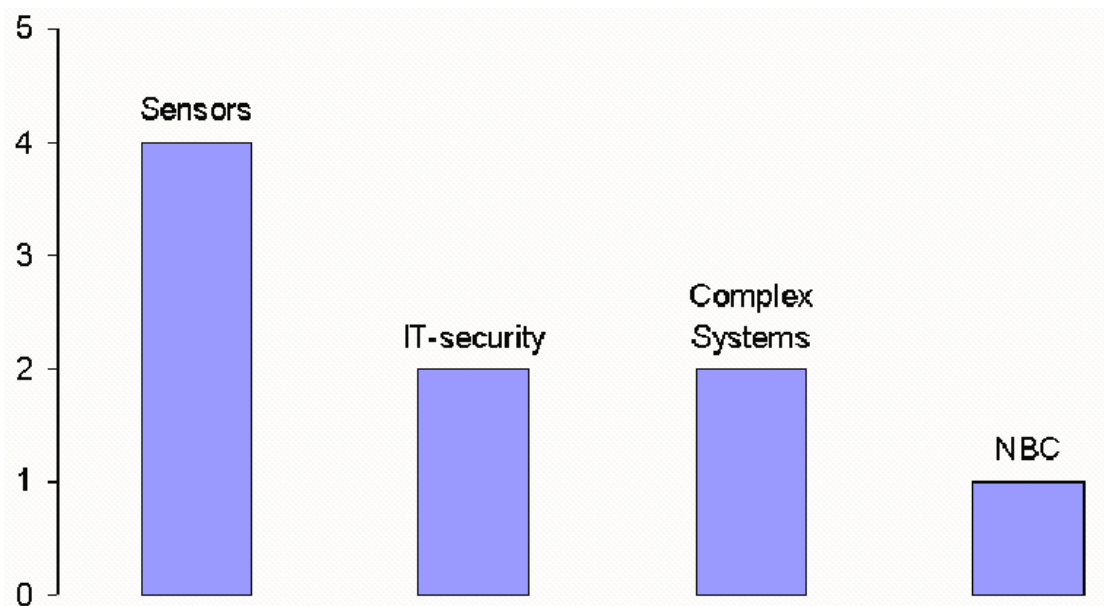


Figure 3-15 Number of sources that have acknowledged growth potential of the particular sector.

Summarizing, the three most potential sectors identified in this chapter are Sensor technology and Complex systems technology and IT-security.

3.4.2. Results from the interviews

In the following section, the results from the interviews on future potential market sand the Swedish strength will be presented. The complete presentation of the interview results can be found in appendix G.

During the interviews, the main sectors identified as potential high growth sectors were sensor technology including biometrics and microwave scanning, and complex systems and systems integration. This is shown in figure 3-16 where the sectors' market potentials are visualized depending on number of interviewees that mentioned applications related to the sector as future potential growth markets. Further, the areas with high growth potential regarding applications are airport and aircraft security and seaport security.

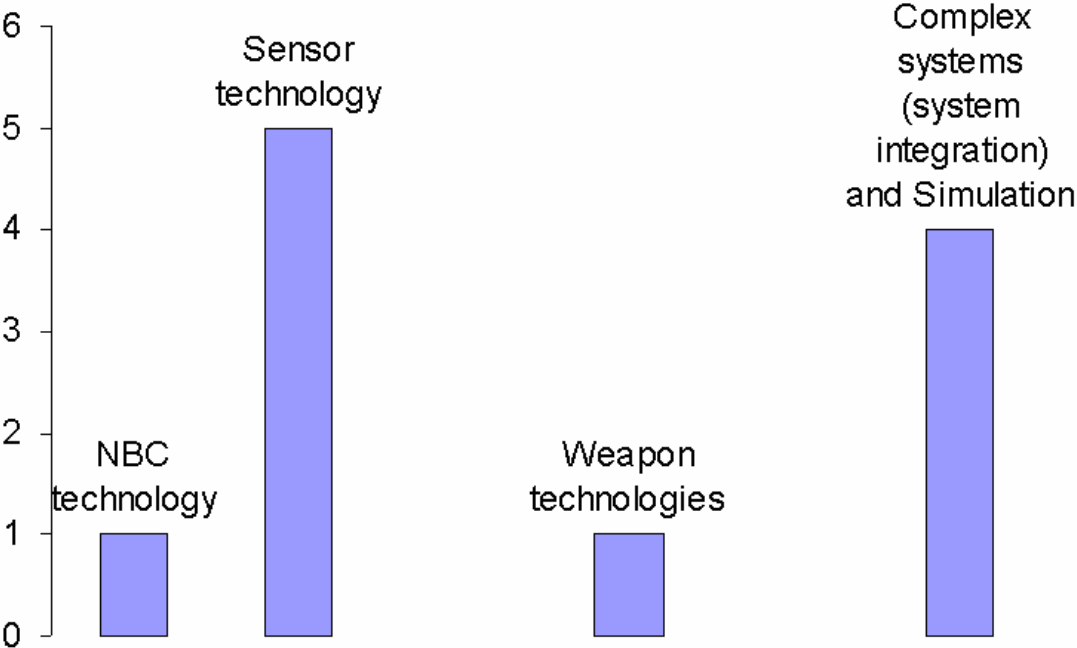


Figure 3-16 Future market potential of the sectors as perceived by the interviewees

Regarding the Swedish strengths related to the different sectors, this was discussed in the presentation of each of the sectors. It has been difficult to draw any conclusions from these results, partly because they are affected by the interests of the interviewees related to corresponding sector. There are several sectors where the Swedish industry is perceived as leading, making it hard to identify a particularly strong sector. However, sensor technology, complex systems (system integration) and simulation and NBC-technology have been perceived as particularly strong.

3.4.3. Results from the hearing

Regarding the hearing held on the 19 of august²⁰⁹, several questions related to future market potential and level of capability of the Swedish industry were discussed. To show how the sectors presented in this report are related to these aspects, a summarization of the answers on these questions was made in order to detect how many of the comments concerning the discussed aspects were related to each sector. The results are illustrated in figure 3-17 and show that complex systems and simulation was the most discussed sector during the hearing. It should also be mentioned that sensor technology has been frequently mentioned during the hearing. Furthermore, mobile solutions are perceived as a stronger sector referring to the capability of the Swedish industry and IT-security seems to have a stronger future market potential.

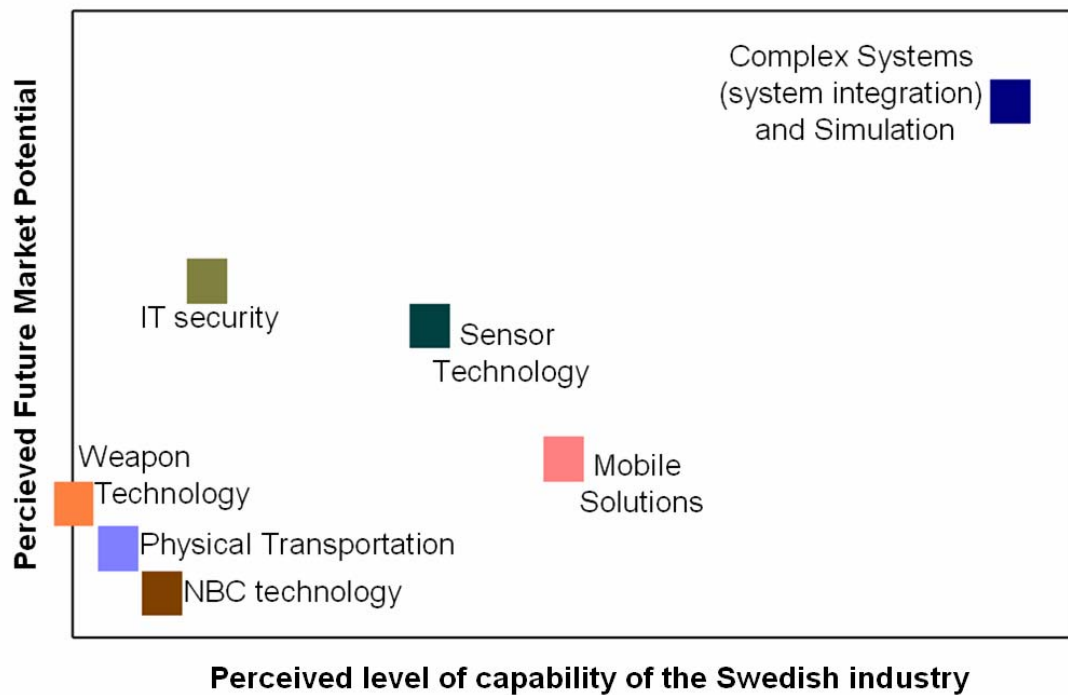


Figure 3-17 Potential growth as according to the results from the Vinnova hearing

3.5. Identification of a potential sector

In this section, the information from section 3.1.3 is weighted together in a graph with the same representative axis as in figure 3-17 above. In figure 3-18, all the information from section 3.4 is summed up and evaluated.

²⁰⁹ Hearing, 19 august 2004

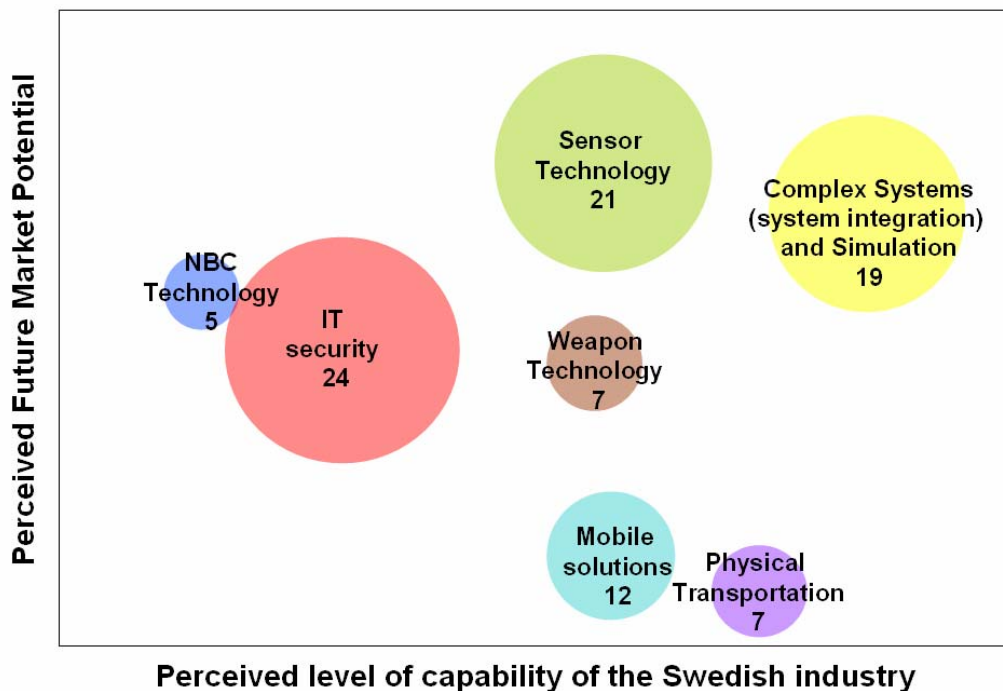


Figure 3-18 The growth potential of the Swedish security industry sectors

As in the previous graph, the capability of the Swedish industry is presented on the X-axis and the Y-axis shows the growth potential of the market. The size of the circles, representing the different sectors, illustrates the relative size of the sector based on the number of companies active within. The number presented below each sector name is the actual number of firms. The perceived future market potential of each sector was based on the information acquired from articles, reports, the hearing and interviews. The perceived level of capability of the Swedish industry was based mainly on results from the hearing, but also from interviews.

Figure 3-18 shows that sensor technology and complex systems (system integration) and simulation were the sectors with the highest growth potential. However, the sector of complex systems (system integration) and simulation is considered to be too extensive and intangible for a future study. This was also confirmed by the project group at Vinnova. Sensor technology was found to be a strong sector considering size, perceived future potential and national capability. It was also clearly defined, which made it the most appropriate sector for further analysis.

4. Innovation system analysis of the security sensor industry

In this chapter, the results of the innovations system analysis of the security sensor industry will be presented starting with the delimitation of the innovation system. The structure of this analysis follows figure 4-1. The structural components of the innovation system will firstly be presented, followed by the analysis of the conduct through the seven functions. This will reveal the achieved functional pattern and further the weaknesses of the innovation system. From these weaknesses, the blockage mechanisms affecting the system performance will be derived. Finally, these blockage mechanisms will lay the base for the recommendations.

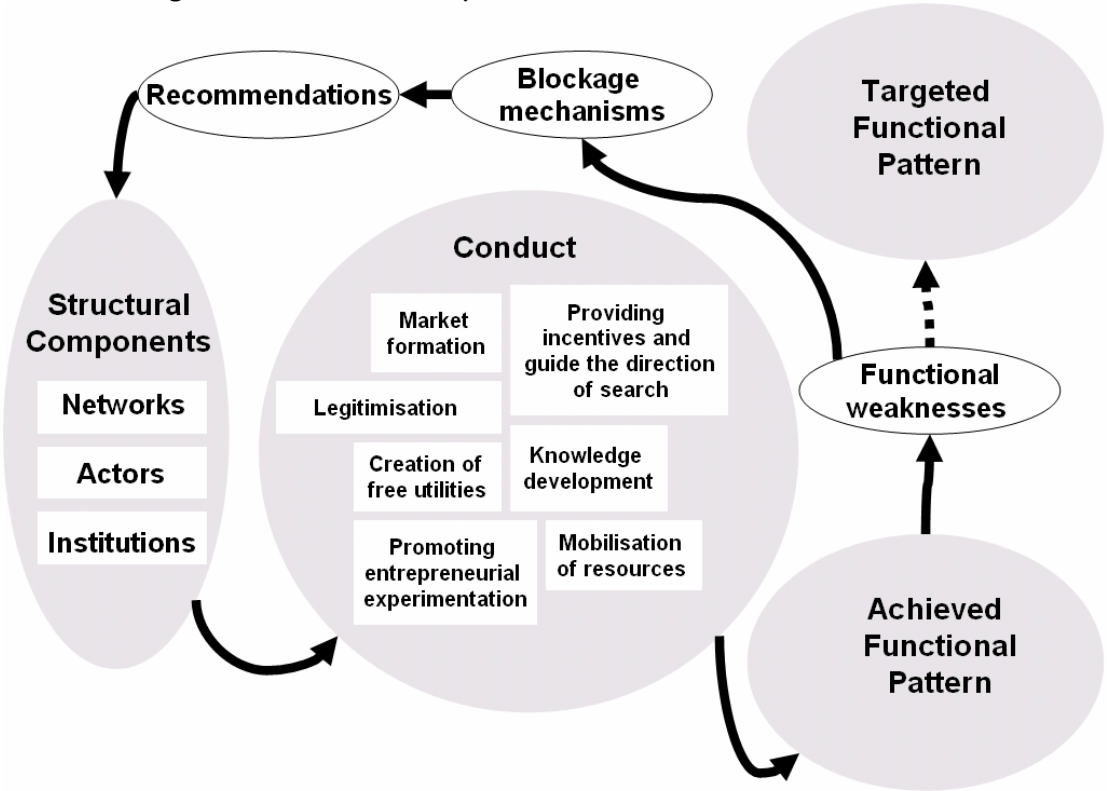


Figure 4-1: Overall structure for the innovation system analysis

4.1. Delimitation of the innovation system

Concerning the delimitation of the innovation system, the technology systems approach was used and the innovation system was delimited by products and application concerning the sensor security sector. Also, a national perspective was applied given that the objective of the thesis is to be a support in the development of a national strategy for the security industry. Considering the definition of the security industry, the sensor product definition, the national perspective and the definition of an innovation system, the delimitation of the Swedish security sensor innovation system can be illustrated as shown in the following figure.

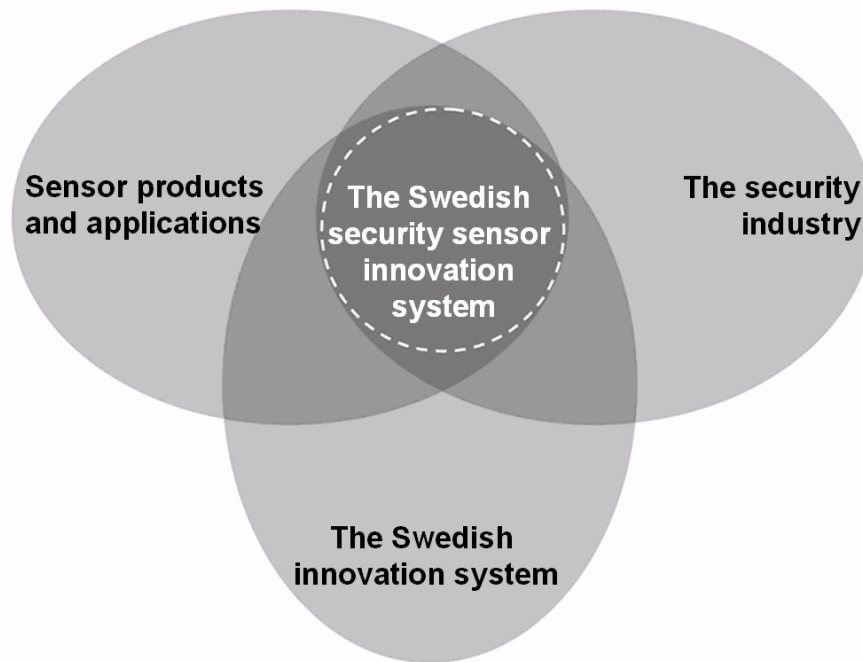


Figure 4-2 The delimitation of the innovation system.

The illustration presents the context in which the innovation system is located and results in the following definition. This innovation system consists of;

The Swedish set of actors, networks and institutions that utilize create and diffuse knowledge, technology and innovations concerning the development and production, on a national level, of a product composed by elements for detection and elements for generating signals that clearly quantifies the detection, with the possible application of managing antagonistic threats and protect the society and its inhabitants against antagonistic acts.

4.2. System structure

In the following section, the structure of the innovation system, i.e. the structural components within the system boundaries, are described. In order to identify the elements of the security sensor industry, a technology chain analysis was conducted. As shown in figure 4-3, the industry includes actors within defined technology and application areas. Also, the customer segments related to the industry is identified in the far right column of figure 4-3.

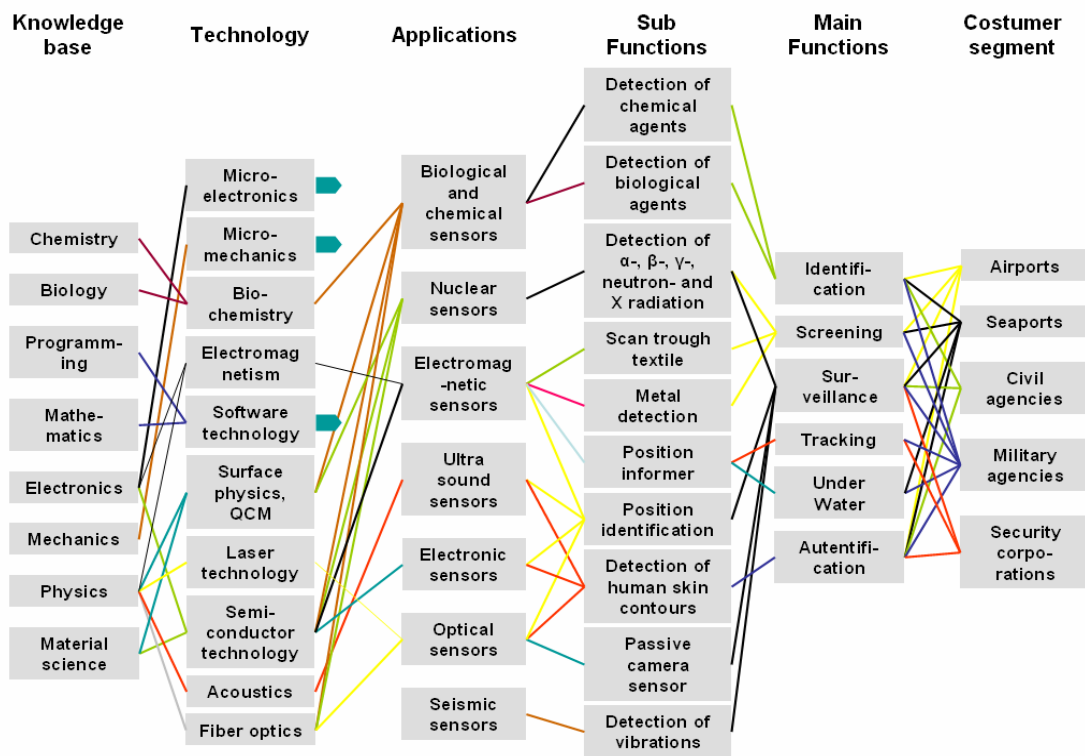


Figure 4-3 Technology chain analysis

To visualize the geographical distribution, and the sectors of applications that the commercial companies are active within, the commercial companies are put out in figure 4-4, together with the research institutes, suppliers, university institutions and the national centres of excellence relevant for the innovation system. The figure reveals two concentrations of actors, one in Linköping built around the two national institutes of excellence ISIS, S-Sence and the research institutes of FOI and Acreo. The other concentration of actors is located in the Stockholm-Uppsala sector and mostly concerns biological sensors. A complete listing of the components of the system structure can be found in appendix D.

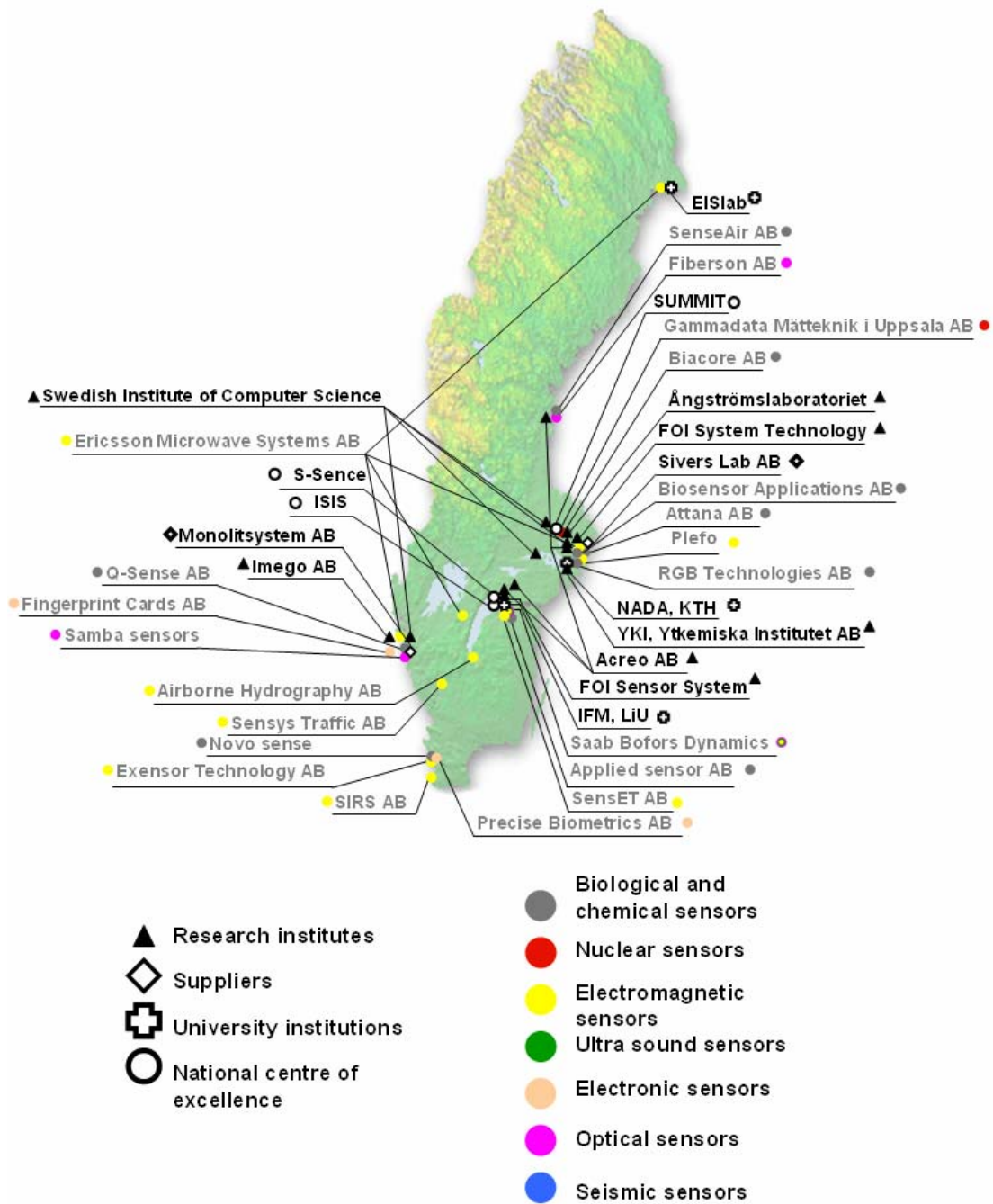


Figure 4-4 Geographical distribution of commercial companies, research institutes, suppliers, university institutions and national centres of excellence

Actors

Commercial companies

An amount of 21 commercial companies have been identified within the system of which three, Ericsson Microwave AB, Saab Bofors Dynamics AB and Airborne Hydrography AB, are active in the defence industry. Eight out of them are active in the application area of electromagnetic sensors. The application area of biological sensors also has eight actors, a relatively high number that can be related to the

Swedish strength and technological inclination towards biotechnology. Together with electromagnetic sensors, the field of biological sensors is one of the two largest application areas in the security sensor industry. The largest actor according to number of employees in the sensor sector is Ericsson Microwave AB²¹⁰, active in the application area of electromagnetic sensors. Consequently, this application area is the biggest one related to number of employees. The absolute majority of the actors, all but Ericsson Microwave AB Saab Bofors Dynamics, are small or medium sized companies. Further, no actors have been identified in the application area of seismic sensors and both the actors related to electronic sensors are active in the field of biometrics.

Suppliers

Two suppliers of components for production of sensors have been identified in the innovation system. These are Monolitsystem and Sivers Lab located in Gothenburg and Kista respectively.

Research institutes

Among the identified research institutes, Acreo is of special interest. Acreo is the only Swedish supplier of silicon components, which are necessary for several sensor applications. Also, they work together with entrepreneurial companies, developing the company specific technology. Other identified research institutes in the sensor security industry are Imego, FOI Sensor System, FOI System Technology, Swedish Institute of Computer Science, YKI, Ytkemiska Institutet and the Ångström Laboratory.

University institutions

Given the fact that sensor technology consists of a great number of sub technologies, it is particularly difficult to identify all the university institutions affecting the system. Many of the commercial actors have expressed that their cooperation with universities is closely linked to location and to the particular needs of the actor. However, three institutions have been particularly mentioned, the Department of Numerical Analysis and Computer Science at KTH, also referred to as NADA, EISlab in Luleå and the Sensor Science and Molecular Physics group IFM at the University of Linköping.

National centres of excellence

The national centres of excellence work as a communicator between university research and industry demands. By conducting this function, they enhance the

²¹⁰ Interview, Oderland, Ingvar; Ericsson Microwave Systems AB; 2004-10-15

efficiency in R&D activities within the innovation system, and have therefore been defined as important actors for increasing system performance. Currently, there are 28 national centres of excellence in Sweden. Three of these constitute actors in the sensor security industry or covers activities related to sensor development, namely ISIS, S-Sence and SUMMIT.

Public authorities

There are a number of public authorities affecting the innovation system in several ways, some of them through regulations and control, others through their role as customers or development partners. These public authorities are The Swedish Radiation Protection Authority, SSI, The Swedish Nuclear Power Inspectorate (SKI), The National Inspectorate of Strategic Products, ISP, The Swedish Maritime Association, The Swedish security police, SÄPO, The Swedish Emergency Management Agency, SEMA, and The European Union.

Customers

There are two major groups of customers in the innovation system. Government authorities form one of them and include the national defence, the Police, the Swedish Customs, the Swedish Coast guard and the Swedish Board of Civil Aviation. The second group is made up by non-governmental sea- and airports and security companies supplying security equipment to end customers.

Industry Associations

There is no particular industry association for the security sector as defined in this report. However, there are industry associations that influence the sensor security industry in different ways. These associations are Swesec, FIF (Försvars Industriföreningen), Sweden Bio and Biotech Forum. Swesec represents Swedish security companies. However, their definition of security differs from this report's, and Swesec is therefore not targeting the industry being analysed, but is more related to the customers of the sensor producers in form of security companies.

Institutions

Concerning regulations and laws that influence structures, six such components have been identified. These are the Ådalen act, regulating the use of military resources concerning civil incidents, the ISP related to strategic products, the LOU that influences all forms of public procurement, and the European Union regulations (EC) 2320/2002 , (EC) 622/2003 and (COD) 2003/0089 that affect security related to air and sea transportation and ports. Regarding standards, it is difficult to state if there exist general established standards for the whole sector given the broad spectra of technologies that concerns sensor development.

However, certain forms of standards exist in particular technology fields, for example in biometrics and radar.

Formal networks

Currently, no formal national networks have been identified in the Swedish security sensor industry.

There are two international networks related to the innovation system, both on a European level. The first one, GOSPEL, is a network concerned with artificial olfaction, funded by the European Commission through the 6th framework programme. The second one is Nose II²¹¹, also a network for artificial olfaction.

4.3. The nature of the security sensor industry as an innovation system

As stated in the method and theory chapter, the evolutionary process of the innovation system can be divided into different phases. Depending on the innovation system's current phase, the importance of functions performed within the system varies. As described in section 2.3.5, in the early phases the functions of knowledge development and market formation bear high importance. In the following phase, the growth phase, providing incentives and guiding the direction of search is emphasized as critical for satisfactory innovation system development. Therefore, it is of particular interest to analyse the maturity of the innovation system in order to define the most crucial functions for prosperous system development.

As described in section 2.3.5, the definition of the evolutionary phase is to a large extent related to market and technology characteristics. The early phases are characterised by high uncertainty and activities in technological research as well as formation of niche markets. The later phases occur when the system goes beyond the first market niches. In these phases a space for growth has been created, which needs to be filled.

Since the sensor security industry is more characterized by the development of a new market and related applications than with emergence of new technology, the theory of innovation system evolution phases is difficult to implement directly. Regarding the sensor security industry, the technology is constantly developing, but at the same time it can be classified as mature. As for example, in the field of electro magnetic sensors, research on radar has been conducted since the 19th century. Therefore, in a technological perspective, the security sensor industry is relative mature.

²¹¹ <http://www.nose-network.org/>, 2004-10-18

Since the technology is overall rather mature, and since the industry has moved from early niche markets to mass markets created by institutional changes, as for example the market related to the DHS, it can be argued that the system has propelled forward, leaving the formative phase to create a space for innovation system growth. Hence, the sensor security industry can be defined as standing on the threshold to the evolutionary phase described as the growth or take off phase.

It is hard to implement existing evolution phase theories in an exact form on the sensor security industry. This depends on the fact that the creation of the innovation system is initiated by institutional changes that have opened new markets for previously existing technologies and applications. It can be argued that different innovation systems, both from the civil and military industries, have emerged to one new system, created to supply the resources demanded by the new security market. Because of this fact, existing resources, technologies, applications, networks and institutions were projected directly onto the new innovation system. Therefore, the formative phase with related uncertainties have never existed or existed only under a brief period of time while the market uncertainty was still very high. The innovation system moved into a growth phase when market uncertainty decreased by the augmented security demand and the implementation of the DHS regulations.

As described in section 2.3.5 concerning the growth phase, the amount of new actors entering into the innovation system is the most critical factor for successful system development. Therefore, related to the sensor security industry the function of creating incentives and guide the direction of search is vital for total innovation system functionality.

4.4. Functional analysis

In this section, the functional analysis will be presented, starting with function 1.

4.4.1. Function 1. Knowledge development

This function will describe and review the strength of the national knowledgebase related to sensor technologies. Firstly, a brief discussion of the fundamental knowledgebase for sensor development will be discussed, followed by a review of the national knowledgebase related to technology, application and production. Secondly, it will be described to what extent knowledge is generated and spread throughout the innovation system. Finally, this section is concluded by a summarization of national strength and weaknesses related to the function of knowledge development.

Fundamental knowledgebase

As identified in the technology chain analysis, in order to be successful in the development of sensor applications and technology, it is important to possess a broad knowledgebase. Depending on what type of sensor being regarded, the knowledgebase alternates. However, micro electronics as well as data- and signal processing are technologies which are frequently recurring in all sensor applications. Hence, it can be argued that the fundamental knowledgebase for sensor development consists of micro electronics as well as data- and signal processing. Depending on the characteristics of the sensor application, a third or fourth technology is combined to the fundamental knowledgebase. As for example, biosensors build on biotechnology, radar sensors on microwave technology and so forth²¹². Since a sensor combines several technologies, the breadth of the knowledgebase is essential in order to be successful in sensor development²¹³.

Technological knowledgebase

The strength of the knowledgebase can be analysed by reviewing national patent activity. Figure 4-5 shows the Swedish number of patents divided into identified sensor technologies. Identified patents originate from 1976 to 2004. The line symbolizes the average ratio of total amount of Swedish sensor patents related to total amount of international sensor patents. The Swedish sensor patenting quota constitutes approximately 0.8 percent of all sensor patents issued during the period analysed. The graph shows that the relative Swedish strength is found in technological fields of nuclear and electromagnetic sensor technologies. The nuclear sensor patents have mainly been issued to FOI, while the electromagnetic sensor patents to a large extent derive from Ericsson Microwave, FOI and Saab Bofors Dynamics. Also, the graph shows on a low patenting activity in ultrasonic and biosensors which could indicate a national weakness in these sensor technologies. Even if it exist a large number of national biosensor actors, the majority of them are small in size. This fact might hinder them from investing resources in seeking American patents.

²¹² Definition, technologies are specific and delimited knowledge. The technologies can be divided into sub-technologies that combined constitutes the superior technology. Knowledgebase is those superior technologies that have to be combined in order to realize an application or function. (F. Hörstedt, A.Rickne: Riktlinjer för teknologioanalys. (2001) institutionen för industriell dynamic, CTH

²¹³ Interview, Krantz-Rülcker, Tina and Lundström, Ingemar; S-sence; 2004-10-19 and Klasén, Lena; FOI Sensor Systems ; 2004-10-26 and Holmberg, Per and Karlsson, Magnus; Applied Sensor Sweden AB; 2004-10-19

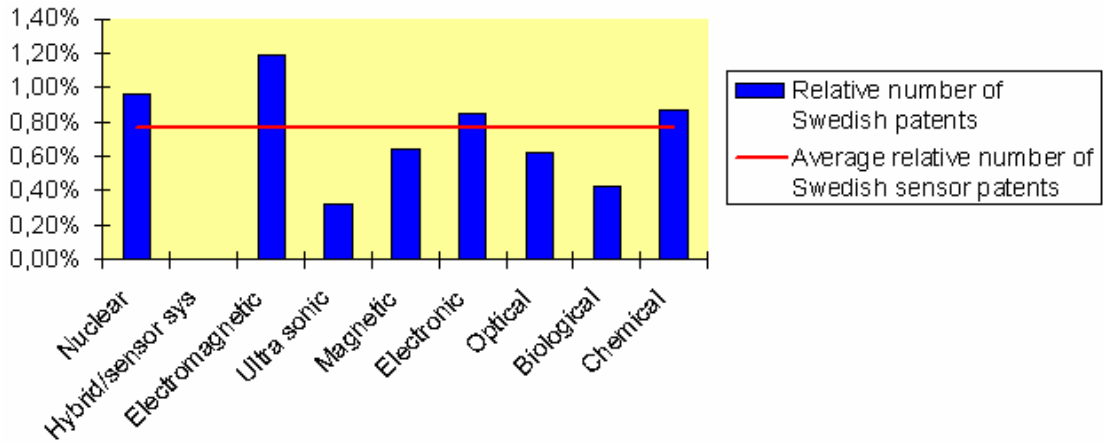


Figure 4-5 Relative amount of Swedish patents in the sensor industry 1976 to 2004²¹⁴

Figure 4-6 also shows the national patenting activity, but here the patents have been granted in 1999 to 2004. Reviewing the graph, it can be concluded that since 1976 Sweden has increased its overall sensor patenting activity from having 0.8 percent of the total amount of sensor patents to having approximately 1.0 percent. However, the increased patenting activity derives from increased activity related to electromagnetic and nuclear sensors. All other sensor fields have experienced a decrease in patenting activity in recent years. The decreases in biological and chemical sensors are critical since these sensors have been identified to have great potential on the security market.

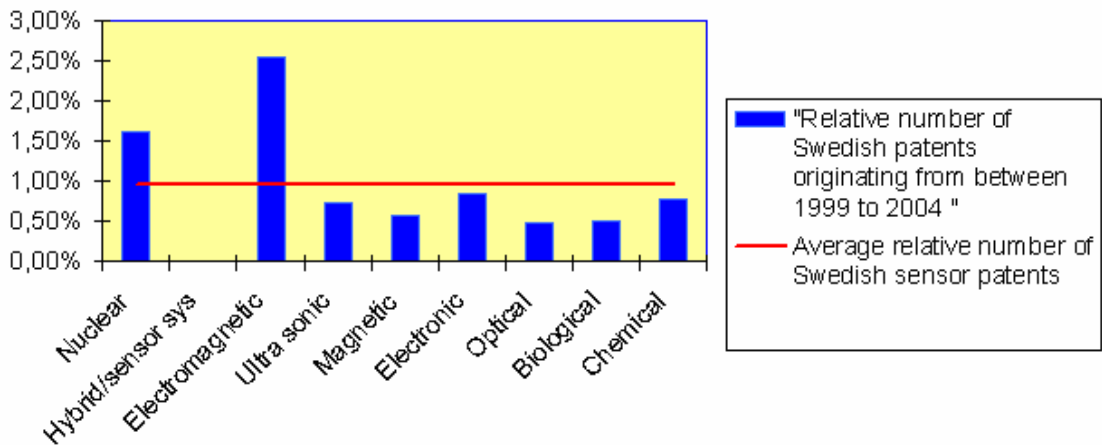


Figure 4-6 Relative amount of Swedish patents in the sensor industry 1999 to 2004

To further evaluate the Swedish technological strength, a comparison of the number of Swedish sensor patents to the Israeli and German number of patents was made, and revealed the results shown in figure 4-7.

²¹⁴ USPTO, www.uspto.com, 2004-11-12

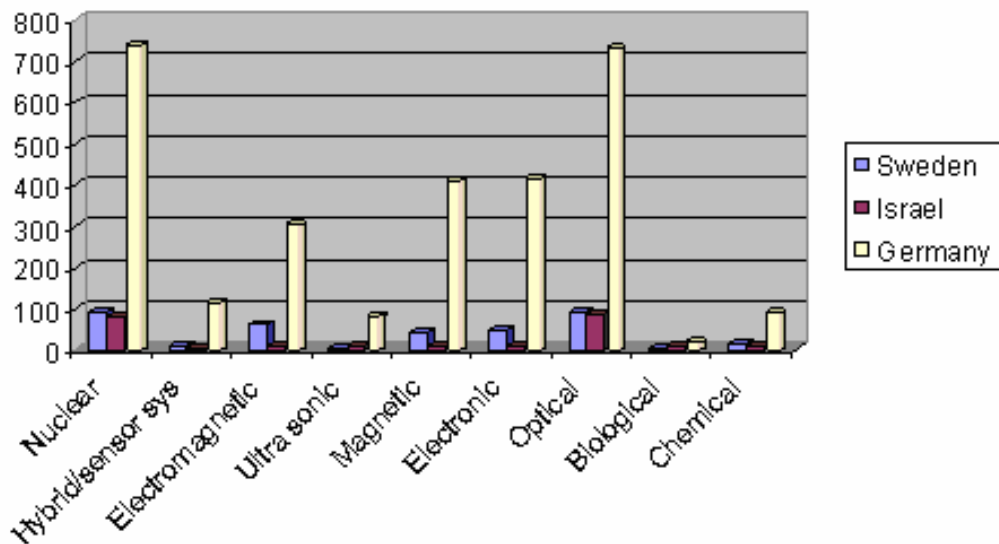


Figure 4-7 The number of sensor patents in Sweden, Israel and Germany 1976 to 2004

Compared to the other countries, Germany has a vastly higher patenting activity. The result is not that surprising regarding the amount of people and companies active on the German market. The next graph in figure 4-8 shows amount of sensor patents divided by the number of citizens of each country respectively. The result shows a slightly higher activity in Sweden than in Germany and Israel.

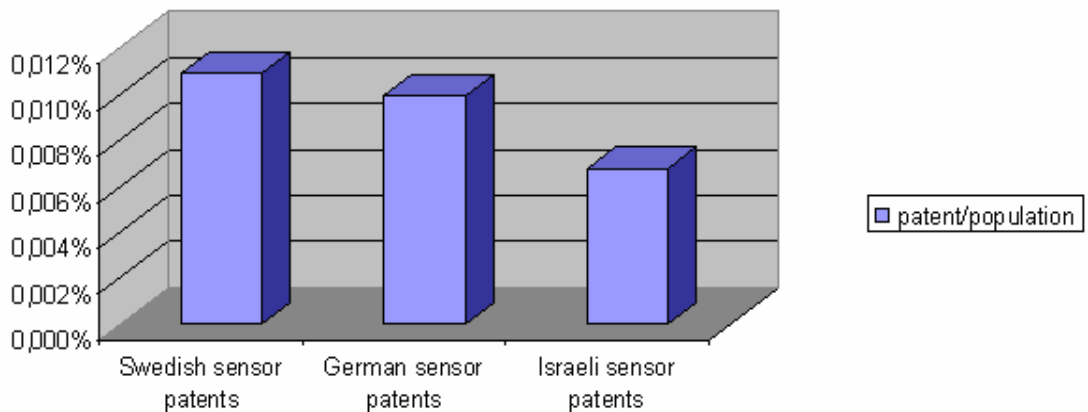


Figure 4-8 Amount of sensor patents per capita for Sweden, Israel and Germany

The patent analysis has identified electromagnetic sensors as Sweden's most prominent field of technology referring to sensors.

This strength has been confirmed by the innovation system actors. Regarding the commercial companies within the electromagnetic field, Ericsson Microwave is world leading in many technological fields related to radar. Also, Saab Bofors Dynamics is number one in the world in specific radar technologies which is accentuated by their role as responsible for the international development project

of the radar-air-to-air missile Meteor²¹⁵. FOI has highly skilled employees working on research and development of radar and optic sensors. The actor is world leader in low frequency radar technology and is also in the front concerning antenna technology²¹⁶.

Concerning electromagnetic sensors, industry actors have identified a knowledge shortage on the market related to radar and sonar technologies. This is a consequence of the fact that no national university education concerns these fields of technology²¹⁷. Therefore, this kind of technological knowledge is found internally within the companies.

Related to nuclear sensors, FOI System is the main actor. FOI System is among the two most prominent sensor developers for detecting inert gases. This is a technology which is used internationally for detecting conducted nuclear bomb tests. Also, FOI System possesses technology which can be very useful for security applications²¹⁸. However, concerns about lack of research related to nuclear physics have been raised. Nuclear physics is an important knowledge component in nuclear sensor development. The problem is derived from the deregulation of nuclear power which in turn has affected the amount of nuclear research conducted²¹⁹.

The amount of optical sensor patents is below the national average. However, both Acreo and Saab Bofors Dynamics are prominent in optic sensors. Acreo positions itself in the lead internationally regarding IR-sensor technology. Their research in this particular technological field is developed into products by the American company Flir Systems²²⁰.

Regarding biological and chemical sensors Sweden hosts several actors which are in the lead of their specific technological field. The Swedish company Biosensor Applications has a unique competence in surface chemistry related to biosensors. Also, Applied Sensor is world leading in their technological field, namely MOS and FE-sensor technologies²²¹. However, The Swedish Emergency Management Agency, SEMA, recognises a lack of research in biosensor technology²²². This standpoint is shared by the research institute IMEGO which also identifies a gap between the potential of biosensors and the research conducted in this

²¹⁵ Interview, Oderland, Ingvar; Ericsson Microwave Systems AB; 2004-10-15 and Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22

²¹⁶ Interview, Klasén, Lena; FOI Sensor Systems ; 2004-10-26 and Josefsson, Anders; Acreo AB; 2004-10-21

²¹⁷ Interview, Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22

²¹⁸ Interview, Olsson, Nils; FOI; 2004-11-10

²¹⁹ Interview, Olsson, Nils; FOI; 2004-11-10

²²⁰ Interview, Josefsson, Anders; Acreo AB; 2004-10-21

²²¹ (MOS) Metal Oxide Semiconductor sensors, (FE) Field Effect sensors

²²² Interview, Stern, Peter; Krisberedskapsmyndigheten; 2004-09-03

technological field. Although, IMEGO insinuates that this is probably an international problem²²³.

Another shortage which has been identified by the actors is the lack of in-depth research in specific technological fields related to biosensors. This fact can result in a shortage of pioneering technological discoveries and applications, which would hinder the Swedish sensor industry from obtaining advantages in an international context²²⁴.

Precise Biometrics and Fingerprint develop electronic sensors for biometric applications. Finger Print has identified a lack of research related to the physics and nature of the human finger. Especially, there is a lack of research on how the electric conductivity is affected by different physical parameters. This knowledge gap directly affects the prospects to enhance functionality of finger scanning applications²²⁵.

Market related knowledgebase

The majority of the Swedish sensor actors do not consider the Swedish market as important, mainly because of few potential customers. Therefore, it can be argued that knowledge about the international market is of higher relevance than knowledge concerning the national market. In general, the Swedish actors are considered to have good market related knowledge. Furthermore, this knowledge is related to both the national and international markets.

However, there exist mainly two important deficiencies concerning market related knowledge. Firstly, Ericsson Microwave, Saab Bofors Dynamics and FOI have all three expressed frustration over not being able to distinguish a national security market. These actors state that it is very important for their business to get clearer directions and indicators related to potential customer and customer demands²²⁶. The reason behind this statement could either be that these actors have recently identified the market and have not yet been able to gather enough knowledge about it, or that the market does not exist, and therefore no market related knowledge can exist. These factors are more thoroughly discussed in function 2.

Secondly, it has been stated that the national university research institutions lack sufficient insight in market demands²²⁷. However, the university institutions that

²²³ Interview, Björkholm, Peter; IMEGO AB; 2004-10-14

²²⁴ Interview, Krantz-Rülcker, Tina and Lundström, Ingemar; S-sence; 2004-10-19

²²⁵ Interview, Svensson, Peter; Fingerprint Cards AB; 2004-10-14

²²⁶ Interview, Oderland, Ingvar; Ericsson Microwave Systems AB; 2004-10-15 and Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22 and Klasén, Lena; FOI Sensor Systems ; 2004-10-26

²²⁷ Interview, Ljung, Lennart; ISIS; 2004-10-22

are part of a national centre of excellence have increased their market related knowledge. The national centres of excellence act as an intermediary in the communication between university research and commercial companies, which increase both technological and market related knowledge.

Application related knowledge

Several actors within the sensor industry mention the breadth in knowledgebase and the skill to combine different technologies as indispensable regarding possibilities to generate high-quality applications. The research institutes FOI and Acreo stress this specific factor as the most important concerning sensor development. Generally, Sweden is very prominent at combining different knowledge bases and technologies into applications providing a comprehensive solution to a specific problem. This is probably a result of the fact that Sweden is a small country geographically, making it possible for companies to easily overview the industry, which in turn enables for interaction with other actors. An example of the contrary is the USA, which possesses more resources but is not as proficient in combining technologies and knowledge²²⁸.

A shortage in application related knowledge related to the civil security market has been identified among the big actors. Mainly this derives from the fact that their main customers, the governmental authorities, do not possess the necessary competence for communicating their needs for security applications²²⁹. It can also derive from the fact that it exist cultural differences between commercial firms and governmental authorities. These differences hinder collaborations and communication, which in turn restrict the possibilities for commercial actors to identify customer demands and needs for security applications²³⁰.

Also, The Swedish biometrics company Fingerprint have expressed concerns about a knowledge shortage related to packaging technology, i.e. knowledge on how to generate a robust product out of existing technology and applications that solves customer demands. This might be a result of that this kind of knowledge is found among the producers of sensor applications. These producers are mainly found abroad, thereof the difficulty of finding sufficient application related knowledge on the national market²³¹.

Production related knowledge

²²⁸ Interview, Klasén, Lena; FOI Sensor Systems ; 2004-10-26

²²⁹ Interview, Olsson, Nils; FOI; 2004-11-10

²³⁰ Interview, Måwe, Karin; Krisberedskapsmyndigheten; 2004-11-10

²³¹ Interview, Svensson, Peter; Fingerprint Cards AB; 2004-10-14

No general shortages related to production knowledge have been identified. However, several actors have questioned the profitability of producing in Sweden since related costs are high.

Knowledge generation

Generally, knowledge is generated internally by R&D projects. This is especially the case when the R&D project is in some form of collaboration between supplier and customer²³². FMV has a reputation of possessing extensive knowledge about Swedish defence industry and its capacity. At several occasions, FMV has contributed to the knowledge generation among Swedish actors. Since the major defence industry actors also have been identified in this report as major actors on the Swedish security sensor industry, the survival of FMV do affect the civil security industry and related knowledgebase. Historically, FMV has guided the companies in a well reasoned direction concerning development and research issues. This guiding action has contributed to the Swedish competitiveness not only in the defence industry but also in related industries, as for example telecom. With substantial foresight and generously financing to FMV initiated projects, FMV has been an important factor when increasing companies' knowledgebase. This means that, because of the strong relationship between defence and civil security products, if FMV loses its resources and becomes less competent as customer, it will also have an impact on the development of the national knowledgebase related to security sensor industry²³³.

Also, as earlier stated, national centres of excellence and research institutes work as intermediaries between universities and companies. They communicate and shape university research or research conducted inside the research institute into profitable sensor applications. The fundamental idea of the national centre of excellence is to provide efficient research environment for the Swedish industry. The increased cooperation between industry and university makes it possible for the industry to articulate their demands for competence directly to the university. Hence, the national centres of excellence possess the role of a competence enhancer²³⁴. Reports on the subject have shown that the national centres of excellence are in fact enhancing the knowledgebase in both industry and university areas²³⁵. Also, the national centre of excellence S-sence is arranging

²³² Interview Rödfalk, Albert; Precise Biometrics AB; 2004-10-28 and Oderland, Ingvar; Ericsson Microwave Systems AB; 2004-10-15 and Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22 and Klasén, Lena; FOI Sensor Systems ; 2004-10-26

²³³ Interview, Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22 and Klasén, Lena; FOI Sensor Systems ; 2004-10-26

²³⁴ <http://www.vinnova.se/main.aspx?ID=EBE6E511-F396-45EB-9046-6602F8F72041>, 2004-11-01

²³⁵ Arnold.E, 2004

university courses in sensor technology. This further enhances the national knowledgebase related to sensor technology.

Furthermore, the Swedish public procurement act, LOU, affects the generation of national knowledgebase in a number of ways. Most importantly the act prevents direct acquisition, and therefore it favours competition between industry actors. Increased competition on the national market improves the abilities of the Swedish actors and makes them more sustainable for international competition²³⁶.

Conclusion

In this section, it has been shown that the functional weaknesses and strengths are:

- There is a strong technological competence in the Swedish security sensor innovation system.
- There is a lack of market related knowledge among the large industry actors.
- There is a need for company internal development of sensor related knowledge.

4.4.2. Function 2. Provide incentives and guide the direction of search

This function describes the incentives that exist for market entry as well as available guidance for Swedish sensor security industry in order to predict and direct their business to meet future demands.

Incentives for market entry

The Swedish security sensor market is relative unimportant to many actors²³⁷. Swedish customers does not posses enough financial capital to be an interesting customer or generate enough revenue for providing an interesting market²³⁸. Newly started small and medium sized companies are less concerned about the Swedish market. These actors assign a minor, if not non-existing, importance to the Swedish market concerning both R&D opportunities as well as for generating revenue. The reason to why these actors are situated in Sweden depends on the fact that the business was established here and factors preventing them from moving are related to cultural issues.

The identifiable drivers or incentives for entry onto the security market are found abroad. The USA and the European Union are investing vast resources on research

²³⁶ Interview, Klasén, Lena; FOI Sensor Systems ; 2004-10-26

²³⁷ Interview, Klasén, Lena; FOI Sensor Systems ; 2004-10-26, and Rödfalk, Albert; Precise Biometrics AB; 2004-10-28 and Svensson, Peter; Fingerprint Cards AB; 2004-10-14

²³⁸ Interview, Svensson, Peter; Fingerprint Cards AB; 2004-10-14 and Holmberg, Per and Karlsson, Magnus; Applied Sensor Sweden AB; 2004-10-19

and development of security applications and technologies. Both the European Union and the USA have, by institutional changes, articulated the potential of the security industry. The PASR articulates the European commitment to invest in security enhancing applications and technologies. Also, it has been decided that the budget for European security research will be further increased in coming years²³⁹. Each of the 25 member countries are eligible to seek financial means for development²⁴⁰. In the USA, the Department of Homeland security posses a strong budget intended for development and acquisition of sensor applications and technologies. Today, there exist no direct hindrances for Swedish companies to seek partnership with DHS²⁴¹. For the moment, at least one Swedish company has taken this opportunity and is developing sensor technology in cooperation with DHS.

Regarding the classical defence companies, such as Ericsson Microwave and Saab Bofors Dynamics, as well as the research institute FOI, they are entering the security market mainly because of the economical cutbacks in the national defence budget. It can be argued that these actors have been more or less forced to discover new markets in order to guarantee the survival of their businesses. However, the transition from defence to civil security industry has been difficult since the transition between the two markets is also characterized by a transition from a mature to an immature market²⁴². The consequences of this phenomenon are described later in this section.

Articulation of demand

Generally, the articulation of demand on the Swedish market is considerably weak²⁴³. In order to achieve R&D guidance, Swedish companies have started to search for indicators abroad. Such indicators are achieved from analysing the investment activity of Department of Homeland Security but also by considering the threat picture of terrorists and organized criminal groups²⁴⁴.

The lack of guidance is especially stressed by the companies operating in the defence industry. These companies are used to having a competent customer, namely FMV, which also has been able to guide the direction of search. FOI, Ericsson Microwave and Saab Bofors Dynamics all think it is absolutely

²³⁹ Kleja.M, 2004

²⁴⁰ Internet, Busquin.P, 2004

²⁴¹ Karlsson. M, 2003

²⁴² Interview, Klasén, Lena; FOI Sensor Systems ; 2004-10-26 and Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22

²⁴³ Interview, Klasén, Lena; FOI Sensor Systems ; 2004-10-26 and Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22, Aastrup, Teodor; Attana AB;2004-10-13 and Månsson, Per; Biosensor Applications Sweden AB; 2004-10-13

²⁴⁴ Interview, Oderland, Ingvar; Ericsson Microwave Systems AB; 2004-10-15

indispensable to have a strong articulation of demand. Today, they all have identified the potential of the civil security market, and they also recognize Sweden as a very strong future market actor, especially regarding sensor technology. These actors believe that the requisite knowledgebase for making Sweden competitive exists. However, the Swedish market is currently invisible. The poorly working market is partly an effect of absent customer competence. Regarding these type of actors, the customers are governmental authorities, as for example the police, the Swedish customs and the Swedish coast guard. It has been stated that all or some of these customers lack sufficient competence related to technology and applications, which disenables them to take the role as a strong customer that possesses the ability to guide the direction of search²⁴⁵. Furthermore, currently no coordination between these governmental authorities concerning purchasing process or correlation in demands for security applications exists. The lack of coordination originates from the fact that no governmental authority sees itself as responsible for initiating procedures in order to become more coordinated or in order to enhance the internal purchasing competence²⁴⁶. A clear and coordinated customer with good insight in sensor technology and related demands is essential to boost the Swedish security sensor market. Hence, a customer with resources to give guidance and initiate long-term projects reaching over several years is requested²⁴⁷. Therefore a civil FMV or similar organisation is demanded by these companies²⁴⁸.

Among the smaller companies, the need of a clear articulation of demand does not seem to be as critical as expressed by the big actors. This can be derived from the fact that the smaller sized companies do not demand the same amount of resources and guidance of direction. It can also be related to the fact that these companies have been active on the security sensor market for a longer time, and have therefore been able to identify other sources that can articulate the demand. As earlier described, the former defence companies have just recently discovered the security market and have not yet had the opportunity to more thoroughly investigate the security market characteristics. However, even in the future, it does not seem likely that these actors will find a potential national customer without any institutional changes regarding the coordination between governmental authorities.

On the other hand, it might be argued that it is not entirely only up to the authorities to improve their work. The companies, which are used to having FMV as their customer, find it very convenient since FMV is a very strong project initiator and leader. However, according to FMV, the actors have to become more

²⁴⁵ Interview, Olsson, Nils; FOI; 2004-11-10

²⁴⁶ Interview, Zachrisson, Elisabeth; Försvarets Materialverk; 2004-11-01

²⁴⁷ Interview Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22

²⁴⁸ Interview Klasén, Lena; FOI Sensor Systems ; 2004-10-26 and Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22

dynamic and energetic in their business approach in order to manage the new business circumstances and meet the international competition²⁴⁹.

Another view on articulation of demand is the one related to university research. Today, extensive sensor technology research is conducted at Swedish universities. In order to facilitate the communication of demand between university research and industry, several national centres of excellence work as forums for cooperation. The fundamental idea of this cooperation is to guide the university research and implement conducted research into competitive industrial products²⁵⁰. S-sence and SUMMIT are examples of such national centres of excellence related to the security sensor industry. Both these national centres of excellence are driven by the expressed needs of the member companies, which often results in one- to two-year-projects.

Regulations influencing the direction of search

Generally, regarding the sensor security market as a whole, there are no regulations or standards affecting the direction of search. In the future, the private integrity discussion may result in regulations affecting sensor technology and applications. However, this discussion is more related to the legitimacy of sensor technology and will therefore be more narrowly described in function 6.

The discussion about regulations and standards and their effect on business is most distinctively expressed in the biometrics sensor industry. The American Identify Card project presidential act 12, as well as European regulations associated with the European Union passport project have provided the industry with directives of demands related to technology and applications²⁵¹. No similar projects or regulations affecting other sensor technologies have been identified.

The regulation concerning improved security at international seaports has given the industry an indication of potential customer segments. This regulation has expressed container screening and container identification applications as important sectors of investments²⁵². Also, an even stronger regulation will be introduced during 2006. This regulation is predicted to express stronger needs for underwater surveillance at seaports²⁵³. These kinds of regulations have provided some guidance related to application design. For example, increased security at seaports have provided guidance related to which applications that are sought after. Several actors also request development of such regulations for local authorities. They mean that such regulations would more efficiently express the

²⁴⁹ Interview Zachrisson, Elisabeth; Försvarets Materialverk; 2004-11-01

²⁵⁰ <http://www.vinnova.se/main.aspx?ID=EBE6E511-F396-45EB-9046-6602F8F72041>, 2004-11-08

²⁵¹ Interview, Rödfalk, Albert; Precise Biometrics AB; 2004-10-28

²⁵² Internet, Enhancing port security, 2003

²⁵³ Interview, Kajrud, Katrin; Göteborgs hamn AB; 2004-09-09

local and national authorities' demands, which is necessary if the big actors are to regard these authorities as potential customers²⁵⁴.

Conclusion

In this section, it has been shown that the functional weaknesses and strengths are:

- There is a lack of incentives for entering the market in Sweden, but incentives can be found abroad.
- The articulation of the government agencies' demand is poor.
- There is insufficient guidance related to direction of search.

4.4.3. Function 3. Promoting entrepreneurial experimentation

The third function aims at identifying factors influencing the capabilities to perform entrepreneurial experiments. This section will identify the numbers of new entrants on the security sensor market, which is an indicator of earlier entrepreneurial experimentation activities. Further indicators revealing currently and future entrepreneurial experimentation will be investigated.

New entrants

Following graph represents the number of entrants per year on the sensor security industry²⁵⁵.

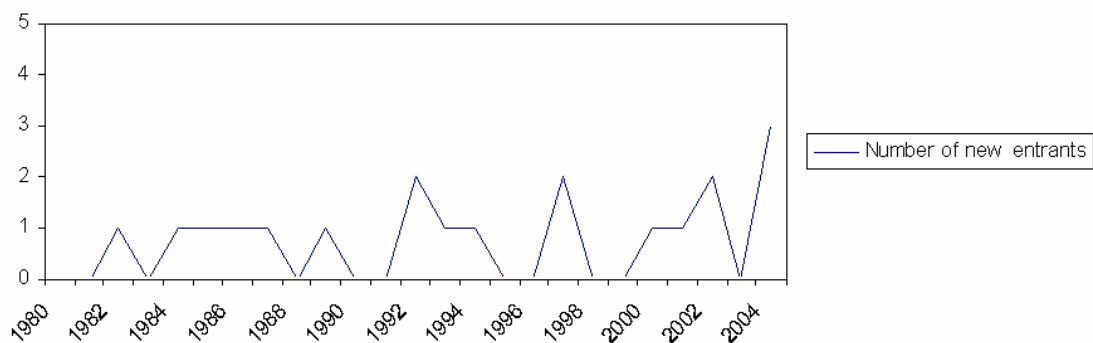


Figure 4-9 Number of entrants per year on the Swedish sensor security industry

Since 1980, the number of new entrants has been constantly fluctuating between none, one or two new businesses per every second year. Interestingly, three companies related to the sensor security industry have been founded during 2004.

²⁵⁴ Interview, Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02 and Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22.

²⁵⁵i.e companies registered in affärsdata

This reveals a possible trend where the number of new entrants is modestly increasing.

Another indication of potential new market entrants can be derived from the number of sensor security patents issued to private persons. It can be argued that these persons are waiting for their patent application to be granted until they set up a business based on the patented technology²⁵⁶. Therefore, by investigating the number of patents issued to private persons, a number of potential future entrepreneurial experiments can be reached. Following graph shows the number of such patents on yearly bases.

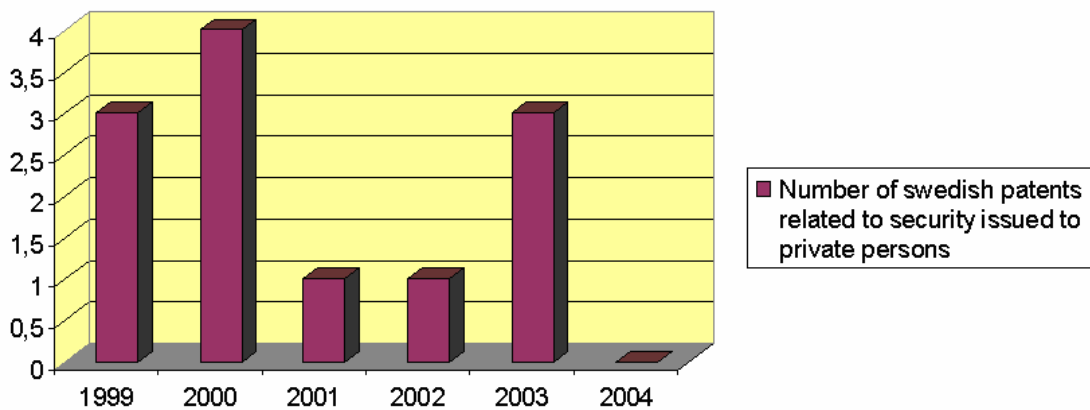


Figure 4-10 Number of Swedish patents related to security sensors issued to private persons

However, there is no obvious trend in the number of Swedish sensor security patents issued to private persons. From a relative high number in 1999 and 2000 the number has then decreased in following two years.

The general opinion in the security sensor industry is that the number of new entrants into the market is stable or even decreasing²⁵⁷. The research centre Acreo works with development of new products and applications for entrepreneurial companies. Hence, Acreo has solid foundation to base there statement on, regarding number of new entrants. Acreo states that the decrease in new entrants could be a result of less venture capital on the market. A couple of years ago it was easier to extract venture capital than it is today²⁵⁸.

Hindrances for establishment

Very few seed capital investments, combined with the fact that several smaller actors perceive the process of seeking research allowances to be time and resource

²⁵⁶ Jacobsson..S, 2004b

²⁵⁷ Interview Holmberg, Per and Karlsson, Magnus; Applied Sensor Sweden AB; 2004-10-19 and Josefsson, Anders; Acreo AB; 2004-10-21 and Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

²⁵⁸ Interview Josefsson, Anders; Acreo AB; 2004-10-21

consuming, can be another explanation to why no increase in new entrants has occurred²⁵⁹. In 2001, the European Union conducted an analysis regarding the innovation climate in the European Union member countries. The report concluded that Sweden was ranked last relating to the amount of seed capital invested²⁶⁰. This fact has been confirmed by the Swedish Venture Capitalist Association that predicts that only 9.3 percent of existing Swedish VCs investments are related to seed projects²⁶¹. The start-up and expansion phases are much more characterized by venture capitalist involvement²⁶². This fact makes it difficult for entrepreneurial experimentation. The newly founded sensor company Airborne Hydrography, expresses the difficulties to extract seed capital. They are also criticizing the efficiency of public funding from national authorities. Airborne Hydrography, with others, perceives the process of seeking allowance as too resource demanding and inflexible. They believe that the authorities should concentrate their resources on helping the companies, and not waste money on complicated application processes²⁶³.

Furthermore, several actors on the security sensor market mention the fact that the sensor industry is characterized by high hindrance for establishment related to high initial capital investments and economics of scale. Investing in necessary capital equipment as well as developing and buying basic components in low volumes demand strong financial resources²⁶⁴. Also, the sensor industry is research intensive and the lead time between R&D and related revenue is long. The fact that the venture capital market is relatively weak regarding seed capital investments creates even stronger hindrances for establishment.

R&D activities within existing actors

In larger companies, a main indicator of entrepreneurial activities can be derived from the breadth of R&D projects. Regarding new approaches in companies R&D strategies, the policies differ between small and large actors. Smaller companies seem to be more focused on surviving which means that they cannot invest resources in broadening their approach to R&D. Also, in order to compete internationally, which is the only possibility to generate revenue since the Swedish market is too weak. The smaller companies need to focus on being world leaders in one specific field of technology. This focus decreases the scope of R&D projects

²⁵⁹ http://www.uppfinnaren.com/nr3_02/sadd.htm, 2004-10-29

²⁶⁰ http://www.uppfinnaren.com/nr3_02/sadd.htm, 2004-10-29

²⁶¹ http://www.vencap.se/article_view.asp?ArticleID=31, 2004-10-27

²⁶² <http://www.vencap.se/docs/2004%20Q2%20Riskkapitalbolagens%20aktiviteter.pdf>, 2004-11-01

²⁶³ Interview Aastrup, Teodor; Attana AB; 2004-10-13 and Engström, Rolf; Airborne Hydrography AB; 2004-10-12

²⁶⁴ Interview, Svensson, Peter; Fingerprint Cards AB; 2004-10-14 and Holmberg, Per and Karlsson, Magnus; Applied Sensor Sweden AB; 2004-10-19, confirmed by Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22

initiated by the companies²⁶⁵. Finally, smaller companies are more dependent on their customers, resulting in that they are developing existent technology to fit the customer's need instead of investing resources on entrepreneurial research²⁶⁶.

Larger companies have generally more resources to spend on research in new technological fields. FOI has an official policy that research in entirely new technologies or directed towards new market shall be given opportunities to emerge. Such projects will be given internal financing up to 20 million Swedish crowns²⁶⁷. Saab Bofors Dynamics has an internal organisation, Venture Council Capital, VCC, that facilitates for company spin-offs. VCC assists promising internal business ideas with resources until they are developed into companies able to generate enough revenues to become self supporting. VCC can help the company by technical consulting and by mediating connections to potential customers and financiers.

Institutions affecting entrepreneurial experimentation

Institutional actions have affected the promotion of entrepreneurial experimentation. For example, the establishment of national centres of excellence has led to increased guidance in companies' R&D trajectories and innovative thinking. Regarding small and middle sized companies, this effect has been observed to exist in the industry. However, it has also been observed that national centres of excellence have only limited impact on larger firms' ability to do the same²⁶⁸. Whether or not large companies are affected in the same degree as smaller ones, it can be concluded that national centres of excellence contribute to promoting entrepreneurial experiments. Since national centres of excellence are not specifically a Swedish phenomenon and since they exist in many technological fields, it is hard to grade the specific impact national centres of excellence generate on the security sensor market. On the other hand, if national centres of excellence had been absent on this particular market, it had definitely weakened the entrepreneurial function.

However, regarding the potential to generate entrepreneurial experiments, the role of national centres of excellence is two folded. The innovations generated under these circumstances are a result of research collaboration between commercial companies and university scientists. Hence, the proprietorship of developed innovations and related intangible assets is somewhat ambiguous. Also, venture capitalists avoid investing in projects where the rights of possessions are indistinct. Consequently, it can be argued that the national centres of excellence can also obstruct development of entrepreneurial experiments.

²⁶⁵ Interview Josefsson, Anders; Acree AB; 2004-10-21

²⁶⁶ Interview, Röd Falk, Albert; Precise Biometrics AB; 2004-10-28

²⁶⁷ Interview, Klasén, Lena; FOI Sensor Systems ; 2004-10-26

²⁶⁸ Arnold.E, 2004

Another institution affecting the entrepreneurial function is the Swedish public procurement act, LOU. The act complicates the process of public agencies' acquisition of supplies. In many cases, suppliers need specialized sales-personnel to be able to fulfil the requirements for the acquisition of supplies. Hence, LOU efficiently shuts out smaller companies from this market, since they do not possess the amount of resources required for seeking the contract.

Finally, the demand for higher degree of coordination between different authorities can affect the entrepreneurial function negatively. A centralized purchasing will create demands of larger volumes. It has been stated that smaller companies are incapable of supplying applications in the volume inquired for. Hence, the smaller companies are not distinguished as potential suppliers²⁶⁹. Therefore, current business environment with low degree of coordination is more suitable for promoting entrepreneurial experiments.

Conclusion

In this section, it has been shown that the functional weaknesses and strengths are:

- The current decentralization of the governmental purchasing function creates an advantageous business environment for entrepreneurial companies.
- There are few new entrants onto the security sensor market.
- There are difficulties in gaining governmental orders among smaller companies.

4.4.4. Function 4. Market formation

This function discusses the market growth and market drivers. To analyse these aspects it is important to first present the market segments and from them further analyse the factors that influence each one. Finally, general aspects of the market formation and the current market status are presented.

Market segments

Both the national and international market for security sensors can be divided into the four following segments.

- Air- and seaports
- Public safety agencies:
 - Police functions

²⁶⁹ Interview Zachrisson, Elisabeth; Försvarets Materialverk; 2004-11-01

- Customs Services
 - Coastguards
- Military defence functions
- Commercial segment including mostly security companies that in turn have their customers in form of:
 - Larger corporations
 - Public event corporations
 - Fairs and exhibitions
 - Hotels
 - Real-estate companies
 - IT hard ware producers²⁷⁰

Market drivers

The main underlying drive that by different elements impels these four market segments is the threat, expressed through threatening pictures. These pictures are created by several organisations and are then applied on the market segments, either directly or indirectly through intermediate organizations and mediators. On an international level, the main organisations that articulate the threat and impact the segments with their threatening picture are NATO, FN and EU²⁷¹. On a national level, the Swedish security police SÄPO, partly in cooperation with the ministry of foreign affairs, influences the governmental agencies²⁷². Also, there is a perceptual threatening picture consisting of an interpretation of the above mentioned pictures mediated by media. This perceptual picture affects the commercial segment by influencing the end customer needs of security. In general, the threatening pictures are influenced by culture and political interest of the organizations creating them. Also, the process of formal and informal interpretation of thereat is somehow related to the political interests of the interpreting bodies²⁷³. As the threatening picture is mediated down to the governmental agencies and is further translated to a direct demand, the process of its interpretation and the customer's role and structure will additionally influence the market conditions. In the same way concerning the commercial segments, the interpretation by media and others together with the customer perception will influence the end demand.

Also, the perceived threat goes much hand in hand with actual incidents that often initiate apparent threats, like in the attacks of 9/11 and the train-bombings in Madrid 2004. These incidents augmented the general security consciousness, and the demand for security products, which created new markets. Hence, incidents

²⁷⁰ Including producers of mobile phones, computers, palms etc. with in-built security functions.

²⁷¹ Interview, Zachrisson, Elisabeth; Försvarets Materialverk; 2004-11-01 and Ramstedt, Annika; Luftfartsverket; 2004-08-30

²⁷² Interview Ramstedt, Annika; Luftfartsverket; 2004-08-30

²⁷³ Interview, Ramstedt, Annika; Luftfartsverket; 2004-08-30

influence the threatening picture and consequently also the market. Incidents can have both a local and an international impact, depending on size and location. Devastating incidents, like the attacks of 9/11, have both an international and national impact on the perceived threat. Local incidents, like augmented crime in a sector, only affect the local demand for security applications²⁷⁴.

Incidents can also influence the market in other ways. An incident affecting the Swedish market related to the security sector is the events of Ådalen, which resulted in a regulation restricting the possibilities of the Swedish defence to be involved in actions regarded as police commissions. This means that the responsibility for the acquisition of goods concerning the detection, prevention and counteraction of organized crime, terrorism etc, is assigned to the police, that is perceived as less competent regarding technicalities of equipment than the national defence²⁷⁵. The lack of competence in the police force restricts the articulation of demand and, in turn, the development of the market. However, the customer role of the defence and the police functions regarding protection against terrorist attacks are not firmly established, and the future practice of the Ådalen regulation is uncertain²⁷⁶.

The following figure illustrates the drive of the market for the segments and it will be further discussed below.

²⁷⁴ Interview, Pettersson, Lars; Vasakronan AB; 2004-11-09

²⁷⁵ Interview, Klasén, Lena; FOI Sensor Systems; 2004-10-26

²⁷⁶ Branacaglioni.M 2004

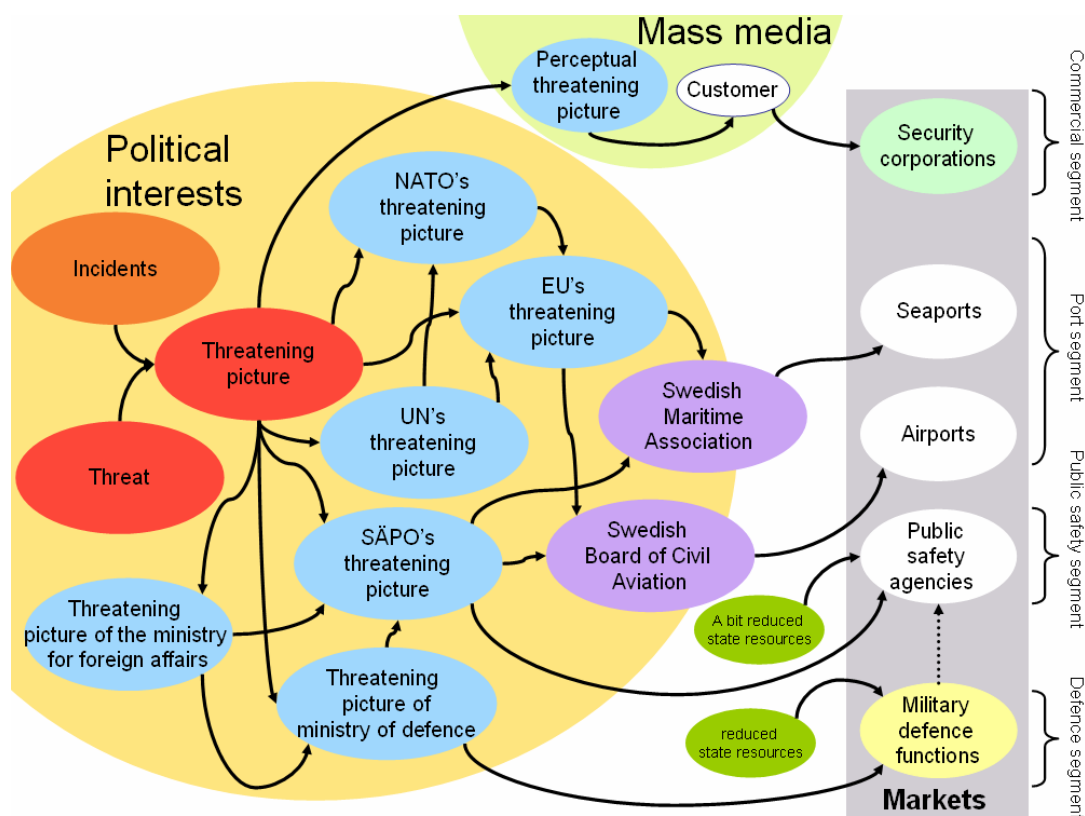


Figure 4-11 Factors driving the market segments

Defence segment drivers

Firstly, referring to the defence market segment, the ministry of defence, affected by the ministry of foreign affairs, articulates the national threatening picture for the Swedish military defence functions as shown in figure 4-11²⁷⁷. FMV plays a central role in the segment as the agency responsible of purchases for the Swedish defence. Secondly, the reduction in financial resources as a result of the disarmament of the Swedish defence is influencing the segment. It has previously been stated that the deregulation of the Swedish defence is highly affecting the innovation system as the role of FMV as a main customer is changing²⁷⁸. This segment is decreasing in size nationally, driving the classical military industry towards a change in their focus from military to civil customers, hence creating new markets. The decreasing government resources in the military segments can be traced back to the, relatively weak national threatening picture, the general reduction in state resources and the changing threat.

Public safety segment drivers

²⁷⁷ Interview, Zachrisson, Elisabeth; Försvarets Materialverk; 2004-11-01

²⁷⁸ Interview, Oderland, Ingvar; Ericsson Microwave Systems AB; 2004-10-15

Secondly, the public safety segment in Sweden, represented by the government authorities, is guided by the threatening picture presented by the Swedish security service, SÄPO²⁷⁹. The established picture drives the needs of the authorities referred to their security requirements²⁸⁰. This segment is currently increasing in importance due to the changing threat and the American initiative to create the Department of Homeland Security. It has been argued that the lack of conformity and knowledge in this segment obstructs the growth of it on the national level. On the international level, there have been some international regulations forming this segment and creating new markets, especially concerning biometrical applications in passports and identity documents²⁸¹.

Port segment drivers

Seaports are generally local government owned and independent from the State²⁸². Airports are all, except for one, governmentally owned through the Swedish Board of Civil Aviation, LFV²⁸³. Seaports and airports are strictly regulated by the Swedish Aviation Safety Authority and the Swedish Maritime Association as ports play a critical role in infrastructure. Like in the case of the public security agencies, SÄPO plays a crucial role in the creation of the threatening picture that affects the market through the two above mentioned regulating authorities. Also, as shown in figure 4-11, the European Union plays a significant role as it gives instructions, separate from the ones SÄPO gives, to concerned authorities on international level that in turn regulates the sea- and airports on national level.

A concrete example on how political decisions drive the market conditions is the effects of the directives from The Swedish Aviation Safety Authority regulating airport and aircraft security. These directives are strictly based on the European Union regulations (EG) 2320/2002 and (EG) 622/2003²⁸⁴, controlling the market of the aviation sector. This was a direct reaction to the incidents of 9/11. Large parts of the regulations concern increased screening of both passengers and goods, leading to a greater demand for applications enabling such procedures, which often are related to sensor technology. Concerning seaports, the European Union, through the act 2003/0089 (COD), has created similar directives on enhancing maritime transport security that has had an important effect on the market related to the demand for sensor applications. The regulation demands a greater supervision of the activities, goods and persons at seaports²⁸⁵. In practise, this has led to a larger request for security products such as detectors of antagonistic agents,

²⁷⁹ <http://www.sakerhetspolisen.se>, 2004-11-03

²⁸⁰ Interview, Ramstedt, Annika; Luftfartsverket; 2004-08-30

²⁸¹ Interview, Rödfalk, Albert; Precise Biometrics AB; 2004-10-28

²⁸² <http://www.sjofartsverket.se/navigering/htm/frameset.htm> 2004-12-06

²⁸³ Interview, Ramstedt, Annika; Luftfartsverket; 2004-08-30

²⁸⁴ Interview, Ramstedt, Annika; Luftfartsverket; 2004-08-30

²⁸⁵ Internet, Enhancing ship and port facility security, 2003

metal detectors and screening equipment, all related to sensor technology²⁸⁶. Consequently, this increased demand has led to an augmented interest in the sensor industry. Both seaports and airports have been considered by several of the actors as presenting an interesting and highly potential future market.

Commercial segment drivers

Finally, the demand of commercial segment is formed by the end customer's perceived threat. The segment does not have the access to the threatening pictures formed by the authority actors. Instead, a perceptual threatening picture is formed by the general notion of the society of the level of threat. Mass media is an important factor which in many cases plays a crucial role as an interpreter and conveyer of directives affecting the governmental sectors and incidents. Generally, including the international market, this segment is growing. However, as stated above, the Swedish threatening picture is weak, which results in a small national commercial market with low demands²⁸⁷.

Factors influencing market formation

Basically all actors agree on the fact that the Swedish market is too small when it comes to generation of large revenues. However, its role as a development market has been stressed. It has also been mentioned that the national market is important when it comes to demonstrating implemented examples of applications²⁸⁸. However, this is not the opinion of all the actors in the security industry. For other Swedish actors, the main role of the national market has been to provide a market for development. It can be argued that this is first and foremost connected to geographical advantages and personal networks. There is also a third group of actors in the sensor industry, often without any customer contact with government authorities²⁸⁹. These are newly started small or medium size companies that assign a minor, if not non-existing, importance to the Swedish market concerning both their development possibilities and profitability.

Still, in the case of seeking a profitable market, many of the actors focus on the USA. The American market is perceived as highly potential and many of the smaller companies are focusing on that market. As stated in the industry survey, the Bush administration has made a huge number of investments in the security sector owing to the creation of the Department of Homeland Security. The driving

²⁸⁶ Interview, Kajrud, Katrin; Göteborgs hamn AB; 2004-09-09

²⁸⁷ Interview, Svensson, Peter; Fingerprint Cards AB; 2004-10-14 and Rödfalk, Albert; Precise Biometrics AB; 2004-10-28

²⁸⁸ Interview, Månsson, Per; Biosensor Applications Sweden AB; 2004-10-13

²⁸⁹ Interview, Svensson, Peter; Fingerprint Cards AB; 2004-10-14

force in this case is the threat as perceived by the American government, highly influenced by the incidents of 9/11.

Further, the Swedish public procurement act, LOU, is a factor that plays an important role in the acquisition of supplies involving local government agencies, county councils, government agencies as well as certain publicly owned companies. The act regulates almost all form of public procurement, which means that above mentioned contracting entities must comply with the act when they purchase, lease, rent or hire-purchase supplies, services and public works²⁹⁰. In the case of sensor products related to security applications, concerned agencies could include the Swedish defence, the Swedish police, non-private airports and seaports, the Swedish customs, the Swedish Rescue Services Agency, etc. Concerning the market conditions, the act influences the market in a number of ways. First, the acquisition of supplies by public agencies is perceived as complicated and time-consuming by many of the industrial producers. In many cases suppliers need specialized sales-personnel to be able to fulfil the requirements for the acquisition of supplies. This restricts small and medium sized firms. However, the act has also resulted in an increased competition, making the Swedish actors more competitive in the international environment²⁹¹. Also, the act gives scope for a direct acquisition of supplies concerning strategically and public security related matters²⁹², giving a certain advantage to Swedish companies²⁹³. On the other hand, this direct form of acquisition of supplies has its disadvantages when it comes to broadening the competence. Since, many of the actors believe that the advantages of having a chance of obtaining a close and long-term relationship that often comes out of a direct purchasing process outweigh the disadvantages related to loss in competitiveness. The resulting closeness to the customer gives the supplier a highly valuable understanding of the needs and expectations of the customer. Concerning civil sectors, direct acquisition of supplies is not possible, excluding purchases relating to small amounts of money. It has frequently been mentioned that it would be advantageous to have the same possibility in the civil sector, given the advantages that could come with a direct acquisition of supplies²⁹⁴.

Another governmental agency forming the market through regulations is the ISP²⁹⁵. This Swedish agency controls the export of military equipment and other products that may have both a civilian and a military use, so-called dual-use products. ISP is also the national authority under the CWC. Military equipment may be exported but only after inspection in relation to the country's foreign policy principles stated under Section 1 of the Swedish Military Equipment Act.

²⁹⁰ Lagen (1992:1528) om offentlig upphandling, ändringar enligt SFS 2002:594

²⁹¹ Interview, Klasén, Lena; FOI Sensor Systems; 2004-10-26

²⁹² Lagen (1992:1528) om offentlig upphandling, ändringar enligt SFS 2002:594

²⁹³ Interview, Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22

²⁹⁴ Interview, Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22

²⁹⁵ <http://www.isp.se/>, 2004-11-12

The inspection of each individual case is based on the guidelines covering the export of military equipment. The Act is a prohibitive piece of legislation and the activities provided for under the Act are forbidden in principle. Therefore, an exemption has to be issued in each individual case. Since many of the companies active in the defence sector of sensor technology, and that sensor technology often is developed in military context, the Swedish Military Equipment Act limits the possibility of these actors to grow.

Another factor influencing the national market is the internationalization. Today, an international threatening picture is applied on the Swedish market, both formally through the EU directives and the influence of FN and NATO on the threatening picture, and also informally through the increased notion of the global status and the general internationalization. A stronger international threatening picture has increased the national market demand given the internationalization.

In Sweden, it is not allowed to give priority to national firms in processes of public acquisition due to LOU. It is, according to LOU, prohibited to give local firms preference because of their geographical location²⁹⁶. The Swedish government can decide on exceptions to this regulation regarding matters concerning defence or security policy. This is the case in some of the acquisitions of goods involving FMV and their suppliers. Abroad there are some extensions of the possibility for national firms to get priority over foreign firms. An example is the buy American act, a law in favour of American investors concerning public acquisition of supplies²⁹⁷. Though, in some cases the Swedish actors find their way around these regulations, as for example Bofors Defence, because of American owners has acquired orders from the American coastguards²⁹⁸. Also, Swedish actors without an American parent company can get access to this market by finding an American business partner. Although the advantages of a propitiation of the Swedish actors in the acquisition of supplies are clear, it can be argued that there is a risk of losing international competitiveness due to a reduced degree of competition on the market²⁹⁹. At se same time, the Swedish market is highly limited compared to the American, leaving Swedish actors with little possibilities to grow.

Conclusions

In this section, it has been shown that the functional weaknesses and strengths are:

- A strong international threatening picture is increasing the Swedish market demand.

²⁹⁶ Lagen (1992:1528) om offentlig upphandling, ändringar enligt SFS 2002:594

²⁹⁷ Förutsättningarna för en överenskommelse mellan EU och USA på investeringsområdet, Dnr 117-2537-98

²⁹⁸ Askman.T, 2004

²⁹⁹ Interview, Oderland, Ingvar; Ericsson Microwave Systems AB; 2004-10-15

- No market where Swedish companies are prioritized exists.

4.4.5. Function 5. Mobilization of resources

This section aims at analysing the supply of resource available on the market, enabling for satisfactory company business development. Firstly, this function will analyse the amount of human resources available, followed by the amount of financial resources.

Mobilization of human resources

Generally, no actor on the security sensor market has expressed any shortages related to the amount of human resources available. Since the start of the economic recession in 2000-2001, skilled labour has been dismissed, resulting in an increase in human capital recourses on the opened labour market. Referring to the sensor market, the reduction of personnel at Ericsson has provided the security sensor market with highly skilled human resources³⁰⁰.

However, industry actors have expressed that it exist a shortage in human resources related to personnel with competence in radar and sonar technology. This is a direct consequence of the fact that no national university education addresses theses technological fields³⁰¹. Also, in coming years, a shortage is predicted to occur related to skilled personnel with competences in nuclear physics. This can be derived to the deregulation of nuclear power, which in turn reduces the possibilities to find work after graduation. Hence, education related to nuclear physics is assumed to be perceived as less attractive in the future, which will decrease the amount of skilled people in this technological field³⁰².

Entrepreneurial companies, which have been created from larger company spin-offs, often receive human resources from the parent company. Such examples have been identified both in spin-offs generated by Saab Bofors Dynamics and Ericsson Microwave. Also, at Saab Bofors Dynamics it exists an internal organisation that helps company spin-offs to find satisfactory resources³⁰³.

The breadth of the knowledgebase is essential for sensor development. It is important to have sufficient access to civil engineers, specialized in the diverse sensor technologies. By reviewing the number of graduated from university

³⁰⁰ Interview, Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22

³⁰¹ Interview, Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22 and Oderland, Ingvar; Ericsson Microwave Systems AB; 2004-10-15

³⁰² Interview, Olsson, Nils; FOI; 2004-11-10

³⁰³ Interview, Engström, Rolf; Airborne Hydrography AB; 2004-10-12 and Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22 and Oderland, Ingvar; Ericsson Microwave Systems AB; 2004-10-15

educations related to sensor development, and by comparing the national number to other country's, an indication of the national resources of civil engineers will be reached. Following graph shows the change over time in students graduating from sensor related educations³⁰⁴.

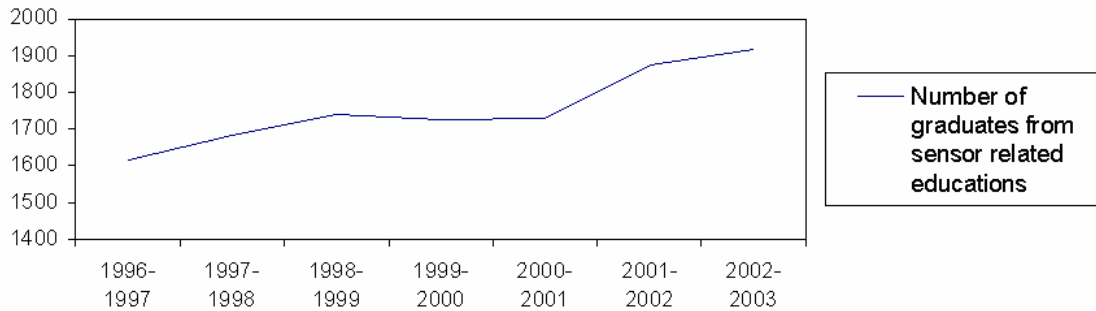


Figure 4-12 Number of graduates from sensor related educations³⁰⁵

After stagnation in graduated students between 1998 and 2001, the number is once again increasing and has today reached above 1900 graduates per year. However, when comparing the ratio between the number of inhabitants related to the total population possessing a Master of Science degree in Sweden compared to Germany and Israel, the Swedish ratio is relative weak. In Sweden the number of graduates with a Master of Science degree related to the total population was 0.11 percent in 2003³⁰⁶. Under the same period Israel had a ratio of 0.26 percent³⁰⁷, and Germany had a ratio of 0.36 percent³⁰⁸.

Mobilization of financial resources

One step in deciding the amount of financial resources within the innovation system is to analyse the amount of venture capital available on the market³⁰⁹. Swedish venture capitalists possess close to EURO 12 billion in total amount of funds. Ten years ago, the amount of venture capital was close to non existent. Currently, the Swedish venture capital market is very strong, and has the highest ratio of investment/GDP in Europe³¹⁰.

³⁰⁴ According to S-sence, suitable educations are Master of Science in or similar education in, chemistry, physics, material technology, microbiology, computer science, and electronics.

³⁰⁵ http://www.scb.se/statistik/UF/UF0205/2002I03/UF0205_GE_Tab3.xls, 2004-10-22

³⁰⁶ http://www.scb.se/statistik/UF/UF0205/2002I03/UF0205_GE_Tab4.xls, 2004-10-22

³⁰⁷ http://www1.cbs.gov.il/shnaton55/st08_41.pdf, 2004-10-24

³⁰⁸ http://www.destatis.de/themen/e/thm_bildung.htm, 2004-10-24

³⁰⁹ Jacobsson. S, 2004b

³¹⁰ http://www.isa.se/upload/english/Publications/Venture_Capital.pdf, 2004-11-03



Figure 4-13 Venture capital investments in Europe 2001³¹¹

The Swedish venture capitalists are mainly investing in the high tech industry and about 60 percent of these investments tech are related to information and telecommunication technology, ICT, or life science technology. Since sensor applications by definition fit in the high tech segment, it can be argued that because of the Swedish venture capitalist's preference for this sector, it would be more likely for sensor technology companies to extract venture capital than for a general, average company.

There is a weak activity in seed capital investments on the Swedish market. Still, the amount of seed capital investments do not effect the total amount of resources on the market, but it do make it more difficult for entrepreneurial experimentation which was more thoroughly discussed in function 3.

Concerning sensor technology, there are no statistics related to the amount of capital invested in this particular technological field. However venture capitalists investing in fields related to sensor technology, such as electronics, computer hardware, biotechnology, industrial products, material science and chemistry, are managing funds of EURO 2.7 billion³¹². The international venture capitalists active on the Swedish market who are investing in these technological fields manage funds of EURO 12 billions³¹³.

Following graph presents statistics concerning the number of national and international venture capitalists active on the Swedish market. It also shows the number of venture capitalists that have invested in sensor companies respectively

³¹¹ http://www.isa.se/upload/english/Publications/Venture_Capital.pdf, 2004-11-03

³¹² <http://www.vencap.se/searchactive.asp>, 2004-11-03

³¹³ <http://www.vencap.se/searchactive.asp>, 2004-11-03

companies that supply security applications, as well as the ones that have invested in the sensor security market. This graph is a result of the venture capital analysis described in the method in chapter 2.

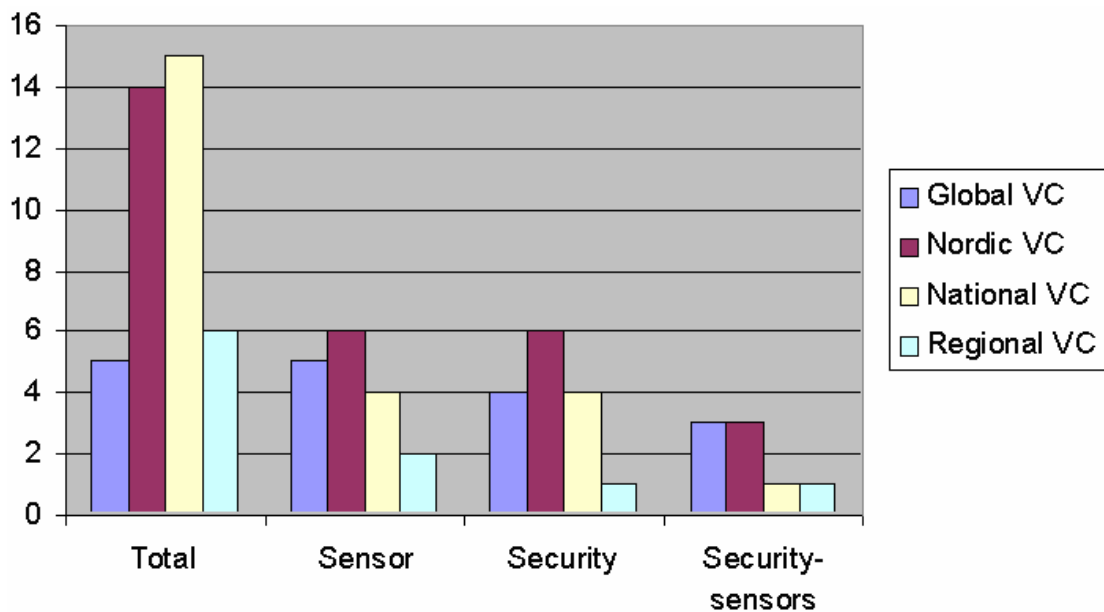


Figure 4-14 Venture capitalist activity sectors in Sweden³¹⁴

The graph shows a total of 40 VC companies investing in sensor technology or related technologies on the Swedish market. 17 of these companies have formerly invested in sensor companies and 15 have invested in the security market. However, these investments are mostly related to IT-security. Eight companies have made investments on the sensor security market.

By analysing the venture capitalist's assessment regarding market potential of the sensor security market, an indication of willingness to invest and provide recourses to these companies can be derived. The dominating opinion is that it is an interesting future market, and a majority of the venture capitalists are willing to invest in related companies. Even though the potential has been identified, the Swedish sensor security market is still immature and weak³¹⁵. But, there also exists reluctance towards investing in Swedish security sensors, originating from a belief that American companies are dominating the market to the extent that investing in a Swedish company would not be regarded as an interesting option³¹⁶.

³¹⁴ Interviews with VC companies, homepages of VC companies and homepage of VENCAP, <http://www.vencap.se>

³¹⁵ Per Nordhagen, Foretagsbyggarna AB; Henrik Blomquist, Skanditek Industriforvaltning; Fredrik Kronquist, Innovationskapital

³¹⁶ Robin Sukja, Affarsstrategerna AB

The Swedish venture capital market is strong, except for seed capital investments. The sensor security industry is a capital intensive business³¹⁷ and therefore, there is a strong need for Venture capital resources. This need is most strongly stressed by relatively newly founded companies. Regarding venture capital investments in the start-up and expansion phases, the supply is relatively good³¹⁸. However, industry actors have mentioned that four years ago it was considerably easier for sensor companies to extract venture capital³¹⁹.

Obviously, the larger actors on the sensor security market are not funded by venture capital. Traditionally, FMV has, at least to a certain extent, funded research and development conducted by Saab Bofors Dynamics, FOI and Ericsson Microwave. However, FMV is becoming weaker and disposes over smaller financial resources, which means that they are unable to take part in development projects in the same extent as before. This is a very big problem for these actors. Their development projects are so large in extent that they need to be co-financed with customers in order for the companies to take the risk to initiate them. However, depending on the lack of coordination between governmental authorities, currently it does not exist any customer on the market that has the resources or competence to engage in such development projects. This means that it is extremely difficult for Saab Bofors Dynamics, FOI or Ericsson Microwave to mobilize enough financial resources to initiate development projects related to the sensor security market.

Regarding company internal resource mobilization, the development of the NBD, has stressed the significance of sensor in security enhancing contexts. This has led to that several actors identify sufficient resources being allocated internally for sensor development activities³²⁰. However, in some cases it exists inertia in the transition from military to civil security sensors. Saab Bofors Dynamics experiences insufficient coordination of resources related to sensors with security applications³²¹.

Conclusion

In this section, it has been shown that the functional weaknesses and strengths are:

- Generally there is sufficient human capital in the industry.

³¹⁷ Interview, Josefsson, Anders; Acreo AB; 2004-10-21 and Holmberg, Per and Karlsson, Magnus; Applied Sensor Sweden AB; 2004-10-19 and Svensson, Peter; Fingerprint Cards AB; 2004-10-14

³¹⁸ Interview, Josefsson, Anders; Acreo AB; 2004-10-21 and Holmberg, Per and Karlsson, Magnus; Applied Sensor Sweden AB; 2004-10-19 and Svensson, Peter; Fingerprint Cards AB; 2004-10-14

³¹⁹ Interview, Josefsson, Anders; Acreo AB; 2004-10-21 and Holmberg, Per and Karlsson, Magnus; Applied Sensor Sweden AB; 2004-10-19 and Svensson, Peter; Fingerprint Cards AB; 2004-10-14

³²⁰ Interview, Klasén, Lena; FOI Sensor Systems; 2004-10-26

³²¹ Interview, Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22

- Sweden has the strongest venture capital market in Europe.
- There are difficulties in mobilising financial resources for larger R&D projects.

4.4.6. Function 6. Legitimization

This function deals with factors that influence legitimacy, what they are and how they affect the function. First, a short discussion concerning the general aspects of legitimacy is presented. This is followed by a survey of the integrity aspects. Finally, the legitimacy and expectations of the technology and the national reliance in Swedish actors will be investigated.

General aspects

It is difficult to discuss the general legitimacy of the industry and the technology related to it, since the technological base in the sector is so broad, and the background and current fields of activity of the firms in the system are relatively diverse. The commercial actors in the innovation system cover a spectrum from medical technology and applications to military related applications. Concerning the medical and biotech sector, Swedish firms have a good reputation on an international level³²², and given the fact that many of the biosensor companies are included in these; a general good international recognition for the Swedish biosensor actors is established, and a positive effect on the legitimization is achieved. The Swedish military industry also plays an important role concerning the legitimization function, as the two biggest actors in the security sensor industry are active in both the civil and the defence industry. The legacy of the Swedish neutrality brought forward the strong tradition of the Swedish defence industry and it can be argued that this in turn paves the way for a strong legitimacy for a future Swedish security industry, including security sensor applications. The Swedish defence industry has a well-reputed name internationally that most likely have favoured the legitimacy of the Swedish security industry. However, the similarity and connection between the Swedish security and defence industry does not solely affect the legitimacy of the security sensor industry in a positive way. It can be argued that as long as there will be interest organisation, like Svenska Fred³²³, working towards limiting the Swedish production and export of defence related applications, the connection to the defence industry and its association with war will negatively affect the legitimacy of the security sensor industry. However, the general impression among the actors is that the current level of legitimacy related to the field is satisfying.

³²² Interview, Hjort, Klas; SUMMIT; 2004-10-28

³²³ Blom. F. 2004

It is interesting to consider the impact that a future Swedish security industry organization could have on the legitimacy aspect since such an organization could stress and influence the general legitimacy of the field. Currently, no industry organization exists for the overall security industry as defined in the report, and consequently, no industry organization exists for the security sensor industry.

Integrity aspects

The augmented security awareness has increased the legitimacy of surveillance, resulting in an increased legitimacy for the use of sensors. The changed threatening picture has resulted in an increased general need and acceptance for surveillance products. The earlier mentioned legislations, concerning increased surveillance in air- and seaports, stand as concrete examples of this. In media there has been a general, but not too frequent, discussion concerning the integrity aspect of supervising and of the possibilities presented by technology. This is often a considered factor in the activities of the actors since sensor technology often is related to some form of supervision. The technological possibilities today lay ahead of the level of maturity concerning the integrity discussion. It can be argued that the integrity discussion is undeveloped and that a future integrity debate will greatly damage the legitimacy of the sector. It is possible that the actors today cross a future limit of tolerance concerning integrity violation, given the fact that no such limit has been clearly defined because of the underdeveloped integrity discussion. It is difficult to state how a deep integrity discussion will affect the innovation system, or if it will emerge at all. At current state, the innovation system is favoured by the undeveloped integrity discussion given the fact that it is not limiting the market and the possibilities of development for the security sensor industry. It can be argued that a general opinion on the issue is that the increased security thinking and the technological developments have restricted the personal integrity. Still, a higher level of perceived potential threat often results in a more likely willingness to be supervised. The majority of the actors do not deliver a product to the end consumer and therefore they do not feel that the ongoing discussion affects them directly. They also generally perceive the current integrity debate as not being that critical; still, there is a notion of the importance of encouraging a continuing discussion parallel with the development of the technology. Also, some firms feel that they may gain benefits from the discussion, given the fact that they perceive their applications to be less violating of the personal integrity than other solutions of the same need³²⁴.

Technological legitimacy

Some actors have detected an over-confidence in the possibilities that the technology presents, often related to costs or timelines in the develop process and

³²⁴ Interview, Rödfalk Albert, Precise Biometrics, 2004-10-28

related to the performance of applications of the technology³²⁵. However, this is not an overall impression from all the actors since it has been mentioned that the customers in some sectors have been impressed by the possibilities presented by the sensor technology³²⁶.

Some of the technologies used in the development of sensors have a strong legitimacy thanks to the earlier discussed authority legacy from the traditional Swedish defence industry³²⁷. However, it has in several cases been mentioned that there exists a general opinion that the American actors are dominating the market and that the Swedish firms do not have the level of competence required to be regarded as an interesting option³²⁸. It has been stated that the Swedish customers in some cases lack confidence in the Swedish suppliers and that foreign firms are preferred because insufficient legitimacy concerning the Swedish competence³²⁹.

Conclusions

In this section, it has been shown that the functional weaknesses and strengths are:

- The relation to the defence industry affects the legitimacy both in positive and negative aspects.
- There is uncertainty regarding the integrity concept.
- There is a national disbelief for Swedish actors.

4.4.7. Function 7. Creation of free utilities

Free utilities are advantages that many of the actors within the innovation system can gain benefits from. This function is concerned with the creation and the absence of these, much related to uncertainties and the insufficient amount of actors. This section starts with the description of free utilities related to networks, pooled labour markets, specialized suppliers for the innovation system and non tradable inputs. Further, the uncertainties related to market and technology will be presented and this section ends with conclusions concerning the evaluation of the function.

Networks

Concerning networks and flow of information, there is no specific network for the innovation system. However, the Swedish National centres of excellence play an

³²⁵ Interview, Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22

³²⁶ Interview, Klasén, Lena; FOI Sensor Systems; 2004-10-26

³²⁷ Interview, Oderland Ingvar, Ericsson Microwave, 2004-10-15

³²⁸ Interview, Sukja Robin, Affärstrategerna AB, 2004-10-27

³²⁹ Interview, Larsson Anders, Fibersson AB, 2004-10-11

important role for the interaction between the actors in the industry. The three centres S-Sence, ISIS and SUMMIT create a network of knowledge and increase the flow of information³³⁰. Since they are interdisciplinary and generally problem-focused they allow a scope for horizontal networking across traditional university structures. This is especially important for the sensor industry given the need of high degree of interdisciplinary technology for sensor development. The National centres of excellence also function as an important information channel between academics and the industrial research community by placing industry personnel onto campus to join in research. This also results in extended personal networks that in turn provide new aspects and contacts³³¹. Also, the centres create networks between the industry actors and it has been mentioned that contacts are established leading to co-operation between competitors outside the centre activities³³².

FOI, together with FMV, has also been mentioned as creators of networks by linking groups of actors. They often include different players in their development projects, generating contacts, both between persons and organization³³³. This increases the spreading of knowledge among the industry actors.

Further, the Swedish security industry currently lacks an industry organization, or a network organization for the civil security market. There is no Swedish organisation that directly posses political power concerning the security sensor industry. However, there is an industry organization for the Swedish defence industry called FIF, but that organization only includes three of the actors in the security sensor market, and this organization has no considerable political power of the industry. Still, some actors stress the need for an industry organization mentioning the possibility of increasing the legitimacy and to work as a united force to create a strong trademark for the Swedish security industry³³⁴. Swesec, an association including 400 Swedish security and safety companies, is the organization closest to an industry organization. Few, if any, of the actors in the Swedish sensor industry are engaged in Swesec, and it can be argued that this is because Swesec mainly covers a different type of market, the safety and security market related to unorganized crime. This is at the other end of the security definition compared to FIF. A trade organization appropriate for the industry covering the presented definition of the security industry would place itself in between FIF and Swesec.

Concerning university relations and networks, a central player is the University of Linköping. Chalmers University of Technology, The Royal Institute of Technology

³³⁰Arnold.E 2004

³³¹Arnold.E 2004

³³² Interview, Krantz-Rülcker, Tina and Lundström, Ingemar; S-sence; 2004-10-19

³³³ Interview, Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22

³³⁴ Alexandrie.L, 2004

and concerning biosensors, Karolinska Institutet, are also mentioned as university partners. Often the geographical location of the actors characterizes their university relations. Also, the actor's involvement in the national centre of excellence engages them to the host university.

There are also networks concerning production technology in which some of the actors are engaged. These networks, often informal, distribute knowledge concerning the production processes³³⁵. Concerning networks for security applications, it has been inquired by several actors that such a network should be established.

There is a concentration of actors in Linköping. Both S-Sence and ISIS are located there, together with Applied Sensor, Saabs Bofors Dynamics sensor unit and FOI Sensor System, all actors of major importance. Concerning biotechnology related to the development of biosensors, the Stockholm-Uppsala region hosts a significant amount of actors creating a network.

The projects related to the European Union Framework Programme for Research and Technological Development have also been mentioned as presenting possibilities of network creation. However, not all actors have fully positive experiences from these projects that in some cases are perceived as heavy going and bureaucratic, and some of the actors are decreasing their involvement in EU co-operations³³⁶. The procedure as regards applications to the programme is perceived as complicated and resource consuming and international cooperation is required, something that some actors are incapable of³³⁷. Still, others see increasing possibilities in these projects concerning development of research and technology and stress the amplified importance of the EU in the development of the industry³³⁸. These EU projects are perceived by some actors as very important concerning distribution of knowledge and updating on new technology³³⁹. It may be argued that the size of the actors influence their point of view on the role of the EU, since smaller firms tend to find these projects less rewarding given the required input, while bigger firms have the possibility of overcoming the requirements. Many of the smaller firms feel that their return on engagement in formal networks in general is too limited to make up for the commitment. Often the personal, informal network is far more valuable and rewarding, especially in an early phase of the company development.

Pooled labour market and free utilities in form of human capital

³³⁵ Interview, Engström, Rolf; Airborne Hydrography AB; 2004-10-12

³³⁶ Interview, Aastrup, Teodor; Attana AB; 2004-10-13

³³⁷ Interview, Svensson, Peter; Fingerprint Cards AB; 2004-10-14

³³⁸ Interview, Oderland, Ingvar; Ericsson Microwave Systems AB; 2004-10-15

³³⁹ Interview, Josefsson, Anders; Acreo AB; 2004-10-21

Regarding the aspect of pooled labour market, no such occurrence has been identified in the innovation system. However, there has been flow of human capital between actors, often in connection to spin-offs, where there is an interchange of employees between the parent company and the spin-off. There has also been an access to dismissed labour from firms like Nokia and Ericsson with competences well suited for the sensor industry. This competence was occupied by many of the smaller companies that took advantage of the disarmament of the bigger firms³⁴⁰. Still, there is no present justified pooled labour market regarding the sensor industry in Sweden. Much of this has to do with the weakness of the innovation system and the absence of an innovation system network.

Another form of free utilities is the human capital shaped by the bigger actors in the innovation system. Through their ability to influence universities due to their size, these actors have the capacity to form the human capital relevant for the innovation system. Their interaction and communication with universities create better conditions for the whole innovation system given the fact that they form the human capital to the sensor industry's advantage, and that this human capital becomes available for all the actors in the innovation system.

Specialized suppliers

Concerning suppliers to the actors on the sensor market, no general specialized supplier has been identified. It is difficult to identify specific specialised providers offering general basic components for sensor production given the fact that the sensor industry covers many technologies and therefore demands many different types of suppliers. There is one identified Swedish supplier, Sivers Lab, which supplies components to the radar industry. Also, there is one firm, Acreo, that can be identified as more a frequently mentioned specialized supplier that supplies and develops basic semiconductors for many of the sensor producers. Many of the actors have been in contact with this firm, as customers, partners, or in other forms of projects. Acreo is often only involved in the early phase of a project when the industry actors need to develop their products. In a later phase when the industry actors seek a higher volume in their sensor components, Acreo is no longer interesting as a supplier since they do not have the capacity of high volume manufacturing. Still, Acreo is important in the development of commercial sensor applications for smaller firms. The knowledge that this actor generates provides a good resource for the firms that are acting on the market. Another interesting company more characterized as a development partner than as a supplier is IMEGO located in Gothenburg. IMEGO is an institute of microelectronics that first and foremost functions as an early partner in projects, connecting research to

³⁴⁰ Interview, Holmberg, Per and Karlsson, Magnus; Applied Sensor Sweden AB; 2004-10-19

market applications and providing the actors with an industry network³⁴¹. Also, there is Monolitsystem in Gothenburg, a less frequently mentioned supplier or development partner of the sensor industry concerning micro-electronic and micro-mechanic product development.

The above mentioned actors can in some aspects be regarded as suppliers even though they often act more as development partners. Still, the Swedish market lack specialized suppliers of higher volume concerning basic sensor components and the actors in the industry are forced to turn to foreign suppliers for higher volume applications. This is particularly the case concerning providers of silicon components.

Non-tradable inputs

Concerning non-tradable inputs specific to the sensor industry, the inheritance from the traditional Swedish defence industry is a major factor. It has been mentioned that the co-operation between FMV and the Swedish defence industry has created a valuable base of knowledge, experience and credibility. The Swedish security industry has inherited a strong image based on the legitimacy derived from the national defence industry which has been perceived as a competent defence equipment provider.

Market related uncertainties

The changed role of FMV creates great uncertainty on the market, especially given the fact that the role of the agency is weakening concerning guidance for the market. At the same time, the new customer, in the form of the public safety agencies, is having problems with the articulation of demand, creating even more uncertainty on the market. Also, the driving force of the market, the threat, can be overstated given the difficulties of establishing a threatening picture that really corresponds to reality. There is a risk that the perceived threat is overvalued and that the market is puffed up. This risk results in uncertainty on the market. Another factor creating uncertainty is the gap between laws concerning the surveillance sector and the technological possibilities. This gap can be considered as a direct result of the underdeveloped integrity discussion and it has given free space for technology development. This fact creates uncertainty on the market because a future legislation can reduce the sector of application for the already developed technology.

In despite of the fact that the market uncertainty is relatively high for the innovation system, there are two factors reducing this uncertainty. Firstly, the

³⁴¹ Interview, Björkholm, Peter; IMEGO AB; 2004-10-14

directives and regulation issued by the European Union give a firm guidance for the actors on the market concerning demand of security applications, in this way clearly reducing uncertainties. Secondly, two research institutes, Acreo and Imego, function as links to the market and reduce uncertainty by decreasing the gap between the technological knowledge and the market. In their role as development partners, discussed above, they present possibilities of taking advantage of their accumulated knowledge for a lot of actors.

Technology related uncertainty

A factor related to uncertainty is the establishment of standards. It is difficult to state if there exist established standards given the broad spectra of technologies that concern sensor development. Certain forms of standards exist in particular technology fields. To start with, biometrical standards are often established in different countries depending on the form of identification information required in the specific nation and the method to collect and store it³⁴². These standards often differ between different countries and no international standards exist. These establishments of standards can both favour and disfavour the actors depending on how well the standard fit the actors technology field. In the USA, a standard concerning format for fingerprint storage in databases has been proposed³⁴³. This could possible lead to the establishment of an international standard that could reduce the technological uncertainty in the field. However, it has been mentioned that the proposed standard does not go hand in hand with best practice technology and is difficult to support with good technical solutions.

Technological fields relatively stable and established are the one concerning radar, fibre optics and laser³⁴⁴, but this is more an exception with reference to standards related to sensor technology. Many technological sectors lack a standard at the same time as standards are important to many customers, like FMV. Also, due to the LOU, European standards must be fulfilled in the purchased product if such a standard is present³⁴⁵, but as mentioned, this is seldom the case in sensor applications. The lack of establishment of standard is however not always perceived as a hindrance for the development of the innovation system, given the fact that an absence of standards creates more space for technological development. Still, in the case of reduction of uncertainties the lack of standards has a negative effect on the function. In many cases the Swedish actors, excluding Ericsson Microwave AB and Saab Bofors Dynamics AB, are too small to participate in the development of standards on international level. This creates a problem given the

³⁴² Interview, Rödfalk, Albert; Precise Biometrics AB; 2004-10-28

³⁴³ Interview, Svensson, Peter; Fingerprint Cards AB; 2004-10-14

³⁴⁴ Interview, Larsson, Anders; Fiberson AB; 2004-10-11

³⁴⁵ Interview, Zachrisson, Elisabeth; Försvarets Materialverk; 2004-11-01

fact that they are not capable of bringing forward their type of technological solutions.

Conclusions

In this section, it has been shown that the functional weaknesses and strengths are:

- The national centres of excellence create knowledge related networks.
- There is no specialized supplier for the innovation system.
- The uncertainty related to technology and market is relatively high.

4.5. Conclusions and recommendations

From the results presented in the function analysis, a summarization of weaknesses of the functions and a number of conclusions concerning blockage mechanisms in the innovation system are presented in this subchapter. Based on these, several recommendations for improvement of the performance and development of the innovation system were established.

4.5.1. Summarization of system weaknesses

The system weaknesses identified in the functional analysis are summarized in the following table.

Function	Weakness
1. Knowledge development	There is a lack of market related knowledge among the large industry actors.
	There is a need for company internal development of sensor related knowledge.
2. Providing incentives and guide the direction of search	There is a lack of incentives for entering the market in Sweden, but incentives can be found abroad.
	The articulation of the government agencies' demand is poor.
	There is insufficient guidance related to direction of search.
3. Promoting entrepreneurial experimentation	Few new entrants on the security sensor market.
	There are difficulties in gaining governmental orders among smaller companies.
4. Market formation	No market where Swedish companies are prioritized exists.
5. Mobilisation of resources	There are difficulties in mobilising financial resources for larger R&D projects.

6. Legitimization	The relation to the defence industry affects the legitimacy both in positive and negative aspects.
	There is uncertainty regarding the integrity concept.
	There is a national disbelieve for Swedish actors.
7. Creation of free utilities	The uncertainty related to technology and market is relatively high.

4.5.2. Blockage mechanisms

This section concerns the blockage mechanisms, i.e. the factors obstructing system performance. These were identified by analysing the weaknesses in the functions and connecting them to the structural components in the system. Further, to evaluate the impact of the blockage mechanisms on the system, a matrix is presented, showing the impact of each blockage mechanisms on each function.

Identification of the blockage mechanisms

By further analysing the identified weaknesses corresponding to each function, a number of blockage mechanisms were identified. The connection between weaknesses and mechanisms is presented in figure 4-15.

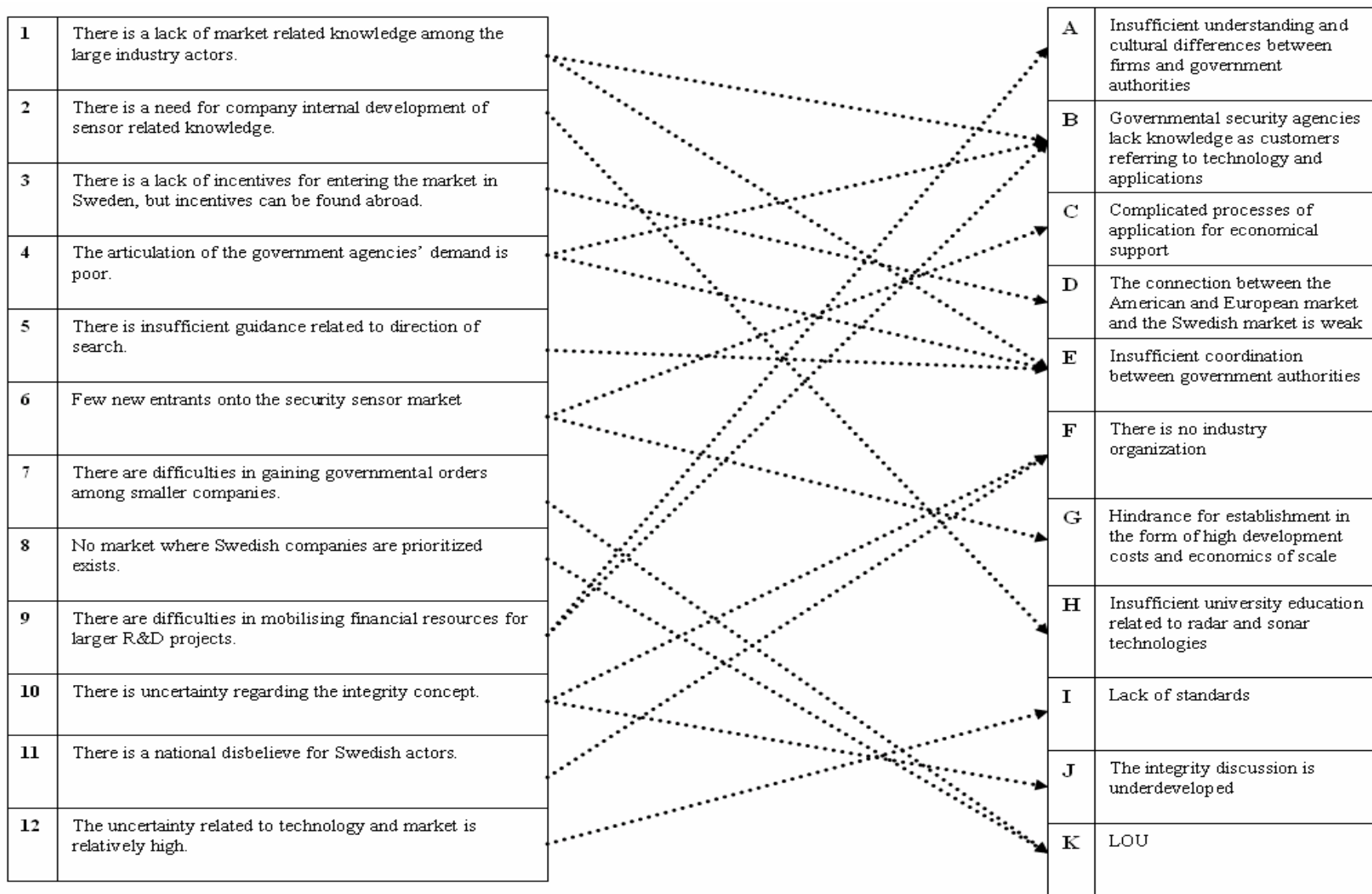


Figure 4-15: Connection between the function weaknesses and the blockage mechanisms

All blockage mechanisms have been identified through the conduct of finding explanations to system weaknesses in the structural components. All blockage mechanisms can be traced back to the presentation of the functions, where a more thorough explanation to how they affect the functional performance is presented. Eleven blockage mechanisms were identified from the weaknesses, of which four seemed more influential. In this section, these four blockage mechanisms will be lifted out and their effect on system weaknesses will be clarified briefly.

Firstly, blockage mechanism **B** was identified from three system weaknesses. The lack of technological competence among security agencies makes them incapable of articulating demands bearing the amount of relevance necessary for guiding the direction of search, resulting in weakness **4**. Furthermore, since the security agencies do not fully understand the activities of the commercial actors, they are less willing to participate in R&D projects. This makes it hard for large actors to mobilize financial resources since their R&D projects need to be co-financed with the customer, resulting in weakness **9**. Also, the lack of competence makes them weak as customers, and renders them incapable of mediating market knowledge to the industry actors, resulting in weakness **1**.

Secondly, blockage mechanism **E** was also identified from three weaknesses. Market knowledge is often mediated from a strong and competent customer. However, the lack of coordination between governmental authorities results in that no such customer exists, resulting in weakness **1**. Also, even if security agencies often have the same needs, the lack of coordination hinders them from combining these needs into one strong demand, resulting in weakness **4** and **5**.

Thirdly, blockage mechanism **F** affects the legitimacy of the innovation system. Since there is no industry organisation it is hard to promote Swedish security sensor actors on the market, resulting in weakness **11**. Also, an industry organisation could effectively develop the integrity discussion, which would decrease the uncertainties that currently exist related to future legitimacy of the industry, resulting in weakness **10**.

Finally, blockage mechanism **K**, was identified from two system weaknesses. Since the act of LOU prohibits that any preferences are given to national companies combined with the fact that the most important customer is obliged to use this act, it is hard to create a market where Swedish actors are prioritized, resulting in weakness **8**. Also, LOU complicates the process of applying the contracts. This efficiently shuts out smaller companies from this market, since they do not possess the resources needed for the application process, resulting in weakness **9**.

Evaluation of the blockage mechanisms

Since it was identified that a blockage mechanism affects more than one function, the blockage mechanisms were weighted depending on their impact on the seven functions to evaluate the impact of the blockage mechanisms on the innovation system performance. The following matrix displays these effects and reveals the impact of the mechanisms on total innovation system performance.

Blockage mechanisms

		Functions							Impact of the blockage mechanism
		1	2	3	4	5	6	7	
		Knowledge development	Providing incentives and guide the direction of search	Promoting entrepreneurial experimentation	Market formation	Mobilisation of resources	Legitimation	Creation of free utilities	
A	Insufficient understanding and cultural differences between firms and government authorities	-	--		--	--		-	8
B	Governmental security agencies lack knowledge as customers referring to technology and applications	--	--	-	-	--			8
C	Complicated processes of application for economical support	-		---		-		--	7
D	The connection between the American and European market and the Swedish market is weak		--	--	--			-	7
E	Insufficient coordination between government authorities	-	--	++	--	--		-	6
F	There is no industry organization		-		-	-	--	-	6
G	Hindrance for establishment in the form of high development costs and economics of scale		--	--				-	5
H	Insufficient university education related to radar and sonar technologies	--		-		--			5
I	Lack of standards	+/-	--	++			-	--	3
J	The integrity discussion is underdeveloped	+			-/+		-/+	--	1
K	LOU	+		--					1

The six most important blockage mechanisms will be presented, and their impact on the functions will be described below. The complete outcome from the matrix regarding blockage mechanisms **G-K** is presented in appendix E.

Firstly, blockage mechanism **A** concerns the insufficiency in understanding and cultural differences between firms and government authorities, which affects all but the functions **6** and **3**. Since the public authorities are a major customer, restricted understanding between authorities and actors results in failure to understand the companies' needs for articulation of demand and guidance of search. It also hinders them to reach enough insight about the companies to articulate demands of high relevance, affecting function **2**. In turn, this results in that few customer needs are communicated, leading to a weak creation of application-specific knowledge, impacting function **1**. Also, if the companies in the industry and the governmental agencies lack an understanding for each other, it can be argued that the market and its needs will be hard to interpret. Therefore, the market formation will be obstructed by this lack of mutual understanding and uncertainty will augment, affecting function **4** and **7**.

Secondly, blockage mechanism **B** concerns the lack of knowledge of the public security agencies as customers, referring to technology and applications. The incompetence results in that the customer is incapable of taking part in the product development process, which is an important source for knowledge creation. This is even more important since these authorities are identified to be the primary customer group. Therefore, this blockage mechanism strongly affects function **1**. Also, this incompetence makes it very hard to articulate demands of relevance or quality, influencing function **2**. It is clear that a higher degree of competence would improve the clarity of the articulation of the needs. Hence, the demands would achieve a higher acceptance by the industry. Further, the deficit in knowledge of the police concerning technology and applications hinders the possibility to concretize the formation of the market, affecting function **4**. Finally, given the fact that this group form a large set of customers, the deficit in knowledge concerning technology and applications leads to a lack of understanding related to coordinated investments. This restricts the amount of resources, negatively impacting function **5**.

The mechanism **C** is concerned with the complicated processes of application for economical support. Since economical support is very important to successfully develop an innovation in to a company, the difficulties of obtaining such decreases the amount of economical support in the industry and hinders function **3** concerning entrepreneurial experimentation. Further, the impact of the blockage mechanism on function **1** concerning knowledge development is mainly a direct cause of the lack in entrepreneurial experiments which is strongly affected by insufficient economical support. Furthermore, the breadth of the knowledgebase is negatively affected by a low numbers of entrepreneurial companies. Also, if the

amount of economical support in the field is small, the total amount of financial capital on the market will be smaller. Therefore, this blockage mechanism will negatively affect function 5. Finally, a limited amount of economical support will decrease the possibilities of reaching an extensive amount of companies, which limits the systems ability to reach its critical mass that creates free utilities, affecting function 7.

Blockage mechanism D is concerned with the fact that the connection between the American and European market and the Swedish market is weak. This leads to that the Swedish market is perceived as weak and the incentives for market entrance are feeble. It can be argued that the industry considers or perceives national incentives as stronger factors for entering the market, especially smaller companies which are more dependent of a national market and lacks the resources to go international from start. Firstly, this will impact function 2 since the lack of this connection will obstruct the provision of incentives and guidance of search. Further, if there is a lack of incentives for entering the home market, there will be fewer newly established companies that in turn negatively affect the entrepreneurial experimentation function, function 3. Also, function 4 is affected by this blockage mechanism since it obstructs the national articulation of demand, hindering the formation of efficient markets. Finally, since blockage mechanism D results in that fewer companies establish on the market affecting function 7.

Insufficient coordination between government authorities creates a sixth blockage mechanism referred to as E. The lack of coordination between authorities hinders the mobilisation of resources that in turn obstructs the initiation of development projects. Since much knowledge is created through development projects, it negatively affects function 1. Further, insufficient coordination between authorities makes it impossible for the larger actors to identify the demand. One authority does not know what other authorities demand even if they have the same needs. This is an example of insufficient articulation of demand and absent guidance of direction that negatively affects function 2. However, if the public authorities are to be coordinated, they will demand applications and services in high volumes, which is difficult for small companies to supply. If the public authorities are centralised, the small companies will not be regarded as potential suppliers. Therefore, the insufficient coordination between government authorities affects the function 3 positively. On the other hand, many governmental agencies are perceived as too shattered to be an attractive customer for the larger actors. Therefore, it can be argued that an increase in coordination between the governmental agencies will create and appropriately form market segments. This means that the current status of function 4, concerning market formation, is negatively affected by the lack of coordination. Furthermore, a coordinated group of agencies would more likely be able to invest in projects as a group than as individuals. This mobilizes resources that else wise would be too small to make an impact. Therefore, the absence of coordination affects function 5, negatively.

Finally, it may be argued that a coordination of the agencies would decrease the uncertainty of the market, create a competent customer and form a market structure available for all industrial actors to take advantage of. The current status of coordination affects function 7, negatively.

Function F concerns the absence of an industry organization. The presence of such could result in a clearer direction of search, which could be an incentive for entering the market. Hence, the lack of such affects function 2 negatively. Further, an industry association could influence the market formation through strengthening the link between the industry and the costumers. Therefore, function 4 is negatively affected by the absence of an industry organization. An industry organization could increase the political power of the security sensor industry. It can be argued that the possibilities to mobilize resources will increase with the presence of an industry organization. Hence, the lack of such will negatively affect function 5. Furthermore, it is obvious that the lack of an industry organization negatively affects function 6 related to legitimacy and creation of such. Finally, since an industry organization is a sort of free utility, the lack of such negatively affects function 7.

To conclude, the blockage mechanisms that have the strongest influence on total system performance are;

- Insufficient understanding and cultural differences between firms and government authorities.
- The lack of knowledge among governmental security agencies referring to technology and applications.
- Complicated processes of application for economical support.
- The weakness in the connection between the American and European market and the Swedish market.
- Insufficient coordination between government authorities.
- The absence of an industry organization.

4.5.3. Recommendations

This section will discuss the actions that can be taken in order to reduce the blockage mechanisms' influence on innovation system performance. This section will include recommendations related to the six most important blockage mechanisms. The recommendations are shown in figure 4-16 below.

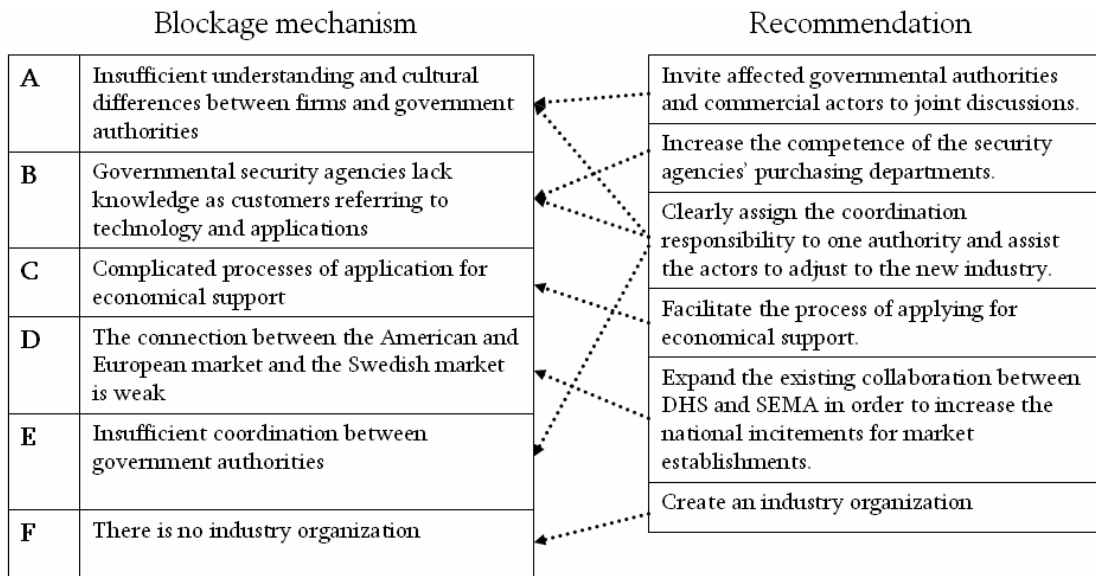


Figure 4-16: The blockage mechanisms with corresponding recommendations

Firstly, it has been concluded that the cultural differences between commercial companies and governmental authority decrease the innovation system efficiency. This blockage mechanism has been ranked one of the strongest. It could be considered as simplistic to believe that these cultural differences can be reconciled. However, by inviting effected governmental authorities and commercial companies to joint discussions, it might be possible to find a solution to what role the authorities and companies should take respectively on the security market. Such act can affect blockage mechanisms **A**.

Secondly, blockage mechanism **B**, the incompetence of several governmental authorities³⁴⁶ related to application and technological aspects, results in insufficient articulation of demand. If these affected authorities can be more closely coordinated, it might be possible to centralise the purchasing process, which also would make it easier to increase its competence. If the competence of the governmental authorities were increased it would decrease the influence of blockage mechanisms **B** on innovation system performance.

Thirdly, the blockage mechanism **E** is concerned with insufficient coordination between governmental authorities. This blockage mechanism originates both from cultural aspects as well as the fact that no authority sees itself as responsible for initiating the coordination process. Because this blockage mechanism strongly affects function number 2, and because this function is crucial for the development of the innovation system given its current phase as described in 3.2.3, it is of major importance to find a solution to this blockage mechanism. One solution to this problem is to give the Swedish Emergency Management Agency, SEMA, extended responsibilities. Currently, SEMA is responsible for coordinating governmental

³⁴⁶ Most strongly expressed concerning the police authority.

authorities. However, SEMA is almost exclusively method oriented in its approach, and consequently gives priority to research projects related to risk and vulnerability analysis, threat and threat development analysis and development of crisis management methods. In order to make SEMA responsible for coordinating the needs and demands of governmental authorities related to the security sensor market, SEMA has to become more technology oriented in their business activities. By doing this, a clear assignment of the responsibility to one authority would be reached. This authority would then work as a driving force, initiating coordination enhancing procedures. By conducting this action it would be possible to increase the articulation of demand, the incentives for entering the market and the possibility to generate sufficient financial resources for the initiation of large R&D projects. Hence, by implementing these solutions, blockage mechanisms **A**, **B** and **E** would be positively affected.

Fourthly, there are strong hindrances for establishment related to high initial costs and economics of scale. This demands for strong financial resources for entering the market. Furthermore, the application process for economical support has been described as complicated and resource demanding, which restricts smaller and newly started companies from mobilising sufficient financial resources. By facilitating this application process, the actors could concentrate their resources to develop their business activities, and the influence of blockage mechanism **C** would decrease. This would also result in a higher success rate among newly started companies, which in turn would increase the amount of actors in the innovation system.

Blockage mechanism **D** has resulted in that the Swedish actors perceive the incentives for market establishment as weak. However, if the already existing collaboration between DHS and SEMA was further developed, it would be possible to project the American incentives for market entrance directly onto the Swedish market. Also, it would be possible for SEMA to get a better understanding of the American needs for security technology and products, which in turn can lead to that these needs are communicated to the Swedish security sensor market. This would clarify the incentives on the Swedish market. Hence, by developing existing collaboration, function 2 would be strengthened and the influence of blockage mechanism **D** on innovation system performance would decrease.

Currently, no organisation in the security sensor innovation system possesses any political power. Furthermore, the integrity discussion is underdeveloped, resulting in high uncertainties of future market development. Also, foreign security sensor suppliers are often prioritized since they are regarded as more competent. The establishment of an industry organisation would increase the possibilities to solve these problems, and decrease the influence of blockage mechanism **F**.

5. Conclusions

This section will conclude the findings presented in this report.

The purpose of this report has been to clarify the Swedish security industry structure, identify the market growth potential related to the different industry sectors and recognize underachieving industry factors that can be targeted in a national research policy. These objectives were transformed into following three research questions:

- *What is the overall structure and dynamics of the Swedish security industry?*
- *What sector of the security industry has the highest growth potential?*
- *On which factors should the government/actors concentrate their resources to create appropriate conditions for development of a well-functioning innovation system in the sector of the Swedish security industry that has the highest growth potential?*

The Swedish security consists of seven industry sectors. These are sensor technology, weapon technology, complex systems and simulation, mobile solutions, IT-security, physical transportation and NBC technology. There exist differences in technologies, applications, actors, regulations and trends regarding each sector. The security industry can be defined as diversified. This diversification within the industry is an industry characteristic, and thus, part of the overall picture. Furthermore, there are mainly three factors that are common to all sectors, and which tie the industry sectors closer together. (1) the market potential is relatively high in all industry sectors. This has resulted in that several companies that previously had exclusively military customers, have now started to analyse the emerging civil security market, and are positioning themselves towards the civil customer segment. (2) the national industry actors are prominent in almost every security industry sector. Sweden are among the leading nations in the world regarding telematics, sensor technology and complex systems. (3) the national security market is weak and the lack of collaboration between local and governmental authorities has been recognized as a vast hindrance for market development. The above mentioned factors present the main characteristics of the Swedish security industry.

The highest growth potential of the security industry is assigned to the sectors of sensor technology and complex systems. Both sectors are allotted large resources in the DHS budget. Also, both sectors have been identified as sectors with strong growth potential by both market research reports and interviewees. Furthermore, the national capability related to these sectors was perceived as strong by the

industry actors. However, depending on the difficulties related to the delimitation of the complex system industry sector, the growth potential of this sector appeared to be more uncertain. Therefore, sensor technology is identified as the security industry sector with the highest growth potential.

Through the analysis of the innovation system of the sensor security industry, six main blockage mechanisms were identified. These were recognized as (1) insufficient understanding and cultural differences between firms and government authorities, (2) lack knowledge as customers referring to technology and applications among governmental security agencies, (3) complicated processes of application for economical support, (4) a weak connection between the American and European market and the Swedish market, (5) insufficient coordination between government authorities and (6) the lack of an industry organization. Based on these mechanisms of major importance, a number of recommendations, as factors to concentrate resources in order to create appropriate conditions for development of a well-functioning innovation system, were identified.

A stronger guidance and coordination among governmental authorities is needed, both referring to the development of technical knowledge of the authorities and coordination of articulation of the demand and the process of acquisitions of supplies. By concentrating resources on creating such guidance and coordination among authorities, the Swedish security sensor innovation system would be improved. One solution to this is to give the Swedish Emergency Management Agency, SEMA, extended responsibilities to also cover more technology oriented aspects. Also, the cultural differences between commercial companies and governmental authority decrease the innovation system efficiency. By concentrating resources on augmenting the interaction between authorities and companies with the aim to achieve a greater understanding and collaboration, the innovation system performance can be improved. Further, the blockage mechanisms revealed that the connection between the European and American market and the Swedish market is weak. By extending the existing collaboration between the DHS and the SEMA, it would be possible to project the American incentives for market entrance directly onto the Swedish market, increasing the perceived incentives on the Swedish market. Therefore, in order to obtain a well-functioning innovation system concerning the Swedish security sensor industry, resources should be invested in these matters.

Although this innovation system analysis was conducted solely on the Swedish security sensor industry, it is interesting to consider how well above stated results apply on the rest of the Swedish security industry. In order to investigate this, it is interesting to regard the general aspects resulting from the Swedish security industry survey presented earlier in this chapter. There it was mentioned that the general technical knowledgebase was strong for all the sectors, as for the specific case with the sensor sector. This draws the first parallel between the characteristics

of sensor industry and the whole security industry. Further, the national market was declared as being generally weak with few, non-profitable customers. This is also the fact for the sensor industry. Further, the difficulties emerging from the relationship to government authorities, mainly as customers, can also be characterize as a general aspect for the whole Swedish security industry. It can therefore be argued that several of the results emerging from the innovation system analysis of the Swedish security sensor industry can be related to general characteristics of the whole Swedish security industry. Consequently, it can be stated that the recommendations presented in this report regarding improvements of the functionality of the specific innovation system can be favourable for the future development of the whole Swedish security industry.

6. Suggestions for future research

There are mainly three areas appropriate for future research.

Firstly, this report has analysed the Swedish security industry. It was concluded that the industry was diversified, hosting several different knowledge bases, applications and customer segments. The differences between the industry sectors combined with a limited timeframe for the conduction of this report restricted the profoundness of the analysis related to each industry sector. Although the industry sectors are accurately presented, a more thorough analysis of the Swedish security industry is an recommended area for future research.

Secondly, this report revealed innovation system blockage mechanisms related to the security sensor industry. However, the authors of this report do not consider themselves having sufficient political competence to formulate more specific recommendations than the ones formulated in this report. The recommendations will enable increased system performance, and are therefore of high relevance for the Swedish security sensor industry. Hence, recommendations of high quality are important, and therefore this is a suitable area for future research.

Finally, the functional analysis concerned only the security sensor industry. Since there are several differences between the industry sectors of the security industry, it is uncertain how many of the recommendations that are applicable in other industry sectors. On the other hand in this report it was stated that some important blockage mechanisms were identifiable in the whole industry, and therefore the recommendations concerned also these sectors. It would be appropriate to conduct a functional analysis on each of the industry sectors identified in this report.

Referenses

Articles

Alexandrie. L, 2004, *Satsa på en branchsförening!*, Detector Scandinavia nr 6.

Arnold.E, 2004, *Impacts of the Swedish Competence Centres*, Report to VINNOVA and the Swedish Energy Agency.

Askman.T, 2004, *Svenska vapen biter igen*, Affärsvärlden, 2004-10-05.

Bergholtz. C, Svensson. M, 2003, *Competitive intelligence- Patent information*, CIP.

Blom. F, 2004, *Avbryt det militära samarbetet med USA*, Göteborgs-Posten, 2004-11-10.

Branacaglioni.M, 2004, *Polisen klarar inte terrordåd*, Göteborgs-Posten, 2004-09-14.

Calsson, B, Jacobsson. S, Holmén M, Rickne. A, 2002, *Innovation systems: analytical and methodological issues*. Department of economics, Case western reserve university.

Calsson. B, Jacobsson. S, 2004, *Dynamics of innovation systems – Policy-Making in a Complex and Non-deterministic World*. Department of Industrial Dynamics Chalmers University of Technology.

Carlsson et al., 2002, *Innovation system analytical a methodological issues, Industrial Dynamics, Chalmers University of Technology*.

Carlsson. B et al., 2000, *Innovations system kluster och kompetensblock*, Eklbads och Co Tryckeri.

Edquist. C, 2004, *Systems of Innovation Perspectives and Challenges*, The Oxford Handbook of Innovation.

Hekkert, M., Suurs, R., van Lente, H. and Kuhlmann.S, 2004, *Functions of Innovation Systems: A new approach for analysing socio-technical transformation*. Utrecht Unioiversity, The Neterlands.

Hörstedt. F, Rickne. A, 2001, *Riktlinjer för Teknologianalys*, Institutionen för industriell dynamik, Chalmers tekniska högskola.

- Johnson. A, 2002, *Innovation System Approaches*, Department of Industrial Dynamics, Chalmers University of Technology.
- Karlsson. M, 2003, *Homeland Security an R&D in the United States*, Swedish institute for growth policy studies.
- Kleja. M, 2004, *IT har nyckelroll i EUs terrorkamp*, Nyteknik 08-12- 2004.
- Mogee. M. E, 1997, *Patents and technology intelligence*, in Ashton, W.B. and Klavans, R. A., eds, *Kepping Abrest of Science and Technology*. Batelle Press.
- Piazza.P, 2003, *Financial companies focuses on Infosec, Security management*, Arlington Aug 2003 vol 47
- Porter M, 1998, *Cluster and the new economics of competition*, Harvard business review, November-December,pp 77-90.
- Porter, M. 1980, *Konkurrensstrategi, Tekniker för att analysera branscher och konkurrenter*, ISL Förlag.
- Pröckl. E, 2004, *Laser vann striden om raket skydd*, Ny teknik no 38, 2004-09-15.
- Pröckl. E, 2004b, *Saabs skenmål utslaget från USAs flygmarknad*, Ny teknik no 38, 2004-09-15.
- Pröckl. E, 2004c *Spetsteknik täpper till flygets säkerhetshål*, Ny teknik no 37, 2004-09-08.
- Ryberg. J, 2002, *Säkerhet ska sälja telematik*, 2002-09-11, Ny teknik
- Sawy. O, Majchrzak. A, 2004, *Critical issues in research on real-time knowledge management in enterprises*, Journal of Knowledge Management, Volume: 8 no 4.
- Schmidt, B, 2004, *Report of the Group of Personalities in the field of Security Research*, European Communities.
- Solana J, 2003, *A secure Europe in a better world*, European Council, 2003-06-20.
- Törnqvist. S, 2004, *Delrapport från arbetsgruppen för nationell strategi för säkerhetsforskning*, Sekretariatet för nationell strategi för säkerhetsforskning. 2004-09-15.

Åkesson. B, *Hotet från biologiska och kemiska vapen samlade forskare lit i Göteborg*, Göteborgs-Posten, 2004-06-07.

Internet

Reports and Articles

Bergin.E, 2003, Stora brister i den mobila säkerheten, Svenska dagbladet, 2004-05-07, www.mediarkivet.se, 2004-08-27

Busquin.P, 2004, Commission Decision ,
http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_067/l_06720040305en00180022.pdf, 2004-09-23

Civitas Group 2004, The Homeland Security Market,
[http://www.maritimesecurityexpo.com/whitepapersarticles/Civitas percent20Report percent20on percent20the percent20Homeland percent20Security percent20Market.pdf](http://www.maritimesecurityexpo.com/whitepapersarticles/Civitas%20Report%20on%20the%20Homeland%20Security%20Market.pdf), 2004-08-10

Civitas Group 2004b, The FY 2005 homeland security budget request
<http://www.civitasgroup.com/reports/20040206.pdf>, 2004-08-10

Enhancing ship and port facility security. Brussels, 2.5.2003,
http://europa.eu.int/comm/transport/maritime/security/doc/com_2003_0229_en.pdf, 2004-09-22

Hansson.O et al, 2002, ..och Sveriges NBCberedskap är god?,
[http://www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/Övriga percent20publikationer/OCB percent20SPF/nbc_bok_2002.pdf](http://www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/Övriga%20publikationer/OCB%20SPF/nbc_bok_2002.pdf), 2004-09-23

Henriksson.O et al, 2003, Telematik 2006, framtidens fordon,
<http://www.teldok.org/pdf/151.pdf>, 2004-08-31

Planing for societys emergency management
http://www.krisberedskapsmyndigheten.se/english/documents/facts/planning_for_societys_emergency_management.pdf 2004-09-14, 2004-09-19

IT-företagen, rapport: Sverige 2.0,
http://www.itforetagen.se/pdf/Sverige_20_Visionsdel_030701.pdf, 2004-08-26

Krisberedskapsmyndigheten NBC-strategi 2004,
[http://www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/Utreddningar percent20och percent20remissvar/Utreddningar-uppdrag/nbc-strategi_kbm-s_nbc-vht_2004.pdf](http://www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/Utreddningar%20och%20remissvar/Utreddningar-uppdrag/nbc-strategi_kbm-s_nbc-vht_2004.pdf), 2004-09-13

NBC håller koll på farlig forskning, 2003,

http://biotech.idg.se/globalincludes/applikationer/utskrift_popup/utskrift.asp?ID=20031126122620_BIO.dbp, 2004-09-10

Project BioShield, CRS Report for Congress, April 28, 2003,

<http://fpc.state.gov/documents/organization/20368.pdf>, 2004-08-31

Sectra årsredovisning 03/04,

http://www.sectra.se/corporate/investor/financial_information/financial_reports/annual_reports/Sectra_2004_0614_sve.pdf, 2004-10-27

Swedish Defence Research Agency Annual Report 2003,

http://www.foi.se/raw/documents/35588_FOI_annual_report_2003.pdf, 2004-09-16

Actors

Comex, http://www.comex.se/itsakerhet_tilltradeskydd.asp, 2004-09-02

Cygate AB, www.cygate.se, 2004-09-03

Dimension AB, www.dimension.se, 2004-09-03

Dynasafe, <http://www.dynasafe.de/explosion-containment-airport-security.html>

EME AB, <http://www.eme.se>, 2004-09-15

Filtrator AB, www.filtrator.se, 2004-09-14

Svenska Riskkapitalföreningen:

http://www.vencap.se/article_view.asp?ArticleID=31, 2004-10-27

<http://www.vencap.se/docs/2004%20Q2%20Riskkapitalbolagens%20aktiviteter.pdf>, 2004-11-01

<http://www.vencap.se/searchactive.asp>, 2004-11-03

Nexus, www.nexus.se, 2004-09-03

Nose, <http://www.nose-network.org/>, 2004-10-18

Sectra, <http://www.sectra.se/security/>, 2004-09-06

SOS-alarm, <http://www.sos.se/hs/beredsk/cbrn.htm>, 04-09-17

Säkerhetspolisen, <http://www.sakerhetspolisen.se>, 2004-11-03

Other Internet sites

<http://courses.washington.edu/i498aa/slides/15>, 2004-08-17

<http://www.bt.cdc.gov/Agent/Agentlist.asp>, 2004-09-16

<http://www.bt.cdc.gov/agent/agentlist-category.asp#a>, 2004-09-16

http://www.destatis.de/themen/e/thm_bildung.htm, 2004-10-24

<http://www.foi.se>, 2004-09-14

<http://www.foxnews.com/story/0,2933,76864,00.html>, 2004-09-16

<http://www.foxnews.com/story/0,2933,76873,00.html>, 04-09-16

<http://www.foxnews.com/story/0,2933,76879,00.html>, 04-09-16

<http://www.foxnews.com/story/0,2933,76887,00.html>, 2004-09-16

<http://www.freedoniagroup.com/pdf/1792web.pdf>, 2004-09-16

http://www.isa.se/upload/english/Publications/Venture_Capital.pdf

<http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html>, 2004-09-14,

<http://www.isp.se/>, 2004-11-12

<http://www.isp.se/nyaengelska/indexeng.htm>, 2004-09-17

<http://www.regeringen.se/sb/d/3795/a/23209/m/wai>, 2004-09-20

http://www.scb.se/statistik/UF/UF0205/2002I03/UF0205_GE_Tab3.xls, 2004-10-22

http://www.scb.se/statistik/UF/UF0205/2002I03/UF0205_GE_Tab4.xls, 2004-10-22

<http://www.sjofartsverket.se/navigering/htm/frameset.htm>, 2004-12-06

http://www.uppfinnaren.com/nr3_02/sadd.htm, 2004-10-29

http://www.uppfinnaren.com/nr3_02/sadd.htm, 2004-10-29

<http://www.vinnova.se/main.aspx?ID=EBE6E511-F396-45EB-9046-6602F8F72041>,
2004-11-01

<http://www.vinnova.se/main.aspx?ID=EBE6E511-F396-45EB-9046-6602F8F72041>,
2004-11-08

http://www1.cbs.gov.il/shnaton55/st08_41.pdf, 2004-10-24

<http://www.isp.se/nyaengelska/indexeng.htm>, 2004-09-17

www.foretagsfakta.se

www.homelanddefensestocks.com//companies/HomelandDefense/News/homeland
, 2004-09-16

Interviews

Mail interviews

Axelsson, Björn; IT-företagen; 2004-09-19

Larsson, Gunn; Rikspolisstyrelsen; 2004-10-21

Ramstedt, Annika; Luftfartsverket; 2004-08-30

Telephone interviews

Aastrup, Teodor; Attana AB; 2004-10-13

Björkman, Conny; TeliaSonera AB; 2004-09-07

Blomquist Henrik, Skanditek Industriförvaltning, 2004-10-29

Carlsson, Per-Göran; Swedish Catastrophe and Safety Center AB; 2004-09-08

Engström, Rolf; Airborne Hydrography AB; 2004-10-12

Fjällström, Jan; Securitas AB; 2004-11-09

Friberg, Nicklas; C-ITS AB; 2004-09-06

Frisell, Therese; Livsmedelsverket ; 2004-08-25

Greg Geiselhart,; Telematic valley; 2004-10-20

Gästgivar, Per; Sjöland & Thyselius ; 2004-09-14

Hjort, Klas; SUMMIT; 2004-10-28

Hörnström, Nils; Alvis Hägglunds AB; 2004-09-07

Josefsson, Anders; Acreo AB; 2004-10-21

Kajrud, Katrin; Göteborgs hamn AB; 2004-09-09

Klarström, Anders; SOS-alarm; 2004-09-02

Kronquist Fredrik, Innovationskapital, 2004-10-27

Larsson, Anders; Fiberson AB; 2004-10-11

Ljung, Lennart; ISIS; 2004-10-22

Lundberg, Bengt; Volvo AB; 2004-11-09

Lundberg, Lars; Luftfartsverket; 2004-09-03

Månsson, Per; Biosensor Applications Sweden AB; 2004-10-13

Måwe, Karin; Krisberedskapsmyndigheten; 2004-11-10

Nilsson, John; Kockums AB; 2004-09-03

Nordhagen Per, Foretagsbyggarna AB; 2004-10-29

Ohlson, Johnny; Dynasafe AB; 2004-08-30

Olsson, Nils; FOI; 2004-11-10

Palm, Per; SOS-alarm; 2004-09-01

Pettersson, Lars; Vasakronan AB; 2004-11-09

Rehnberg, Hans; Saab Bofors Dynamics AB; 2004-09-15

Rosell, Sune; Innate Pharmaceuticals AB; 2004-08-27

Rödfalk, Albert; Precise Biometrics AB; 2004-10-28

Stenström, Olle; Luftfartsverket; 2004-09-03

Stern, Peter; Krisberedskapsmyndigheten; 2004-09-03

Sukja Robin, Affärsstrategerna AB, 2004-10-27

Zachrisson, Elisabeth; Försvarets Materialverk; 2004-11-01

Åhlström, Lucas; Handels och Konsulthuset Plefo AB; 2004-10-26

Interviews in person

Björkholm, Peter; IMEGO AB; 2004-10-14

Dimming, Janerik; Gunnebo AB; 2004-09-08

Ehlersson, Tor; Ericsson Microwave Systems AB; 2004-09-02

Eriksson, Anders; FOI; 2004-09-13

Holmberg, Per and Karlsson, Magnus; Applied Sensor Sweden AB; 2004-10-19

Klasén, Lena; FOI Sensor Systems; 2004-10-26

Krantz-Rülcker, Tina and Lundström, Ingemar; S-sence; 2004-10-19

Kvarnström, Bengt and Lind, Peter; Saab Bofors Dynamics AB; 2004-10-22

Oderland, Ingvar; Ericsson Microwave Systems AB; 2004-10-15

Rosenqvist, Mats; Volvo Technology AB; 2004-09-06

Svensson, Peter; Fingerprint Cards AB; 2004-10-14

Other sources

Försvarsindustrin, en del av säkerhetspolitiken, Sveriges försvarsindustriförening (brochure).

Hearing om nationell strategi för säkerhetsforskning, Finlandshuset Stockholm, 19 augusti 2004.

Jacobsson. S, 2004, Lecture slides, Innovation systems (1) *Transforming the energy sector* (2) *The evolution of new technological systems in renewable*, Chalmers University of Technology

Jacobsson.S, 2004b, *Analysing the dynamics and functionality of a sectoral innovation system.*(Working paper).

On the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security research, Towards a programme to advance European security through Research and Technology, Commission communication, 2004, Commission of the European Communities.

Parhankangas, A, 2004, *Lecture on Innovation Systems*, Industri och teknikanalys, Chalmers University of Technology

Svensk försvarsindustri, avveckling eller utveckling?, ISBN 91 - 631 - 5354 - 8 Symposium in Stockholm, 2004-03-31.

Appendices

Appendix A: Interview questions for the industry survey (in Swedish)

- Vilket är det största kundbehovet idag?
- Hur definierar ni "säkerhetsindustrin"?
- Vilka områden anser ni att man kan dela in säkerhetsindustrin i?
- I vilket område/nisch inom säkerhetsindustrin placerar ni er själva?
- Vilka är era konkurrenter? På vilket sätt konkurrerar ni, vad gör er till konkurrenter, är det om samma teknologiområde/produkt/tillfredsställer samma behov?
- Hur ser er samverkan ut med övriga aktörer, vilka nätverk tar ni del av, joint ventures, strategiska allianser, gemensam forskning?
- Hur sköts er FoU, internt, externt?
- Inom vilket område av säkerhetsindustrin anser ni att Vinnova skall koncentrera sina resurser för att gynna tillväxten för industrin?
- Inom vilka områden forskar ni idag? Vilka områden verkar intressanta för framtida forskning?
- Ser ni någon trend i kundernas efterfrågan? Har det förändrats under de sista åren?
- Vilka trender ser ni för er verksamhet i framtiden med avseende på behov, produkter, teknologier och hotbilder/möjligheter?
- Hur ser tillväxten ut för ert företag och hur ser det ut för ert marknadssegment?
- Vilka faktorer anser du kan förhindra tillväxt av säkerhetsindustrin?

Appendix B: Interview questions for the innovation system analysis (in Swedish)

1. Antal anställda:
 - Hur många anställda arbetar med sensorer?
 - Hur stor del av den totala omsättningen är knuten till verksamhet kring sensorer?
2. Vilka teknologier används i samband med sensorutveckling?
 - Vilken teknologi anser ni vara viktigast i sammanhanget?
3. Vilken teknologi är ni starkast inom? Hur starka är ni globalt/nationellt?
 - Hur skapas kunskapen? Internt/Externt?
4. Vilka kunskapsområden identifierar ni som bristvaror? Hur relevant/kritisk är denna eventuella brist för sensorutvecklingen?
5. Hur många FoU projekt har ni inom sensorområdet?
 - Hur mycket resurser satsas det på dem?
 - Vad handlar de om?
6. Anser ni att det finns ett uttryckt behov från kund?
 - Finns en stark kund?
 - Driver detta behov er forskning, finns det någon annan faktor som är drivande?
7. Hur spås marknadstillväxten bli de kommande åren?
8. Finns det någon standardisering av teknologin?
9. Vad anser ni driver marknadsutvecklingen bortom kund?
 - Finns det någon tydlig drivare av utvecklingen, kunderna, staten eller regleringar?
10. Hur stor del av er forskning är relaterad till helt nya marknader och tekniker?
 - Har ni haft några spinn-offs?
 - Finns det något hinder för nya företag att etablerar sig så som, kostnadshinder, patent, politik eller tillgång till distributionskanaler?
11. Vilka marknader identifierar ni och vilka är kunderna?
12. Kan ni klassificera den/de befintliga marknaden/erna (Nursing, Bridging eller mass markets)?
13. Finns det någon marknad där svenska företag privilegieras?
 - Hur ser ni på hemmamarknadens potential?
14. Hur ser marknadens tillgång på resurser ut i form av human kapital, etc.?
15. Hur stark anser ni legitimiteten för ert område vara?
 - Hur finansieras er FoU verksamhet?
16. Finns ett välutvecklat nätverk?
 - med universitet?
 - med forskningsinstitut? (statliga/kommersiella)

17. Finns specialiserade leverantörer?
18. Finns pooled labour market?
19. Finns politisk makt?

Appendix C: Search strings used in the patent analysis

Search strings used in patent analysis. In the patent analysis these strings were alternated in time period by including the string AND ISD/19990101->20040901, and by origin by including the string AND ACN/SE for identification of Swedish sensor patents.

Optic sensors:

((ABST/((optic OR optical) OR optics) AND ABST/((((sensor OR sniffer) OR screening) OR biometrics) OR radar) OR surveillance) OR detector))

Electronic sensors:

((ABST/(electric)) AND ABST/((((sensor OR sniffer) OR screening) OR biometrics) OR radar) OR surveillance) OR detector))

Magnetic sensors:

((ABST/((magnetic OR magnetical) OR magnetism) AND ABST/((((sensor OR sniffer) OR screening) OR biometrics) OR radar) OR surveillance) OR detector))

Ultra sonic sensors:

((((ABST/((ultrasound OR ultrasonic) OR ultrasonics)) AND ABST/((((sensor OR sniffer) OR screening) OR biometrics) OR radar) OR surveillance) OR detector))

Electromagnetic sensors:

((((ABST/((("terra hertz" OR radar) OR RFID) OR GPS)) AND ABST/((((sensor OR sniffer) OR screening) OR biometrics) OR radar) OR surveillance) OR detector))

Hybrid sensors:

((((ABST/(hybrid OR "sensor system")) AND ABST/((((sensor OR sniffer) OR screening) OR biometrics) OR radar) OR surveillance) OR detector))

Nuclear sensors:

((((ABST/((radiation OR x-ray) OR nuclear)) AND ABST/((((sensor OR sniffer) OR screening) OR biometrics) OR radar) OR surveillance) OR detector))

Biological sensors:

((((ABST/((biology OR biological) OR bio)) AND ABST/((((((sensor OR sniffer) OR screening) OR biometrics) OR radar) OR surveillance) OR detector))

Chemical sensors:

((ABST/((chemistry OR chemical) OR chemically) AND ABST/((((((sensor OR sniffer) OR screening) OR biometrics) OR radar) OR surveillance) OR detector))

All sensors:

((((ABST /((((((sensor OR sniffer) OR screening) OR biometrics) OR radar) OR surveillance) OR detector))AND ACN/SE)

When conducting the patent analysis for measuring the amount Swedish patents on a yearly bases, following search strings were used:

((ABST/((((((sniffer OR detector) OR Screening) OR surveillance) OR sensor)OR radar) OR biometrics) AND ICN/SE) AND ISD/19990101->20000101)

((ABST/((((((sniffer OR detector) OR Screening) OR surveillance) OR sensor)OR radar) OR biometrics) AND ICN/SE) AND ISD/20000101->20010101)

((ABST/((((((sniffer OR detector) OR Screening) OR surveillance) OR sensor) OR radar) OR biometrics) AND ICN/SE) AND ISD/20010101->20020101)

Appendix D: Security sensor industry actors, regulations and networks

Commercial companies

Airborne Hydrography AB

Airborne Hydrography AB is a Management Buy Out from Saab AB that supplies laser bathymetry systems and hydrographical laser survey services. They have 4 employees, were established 2004 and are located in Jönköping.

Applied sensor AB

Applied sensor was established in 1994. The company has 11 employees and is situated in Linköping. The company is a spin off from Linköping University and a member actor of the competence centre S-Sence. Applied sensor is world leading in biological sensor technologies such as FE and MOS technologies.

Attana AB

Attana AB is a supplier of biosensors, based on the QCM technology, with applications within pharmaceutical and life-science research (Proteomics). They have seven employees and are located in Stockholm. They also have an office in the UK. Attana was founded in 2002.

Biacore AB

Biacore AB is a supplier of analytical systems for life science that generate data on protein interactions. The company was created in 1984, is based in Uppsala and has 184 employees.

Biosensor Applications Sweden AB

Biosensor develops and manufactures a biotechnology-based system for detection of chemicals such as explosives and drugs, and of bacteria. The company have 22 employees and was established in 1989. They are located in Sundbyberg.

Ericsson Microwave Systems AB

The company has slightly more than 1500 employees and is located in Gothenburg (Main Office), Skövde, Stockholm and Luleå. Their activity is related to radar sensors, but also to information networks, primarily acting on the defence market. The company was established in 1956.

Exensor Technology AB

Exensor Technology AB was established in 1987. The company has 6 employees and is situated in Lund. The main business includes the areas of ground sensors and ground sensor systems. Their vision is to be leading in mobile, flexible ground sensor systems.

Fiberson AB

Fiberson originated as a spin-out from Ericsson Network Technologies and develops fibre optic sensors for humidity, temperature, mechanical movement and components for fire detection systems. They have 6 employees, are located in Hudiksvall and were established in 2000.

Fingerprint Cards AB

The company develops biometrical solutions and in particular fingerprint technology with the objective to gain royalties from licences to its developed technology. They have 15 employees and are located in Gothenburg. The company was established in 1971.

Gammadata Mätteknik i Uppsala AB

This company was established in 1986 and is located in Uppsala. They conduct research and development concerning applied nuclear, atomic and surface physics. The company has 15 staff members and creates instrumentation and solutions for radiation analysis and high-resolution spectroscopy.

Novo sense

Novosense AB was established in 2004, as a result of research collaboration between Acreo AB, Protego AB, Tilly Medical AB and Fredrik Sebelius. The company produces a wireless system for ECG monitoring equipment, is located in Lund and has one employee.

Plefo

Plefo was originally founded in 1970. The company is situated in Stockholm and for the moment they have 7 employed consultants. The company develops RFID security applications for tracking dangerous goods and luggage.

Precise Biometrics AB

This company is located in Lund and was established in 1997. Precise Biometrics AB has 45 employees. They develop biometrical solutions from ready made sensors. The main activity is the development of the algorithms and the integration of the solution.

Q-Sense AB

Q-Sense AB develops and markets research instruments for molecular binding events taking place on various surfaces based on the patented QCM-D (Quartz Crystal Microbalance with Dissipation Monitoring) technique. The company was established in 1997, has 7 employees and is located in Gothenburg.

RGB Technologies AB

The company develops and markets software, applications and technology for chemical analysis. RGB Technologies AB was established in 2004 and is located in Stockholm. The company has strong relations to, and was partly established tanks, to S-Sence.

Saab Bofors Dynamics

Saab Bofors Dynamics was established in 1985. The company's sensor system division has 120 employees and is located in Linköping. The company is world leading in optic sensor technology and signal processing technology.

Samba sensors

The origin of the Samba Sensors is research on the use of fibre optic technology and micro mechanics for pressure measurement done at Chalmers University of Technology in Gothenburg. Samba Sensors was founded in 1992 and has commercialised the prototype developed at Chalmers. Samba Sensors' market focus is on pressure measurement in medical applications. They have 6 employees and are located in Gothenburg.

SenseAir AB

SenseAir AB is a development and production company within the gas analyzing business, and in particular they manufacture gas sensors and instruments. They are located in Hudiksvall and were established in 1993. SenseAir has 40 employees.

SensET AB

The company was established 2001 and is located in Linköping. They have one employee. Senset AB develops electrical sensors for liquid substances, often reverred to as the electric tongue.

Sensys Traffic AB

This company is active in the area of sensors and systems for informatics for traffic surveillance. They produce applications related to creating safety in logistical infrastructure. Sensys Traffic AB was established in 1982, has 14 employees and is located in Jönköping.

SIRS AB

SIRS AB is a one man company founded in 2002. The company is a spin out from Saab Bofors Dynamics and is developing SIRS radar applications. SIRS is an entirely new radar technology with security applications fields.

Suppliers

Monolitsystem AB

Monolitsystem AB was established in 1982. The company has two employees and is situated in Gothenburg. The company is a supplier or development partner of the sensor industry. Monolitsystems is active in the area of ASIC-development, a component used in MEMS-sensors.

Sivers Lab AB

Sivers Lab AB was established in 1990. The company has 45 employees and is located in Kista. The company is a supplier to the radar industry, and is conducting research and developing applications in electro magnetic microwave components. Sivers Lab is world leading in their fields of application.

University institutions

Department of Numerical Analysis and Computer Science, KTH, NADA

The department conducts fundamental research on Numerical Analysis, concerning development of the algorithms related to sensor development. They are located in Stockholm and were established in 1962.

EISlab

EISlab has 30 employees including two professors. EISLAB is a research and teaching division at Luleå University of Technology. Among other fields of activity, the division conducts research in sensor system of ultrasonic and optical sensors.

Sensor Science and Molecular Physics group IFM, Linköping University

This department at Linköping University is involved in research and development concerning chemical sensors. They are performing cross-disciplinary research in the areas of biochemical sensing, chip technology, self-assembly, interfacial water and surface analysis.

National Networks

No formal national networks have been identified.

International Networks

Gospel

GOSPEL is a Network of Excellence (NoE) funded by the European Commission in the 6th framework programme concerned with Artificial Olfaction. GOSPEL aims to establish Europe as a world leader in the field by developing the scientific understanding and expanding it into the technological development and commercial exploitation.

Nose II

This is a network for “artificial olfaction”, including sensor and sensor system technology, sampling & sample treatment, data evaluation as well as standardisation of procedures and equipment. NOSE II is financed by the European Commission and consists of end-users, researchers, developers, and manufacturers communicating via the NOSE II web-site.

National centre of excellence

ISIS

ISIS is a centre of excellence concerning information systems for industrial control and supervision. 30 people at Linköping's University of Technology are active in this centre. ISIS conducts research in signal processing which is a vital technology for sensor development.

S-Sence

S-sence is the Swedish national centre of excellence in bio- and chemical sensor science and technology, comprising a co-operation between the Division of Applied Physics at Linköping University and industrial partners. The goal of S-SENCE is to develop bio- and chemical sensors for industrial applications.

SUMMIT

SUMMIT is the Swedish national centre of excellence in surface and microstructure technology. SUMMIT is located at Uppsala University and is closely affiliated to the Royal Institute of Technology (KTH) and ACREO AB.

Research institutes

Acree AB

Acree is a R&D company that functions as an intermediate between research and applications in the area of fibre optics, microelectronics and communication technologies concerning system solutions. They have 172 employees and are located in Kista (Head office), Norrköping, Hudiksvall and Jönköping. The company was established in 1996.

Imego AB

This is an institute of microelectronics located in Gothenburg. They develop customer specific micro-sensor systems within the fields of MEMS, biotechnology, magnetism and optics. Often, they function as a link between university research and the market. Imego AB was established 1999 in and has 35 employees.

FOI Sensor System

FOI Sensor System has 120 employees and is situated in Linköping. FOI Sensor Systems is a military research institute conducting research in radar technology and optic sensor technology. The institute is a world leader in low frequency radar technology and antenna technology.

FOI System Technology

FOI System Technology is situated in Stockholm. The institute conducts prominent research in the sensor technology fields of underwater and nuclear sensors.

Swedish Institute of Computer Science

SICS, is an independent non-profit research organization. The mission of SICS is to contribute to the competitive strength of Swedish industry by conducting advanced and focused research in strategic areas of computer science, to a certain extent, related to sensor systems. They are located in Kista (main office), Uppsala, Västerås and Gothenburg, were established in 2000 and have 102 employees.

YKI, Ytkemiska Institutet AB

YKI is an institute for surface chemistry with knowledge in applied surface and colloid chemistry. 50 percent of the industrial partners are based in Sweden, but any company or association can become a member. YKI is located I Stockholm and has 67 employees.

The Ångström Laboratory

The Ångström Laboratory accommodates most of the physics, astronomy and materials science departments of Uppsala University and there are several Research centres and Graduate schools connected to the laboratory, like the Department of Physics, the Department of Radiation Sciences, Department of Engineering Sciences, Department of Materials Chemistry and SUMMIT.

Industry Associations

There is no particular industry association for the security sector as defined in this report. However, the following three are relevant for the sensor technology area.

FIF

FIF is the industry organisation for the Swedish defence industry. They work as a network for companies producing military applications and technologies. The two major actors in the sensor industry, Saab Bofors Dynamics and Ericsson Microwave, are members of FIF.

Sweden Bio and Biotech Forum

Sweden Bio and Biotech Forum are two industry organisations founded during 2000 and 2002 respectively. The organisations work on developing a network between biotech companies, universities and organisations with interest in biotech. They have no direct connection to the sensor industry except for some common fields of technology shared with biosensor technology. Attana is a member of Sweden Bio.

Swesec

Swesec is an industry organisation representing the Swedish security companies. However, their definition of security is more characterized by security related to the private persons and is therefore not aligned with the definition of this report. Swesec also represents sub industry organisations such as SWEGROUP, Sweguard and SWELARM.

Public authorities

The Swedish Radiation Protection Authority, SSI

SSI is responsible for nuclear radiation tasks including protecting the society and environment from harm caused by inappropriate conduct. The authority is strongly guided by the Strålskyddslag, which regulates the circumstances that have to be fulfilled in order to use any nuclear substances for research etc. Hence, this law also affect research on nuclear sensors.

The Swedish Nuclear Power Inspectorate, SKI

SKI is responsible for enhancing the security at nuclear power plants. The public authority is also responsible for controlling and protecting nuclear material from entering or exiting Sweden illegally.

The National Inspectorate of Strategic Products, ISP

ISP is a Swedish governmental agency that controls the export of military equipment and other products that may have both a civilian and a military use, so-called dual-use products. ISP is also the national authority under the Chemical Weapons Convention (CWC). Not only are exports from Sweden controlled but all production of military equipment in Sweden, military training in Sweden, production under licence of Swedish equipment overseas, joint development of equipment with a party overseas, mediation in procurement of military equipment overseas are also subject to controls.

The Swedish Maritime Association

This public authority is responsible for the naval security. They are also responsible for commercial ship inspections.

The Swedish security police, Säpo

Säpo is part of the National Police Board and responsible for the national security. Their work task includes police activities related to counter-terrorism and protection of the Swedish government. Säpo is also responsible for updating the national threat picture posed upon the Swedish society.

The Swedish Emergency Management Agency, SEMA

This authority is responsible for supporting the local and public authorities in their work to become more security oriented. The authorities are funded by SEMA to carry out security enhancing actions.

The European Union, EU

EU possesses the authority to implement regulations affecting all member countries. Since several regulations concerning increased security are issued by the European Union, this authority highly affects the demand of security related products, including the sensor industry.

Customers

Government agencies

The government agencies are autonomous authorities. Established by either the government or local authority, the public authorities are created to manage one or several work tasks. Those authorities identified as customers have primary or secondary responsibility for public safety. These public authorities are:

FMV; is the responsible agency for the supply of material to the Swedish national defence. For the moment, the Networked Based Defence is among the top priority projects.

The Police; safeguards and prevents crimes. The police authority is managed by the National Police Board.

The Swedish Customs; carries out crime fighting tasks and prevents narcotics, weapons and other band substances to pass the national borders. The Swedish customs is divided into six regional offices which are managed by one head office.

The Swedish Coast guard; is a governmental established authority which exercises protection, control and surveillance of national borders. The Swedish coast guard is divided into five operational areas and manage by a central board of directions.

The Swedish Board of Civil Aviation; is the responsible authority for civil aviation security and also responsible for managing a vast majority of the Swedish airports.

Other customers

Sea and Airports; are affected by several international regulations, demanding increased security at international Sea and Airports. These regulations include new technological applications such as sensors.

Large Companies; include all companies with interest in enhanced security by sensor application implementations. For example, such companies are large commercial companies implementing sensor applications for safeguarding company secrets etc, or companies hosing big public events which call for increased security.

Institutions

Ådalen

Since the incident in Ådalen 1931, the use of military recourses for civil objects has been strongly restricted. The government can only demand for use of military resources for defending Sweden against armed attacks. Using military resources for other purposes has to be authorized by the Swedish parliament. According to the police act, the police have

monopoly on the right to use violence on persons. This regulation restricts the use of the military force for prevention of antagonistic acts. However, a discussion about an abrogation of the restrictions related to Ådalen has been raised.

LOU

The LOU regulates almost all public procurement which means that contracting entities, such as local government agencies, county councils, government agencies as well as certain publicly owned companies etc, must comply with the act when they purchase, lease, rent or hire-purchase supplies, services and public works. The rules are different for public procurement above and below a number of so-called threshold values. For procurement above the threshold values, the LOU is based mainly on EC directives. Below the threshold values the provisions are national and the EC directives do not apply. The fundamental principles of European Community law with regard to public procurement are the principles of non-discrimination, equal treatment, transparency (openness and predictability), proportionality and mutual recognition. This regulation came in to force on January 1st 1994, and it affects the sensor industry given the fact that many of the customers are publicly authorities.

Regulation (EC) 2320/2002

This regulation came in to force on January 19th 2003 and is related to common security rules concerning the civil air traffic. The directive was issued by the European Community and the Swedish Board of Civil Aviation conduct inspections based on the regulation.

Regulation (EC) 622/2003

This regulation came in to force on April 4th 2003 and is related to proceedings concerning common basic standards for protection of the air traffic. The directive was issued by the European Community and the Swedish Board of Civil Aviation conduct inspections based on the regulation.

Regulation (COD) 2003/0089

This regulation concerns improvements of the protection of shipping and navigation associated to security on ships and in seaports. This regulation came in to force in March 2004 and it will be complemented in 2006 with regulations concerning under water surveillance.

Appendix E: Clarification of grading of the blockage mechanism G-K in the matrix

The blockage mechanisms are presented according to their designation in the matrix. The number in the index of the following list is referred to the function that the blockage mechanism is affecting.

G.1

The incentives for entering the market are affected by the fact that big financial resources are needed for product development. Also, high volume is needed to reach competitive prices, which is a hindrance for establishment related to production of scale.

G.2

The hindrances stop new entrances into the market and therefore affect the function of entrepreneurial experiments.

G.3

No noticeable relation has been identified.

G.4

No noticeable relation has been identified.

G.5

No noticeable relation has been identified.

G.6

No noticeable relation has been identified.

G.7

The high costs for entering the market will decrease the possibilities of the industry to reach an extensive amount of companies, limiting the system's ability to reach its critical mass that creates free utilities.

H.1

The lack of competent people within this technological field has a direct impact of the system's knowledge base.

H.2

No noticeable relation has been identified.

H.3

Given the fact that knowledge and diversity is needed for entrepreneurial experiments, it can be argued that the diversity of knowledge that emerges from a larger supply of human capital creates favourable conditions for entrepreneurial experiments. Therefore, a shortage in human capital concerning the area of radar and sonar technologies limits the amount of entrepreneurial experiments.

H.4

No noticeable relation has been identified.

H.5 Since the shortage has been expressed by the actors it identifies a problem in the process of mobilizing human capital.

H.6

No noticeable relation has been identified.

H.7

No noticeable relation has been identified.

I.1

The absence of standard is two folded. Several actors have expressed that the technology is too young to be restricted by a standard. In this case a standard would hinder the technology and knowledge development. On the other hand it can be argued that a standard would concentrate existent resources to deepen the knowledgebase.

I.2

Standards have the ability to guide the direction of search. Therefore, the lack of standard hinders this function

I.3

The lack of standard does not restrict companies to specific technological fields. The absence of standards leads to more exploring of new technological areas and more diversity in R&D which encourages entrepreneurial experiments.

I.4

No noticeable relation has been identified.

I.5

No noticeable relation has been identified.

I.6

It can be argued that a standard would increase the legitimacy of the technology given the fact that it formally establishes the technology.

I.7

It is highly likely that a standard would reduce uncertainties concerning the technology of the area and create favourable conditions for all the actors on the market.

J.1

In the absence of a developed integrity discussion, there are no restrictions related to technology or application. Therefore, a broader knowledge base will develop.

J.2

No noticeable relation has been identified.

J.3

No noticeable relation has been identified.

J.4

The integrity discussion can affect sensor applications differently depending on the technology used. This means that if new regulations appear some applications will be affected more than others, creating new markets for these new applications.

J.5

No noticeable relation has been identified.

J.6

Given the fact that it is uncertain if the integrity discussion will emerge and how it will affect the legitimacy of the area, it is hard to establish if it will favour or disfavour the legitimacy. However it certainly will affect the legitimacy.

J.7

An undeveloped integrity discussion creates uncertainty on the market, and therefore reduces the possibilities of creating free utilities.

K.1

It has been established that the competition created by the process enclosed with LOU favours competitiveness. The competition leads to development of applications and technology which in turn generates new knowledge.

K.2

No noticeable relation has been identified.

K.3

It has been argued that LOU favours larger corporations and that it is hard for small sized ones to gain benefits from LOU given the fact that it requires a resource related to the purchasing process. This leads to a tougher business climate for the smaller firms resulting in a loss in diversity due to a lowered number of firms. In turn, this limits the amount of entrepreneurial experiments.

K.4

No noticeable relation has been identified.

K.5

No noticeable relation has been identified.

K.6

No noticeable relation has been identified.

K.7

No noticeable relation has been identified.

Appendix F: Top 13 private sector opportunities according to Civita Group

- *New Bio Surveillance and Bio sensor systems*, \$118 million will be spent in this area in 2005. It is a 100 percent increase since 2004.
- *US-VISIT program*, \$180 million will be spent in 2005 on passenger screening devices. This is an increase by 100 percent since last year.
- *Radiation detection and technology*, \$100 million (100 percent increase) will be spent on technology for recognizing radiation materials on people and in containers.
- *Anti missile technology for commercial aircrafts*, \$61 million will be spent (2 percent increase)
- *Intelligence Integration and Risk analysis systems*, \$80 million will be spent in this area.
- *Explosive detection and Baggage systems* \$400 is to be spent for redesigning baggage systems at American airports.
- *Air cargo screening*, \$140 for research in new airport screening devices.
- *Remote video surveillance equipment*, \$65 million for monitoring borders.
- *Identification and Credentialing Systems and technologies*, including programs for identifying travellers and workers and connect them to their background previously stored. In 2005 \$89 million will be spent. The budget resources in this area are predicted to rise to several hundreds in coming years.
- *Vaccine and Medication*, \$840 will be spent on stockpiling vaccines used in case of biological terrorism.
- *Cyber security*, \$79.8 in 2005.
- *DHS Human resources system*, approximately \$133 million will go to security training and consulting activities.
- *Operation centre establishment and management*, \$35 million will be used for establishing command centres spread over the USA for handling terrorist attacks.

Appendix G: Results from the interviews concerning sector evaluation.

During the interviews, a number of potential future markets and industry sectors were mentioned. However, when interviewing companies, their activity often influenced their answers. Even though, the interviews will reveal some trends regarding the particular sectors.

Johnny Ohlson, Dynasafe AB, mentioned airport security as an area with high future potential. He detected an increase in the demand of airport and aircraft security on the market. Also, he mentioned an increased need for weapon destruction applications since the increased instability in the world has elevated the costs of weapon stock-keeping, given the augmented demand for costly security at the warehouses.

It has also been mentioned that laws and regulations create new markets. An example is the above mentioned area of airport and aircraft security that has been built up around rules and regulations following the terrorist attacks on 9/11. Janerik Dimming at Gunnebo AB stresses this matter and also mentions the current regulation on extended security in seaports where the aim is to achieve the same level of security as in airports. Naturally, this presents a big future market. Tor Ehlersson, Ericsson Microwave, also stresses regulations as an important power in creation future markets. He implies that airports have a good international network that creates the possibility of international regulation and common demands. He also identifies seaports as a main future customer segment.

Further, Janerik Dimming points out the use of microwaves for scanning, as an area that could be applied both in connection with airport and seaport security. He refers to the area as strongly growing. Also referring to Hans Rehnberg from Saab Bofors Dynamics, sensor technology for seaport protection is a high potential market also. Furthermore, Janerik Dimming mentions biometrics as an area of high growth potential, but he inquires a standard in the area to focus the research. Olle Stenström from the Swedish Civil Aviation Administration also stresses the future importance of biometrics for airport security and points out facial recognition as the most interesting among the biometric technologies. Conny Björkman, TeliaSonera, is yet another interviewee that states the importance of biometrics, adding network user identification as a possible area of application.

Sune Rosell, vice president for Innate Pharmaceuticals AB, mentions antidotes against plague, anthrax, smallpox and botulinustoxin, which is the market related to NBC-technology, as a strong future market. He states this given the priority of the US government of creating a protection against biological weapons through the BioShield project. It has been stated that this focus from the US government has

increased the potential of the area and will probably continue to do so. It is also probable that this will influence others to follow the US example.

Per Palm, SOS-alarm, introduces system integration and digital communication as areas of major growth potential. He mentions integration with intelligent buildings, security systems and emergency services centres as a concrete application, giving the advantage of coordination of information for verification and survey, and greatly facilitating rescue operations. However, the present situation does not permit such a system, given limited resources. Tor Ehlersson from Ericsson Microwave shares the perception and mentions the Network Based Defence as a model for a future network based system for civil use. Further, he states that much of Ericsson's future lays in the concept of Network Centric Systems, especially Network Sensor systems. Mats Rosenqvist, Volvo Technology, also stresses the potential of complex systems and systems solutions. Furthermore, he mentions the possibility of integration sensors in existing systems and he extends the spectra of possible customers from government authorities to also include large companies, and in the future also smaller companies. Anders Eriksson, FOI, is yet another interviewee that thinks the growth of the system concept is a strong trend. He mentions complex sensor systems with automatic fusion of sensor data as an interesting application and border control in airports and seaports as a possible application markets.

Bilaga 3.

Security Research in selected EU member states.

How Austria, the Czech Republic, Estonia, Finland, France, Germany, Poland, The Netherlands, and the United Kingdom are preparing for the European Security Research Programmes.

Studie genomförd av Dr Mathias
Kirsten Fraunhofer-
Gesellschaft/VINNOVA



Security Research in selected EU member states

How Austria, the Czech Republic, Estonia, Finland,
France, Germany, Poland, The Netherlands, and
the United Kingdom are preparing for
the European Security Research Programmes

Mathias Kirsten

December 2004

Content

1	Executive Summary	4
1.1	Background	4
1.2	Survey goals	4
1.3	Methodology	5
1.4	Survey summary	6
1.5	Literature	9
2	Introduction	10
3	Objectives and scope	12
4	Methodology	14
5	Austria	17
5.1	Status regarding PASR and ESRP	17
5.2	National activities	18
5.3	Divide between civil and defence research.....	20
5.4	Summary.....	20
5.5	Links.....	20
5.6	Source of Information.....	20
6	Czech Republic	22
6.1	Status regarding PASR and ESRP	22
6.2	National activities	23
6.3	Divide between civil and defence research.....	24
6.4	Conclusion	24
6.5	Links.....	24
6.6	Source of Information.....	25
7	Estonia	26
7.1	Status regarding PASR and ESRP	26
7.2	National activities	26
7.3	Divide between civil and defence research.....	27
7.4	Conclusion	27
7.5	Links.....	28
7.6	Source of Information.....	28
8	Finland	29
8.1	Status regarding PASR and ESRP	29
8.2	National activities	30
8.3	Divide between civil and defence research.....	31
8.4	Summary / Conclusion.....	32
8.5	Links.....	32
8.6	Source of Information.....	32

9	France.....	33
9.1	Status regarding PASR and ESRP	33
9.2	National activities	34
9.3	Divide between civil and defence research.....	35
9.4	Summary / Conclusion.....	36
9.5	Links.....	36
9.6	Source of Information.....	36
10	Germany	37
10.1	Status regarding PASR and ESRP	37
10.2	National activities	38
10.3	Divide between civil and defence research.....	39
10.4	Conclusion	40
10.5	Links.....	40
10.6	Source of Information.....	40
11	Poland.....	41
11.1	Status regarding PASR and ESRP	41
11.2	National activities	41
11.3	Divide between civil and defence research.....	42
11.4	Conclusion	43
11.5	Links.....	43
11.6	Source of Information.....	43
12	The Netherlands	44
12.1	Status regarding PASR and ESRP	44
12.2	National activities	45
12.3	Divide between civil and defence research.....	47
12.4	Conclusion	47
12.5	Links.....	48
12.6	Source of Information.....	48
13	United Kingdom.....	49
13.1	Status regarding PASR and ESRP	49
13.2	National activities	50
13.3	Divide between civil and defence research.....	53
13.4	Conclusion	53
13.5	Links.....	54
13.6	Source of information	54
14	Summary	55
14.1	Literature	59
15	Acknowledgement.....	60
16	Appendix	61
16.1	Contact persons (December 2004)	61
16.2	Abbreviations	63
16.3	Questionnaire	65

1 Executive Summary

This report investigates the situation of nine EU member states in regard to the European programmes on security research and has been ordered by the Swedish Government working group on security research. The survey was carried out between July and November 2004 and provides a snapshot view of the situation in Austria, the Czech Republic, Estonia, Finland, France, Germany, Poland, The Netherlands, and the United Kingdom as of that period.

1.1 Background

The survey is part of ongoing work in Sweden to develop a national strategy for security research. This strategy should complement the European Union's efforts to establish a new "security culture" within Europe while taking care of the Swedish specificities and requirements.

The EU reacted on the need for establishing a new "security culture" (as recommended by [2]) by implementing PASR, the Preparatory Action on the enhancement of the European industrial potential in the field of Security research. The preparatory action and the European security research programme that should result from it both aim at harnessing and strengthening industries and research communities that are (or will be) involved in "advanced security". These measures should help to enable the EU member states to effectively and innovatively address existing and future security challenges and also to gather, develop and put forth their economic strength in that area.

The Swedish Government took up the EU initiative and ordered the development of a national strategy for security research in April 2004. The working group that has been established to carry out the working is chaired by VINNOVA, Swedish Agency for Innovation Systems, and furthermore consists of members from the Swedish Armed Forces, the Swedish Emergency Management Agency, the Swedish Defence Materiel Administration (FMV), and the Swedish Defence Research Agency (FOI). The group also collaborates with industry, universities and other public authorities relevant to the issue.

1.2 Survey goals

The Swedish Government working group on security research has ordered this report as an addition to the development of the Swedish security research strategy. The survey should investigate how other European countries, especially those that are somehow similar to Sweden or have close

economical ties with Sweden, are preparing to develop the envisaged European “security culture”. The main goal is hence, to provide a general picture of each government’s status, activities, and plans regarding security research. More specifically, the descriptions should answer the following questions:

- Who, within Government, is responsible for security research on a national level respectively in regard to PASR and ESRP?
- What is the Government’s position in regard to a national security research strategy and security research programmes?
- Who are the main national actors within the national and the EU programmes on security research?
- Which role does industry play in the security field?
- What happens with the continuum between civil and defence research in the security area?

What we could not take up here are the preparations and developments that are going on in industry. Although industrial aspects are touched, the focus is clearly on governmental measures.

1.3 Methodology

The information and facts given in this survey were collected via questionnaires sent to representatives from government and research, follow-up telephone conversations and official government web sites.

In order to acquire the necessary information, we designed a questionnaire, which was sent to appropriate government representatives in the nine countries. For each country we verified a single government contact person via personal telephone conversations. This was successful for eight of the nine countries, with Estonia being the only exception. Seven of the eight governments answered the questions in the questionnaire. Only from the United Kingdom we were unable to receive an answer for the time being.

In addition, we identified additional representatives from research in five of the nine countries, in order to get additional feedback on the questionnaire.

Moreover, information was collected via the Swedish Military Attachés in the different countries and via informal telephone conversations with government representatives.

The compilation of the gathered information resulted in separate Chapters for each country. In order to avoid misunderstandings and to improve the overall reliability of the report, each government contact was asked to comment on the respective Chapter. Such additional feedback was provided

by Austria, the Czech Republic, Finland, France, Germany, and The Netherlands.

1.4 Survey summary

Potential participants in PASR and ESRP

The potential participants in PASR and ESRP are research organisations, companies, and also universities. In some countries, like Germany for example, also governmental agencies will contribute to the programmes. The importance of the different kinds of participants (research organisations, universities, companies, other governmental agencies, other institutions) is not clear and varies between the countries. It is clear, however, that in all countries investigated, defence-related research and also defence industry is strongly involved in the security research programmes (may be except Austria and Estonia, where defence industry is not so distinct). Furthermore, almost all countries exhibit major participants from Information & Communication Technology and the aerospace sector. Exceptions might be the Czech Republic and Estonia for which we received no explicit information. Other sectors, namely logistics and transport, bio- and chemical industry, consultancy, and the medical sector, were also mentioned.

Technological areas

All of the governments, except Estonia and the UK, are planning to especially support and encourage companies to take part in the PASR and ESRP. This support does most often mean the organization and dissemination of information via official channels, personal contacts and networks. Furthermore, Germany, Poland, and The Netherlands stated that they want to organize special information workshops and seminars, some of which will be hosted by intermediary organizations (like TNO, DLR, etc.). Austria, moreover, intends to set up a national security research programme that should complement PASR and ESRP and will provide companies with access to relevant research infrastructure and facilities. These Austrian activities, however, are not entirely targeted towards industry but should benefit other research groups, too. In general it can be suspected, though, that many of the above-listed activities do not differ significantly from support for other research areas in the European Programmes. It should also be noted, that the UK Government apparently does not plan any supportive activities. Instead, some actions will probably be taken by the UK Trade Associations.

Does Government encourage industry to participate?

National responsibility in PASR and ESRP

Since security research touches many different policy areas, it is not ultimately decided in several countries, which ministry and which division should be put in charge of the actions regarding PASR and ESRP. Except Poland and the Czech Republic, all other countries declared that a final decision on responsibility has not been agreed. These decisions depend heavily on the final context the ESRP will be placed in, for example whether ESRP

will be part of FRP 7, and which role defence-related research will be playing.

In the meantime, Austria, Finland, France, the Netherlands and the United Kingdom, are setting up (informal) cross-governmental working groups bringing together all ministries involved in security aspects. These working groups act as forums to co-ordinate the national positions regarding PASR and ESRP. The lead role, i.e. convening or driving the working group, is often taken by those ministries that have already been in charge of European research issues. Although it has not been said that there exists a respective working group in Germany, it is apparent that a dialogue between interested ministries is being initiated.

Cross-governmental working groups

By contrast, the responsibility for the PASR and ESRP policy in the Czech Republic respectively in Poland has already been assigned and rests with the Ministry of the Interior (in close co-operation with the Defence Ministry) respectively with the Ministry of Research and Information Technology.

The Estonian position in PASR is so far taken care of by the Estonian Public Services Academy.

National activities in security research

While all of the nine countries have already devised national cross-governmental strategies on security, only Poland and the Czech Republic declared to have a national strategy on security research and also dedicated research programmes. In Austria, a dedicated strategy is under preparation as well as a research programme that should complement PASR and ESRP. In Germany the development of a security research strategy is under consideration but not the establishment of a related research programme.

National strategy and programmes

In fact, in all countries, including Austria and Germany, security research is so far taken care of in individual policy areas on the departmental level. A natural explanation is that in most of the countries, each ministry has its own research budget and issues its own research programmes according to its needs and strategies. These naturally reflect certain policy areas and often include security relevant aspects without making this explicit. Hence, security research is heavily fragmented and it is impossible to estimate the amount of money spent. It seems, however, that most of the countries realize a need for an overarching approach to security research.

Research by policy areas

Following from the above paragraph, the responsibility for security research on the national level typically rests with a number of different ministries, especially those ministries that are concerned with security-related areas, for example internal affairs, research, defence, economic affairs, transport, health, justice, etc. The Defence Ministries take up a special role here to which we will return later on in this Chapter.

Responsibility for Security Research

Putting the focus on security research requires considerable cross-governmental co-ordination efforts (may be except for the Czech Republic and Poland where responsibility for security research is already assigned to a respective ministry). While several countries, for example Austria, The Netherlands, and France, are in the process of establishing cross-departmental working groups, it is also know that the UK Government has established a huge cross-governmental programme on resilience, which should improve co-ordination of civil counter-terrorism research across Government.

Focussing on Security Research

Analogous to the European programmes, participants expected to play relevant roles in PASR and ESRP are in most cases major players in the national programmes, too. There are only few exceptions where, for example in Austria, defence-related research institutes carry out defence research but do not compete on the open research market.

Participants in the national programmes

In none of the countries do funding schemes for security-related research differ significantly from funding schemes of other programmes.

Funding schemes

The role of industry in European security research is not clearly defined. While industry and especially the defence industry tries to get into the security market, it is often unclear whether the term “security industry” can already be applied (especially considering a definition of “industry” from which follows that “security industry” should be interpreted as a set of companies that sees its main business activity in the security area¹). However, in the United Kingdom, for example, a security industry already exists and has its own association (BSIA) but spans a much broader range of products and services.

Security industry

Separation between civil and defence research

The divide between civil and defence research is clearly evident also in security research. Special government programmes to bridge this gap from the civil side do rarely exist. An exception is France, where approximately 200 Million Euro of the civil research budget (BCRD) are especially allocated for dual-use research in general. Although we have got the impression that civil aspects like health, citizen and infrastructure safety, respectively “homeland defence” prevail in security research, many defence-related actors from research and industry are trying to transfer their know-how into civil and security markets.

Mechanisms for exchange and collaboration

From a funding point of view, it is apparently also more common to bridge the continuum between civil and defence security research from the defence side. This means that institutions or companies carry out military research that also have relevant civilian activities and collaborations. Obvious exam-

¹ cf. http://www.advfn.com/money-words_term_2447_industry.html

ples for such a coupling are the defence-related institutes of the German Fraunhofer-Society (FhG) and the Netherlands Organization for Applied Scientific Research (TNO), which are both competing on the civil research market, too. But also the UK's Defence Science and Technology Laboratory (DSTL) can be named, which is subcontracting 20% of its research in the CBRN² area to companies and universities.

While these kinds of collaboration and exchange exist, it is nonetheless our impression that the overall divide is still strong, due to the fundamentally different requirements (and cultures) of the two sides. However, as several government and research representatives pointed out in our investigation, the fast-growing demand and the (increasing) development costs for dual-use technologies are seen as major indicators that collaboration between civil and defence R&D has to increase significantly in order to exploit synergies and to improve efficiency in the future. Whether "Security Research" will be a key factor in this process is not undisputed, however.

Future trend
of separation

1.5 Literature

- [1] "On the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security research; Towards a programme to advance European security through Research and Technology", Commission of the European Communities, Commission Communication COM(2004) 72 final, Brussels, 2004.
- [2] Research for a Secure Europe – Report of the Group of Personalities in the field of Security Research; Luxembourg: Office for Official Publications of the European Communities, 2003, ISBN 92-894-6611-1

² CBRN: Chemical, biological, radiological, nuclear

2 Introduction

This survey was conducted between July and November 2004 and should give an overview on how selected EU member states are preparing for the security research programmes of the EU. Ordered by the Swedish Government's working group on security research, the survey should add to the national strategy on security research the group is developing. Our main objective is to deliver a general description of governmental status and measures regarding security research in the following nine countries: Austria, Czech Republic, Estonia, Finland, France, Germany, Poland, The Netherlands and the United Kingdom.

Each country is addressed in a separate Chapter and the appendix supplies the reader with a list of government contacts (as of December 2004).

A Preparatory Action on Security Research

With PASR, the Preparatory Action on the enhancement of the European industrial potential in the field of security research, the EU reacted on the need for establishing a new "security culture" within Europe. The preparatory action and the programme that should result from it both aim at harnessing and strengthening industries and research communities that are (or will be) involved in "advanced security". This should help to enable the EU member states to effectively and innovatively address existing and future security challenges and also to gather, develop and put forth their economic strength in that area.

The Swedish national strategy on Security Research

In order to tackle the security-related and economical challenges on a national level and to complement the EU actions, the Swedish Government ordered to develop a national strategy for security research (Government decision V2, 15th April 2004). The working group should be chaired by VINNOVA, Swedish Agency for Innovation Systems, and furthermore consist of members from the Swedish Armed Forces, the Swedish Emergency Management Agency, the Swedish Defence Materiel Administration (FMV), and the Swedish Defence Research Agency (FOI). The group should also collaborate with other actors involved, like industry, other public authorities, and universities.

The resulting strategy should take its origin in the EU Commission's communication COM(2004) 72 final "On the implementation of the Preparatory Action on the enhancement of the European industrial potential in the area of security research" and be adapted to the Swedish circumstances in respective parts.

The context and ratio of this survey

The survey should be an addition to the Swedish strategy on security research and should provide general information on the situation in the selected European countries named above. It supplies information on the general governmental setup regarding the responsibility, funding and organization of security research – on the national and on the European level. The descriptions in this survey are, of course, only snapshots of an environment that is rapidly developing, not at least in preparation of the expected European Security Research Programme, which should start in 2007.

While the primary goal of this report is to provide a snapshot view of the general situation, a secondary goal is to further networking in that area. The Appendix therefore contains contact information to government representatives from the countries covered in this survey and also Sweden (as of December 2004).

In the following Chapters, we will first detail the objectives and the scope of this study in Chapter 3, while Chapter 4 describes the methodology applied. The subsequent Chapters are dedicated to the descriptions of the individual countries. Last but not least, the report finishes with a summary, in which we put together the main trends and findings from the different Chapters.

3 Objectives and scope

The main objective of this survey is to show how the different European countries prepare for the European programmes on security research (PASR and ESRP). Especially questions regarding governmental responsibilities on the policy level, governmental activities on the national level, and the relation between civil and defence research are taken up.

Since the term “Security Research” plays a major role in this report, we will first clarify its connotation and afterwards describe the scope of this survey.

The meaning of “Security Research” in this survey

This survey builds on the terminology used by the European Commission in its communications on the PASR and ESRP programmes. While the Commission avoids an explicit definition of “Security Research”, it points out the importance to tackle the (new) threats by more innovative means that enable us to deal with complex situations and to address security in a comprehensive manner [1]. In this regard, five priority areas were defined in which research activities should be strengthened:

- Improving situation awareness;
- Optimising security and protection of networked systems;
- Protecting against terrorism (including bio-terrorism and incidents with biological, chemical and other substances);
- Enhancing crisis management (including evacuation, search and rescue operations, active agents control and remediation);
- Achieving interoperability and integrated systems for information and communication.

Therefore, we see “Security Research” as research that touches on at least one of the above areas.

Countries investigated

The countries we investigate in this survey are: Austria, the Czech Republic, Estonia, Finland, France, Germany, Poland, The Netherlands and the United Kingdom. This set of countries covers, on the one hand, the major economical powers in Europe, i.e. Germany, France and the United Kingdom. On the other hand, it includes countries that are in some way comparable to Sweden, for example in size or economical strength, or that have close economical ties in the defence sector.

Scope of the survey

The survey focuses on the following questions:

- Who, within Government, is responsible for security research on a national level respectively in regard to PASR and ESRP?
- What is the Government's position in regard to a national security research strategy and security research programmes?
- Who are the main national actors within the national and the EU programmes on security research?
- Which role does industry play in the security field?
- What happens with the continuum between civil and defence research in the security area?

These questions should be answered in a general and descriptive way. For a more detailed investigation of individual countries, the Appendix provides the contact information for the different countries. It is furthermore not intended to assess countries or compare them against each other. Due to the nature of our investigation this is neither possible nor wanted.

4 Methodology

In close collaboration with the Swedish working group on security research we identified a set of key questions the report should answer. To acquire the necessary information, we tried to identify relevant contact persons in government and research, one for each country. These persons were asked to fill in a questionnaire thus providing the basis. Additional information was gathered by follow-up telephone conversations, support from the Swedish military attachés in the respective countries, and official government web sites.

Questionnaire setup

The contents of the questionnaire were discussed and developed in collaboration with the Swedish working group on security research. It consists of three parts. The first part focuses on the European aspects of security research, especially the issue of responsibility and co-ordination of the countries' positions regarding PASR and ESRP. The questions in the second part are concerned entirely with the national situation, for example the assignment of responsibility, existence of a national strategy, existence of national research programmes, and the main security research-actors in research and industry. The third part investigates the national divide between civil and defence research, especially with respect to security research. This partitioning is also used in the country-specific Chapters later on in this report. The questionnaire itself is supplied in Appendix 16.3.

Target group for the questionnaire

The questions taken up in this survey focus on facts, not so much on opinions. Hence, a large and representative sample-population was not needed. Instead, we were looking for government representatives involved or responsible for security research and with considerable overview to answer the questionnaire on a general basis. We also tried to find research representatives with relevant experience who could answer the questionnaire from their point of view. This was mainly meant as a means to uncover misunderstandings and to complement the views presented by the government contacts. Therefore, we tried to identify a government contact and a research contact for each country.

Acquiring information via the questionnaire

The contact persons in government and research were identified and verified by research via telephone. Starting points were the members of the EU's Aerospace and ICT committees. This approach was successful in eight out of nine countries. Estonia remained the only country where we eventually did not succeed in identifying an official government representative.

Contacting these government representatives via telephone and asking them to fill in the questionnaire resulted in answers from seven of the eight countries: Austria, the Czech Republic, Finland, France, Germany, Poland and The Netherlands. Unfortunately, it was not possible to get an official answer from the responsible authorities in the UK Government at this point in time.

In addition, we also identified relevant research contacts in six countries, five of which answered the questionnaire.

Additional sources of information

Further information was acquired by informal telephone conversations with government and research representatives and from the official governmental web sites. In addition, an official request was sent to the Swedish Military Attachés in the respective countries, asking them to answer a reduced set of questions. By this way we received additional answers from Austria and Finland.

Additional feedback from the Governments

The compilation of the gathered material resulted in a separate Chapter for each country. In order to verify correctness, we asked our government contacts to review their respective Chapters and to give feedback. Austria, the Czech Republic, Finland, France, Germany and the Netherlands were so kind and provided additional input, which was then incorporated.

It must be noted, however, that despite the feedback from several governments, this does not necessarily mean that the Chapters express the official government point of view.

Risks in comparing and assessing information

We cannot assume that the people who contributed to our survey exhibit a common understanding of the term “Security Research”. Although we referred to PASR and the ESRP in conversations and in the questionnaire, it is clear that each person provided answers from his or her own perspective. Compiling the information from these answers into the context of this survey (i.e. a single context) we run the risk that pieces of information are compared or assessed in a way that is not supported by the information base we have. Therefore, we completely omit graphical visualizations, which typically lend themselves easily to all kinds of interpretations. In fact, to be as correct as possible, the information in each Chapter should be considered isolated at first. The missing links between the countries should then be filled in by the reader’s own knowledge and experience.

Timeframe of the survey

The survey was carried out between July and November 2004. While the questionnaire was sent out in August and early September, information from additional feedback and other sources was acquired until the end of

October. The information supplied in this report hence gives a snapshot view of the security research situation in the summer respectively autumn of 2004.

The information on government contacts that we provide in the Appendix is of December 2004.

5 Austria

Security Research is an issue that has raised much interest in Austria. The ongoing preparation of a national strategy on security research, as well as the goal of establishing a national research programme on the subject, documents this. The inter-departmental working group that is currently reviewing Austria's situation and working on a national strategy is also meant to become part of a "security research platform". This platform should further information dissemination and communication between all actors and support (potential) participants in the national and European programmes. While it is not intended for the time being to include defence research in PASR and ESRP, the current discussion in Austria involves both civil research and also prevention-related defence research that is relevant from an security perspective. Hence, the national research programme could also cover some dual-use research and might become a means to couple civil and defence research, aiming to achieve capability needs relevant to security and defence tasks.

5.1 Status regarding PASR and ESRP

Austria is actively preparing to take part in PASR and the ESRP. Besides the already existing interest from research organisations and companies, documented within the first call of PASR, the Government will further encourage potential participants by providing clear information and communication structures as well as financial and infrastructural support.

Expected main participants in PASR and ESRP

The expected participants come from both research and industry: Non-university research (e.g. Austrian Research Centres, Joanneum Research, Austrian Academy of Sciences), universities (e.g. Technical University of Vienna), companies (e.g. ESL Advanced Information Technologies, Frequentis, VCE Holding), but also agencies like *via domau* and Tricon Consulting – all of which have already been participants in the first PASR call.

For the above-mentioned participants it is the universities and some of the research establishments and organisations that are supplied with public base funding, to different degrees though. Companies and private research establishments receive no basic funding from government. The fully funded defence research units, affiliated to the National Defence Academy and the Austrian Armed Forces, do not play a significant role in PASR or ESRP, since they are relatively small and have not participated in national or European programmes so far.

Funding schemes

The main technological areas represented by the expected participants are not yet clear. It is assumed however, that it could be the Information & Communication Technology sector (ICT) that will be involved most. This is also supported by the results from the first PASR call, where many of the successful applicants belong to the ICT sector. But also logistics, chemical industry, and defence are represented. Considering that Austria's defence industry is relatively small, consisting of a few actors, which usually do not count defence activities under their main business activities [1], the less prominent role of defence industry among PASR participants becomes apparent.

Technological areas

Role of defence industry / research

In addition to the active role that research and industry have already taken up in the first call of PASR, the Austrian Government intends to further support and encourage (potential) applicants by the following measures:

Does Government encourage industry to take part? How?

- Establish a national programme on security research that complements the European Programmes PASR and ESRP (see 5.2 National activities)
- Provide access to relevant research infrastructure and facilities (e.g. at the Austrian Research Centres)
- Provide dedicated information and communication structures on both policy and operative level

These measures are, of course, not exclusively targeted towards industry but should similarly benefit research institutions. The mechanisms should apply to the national programme mentioned above as well.

Co-ordination of national position in PASR / ESRP

The final responsibility has not yet been decided but is subject to decision by the Austrian Government in autumn 2004. It is proposed that the Ministry for Transport, Innovation and Technology (BMVIT, "Sektion III, Bereich Innovation") and the Ministry for Education, Science and Culture (BMBWK, "EU co-ordination unit") take over responsibility and co-ordination of the issue within Austria. Communication with the European Commission regarding PASR and ESRP is probably being covered by the BMBWK.

5.2 National activities

Under the co-ordination of the BMVIT and the BMBWK an interdepartmental working group is being built, which consists of members from different ministries, also involving industry and research stakeholders. The group is reviewing the Austrian situation in regard to security research and is also expected to propose a national strategy on that matter.

National strategy, programmes, and responsibilities

A national strategy on security research does not exist but is under preparation. Although it is not yet officially decided, the above-mentioned interdepartmental working group will probably be responsible for this task. In addition to developing the national strategy, the working group is also supposed to become a permanent institution acting as an advisory committee in regard to content and focus of the Austrian security research policy and the national programme. It is also proposed that the working group should operate with a mandate from the Austrian National Security Council (which is the central organ of the Austrian Federal Chancellery advising the federal Government in aspects of foreign, security, and defence politics). The Government's decision on this matter is expected in autumn 2004³.

Existence of a national strategy

Responsibility for strategy

As mentioned in 5.1 above, the BMVIT together with the National Research Council is also preparing a national research programme dedicated entirely to security research, which should support and complement the European programmes. The content of the programme is going to be elaborated together with the members of the above-mentioned working group and its budget is said to be "relatively large" in a mid term perspective. Furthermore, it should be noted that the programme might cover the security R&D needs from both the civil and the defence actors (prevention only), which would be a renunciation from the strict separation between civil and defence that is in effect now. However, this also depends on the budgetary sources that will eventually be made available to the programme. But so far, nothing has been decided. Nonetheless, it is anticipated that the programme will come into effect after summer 2005.

National research programme

Scope of national programme

Divide between defence and civil side

While the national programme is still in preparation, research relevant for safety and security has so far been funded through various other national programmes, for example in IT, Space, Aeronautics as well as through horizontal programmes (i.e. programmes that aim at structures and which are unrestricted regarding subject matter). However, these programmes excluded defence related projects.

National Security Industry

As a transit country and in the vicinity of the Balkan, Austria has become very active in the area of security, especially the fight against organised crime and also anti-terrorism. Many companies, for example from the IT, defence and automotive sector, are producing and delivering advanced security solutions. In niches of the security market, like reliable voice communication systems, Austrian companies have assumed a leading role internationally.

³ Update: Not yet decided, as of 3rd December 2004

5.3 Divide between civil and defence research

Defence and civil research have so far been strongly separated in Austria. Research demands from the defence side are dealt with in (small) research institutes affiliated to the National Defence Academy and also in small groups within the Austrian Armed Forces. These institutes and groups have co-operations with other national and international institutes but they have not been competing on the open research market. The latter is due to the fact that national research programmes have not hosted defence related research, so far.⁴

Funding of
defence research

This policy might slightly be changing with the issue of the Austrian Security Research Programme, since the programme could also cover certain preventive defence related demands in research and development. Hence, security research might play a role in bringing together civil and defence research.

Future trend
of separation

5.4 Summary

With the implementation of the interdepartmental working group on security research, the Austrian Government is introducing an instrument that tries to gather and bundle the existing security research-related actors. Like in most other countries, security-related research activities have already existed – although not under the brand name “Security Research”. The Government activities can therefore be seen as a concerted measure to increase awareness of the overarching idea, and thus to improve the ability of Austrian companies and research organisations to integrate easily into European networks and to successfully participate in PASR and ESRP.

5.5 Links

- [1] <http://www.bmlv.gv.at/omz/ausgaben/artikel.php?id=126> , „Sicherheitspolitik und Wirtschaft“, Sicherheitspolitik und Wirtschaft, Strunz, Herbert and Dorsch, Monique, Österreichische Militärische Zeitschrift - Coverpage - Issue 4/2003

5.6 Source of Information

The information in this Chapter relies on the answers to our questionnaire provided by Dr Birgit Blasch, Federal Ministry for Traffic, Innovation and Technology (BMVIT) as well as further feedback received from Mag. In-
golf Schädler, BMVIT, and ObstdIntD Hans Starlinger, Federal Ministry of

⁴ Basic research that is funded by the Austrian Science Fund (FWF) can, of course, be seen as “dual-use” since it is not geared towards any application area. Applied research as funded mainly by the Austrian Research Promotion Agency (FFG) (formerly the Austrian Industrial Research Promotion Fund, FFF), has been dedicated to civil use only.

Defence. Minor additions are based on information from Austrian Government's websites and e-mail exchange with the Austrian Research Promotion Agency (FFG).

6 Czech Republic

The Czech Government has already established a national strategy on security research and dedicated research programmes exist, too. The Ministry of the Interior – in close co-operation with the Defence Ministry – is in charge of security research in regard to both the national and the European policy. Since Czech defence research and security research overlap to 100%, security research is entirely financed by the Defence Ministry. The main industry participants in the Czech national programmes come from the Association of the Defence Industry. It is thus the Czech defence industry that is also regarded as the Czech Republic's security industry.

6.1 Status regarding PASR and ESRP

The participants from the Czech Republic are expected to cover the different organisations like universities, industry and research institutes, some of which also have relations to the defence area. Responsible for the Czech position in PASR and ESRP is the Ministry of the Interior in co-operation with the Ministry of Defence.

Expected main participants in PASR and ESRP

The main Czech participants within PASR and ESRP are expected to come from universities, research organisations and industry. Examples are the Military Technical Institute of Protection in Brno, the National Authority for NBC Protection (SÚJCHBO) in Příbram and also companies from the Association of the Defence Industry. While companies can be partly funded for their research, research institutions and universities are fully government financed. It is also apparent from the above examples that some of the participants in PASR are strongly related to defence research. Moreover, the Czech Government supports and encourages industry to participate in PASR and ESRP through its national programmes on security research.

Funding schemes
Participation of defence research
Does Government encourage industry to take part? How?

Co-ordination of national position in PASR / ESRP

The co-ordination of actions and policy with respect to PASR and ESRP lies with the Czech Ministry of the Interior (in close co-operation with the Ministry of Defence). There exist no plans for an alteration.⁵

⁵ Update: According to latest information from early December 2004, it is planned that the Czech Ministry of Defence should take over responsibility for security research completely in the near future.

6.2 National activities

Besides a dedicated national strategy on security research, the Czech Republic has also established dedicated security research programmes. These programmes are co-ordinated by the Ministry of the Interior in co-operation with the Defence Ministry. The latter also provides the whole budget for security research in the Czech Republic, which amounts to approximately 500 Million CZK (about 16 Million Euro). Since security research is basically seen as defence research, the main industrial participants of the programmes are related to defence. These companies are also said to form the Czech security industry.

National strategy, programmes, and responsibilities

The Czech Government has already devised a national strategy on security research as well as research programmes dedicated to that subject. For the research programmes it is the Ministry of the Interior in close co-operation with the Defence Ministry that holds responsibility.

Existence of national strategy
Responsibility on national level

The civil research budget is co-ordinated by the Ministry of Education, Youth and Sports (MEYS) and the individual programmes and parts of the budget lie in the responsibility of the individual ministries, including the MEYS but also the Czech Academy of Sciences [1]. Apart from that, defence-related research and the resulting defence research programmes are handled and accounted for exclusively by the Defence Ministry. Czech Republic's defence research and security research are basically the same. Therefore, the budget for the Czech security research programmes is entirely supplied by the Defence Ministry and amounts to approximately 500 Million CZK per year, which is about 16 Million Euro respectively 130 Million SEK and makes up approximately 4% of the Czech Republic's entire defence budget [3]. Areas of interest in this research are, for example "measures to counter the effects of directional energy weapons on information systems and military technology", "increasing protection of the life force against the effects of weapons of mass destruction", and "increasing protection of ACR⁶ sites" (see [4] for more detailed information). In addition to the existing programmes, new security research programmes are in preparation. It is anticipated that the future will see an annual increase of 5% in the security research budget.

National programmes on security research

As in most of the other countries in this survey, actors that play major roles in the national programmes are also expected to be relevant participants within the European programmes. The main private sector-participants on the national level are companies associated in the Association of the Defence Industry. A security industry is said to exist and is mainly equivalent with the Czech defence industry. In analogy to the European programmes,

Participants in national programmes
New programmes
Technological areas
Budget development
Security industry

⁶ ACR: Army of the Czech Republic

the Government is trying to encourage industry to take part in the national security research programmes by providing information and conducting special workshops thus creating awareness for the opportunities. Yet, the funding schemes for the security research programmes do not differ from other national research programmes. The co-financing required from companies is typically 50%. Furthermore, it is not intended to alter the funding schemes for security research in the future.

6.3 Divide between civil and defence research

In the Czech Republic, responsibilities and budgets for civil and defence research are assigned to separate ministries and a general divide between civil and defence research is apparent. Like in other European countries, research institutes exist that are involved in both civil and defence related projects and thus provide links between civil and defence research know-how. Nevertheless, there do not exist dedicated mechanisms to couple civil and defence research. To which extent this separation truly affects security research is not clear, since dedicated security research is entirely funded and commissioned by the Defence Ministry. Nonetheless, it is expected that security issues and security research will probably bring civil and defence markets closer together. Moreover, it is anticipated that the Czech institutions dedicated to defence research will not change in size or budget. Therefore, the increase that is seen in the future security research spending might benefit non-defence institutions and, furthermore, might also benefit the coupling between defence and civil research.

6.4 Conclusion

The Czech Government has already devised a national strategy on security research and funding programmes explicitly dedicated to security research exist. The Czech Ministry of the Interior (in close co-operation with the Defence Ministry) is in charge of the strategic aspects of security research, including the national strategy and the co-ordination of the Czech Republic's position regarding PASR and ESRP. The budget for the security research Programmes is provided entirely by the Ministry of Defence, which distinguishes the Czech Republic from other countries covered in this survey, in which a significant part of security research is financed by civil sources.

6.5 Links

- [1] „About the Ministry“, web side of the Czech Ministry of Education, Youth and Sports, 2004
<http://www.msmt.cz/DOMEK/default.asp?ARI=102645&CAI=2887>

- [2] “National Research and Development Policy of the Czech Republic for 2004 – 2008 / National Research Programme”, Czech Ministry of Education, Youth and Sports, 2004
<http://www.msmt.cz/Files/PDF/KFNarodnipolitikavAJ.pdf>
- [3] “Budget 2004”, Czech Defence Ministry, 2004, [Czech version only]
<http://www.army.cz/mo/doc/rozpocet2004cz.pdf>
- [4] “National Action Plan to Combat Terrorism – wording 2003”, Czech Ministry of the Interior, 2003,
http://www.mvcr.cz/odbor/bezp_pol/english/dokument/ang_nap.pdf

6.6 Source of Information

The information in this Chapter relies on answers to our questionnaire provided by Prof. Dr. Blahoslav Dolejší, Deputy Director at the Department for Programme Management, Research and Development, Czech Republic’s Ministry of Defence. Additional information regarding co-ordination and funding of civil research comes from the above-cited official websites of the Czech Ministry of Education, Youth and Sports and the Defence Ministry of the Czech Republic.

7 Estonia

The awareness for security research apparently offers space for improvement, at least within the civilian parts of the Estonian Government. Except the Estonian Public Service Academy, which is trying to further the discussion, we could not identify relevant government authorities that have already taken up this issue. It is hence undecided, which government authority is going to become responsible for the subject on the national and also on the European level.

7.1 Status regarding PASR and ESRP

Estonia's status in PASR and ESRP is so far unclear. While universities and higher-educational institutions are likely to contribute, the role that industry will take up is unknown. While a national contact point exists with the Estonian Public Service Academy in Tallinn, a formal responsibility within Government is apparently missing.

Expected main participants in PASR and ESRP

First of all, universities and higher educational institutions are expected to participate but also other research groups might play a relevant role. This includes defence-related institutions like the Baltic Defence College in Tartu. Moreover, companies might also take part although it is not clear which ones this could be at the moment. Government is providing basic funding to universities and research groups, although no full funding. Additionally, co-financing, for example in addition to EU funding, is supplied, too.

Funding schemes

Since the Government's awareness regarding PASR and ESRP is so far limited, there are no plans to especially encourage or support companies to participate in those programmes.

Co-ordination of national position in PASR / ESRP

The Ministry of Education and Research has shown initiative in taking up the security research issue, lately. However, it is not foreseeable which authority is going to become responsible in regard to co-ordinating the Estonian position in PASR and ESRP. So far, a national contact point exists in Dr. Tiiu Pohl from the Estonian Public Services Academy in Tallinn.

7.2 National activities

Security research as a whole has so far not been an important issue in Estonian Government, at least not on the civil side. Although it can be assumed that security-related research is conducted, it is apparently not carried out

under the label “security research”. An official responsibility for the subject is undecided and the discussion has not yet started.

National strategy, programmes, and responsibilities

Although Estonian Government is active regarding security, “Security Research” as a dedicated subject has so far not been an issue. Hence, neither a national strategy nor research programmes on this subject exist. At least from the civil side, the development of such programmes is not considered yet. The only exception is a special budget line on security research from the Estonian Public Service Academy, which is to be included in the state budget. The outcome, however, is still unknown.

Existence of national strategy

National programmes on security research

Furthermore, the responsibility for security research on behalf of the Government lies undecided and it is not clear when the discussion will be taken up. A driving force behind this issue is the Estonian Public Service Academy as a national education and research institution in safety and security.

Responsibility for security research on national level

It might be interesting to note that, considering Estonian research in general, the Estonian Government is planning to introduce a range of new instruments aimed at strengthening the country’s research base. The initiatives shall include establishing new industrial research and technology centres, graduate schools, a new grant system and a programme to send students abroad [1]. Whether this is going to affect security research must be left to speculation.

Development in national research

National Security Industry

There are some industries producing various technologies that might support possible future programme(s).

7.3 Divide between civil and defence research

The divide between civil and defence research is difficult to estimate. In fact, security related research is carried out at defence as well as civil research sites. Dedicated mechanisms to couple defence and civil research do not exist. Hence it is also difficult to anticipate the future developments with respect to the coupling of defence and civil research and the role security research might play therein.

7.4 Conclusion

The awareness for security research is not reasonably pronounced in Estonia. While Government, at least its civil part, has not taken up the subject, the Estonian Public Service Academy is trying to initiate the discussion and simultaneously acts as a national contact point for the European activities in this regard.

7.5 Links

- [1] „Increased mobility and access to Structural Funds should lift research after 1 May, says President of the Estonian Parliament”, Cordis News, 2004-04-27, http://dbs.cordis.lu/fep-cgi/srchidadb?CALLER=EN_NEWS&ACTION=D&SESSION=&RCN=EN_RCN_ID:21943

7.6 Source of Information

The information in this Chapter relies on the answers to our questionnaire provided by Dr. Tiiu Pohl, Vice-rector Research and Development for the Estonian Public Service Academy in Tallinn. Minor additions were taken from the Cordis News interview with Prof. Ene Ergma, President of the Estonian Parliament cited in [1].

8 Finland

Finland is employing existing government structures to co-ordinate the national and European security research issues. Driven by the Ministry of Trade and Industry as well as the Ministry of Defence, security research has been introduced into relevant cross-departmental committees and a special "theme group" has been established. While a national strategy or national research programmes on security research do not exist, the Defence Ministry's MATINE programmes include relevant security-related research. These projects are carried out in co-operation between defence and civil research institutes.

8.1 Status regarding PASR and ESRP

The Finnish Government co-ordinates the PASR and ESRP activities through its existing committee concerned with EU research policy, which is chaired by the Ministry of Trade and Industry. The committee has established a special "theme group" to follow the PASR development.

Expected main participants in PASR and ESRP

The Finnish main participants in PASR and ESRP will probably be VTT Technical Research Centre of Finland, the Crisis Management Initiative (CMI), the electronic industry, the Defence Forces' Technical Research Centre, and the Radiation and Nuclear Safety Authority. Government provides funding to research institutes and universities, for example VTT receives 30% base funding from Government, the amount for the universities varies and is hence difficult to calculate. Some of the above named participants are also related to defence research. Besides the Defence Forces' Technical Research Centre also companies like Patria, Instrumentointi (Insta) and Environics are involved.

The Government encourages companies to apply within PASR mainly through direct contacts via its different networks and also via the technology programmes funded by the Ministry of Defence. In addition, the EU R&T secretariat (part of TEKES⁷) provides information on PASR via the Internet (as it also does for other EU research and technology programmes). Special measures in this regard, like workshops and seminars, are so far not planned.

Does Government encourage industry to participate? How?

⁷ TEKES is the Finnish National Technology Agency and is the main public financing and expert organisation for research and technological development in Finland (Source: <http://www.tekes.fi/eng/tekes/>).

Co-ordination of national position in PASR / ESRP

Since there is no special organ in the Finnish Government for dealing with (EU-) Security Research, it has been set on the agenda of a committee responsible for EU research policy in general. This committee is chaired by the Ministry of Trade and Industry⁸, which is responsible for technology and innovation policy. The committee has established a security research “theme group”, which follows the development of the PASR and provides support on a practical level.⁹ All official national positions and decisions will go through the relevant EU committee structure.

In addition, the Defence Ministry has introduced the issue of security research into the Government’s committee dealing with “*Security and defence*” and the “*Implementation of the strategy for securing the functions vital to society [1]*”. This committee, which is viewed as a “client” of security research, is expected to contribute in defining substantial aims security research should achieve.

In addition to the Ministry of Trade and Industry and the Ministry of Defence, also all other relevant ministries are involved in the committees mentioned above as well as in the security research theme group.

It is not expected that the current assignment of responsibilities is going to be changed in the future.

Future responsibility

8.2 National activities

Similar to the responsibility for the European level, it is the Ministry of Trade and Industry in close co-operation with the Ministry of Defence that is responsible for security research on the national level. Although a national strategy does not exist, security-related research projects are carried out, for example under the auspices of the Scientific Advisory Board for Defence, MATINE. Participants of these projects are mainly identical with the expected participants in PASR/ESRP and come from the IT sector, electronic industry, and B/C detection technology.

National strategy, programmes, and responsibilities

So far, a national strategy dedicated to security research does not exist. However, the government resolution on “Securing the Vital Functions of Society” [1] provides a basis for research, too. The committee for “*Security and Defence*”, which is working on the “*Implementation of the strategy for securing the functions vital to society [1]*”, is also expected to contribute to the definition of the basic aims that security research should achieve. On a

Existence of national strategy

⁸ Convenor of the committee is Mr. Timo Kekkonen, Ministry of Trade and Industry

⁹ The theme group is chaired by a member of the Defence Ministry and includes participants from the Ministries of the Interior, Social Affairs and Health, Transport and Communications, and the Ministry of Trade and Industry.

more concrete level, it is the security research theme group, which elaborates more detailed issues. As mentioned above, this group involves all other relevant ministries and is chaired by the Ministry of Defence. The overall political responsibility for security research lies with the Ministry of Trade and Industry.

Responsibility for security research on national level

While there are no programmes on security research, the programmes issued by MATINE, the Scientific Advisory Board for Defence, include elements of security research. The establishment of such research programmes is decided by MATINE's board. But since its funding is mainly focused on defence research, the budget for security-related research is very limited. From an overall budget of approximately 1 Million Euro for MATINE, the estimated amount that goes to security is about 100,000 Euro per year and is likely to increase only slightly in the future.

National programmes on security research

Although the Finnish Government is not intending to establish a dedicated programme on security research, new security-related projects are in preparation. Furthermore, VTT is also starting a preparatory programme.

New programmes

Participants in the national programmes are the same as those expected to take part in PASR and ESRP. The participating companies come from the IT sector, electronic industry, and B/C detection technology. Industry is especially encouraged to take part in the national programmes.

Participants in national programmes

The funding schemes for the programmes with security-related parts do not differ from other funding programmes. This might be changed in the future but there are no specific plans yet.

Funding schemes

National Security Industry

Although there are companies active in the security area, it might be too early to apply the term "security industry".

8.3 Divide between civil and defence research

The separation between civil and defence research is said to be flexible. Of course, differences exist, but civil and defence research use the same technological knowledge and skills. Although the Defence Forces have their own (rather small) institutes, the MATINE programmes, which amount to approximately 1 Million Euro per year, are carried out jointly with civil organisations. For the future it is expected that the collaboration might intensify further. This goes especially since defence and civil markets are expected to move closer together as they build on the same technologies. In a small country like Finland, with limited resources, such a development is a necessity.

8.4 Summary / Conclusion

Finland is employing existing government structures to co-ordinate the national and European security research issues. Security research has been introduced into relevant cross-departmental committees by the Ministry of Trade and Industry and also by the Defence Ministry. To follow the development of the PASR the committee responsible for the EU research policy furthermore established a special "theme group", which is chaired by the Ministry of Defence.

While a national strategy or research programme dedicated to security research does not exist, security-related research is carried out within the Defence Ministry's MATINE programme. In this programme, civil and defence research organisations are using the same knowledge base and are collaborating closely. The exploitation of such synergies is essential, especially for a small country with limited resources.

8.5 Links

- [1] „Stadsrådets Principbeslut om tryggande av samhällets livsviktiga funktioner“ / “Government resolution on Securing the Functions Vital to Society”, Finnish Government, November 2003,
http://www.defmin.fi/chapter_images/2047_Government_Resolution_On_Securing_The_Functions_Vital_To_Society.pdf
- [2] “Security Research: The Next Steps”, Communication from the European Commission, COM(2004) 590 final, 2004
http://europa.eu.int/eur-lex/en/com/cnc/2004/com2004_0590en01.pdf

8.6 Source of Information

This Chapter relies mainly on the answers to the questionnaire we received from Dr Matti Vuorio and Ms Marikaisa Tiilikainen, both from the Finnish Ministry of Defence and Mr Heikki Kleemola, Research Director, VTT Industrial Systems.

9 France

The first call of the Preparatory Action PASR has been very well received among French companies and research organisations. All actors that were expected to take main roles in PASR and ESRP have already been active in the first call. In order to co-ordinate the French position, an interdepartmental working group involving all relevant ministries and led by the Prime Minister Service SGCI has been set up.

While neither a national strategy nor a unique security research programme exists, France has already launched a large number of initiatives on security research whose responsibilities lie with the issuing ministries. The participants in these actions are the same as in PASR and cover all technological areas. While the defence area is still divided from the civil research, it is anticipated that the growing demand for dual-use know-how is also leading to an intensified co-operation between civil and defence research.

9.1 Status regarding PASR and ESRP

French companies and research organisations have been very active in the first call of PASR. In order to co-ordinate actions and policy in regard to PASR and ESRP, the French Government has set up a working group consisting of members from all ministries involved in security aspects. Besides the major roles that the French Home Office, the Defence Ministry, and the Ministry of Research play, it is the Prime Minister Service SGCI that co-ordinates the French position in PASR.

Expected main participants in PASR and ESRP

French research organisations and companies received the first call of PASR very well and those that were expected to be main players have already been active in that call. Amongst those applicants are fully funded organisations like universities and governmental research organisations as well as partially funded organisations such as companies and private research.

Funding schemes

Only very few research entities in France are entirely dedicated to defence research. Most of the institutions are concerned with civil or dual-use technology studies. Nevertheless, it is not regarded as a problem if defence research organisations want to participate in PASR as long as the studies address dual-use technology issues.

Participation of defence research

Like many other governments in this survey, France's Government intends to actively encourage companies to participate in PASR and ESRP. All French ministries concerned by security are involved in the EC initiative and take appropriate action. For example, the ministries organize and dis-

Does Government encourage industry to take part? How?

seminate information on PASR and ESRP and are furthermore active in the above-mentioned national working group on security research.

Co-ordination of national position in PASR / ESRP

All ministries of the French Government are considered to be affected by security issues and are therefore involved in the decision processes (i.e. in the interdepartmental working group mentioned above). Four of them play a major role: The Home Office, the Prime Minister Services SGDN and SGCI, the Ministry of Defence and the Ministry of Research. As always when European affairs are concerned, the co-ordination of the French position lies with the SGCI.

9.2 National activities

France has already launched a huge number of actions and initiatives regarding security research, even though there is no unique national strategy and no national security research programme. While different ministries are responsible for the current initiatives and while there are ongoing discussions on how the existing fragmentation of actions and responsibilities can be overcome, it is not foreseeable that this constellation will change in the short term.

National strategy, programmes, and responsibilities

The French Government has already launched many actions in the field of security research although there is no unique strategic document. All French Ministries concerned with security are involved. If appropriate, the co-ordination of such actions is assumed by the Prime Minister Service SGCI. Within those actions, most technological areas are covered – as it also appears to be the case within the first PASR call.

Existence of national strategy

Responsibility for security research on national level

While there is no unique national security research programme, a huge number of actions with separate contracts exists. There are many initiatives currently in progress that deal with specific and confidential areas. Responsible for actions and initiatives are the respective ministries. Although the French budget for civil research and development (“*Budget civil de recherche et développement*”, BCRD) is co-ordinated by the Ministry of Research, each ministry has its share in that budget – except for the Defence Ministry, which has a separate budget. Each ministry organises its own research programmes (on both national and regional level) according to its funding, its priorities and its needs. Depending on appropriateness, decisions regarding the programmes are taken at Prime Minister, ministry, national or regional level. Because of the fragmentation of the actions, the different sources of funding, and the different levels at which decisions are taken it is not possible to estimate the overall budget spent on security related research.

National programmes on security research

In addition to the existing activities, new research programmes on security research are in preparation. The budget for 2005 is currently negotiated but it is likely that certain fields, such as “*fight against terrorism*”, are considered as high priority and will therefore receive additional funding. There is also a discussion in progress if and how the responsibility for programmes and policy can be altered and adapted to future needs. So far, however, there are no indications what the outcome of the discussion will look like. Hence, it is unlikely that the situation will change in the short term.

Programmes
in preparation

Change of
responsibility

Analogous to PASR, it is the same set of institutions and companies that participate in the national research programmes. Funding schemes in the national programmes depend on the kind of participant (university, company, etc.) but also on the chances in regard to a successful commercialisation of the results, i.e. even research at companies or private research organisations can be fully financed, if the subject requires it. If a commercial market exists, companies or research organisations typically have to supply appropriate co-financing. In this respect, funding for security related research does not differ from other research subjects. Whether this practice is going to be altered in the future has so far not been decided. It is unlikely, however, that things will change in the short term.

Funding schemes in
national programmes

National Security Industry

The French industrial structure covers all technological areas relevant to security and a security industry is thus considered to exist (although it is not clear to which degree these companies are linked with each other compared to more mature respectively traditional sectors). Although many initiatives exist that are related to security research, the Government did not take specific action to strengthen the profile of a French security industry by a coordinated programme.

9.3 Divide between civil and defence research

Although there are separate budgets for civil and defence research as well as separate responsibilities and programmes, too, there are also more and more dual-use subjects coming up. Since competencies exist either in the defence or in the civil area, more and more relations between civil and defence organisations are being generated to meet the growing demand for technology transfer and technology insertion. There exist a number of technical research centres on the civil side, for instance in biological technologies, that develop abilities useful for defence as well as for civilian use. But also the French defence research institutions document the trend towards and demand for dual-purpose activities, by engaging in a growing number of such activities.

Additionally, the French civil research budget (BCRD) provides mechanisms to address dual-use research purposes. The budget is called “Budget civil de recherche et développement” and excludes the Defence Ministries’

Exchange mechanisms between
defence and civil side

research budget, but around 200 Million Euro within BCRD are allocated for dual-use technologies. The CNES (Centre National D'Études Spatiales, French National Research Centre for Space) and the CEA (Commissariat à l'Énergie Atomique, French Research Centre for Atomic Energy) are the main beneficiaries. The budget share on research and technology within BCRD that is dedicated to security matters will probably increase in the future. Even so, and despite the fact that the technologies of the civil and defence markets may become more and more dual, it is seen as likely that the civil and defence markets will stay apart because their goals, their environments and their customers are so different.

9.4 Summary / Conclusion

While many actions on security research are ongoing, an ultimate point of contact for the European activities has not been assigned, yet. The French Government and its ministries, however, follow the (European) discussions on security research intensely. For a final decision about the placement of responsibility for security research, a clarification would be welcome which parts of Research & Technology are going to be managed by the European Defence Agency and which will be dealt with by the future European programme on security research. Nevertheless, the French Government is deeply convinced of the need of a specific programme on security. The fact that many French organisations and companies already took the chance and applied to the first Request for Proposals in PASR is greatly appreciated by the Government and also documents the great interest that research and industry exhibit in that area.

9.5 Links

- [1] « Recherche et développement technologique de la France », Ministère délégué à la Recherche (French Ministry of Research), 2003, <http://www.recherche.gouv.fr/brochure/index.htm>
- [2] Overview of Science and Technology in France in 2003, Department of International Trade Canada, 2003, http://www.infoexport.gc.ca/science/France_2003-en.htm

9.6 Source of Information

The information in this Chapter relies on the answers to our questionnaire on security research provided by Mr Michel Gaillard (Chef de la Mission et chef du Bureau, Mission Affaires Européennes, Direction de la Technologie, Ministère délégué à la Recherche). Minor additions regarding the civil research budget are based on information from the websites of the French Ministry of Research and the Canadian Department for International Trade.

10 Germany

In Germany, the discussion on security research is starting and the preparation of a national strategy is under consideration. So far, the lead rests with the Federal Ministry of Education and Research and the Federal Ministry of the Interior, in regard to policies on both the national and the European level. The national research programmes do not focus on security research but cover security-related aspects. From industry it is mostly companies from the defence sector that are involved in security research and also in PASR.

10.1 Status regarding PASR and ESRP

The German position regarding PASR and ESRP is co-ordinated by the Ministry of Education and Research (BMBF) and the Ministry of the Interior (BMI). Since research units of several Federal Offices are already active in security-related research, these research units are also likely to play a relevant role besides the German PASR/ESRP participants from research and industry. Furthermore, Government intends to encourage industry to take part via targeted dissemination of information. The German network of national contact points is currently preparing to meet the future demand for information and advice regarding the European security research programmes.

Expected main participants in PASR and ESRP

In Germany, the main contributions to PASR and ESRP are expected to come from four types of institutions. These institutions are research organisations, especially institutes of the application oriented Fraunhofer-Gesellschaft, some of which are closely related to defence research. Also German industry, especially the defence sector, is expected to play a major role. Furthermore, some universities are likely to apply, for example the “Security Cluster” from the Free University of Berlin and the University of Bonn. Contributions are also expected from several federal agencies and their research units, for example the Federal Office for Criminal Investigation (Bundeskriminalamt), the Federal Office for Security in Information Technology (Bundesamt für Sicherheit in der Informationstechnik), the Federal Office for Civil Safety and Emergency Aid (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe), and also the Federal Border Guard (Bundesgrenzschutz).

While Federal Offices, as part of the Government, are fully financed, other research organisations and universities receive base funding to different degrees.

Funding schemes

Although a final categorization of potential participants into technological areas is not possible, it is likely that the information and communication technology sector and the defence sector are going to play important roles.

Technological areas

The Government is planning activities to encourage companies to take part in PASR and ESRP. These activities will focus on setting up information networks, mailing activities, organization and execution of information workshops respectively supporting information events held by other research organisations or universities. Responsible for setting up these activities and also for co-ordinating the German position and policy in regard to PASR and ESRP are the Ministry of Research (BMBF, EU Division) and the Ministry of the Interior (BMI, Division V 4). The final decision, which ministry is going to be co-ordinating the European security research policy in the future, has not been met yet.¹⁰

Does Government encourage industry to take part?

Responsibility for policy in PASR/ESRP

In addition, the German network of National Contact Points, which provides advice to applicants of the EU research programmes, is currently preparing to meet the oncoming demand for information from the potential applicants in the security research programmes.

10.2 National activities

The development of a national security research strategy is currently under consideration in Germany. In analogy to the PASR / ESRP policy, this activity would be co-ordinated by the Ministry of Education and Research together with the Ministry of the Interior, involving all other German stakeholders, like the Defence Ministry. While dedicated security research programmes do not exist, respective research is conducted via many other research programmes that exhibit areas relevant to security. From an industry point of view, it is especially companies from defence industry that try to transfer their know-how into this area, too.

National strategy, programmes, and responsibilities

To devise a national strategy on security research is part of ongoing considerations. The Ministry for Education and Research and the Ministry of the Interior would be in charge of such a strategy. The Defence Ministry would be involved, too.

Existence of national strategy

Responsibility for security research on national level

Dedicated programmes on security research do not exist so far. The need for research and development is mainly taken care of in civil research programmes from other areas where security aspects play a role, and in the

National programmes on security research

¹⁰ Update: As of December 2004 the divisions responsible for security research are division 113, "EU Research Policy, EUREKA", Federal Ministry for Research and Education and division P I 1, "General crime fighting, prevention, office of the Conference of the Interior Ministers", Federal Ministry of the Interior. See Appendix 16.1 for contact information.

agencies and research units affiliated to the Ministry of the Interior and the Defence Ministry.

Within civil research programmes, which are issued and funded exclusively by the Research Ministry, security-relevant work is mainly conducted in the space sector, in IT security as well as in nano and optical technologies. The Ministry of the Interior and its affiliated research units cover especially the areas of IT security, technology in criminology, border control at harbours and airports, inspection of persons and luggage at airports, biometry, and the development of detection technology for biological¹¹, chemical and radioactive agents.

The research activities of the Defence Ministry are carried out as mission oriented research / applied research and build on results from civilian research and technology activities. It is noted by the German Defence Ministry that future military research must be secured and executed on the national and European level independently of the European Security Research Programmes. It is not seen as sensible, however, to separate civil and defence activities in the security research area because of the large share of dual-use technology and the resulting synergies. The Defence Ministry will hence also be involved in the national discussion.

The institutions and companies that conduct security-related research on the above-described national level are identical with those expected to be relevant to PASR and ESRP as listed in 5.1.

National Security Industry

Many companies from the defence sector are also active within (advanced) security and try to transfer their competencies to that market. It is, however, not clear if this group can already be seen as a separate industry. This goes especially since the overlap with the defence industry is significantly large.

10.3 Divide between civil and defence research

The separation between civil and defence research in Germany is very strict and deliberate. Defence research is conducted at the institutes of the FGAN (Research Establishment for Applied Science), at research units affiliated directly with the Defence Ministry and also at the Fraunhofer institutes associated in the Fraunhofer defence and security alliance. FGAN and especially the Fraunhofer institutes also take up relevant roles among the German PASR and ESRP participants.

¹¹ In regard to biological agents, the Robert Koch Institute in Berlin should be named, which houses the Federal Information Centre for Biological Safety, affiliated to the Federal Ministry of Health and Social Security [1].

While civil and defence research are kept apart from each other deliberately, an exception – and perhaps a first step in that direction – exists with the defence research conducted by the Fraunhofer institutes. These institutes engage strongly in civil projects, too, and are hence able to build up and deliver know-how from both defence and civil experience.

10.4 Conclusion

In Germany, the discussion on security research is starting and the preparation of a national strategy is under consideration. So far, the EU-related divisions within the Research Ministry and the Ministry of the Interior coordinate the German position regarding PASR and ESRP. Although the Government sees security research as an important subject, actions dedicated exclusively to security research are not evident so far. In contrast to other Western European countries, for example, an inter-departmental working group on security research has not yet been established. Instead, the coordination is done along the existing organizational and communication structures.

10.5 Links

[1] „Centre for Biological Security, Robert Koch Institute“,
http://www.rki.de/UEBER/UEBER_E.HTM?/UEBER/RKI/ZBS_E.HTM&1

10.6 Source of Information

The information in this Chapter relies on the answers to our questionnaire provided by Wolfgang Mosbacher, German Ministry of the Interior, Division V 4a. The answers were co-ordinated within the Ministry of the Interior, in accordance with the Ministry for Economic Affairs, the Research Ministry, and the Ministry of Defence. Additional information, for example regarding the divide between civil and defence research, originates from the answers supplied by Prof. Dr. Klaus Thoma, head of the Fraunhofer-Institute for High-Speed Dynamics, Ernst-Mach-Institute and chairman of the Fraunhofer Defence and Security Alliance.

11 Poland

Together with the Czech Republic, Poland is the other country in this survey that has already established both a national strategy as well as dedicated research programmes on security research. The Ministry for Science and Information Technology is in charge of organizing the Polish position within PASR and ESRP and it is also responsible for the national strategy. The national research programmes are devised by the State Committee on Scientific Research (KBN) respectively by the Defence Ministry in case of defence-related programmes.

The divide between civil and defence research is not considered to be strong in Poland since only rather few institutes exist that are entirely dedicated to defence research. Most of the research is hence carried out in collaboration with civil institutes and universities.

11.1 Status regarding PASR and ESRP

Expected main participants in PASR and ESRP

In Poland, the main participants in PASR and ESRP are expected to come from companies, research groups from R & D units, and universities, some of which are also related to defence research. Companies are likely to come from the bio and information technology area.

Technological areas

The Polish Government also intends to encourage and support companies to take part in the EU programmes by increasing awareness of the opportunities and providing information via special workshops.

Does Government encourage industry to take part? How?

Co-ordination of national position in PASR / ESRP

Responsible for the co-ordination of the Polish position in regard to PASR and ESRP, is the Polish Ministry for Science and Information Technology.

11.2 National activities

A national strategy on security research exists and dedicated research programmes have already been established in Poland. While the Ministry for Science and Information Technology is in charge of the strategy, it is the KBN and the Defence Ministry who are in charge of the civil respectively the defence-related programmes on security research. The main actors in these programmes come from the IT, aerospace, telecommunication and defence sectors.

National strategy, programmes, and responsibilities

Poland has already devised a national strategy on security research. In analogy to the co-ordination within PASR and ESRP, it is the Ministry for Science and Information Technology that is in charge of this strategy.

Existence of national strategy

Responsibility for security research on national level

Moreover, national programmes on security research exist and further ones are in preparation. Research programmes and their budgets lie in the responsibility of the State Committee of Scientific Research (KBN), which is the supreme authority on state policy in the area of science and technology and also the major governmental source of funds for research [2]. In addition to the research funded by KBN comes the military-related research accounted for by the Defence Ministry [1]. The funding for the security research programmes comes from both civil and defence sources and is expected to increase with 3.5% per year. Yet, the ratio between civil and defence spending as well as the actual amount of money allocated to security research is classified information.

Research programmes

Responsibility for research budgets

To take part in the national programmes, typically requires 50% co-financing by the participants, which holds for all research programmes. Hence, there is no special treatment for security research although the funding schemes might be changed in the foreseeable future according to ministerial preferences. There are also no special measures to encourage industry to take part in the national programmes. The amount of co-financing for industry participants is also 50%.

Funding schemes

Conditions for industry

In the national security research programmes all kinds of R&D units are involved, including those from universities and companies. The main industrial actors come from the IT, aerospace, telecommunication and defence sectors. A national “security industry” is considered to exist.

Participants in national programmes

Security industry

11.3 Divide between civil and defence research

The responsibilities for military research and civil research are placed with separate authorities, namely the Defence Ministry and the State Committee of Scientific Research KBN [1]. Nonetheless, the divide between defence and civil research is said to be not so strong in Poland. This might result from the fact that only a few research institutions in Poland conduct exclusively defence research. Like in other European countries, non-military research groups that carry out defence and civil research might provide the coupling. Explicit governmental mechanisms to couple defence and civil research do not exist.

It is anticipated that the number of dual-use products will increase further and thus move civil and defence markets closer together. Nevertheless, this is seen to happen independently of security and security research matters.

11.4 Conclusion

Poland is one of two countries in this survey that already have a national strategy as well as dedicated funding programmes for security research in place. The Ministry of Science and Information Technology is in charge of co-ordinating the Polish position with respect to PASR and ESRP and also in regard to the national security research strategy. Furthermore, research programmes dedicated to security research exist, which are devised by the State Committee on Scientific Research KBN respectively by the Defence Ministry in case of programmes that are defence-related. Despite separate responsibilities and separate budgets on civil respectively defence side, the divide between civil and defence research in Poland is not seen as particularly strong. The increasing demand in dual-use services and products is seen to further the coupling between defence and civil research, although this development is not attributed to security and security research.

11.5 Links

- [1] „Financing of R&D“, web side of the Polish Ministry for Science and Information Technology
http://www.mnii.gov.pl/mnii/index.jsp?place=Menu08&news_cat_id=298&layout=5

- [2] „General Information about KBN“, web side of the Polish Ministry for Science and Information Technology
http://www.mnii.gov.pl/mnii/index.jsp?place=Menu08&news_cat_id=292&layout=5

11.6 Source of Information

The information in this Chapter relies on the answers to our questionnaire provided by Prof. Dr. Jacek Ronda, Senior Advisor to the Minister of Science and Information Technology. Additional information regarding the overall organization of funding and research, we have gathered from the ministry websites cited above.

12 The Netherlands

In preparation of the ESRP and accompanying the PASR, the Dutch Ministries involved in security research are setting up an interdepartmental working group co-ordinated by the Ministry of Economic Affairs. While the working group is a forum to co-ordinate the Dutch policy in regard to PASR and ESRP, for the time being, its final goal has still to be determined. A national strategy and a dedicated research programme on security research do so far not exist but national research programmes in different policy areas are running that include security components.

12.1 Status regarding PASR and ESRP

By setting up a cross-departmental working group the Dutch ministries involved in security research are in the process of establishing a forum to exchange information and to co-ordinate government activities in regard to PASR and ESRP. In order to further support potential PASR/ESRP applicants, the Government intends to inform and actively create awareness of the opportunities among companies and research institutes.

Expected main participants in PASR and ESRP

It is likely that TNO, the Netherlands Organization for Applied Scientific Research and NLR, the Dutch National Aerospace Laboratory, will play the main roles among the Dutch research institutions and universities in PASR and ESRP. Both organisations are partly government funded and have also strong competencies in defence research. The major industry participants are expected to comprise of Stork, Capgemini, Siemens, Logica-CMG and Thales NL, thus covering technological areas like information & communication technology, manufacturing, space, defence, transport and consultancy. There might also be participants from the food, medical and agricultural sector.

Technological areas

Defence-related participants

In order to create awareness of the opportunities of PASR and ESRP among companies and research institutes, the Dutch Government intends to actively inform potential participants via different means of communication. For example, special workshops for Dutch companies are envisaged (in cooperation with TNO and other intermediary organisations like NIVR¹² and NIID¹³ and also EGL¹⁴).

Does Government encourage industry to take part? How?

¹² NIVR: Netherlands Agency for Aerospace Programmes

¹³ NIID: Netherlands Defence Manufacturers Association

¹⁴ EGL: EG-Liason, Netherlands national contact point for FP6

Co-ordination of national position in PASR / ESRP

The Dutch activities regarding PASR and ESRP on the policy level involve nine different ministries among which the Ministry of Economic Affairs has assumed an informal role as a “primus inter pares”¹⁵ in furthering the co-ordination process. In regard to a vision point of view, the lead rests with the respective ministries, for example with the Ministry of the Interior for aspects of public safety, with the Ministry of Justice regarding counter-terrorism, and with the Ministry of Economic Affairs for all economical aspects to name just three. The other ministries involved are the Ministry of Defence, the Ministry of Finance, the Ministry of Transport and Water Management, the Ministry of Public Health, Welfare and Sport, the Ministry of Agriculture, Nature Management and Fisheries, and last but not least the Ministry of Education, Culture and Science.

12.2 National activities

Security Research in The Netherlands is dealt with in a number of research programmes from different policy areas. With the exception of the National Defence Research Programmes, no overarching national R&D activities exist that are dedicated explicitly to security research, so far.

National strategy, programmes, and responsibilities

Since each ministry decides about its own research programmes, the responsibility for the development of research programmes and policies lies with the respective ministries. A super ordinate national strategy on security research or a dedicated security research programme neither exists nor is it under preparation. Instead, the need for research and development in security-related areas is taken care of in several research programmes that include relevant security components. Hence, security research appears in several different guises. These guises are TNO programmes on defence and public safety, research & technology defence programmes of the Ministry of Defence, counter terrorist programmes of the Ministry of Justice, safety programmes of the Ministry of Housing, Spatial Planning and the Environment, and security programmes of the Ministry of the Interior.

Existence of a national strategy

Responsibility for strategy

Research programmes

The following (not necessarily complete) list in Table 12.1 gives an idea about technological areas with ongoing security-related research:

¹⁵ First among equals

Besides the existing programmes, additional research programmes with relevant security related parts are under preparation. However, these are not

New programmes

Defence:	Security is an integral part of any defence research, but focuses mainly on the safety of personnel and material, for example, decreasing the chance of detection. Furthermore, a special programme focuses on detection and border control issues for military police, for example iris scans, biometrics, mobile police and military police communication networks. Another programme focuses on protection against explosives and weapons of mass destruction (for example NBC protection).
Aeronautics:	Aircraft safety and security, and the use of Remote-Piloted Vehicles (RPVs)
Genomics:	Genome sequence analysis studies
Food quality and safety:	Protection of food production chains
External safety:	Concerns the impact of dangerous substances on the environment, including terrorist attacks on dangerous goods and the impact of attacks on complex infrastructures (like airports or harbours).
Social safety and security:	Maintenance of law and order as well as crisis and crowd control
Applied information technology re-search:	Safety and security of digital systems, intelligent systems, development and security of eBusiness, eCommerce, eLearning and e-government concepts
Personal safety & health:	Inoculation programmes and health incident crisis scenarios

Table 12.1: Examples for technological areas with ongoing security related research in The Netherlands.

going to be exclusively dedicated to security research but include the security-related issue for a given application or research issue. A representative for TNO Defence, Security and Safety estimates that the budget allocated for security research within the government programmes might increase by 200% in the future.

Depending on their size, the decision to establish research programmes is met by the Secretary General or the Director General of the ministries, up to the Ministers and the Lower House (Tweede Kamer) for larger programmes.

Responsibility for establishing programmes

Participants in the national programmes are the same ones that are expected to apply within PASR and ESRP. Additionally, universities, the Dutch institute for public health and environment (RIVM) and the private Institute for Safety, Security and Crisis Management (COT) play relevant roles.

Participants in national programmes

The co-financing required from the participants in the national programmes usually lies between 0% (fully funded institutions like RIVM) and 50%,

Funding schemes in national programmes

depending on the programme. To make participation for industry more attractive, special funding for economic development is available to companies. This funding, however, is also available within non-security programmes.

National Security Industry

Although companies exist whose business is related to advanced security, they are, however, not considered as an existing “security industry”.

12.3 Divide between civil and defence research

The separation of research into defence and civil research is quite strong in the Netherlands. Defence research is carried out completely by the Dutch Ministry of Defence respectively by the dedicated defence research institutions like NLR (partly), TNO’s laboratories FEL, PML and TM, and the Maritime Research Institute Netherlands MARIN (partly). Within TNO, NLR, and MARIN, however, the co-operation and dual-use is quite strong. Besides research for the Defence Ministry and the Armed Forces, these laboratories are also active in European research programmes and participate in (selected) civil applications. This is especially interesting since, for example, TNO’s involvement in civil projects provides the civil side with opportunities to access know-how acquired in defence research [1]. Mechanisms to couple defence and civil research exist in form of integrated TNO and NLR programmes with an annual spending of approximately 65 Million Euro in defence and 5 Million Euro in civil security activities. It is probable that non-defence programmes will be started along the same model.

Mechanisms
for exchange

Besides those integrated research programmes within TNO and NLR, there are no other official mechanisms to couple defence and civil research. But since a decrease in government spending on defence research is expected, civil and dual-use projects might become more important and further enhance co-operation across the divide, especially if budgets will be increasingly linked to the integration of civil and defence research.

Future trend
of separation

It is thus also anticipated that civil and defence markets will come closer together and that security might be a driving application therein. Nevertheless, defence and also security markets exhibit special requirements, which will always keep them apart from being open markets.

12.4 Conclusion

While no overarching national activities regarding security research exist, the need for security-related research has been taken care of in several research programmes from different policy areas and hence under different responsibilities. In order to co-ordinate a common Dutch position and policy with respect to PASR and ESRP, the ministries involved are in the process

of setting up an inter-departmental working group convened by the Ministry of Economic Affairs. On the national level, the responsibility for security research resides with the respective ministries and it is not considered to change this.

With regard to the divide between civil and defence research, the situation is similar to the other countries in this report, which exhibit a strict separation of responsibilities for civil respectively defence research. While no governmental mechanisms exist to couple defence and civil research it is the defence research laboratories themselves (and may be some companies in the defence area) that engage in civil and dual-use projects and thus provide defence know-how also for non-defence markets.

12.5 Links

- [1] TNO Defence, Security and Safety web portal,
http://www.tno.nl/en/core_areas/defence_security_safety/index.html

12.6 Source of Information

The information in this Chapter relies on the answers to our questionnaire provided by Astrid Boschker, Advisor Industrial Benefits and Offsets at the Dutch Ministry of Economic Affairs and by Peter Schulein, TNO Account director Public Safety, TNO Defence, Security and Safety. Additions in regard to defence research originate from TNO's website cited in [1] and [2].

13 United Kingdom

Security and especially counter-terrorism receives strong attention in the UK, which is apparent from over 30 years experience in dealing with domestic terrorism. While there is no unique national strategy on security research, the responsibility for security-related research rests with the different ministries and the respective policy areas. In addition to the existing activities on the departmental level, the UK Government ordered a huge cross-governmental programme on “CBRN resilience”¹⁶ in October 2001, which was set up to improve the inter-departmental co-ordination and also to specify research needs, especially in the area of CBRN counter-measures.

The international co-operation and co-ordination of security related research with research partners and authorities in the United States is said to be excellent but to leave considerable space for improvement with the European partners.

13.1 Status regarding PASR and ESRP

The lead for the UK position regarding PASR and ESRP rests with several government authorities. It seems that the Transdepartmental Science and Technology Group (TDST) at the Office for Science and Technology (OST) is initiating a cross-governmental co-ordination across the group of involved authorities. However, since we were unable to receive an official statement from the UK Government, the formal status of this co-ordination remains unclear.

In contrast to most of the other countries in this report, there are no indications that the UK Government is planning to especially encourage industry to take part in the programmes. Instead, the UK trade associations might take some actions.

Expected main participants in PASR and ESRP

Proposals from the United Kingdom are likely to be industry led, forming teams that involve universities and special defence analysis experts working in partnership with other European collaborators. Major players in the programmes will probably be EADS Astrium (UK), ESYS, Logica, and QinetiQ, which is the now privatized part of the former British Defence Evaluation and Research Agency DERA.

Participants

Since it is expected that industry will take up a leading role, the need for special government encouragement or support for companies is not appar-

Government support to industry

¹⁶ CBRN: Abbreviation for “Chemical, Biological, Radiological, and Nuclear”.

ent. Some actions are probably taken by the UK Trade Associations, for example UKISC in the Space domain.

Co-ordination of national position in PASR / ESRP

The lead for the PASR activities rests with more than one government department and also the British National Space Centre (BNSC). It seems that the Department for Industry and Trade (DTI), in particular the Transdepartmental Science and Technology Group (TDST) within DTI's Office for Science and Technology (OST), has initiated a cross-governmental table to co-ordinate the British position within PASR.

OST is responsible for funding basic research via UK's seven Research Councils. It also supports the Chief Scientific Adviser to the UK Government¹⁷, Professor Sir David King, in his role co-ordinating science and technology across Government ([2] Table 1). It is the Chief Scientific Adviser who is responsible for the Government's international science and technology policy including co-ordinating the UK's position on EU Framework programmes [6].

Responsibility for international science & technology policy

13.2 National activities

The UK exhibits a large set of activities regarding security research. While there is no overarching national strategy, research lies in the responsibility of each respective ministry and its policy/application areas. In addition to the departmental activities, and possibly most remarkably among the Government's activities in this area, is the huge cross-governmental programme on CBRN resilience, which is led by the Home Office and which has been spawned in October 2001.

National strategy, programmes, and responsibilities

The UK has apparently strong national activities going on in security research. Moreover, especially on anti-terrorism, the UK has a high level of scientific collaboration with the US. However, the UK Government itself notes that there is "*particular scope*" for developing such links with the EU partners ([3], paragraph 136).

Existence of national strategy

While there is no overarching national strategy on security research, the responsibility for the subject is handled and organized on the policy level

Responsibility for Security Research on national level

¹⁷ The Chief Scientific Adviser is responsible to the Prime Minister and members of the Cabinet for the quality of scientific advice within government and for providing personal advice to them on any aspect of the Government's policy on Science and Technology. In particular the Chief Scientific Adviser has responsibility for the Government's guidelines on advice and policy making and for their implementation; for ensuring the co-ordination of Science policy issues within government and with the devolved administrations; for maintaining an overview of government policies affecting the UK Science base; and for the Government's international science and technology policy including co-ordinating the UK's position on EU Framework programmes [6].

within the different departments (ministries). In fact, setting up strategies and research programmes is driven by demand via the individual policy areas and their focus on subject matters like anti-terrorism, crime prevention or transport security. Examples for the development of departmental strategies in the security area are the DTI's strategy on security and the Home Office's strategy on a scientific response to terrorism.

There also exist cross-governmental initiatives. The most prominent example is the Government's "CBRN Resilience Programme"¹⁸, which is led by a team at the Home Office and was set up in October 2001. Its research and development is aimed at strengthening UK's response to a CBRN terrorist incident. It should identify all relevant research, national and international, and identify gaps in the evidence base and how they can be filled ([1], 4.13). It should also improve the co-ordination of civil counter-terrorism research across Government [4]. According to [3] (paragraph 5), this programme involves scientific competencies from different government departments, industry, academia and international partners.

Cross-governmental programme

Additionally, the ministries conduct security relevant research in their own research departments and by utilizing departmental research programmes. We do not know how much of this research is carried out externally, for example by non-governmental research units or companies.

Departmental research

Besides the departmental programmes, there are also programmes for academic research funded by the UK Research Councils. The Research Councils account for 2,4 Billion £ in the 2004/05 research budget according to their own press releases in July [5]. Some of the programmes are related to security, for example, in the areas of detection techniques for bacteria and viruses, unobtrusive security devices for detecting people and weapons, crime prevention and detection, including support for anti-terrorism technologies, advancement in forensic science techniques and personal security devices. Furthermore, the programmes include research on domestic management of terrorist attacks, including public communication and understanding the causes and social effects of terrorism.

Academic research

Although the report of the Science and Technology Committee [3] and the report of the Royal Society [4] indicate a lack of involvement of non-governmental research institutions in the CBRN-programme and also a lack of co-operation with the UK's civil knowledge base by the defence-related research organisations (e.g. the Defence Science and Technology Laboratory (DSTL), see [3], paragraphs 51 – 54), it is unclear whether this is "complaining on an already high level" or an actually serious problem.

Coupling of governmental and academic research

¹⁸ CBRN: Abbreviation for "Chemical, Biological, Radiological, and Nuclear".

The report of the Science and Technology Committee furthermore mentions that the role of science in the efforts against terrorism is underestimated in the UK Government (in contrast to the United States, as the report points out in paragraph 186). To improve the scientific base and the scientific culture within the Home Office, which is responsible for homeland defence issues, Government appointed a high-ranking Chief Scientific Adviser for the Home Office in November 2002¹⁹.

Scientific advisers in Government

In addition, scientific advisory groups related to security have been installed within Government. The CBRN Science Working Group, chaired by the Chief Scientific Adviser, was established to look at specific areas of CBRN resilience in December 2001 and included academic, industry and government specialists. SAPER, the Scientific Advisory Panel for Emergency Response, should complement existing mechanisms for providing scientific advice to the Government. While the groups' existence is in the public domain, their memberships and activities are classified ([2], paragraphs 20 – 21).

Scientific advisory groups on security

It is hence evident that the awareness of the need for science in security-related issues is rather strong. The Government made clear, however, that the existing funding level is believed to be sufficient and that no additional money is going to be spent ([3], paragraph 3). It is more likely that a modification of priorities for the existing programmes is required.

Future budget for security-related research

Since research and research programmes do not specifically focus on security research but are established to meet concrete scientific demand, there do not exist special funding schemes for those parts that are related to security.

Funding schemes

Participants in the national programmes are research departments from the Home Office, the Ministry of Defence, the Department of Health and other ministries as well as the research organisations and companies already listed as potential PASR and ESRP participants in 13.1.

Participants in national programmes

National Security Industry

While the above descriptions focus mainly on the government-driven activities, the United Kingdom also exhibits a relatively mature industry that already participates in the security domains (see for example the BSIA, British Security Industry Association). PASR is no new world, in this regard. However, the firms within BSIA span a much broader range of activities.

¹⁹ Government's science and innovation strategy, Investing in Innovation, published in 2002, stated that all departments that use or commission significant amounts of research should have a Chief Scientific Adviser (CSA) [1]. Source: <http://www.ost.gov.uk/policy/invest-innovation/rec5.htm>

13.3 Divide between civil and defence research

The separation between civil and defence research seems to be relatively strong. The Home Office, for example, is in charge of research strategies and programmes related to homeland defence while the Defence Ministry is exclusively responsible for the military research needs. Hence, the Ministry of Defence has no formal role and no obligations in the “scientific response to terrorism”, even though its research agency, DSTL, is the primary source of government-funded technologies with application to CBRN countermeasures ([2], paragraph 31).

However, connections between civil and military research exist. Industry and universities provide the bridge as regards technology and know-how. For example in the area of CBRN, the Defence Science and Technology Laboratory (DSTL) subcontracts 20% of its research to universities and companies. Furthermore, the transfer of military technologies to industry was the basis for setting up the Defence Diversification Agency (DDA) in 1999, which is offering access to the UK’s defence science and technology knowledge base. However, in its report the Science and Technology Committee points out certain shortcomings of the current situation and strongly recommends making greater efforts to explore synergies and joint projects between civil and defence research.

Coupling of defence and civil knowledge bases

13.4 Conclusion

Security Research as a topic of its own has not attracted attention in the UK but has always been strictly coupled to concrete needs in the different policy areas. The UK Government has been very active in improving resilience and counterterrorism measures across Government, and to identify research and development needs in these fields. While we cannot assess the scientific culture in UK’s Government, it is clear that the Government and its departments have huge practical experience in coping with security threats from dealing with domestic terrorism for over 30 years. New threats, which became evident for example in the nerve-gas attack against Tokyo’s subway in 1995²⁰, were taken up by the UK Government and led to the establishment of countermeasures, including setting up/optimizing organizational structures and research, especially in the CBRN area. Scientific collaboration with the United States in the security area is excellent but offers scope for improvement regarding the EU partner countries.

²⁰ On March 20th, 1995, members of the Japanese cult Aum Shinrikyo (Supreme Truth) released the chemical nerve agent sarin in a subway train in Tokyo, Japan. The attack killed 12 people and injured over 1,000.

13.5 Links

- [1] “Investing in Innovation: A Strategy for Science, Engineering and Technology”, July 2002, HM Treasury.
- [2] „Eighth Report“, House of Commons, Committee on Science and Technology, Session 2002-03 HC 415-I,
<http://www.publications.parliament.uk/pa/cm200203/cmselect/cmsctech/415/415.pdf>
- [3] “The Government Reply to the Eighth Report from the House of Commons Science and Technology Select Committee, Sessions 2002-03 HC 415-I”, UK Government January 2004,
http://www.homeoffice.gov.uk/docs2/stc_report_reply.pdf
- [4] “Government Response to Royal Society Report: Making the UK safer, detecting and decontaminating chemical and biological agents”, Press Release of the UK Home Office, Stat018/2004, 26th May 2004,
http://www.homeoffice.gov.uk/n_story.asp?item_id=965
- [5] “Research Councils enthusiastic about strengthened infrastructure for UK science”, News release by Biotechnology and Biological Sciences Research Council (BBSRC) on behalf of the Research Councils UK, 12th July 2004,
<http://www.rcuk.ac.uk/press/2004071310yearinvestment.asp>
- [6] ”New Government Chief Scientific Adviser announced”, Press note, Prime Ministers Office, 5th October 2000, <http://www.number-10.gov.uk/output/Page2863.asp>

13.6 Source of information

This Chapter relies on official information from the UK Government and its departments that was available via the above-mentioned web sites. Especially information and opinions from the report cited in [2] and the respective government response [3] provided the base for the description. Additional information regarding potential participants in PASR and the national programmes were gathered via informal telephone conversations with officials at the TDST Directorate, the BNSC and the PSDB. Unfortunately, we were not able to receive an official answer to our questionnaire from the responsible authorities in the British Government.

14 Summary

This survey investigates the situation of nine EU member states in regard to the European programmes on security research and has been ordered by the Swedish Government working group on security research. The nine member states under investigation are: Austria, the Czech Republic, Estonia, Finland, France, Germany, Poland, The Netherlands, and the United Kingdom.

As an addition to the development of the Swedish strategy for security research, the survey should investigate how other European countries are preparing to develop the envisaged European “security culture”. The main goal was to provide a general picture of each government’s status, activities, and plans regarding security research. More specifically, the descriptions should have answered the following questions:

- Who, within Government, is responsible for security research on a national level respectively in regard to PASR and ESRP?
- What is the Government’s position in regard to a national security research strategy and security research programmes?
- Who are the main national actors within the national and the EU programmes on security research?
- Which role does industry play in the security field?
- What happens with the continuum between civil and defence research in the security area?

What we could not take up here are the preparations and developments that are going on in industry. Although industrial aspects are touched, the focus was clearly on governmental measures.

Potential participants in PASR and ESRP

The potential participants in PASR and ESRP are research organisations, companies, and also universities. In some countries, like Germany for example, also governmental agencies will contribute to the programmes. The importance of the different kinds of participants (research organisations, universities, companies, other governmental agencies, other institutions) is not clear and varies between the countries. It is clear, however, that in all countries investigated, defence-related research and also defence industry is strongly involved in the security research programmes (may be except Austria and Estonia, where defence industry is not so distinct). Furthermore, almost all countries exhibit major participants from Information & Communication Technology and the Aerospace sector. Exceptions might be the

Technological areas

Czech Republic and Estonia for which we received no explicit information. Other sectors, namely logistics and transport, bio- and chemical industry, consultancy, and the medical sector, were also mentioned.

All of the governments, except Estonia and the UK, are planning to especially support and encourage companies to take part in the PASR and ESRP. This support does most often mean the organization and dissemination of information via official channels, personal contacts and networks. Furthermore, Germany, Poland, and The Netherlands stated that they want to organize special information workshops and seminars, some of which will be hosted by intermediary organizations (like TNO, DLR, etc.). Austria, moreover, intends to set up a national security research programme that should complement PASR and ESRP and will provide companies with access to relevant research infrastructure and facilities. These Austrian activities, however, are not entirely targeted towards industry but should benefit other research groups, too. In general it can be suspected, though, that many of the above-listed activities do not differ significantly from support for other research areas in the European programmes. It should also be noted, that the UK Government apparently does not plan any supportive activities. Instead, some actions will probably be taken by the UK Trade Associations.

Does Government encourage industry to participate?

National responsibility in PASR and ESRP

Since security research touches many different policy areas, it is undecided in many countries, which ministry and which division should be put in charge of the actions regarding PASR and ESRP. Except Poland and the Czech Republic, most other countries stated that a final decision on responsibility has not been agreed. These decisions depend heavily on the final context the ESRP will be placed in, for example whether ESRP will be part of FRP 7, and which role defence-related research will be playing.

In the meantime, Austria, Finland, France, the Netherlands and the United Kingdom, are setting up (informal) cross-governmental working groups bringing together all ministries involved in security aspects. These working groups act as forums to co-ordinate the national positions regarding PASR and ESRP. The lead role, i.e. convening or driving the working group, is often taken by those ministries that have already been in charge of European research issues. Although it has not been said that there exists a respective working group in Germany, it is apparent that a dialogue between interested ministries is being initiated.

Cross-governmental working groups

By contrast, the responsibility for the PASR and ESRP policy in the Czech Republic respectively in Poland has already been assigned and rests with the Ministry of the Interior (in close co-operation with the Defence Ministry) respectively with the Ministry of Research and Information Technology.

The Estonian position in PASR is so far taken care of by the Estonian Public Services Academy.

National activities in Security Research

While all of the nine countries have already devised national cross-governmental strategies on security, only Poland and the Czech Republic declared to have a national strategy on security research and also dedicated research programmes. In Austria, a dedicated strategy is under preparation as well as a research programme that should complement PASR and ESRP. In Germany the development of a security research strategy is under consideration but not the establishment of a related research programme.

National strategy and programmes

In fact, in all countries, including Austria and Germany, security research is so far taken care of in individual policy areas on the departmental level. A natural explanation is that in most of the countries, each ministry has its own research budget and issues its own research programmes according to its needs and strategies. These naturally reflect certain policy areas and often include security relevant aspects without making this explicit. Hence, security research is heavily fragmented and it is impossible to estimate the amount of money spent. It seems, however, that most of the countries realize a need for an overarching approach to security research.

Research by policy areas

Following from the above paragraph, the responsibility for security research on the national level typically rests with a number of different ministries, especially those ministries that are concerned with security-related areas, for example internal affairs, research, defence, economic affairs, transport, health, justice, etc. The Defence Ministries take up a special role here to which we will return later on in this Chapter.

Responsibility for Security Research

Putting the focus on security research requires considerable cross-governmental co-ordination efforts (may be except for the Czech Republic and Poland where responsibility for security research is already assigned to a respective ministry). While several countries, for example Austria, The Netherlands, and France, are in the process of establishing cross-departmental working groups, it is also known that the UK Government has established a huge cross-governmental programme on resilience, which should improve co-ordination of civil counter-terrorism research across Government.

Focussing on Security Research

Analogous to the European programmes, participants expected to play relevant roles in PASR and ESRP are in most cases major players in the national programmes, too. There are only few exceptions where, for example in Austria, defence-related research institutes carry out defence research but do not compete on the open research market.

Participants in the national programmes

In none of the countries do funding schemes for security-related research differ significantly from funding schemes of other programmes.

Funding schemes

The role of industry in European security research is not clearly defined. While industry and especially the defence industry tries to get into the secu-

Security industry

rity market, it is often unclear whether the term “security industry” can already be applied (especially considering a definition of “industry” from which follows that “security industry” should be interpreted as a set of companies that sees its main business activity in the security area²¹). However, in the United Kingdom, for example, a security industry already exists and has its own association (BSIA) but spans a much broader range of products and services.

Separation between civil and defence research

The divide between civil and defence research is clearly evident also in security research. Special government programmes to bridge this gap from the civil side do rarely exist. An exception is France, where approximately 200 Million Euro of the civil research budget (BCRD) are especially allocated for dual-use research in general. Although we have got the impression that civil aspects like health, citizen and infrastructure safety, respectively “homeland defence” prevail in security research, many defence-related actors from research and industry are trying to transfer their know-how into civil and security markets.

Mechanisms for exchange and collaboration

From a funding point of view, it is apparently also more common to bridge the continuum between civil and defence security research from the defence side. This means that institutions or companies carry out military research that also have relevant civilian activities and collaborations. Obvious examples for such a coupling are the defence-related institutes of the German Fraunhofer-Society (FhG) and the Netherlands Organization for Applied Scientific Research (TNO), which are both competing on the civil research market, too. But also the UK’s Defence Science and Technology Laboratory (DSTL) can be named, which is subcontracting 20% of its research in the CBRN²² area to companies and universities.

While these kinds of collaboration and exchange exist, it is nonetheless our impression that the overall divide is still strong, due to the fundamentally different requirements (and cultures) of the two sides. However, as several government and research representatives pointed out in our investigation, the fast-growing demand and the (increasing) development costs for dual-use technologies are seen as major indicators that collaboration between civil and defence R&D has to increase significantly in order to exploit synergies and to improve efficiency in the future. Whether “Security Research” will be a key factor in this process is not undisputed, however.

Future trend of separation

²¹ cf. http://www.advfn.com/money-words_term_2447_industry.html

²² CBRN: Chemical, biological, radiological, nuclear

14.1 Literature

- [1] “On the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security research; Towards a programme to advance European security through Research and Technology”, Commission of the European Communities, Commission Communication COM(2004) 72 final, Brussels, 2004.
- [2] Research for a Secure Europe – Report of the Group of Personalities in the field of Security Research; Luxembourg: Office for Official Publications of the European Communities, 2003, ISBN 92-894-6611-1

15 Acknowledgement

The author is most grateful for the support received from the Fraunhofer-Gesellschaft, Germany, which partly funded the author's stay at VINNOVA and provided leave to him, the latter making it at all possible to carry out this survey in time.

Furthermore, we would like to thank all who supported us and contributed in the making of this report:

- The people who actively helped to identify appropriate contact persons within government and research.
- The representatives from government and research who dedicated time and effort to answer the questionnaire and who spent additional time on the phone to clarify questions and to provide further background information.
- All people in the different ministries who were involved in answering the questionnaire but have not been mentioned so far.
- The members of the Swedish working group on security research

We also like to emphasize that we greatly appreciated the openness and interest with which our enquiry was met by the different governments and research organisations involved.

16 Appendix

16.1 Contact persons (December 2004)

Due to the fact that the responsibility for security research has not finally been decided in some of the countries, the following list of government contacts should be considered as provisional information.

Austria

Mag. Ingolf Schaedler
Federal Ministry for Traffic, Innovation and Technology (BMVIT)
Deputy Director General Section III
Renngasse 5
1010 Wien

Email: ingolf.schaedler@bmvit.gv.at

Czech Republic

Antonín Zlínký
Ministry of Defence
Armaments Division
Programmes' Control, Research and Development Branch
Nám. Svobody 475
160 01 Prague 6

Email: zlinskya@army.cz

Estonia

Dr. Tiiu Pohl
Estonian Public Service Academy
Kase 61
12012 Tallinn

Email: tiiu.pohl@sisekaitse.ee

Finland

Marikaisa Tiilikainen
Ministry of Defence
Eteläinen Makasiinikatu 8
PO Box 31
FIN-00131 Helsinki

Email: marikaisa.tiilikainen@plm.vn.fi

Jouni Taivalkoski
Finnish Defence Forces Headquarters

PO Box 919
FIN-00131 Helsinki

Email: jouni.taivalkoski@mil.fi

France

Michel Gaillard
Direction de la Technologie - Mission Affaires Européennes
Ministère délégué à la Recherche
1 rue Descartes
75231 Paris Cedex 05

Email: michel.gaillard@technologie.gouv.fr

Germany

Dr. Brunhild Spannhake
Federal Ministry for Research and Education
Division 113, EU Research Policy; EUREKA
Heinemannstr. 2
53170 Bonn

Email: brunhild.spannhake@bmbf.bund.de

Hans-Leo Dirks
Federal Ministry of the Interior
Division P I 1, General crime fighting, prevention, office
of the Conference of Interior Ministers
Directorate for police affairs and counter terrorism
Alt-Moabit 101 D
10559 Berlin

Email: hansleo.dirks@bmi.bund.de

Poland

Prof. Dr. hab. inz. Jacek Ronda
Senior Advisor to the Minister of Science and Information Technology
Ministry of Science and Information Technology
ul. Wspólna 1/3
00-529 Warszawa 53

Email: jronda@mii.gov.pl

The Netherlands

Drs. Astrid Boschker
Advisor Industrial Benefits and Offsets
Ministry of Economic Affairs
30, Bezuidenhoutseweg
P.O. Box 20101
2500 EC The Hague

Email: A.Boschker@minez.nl

Sweden

Dr. Eva Lindencrona
Chair of the Swedish Working Group for Security Research

Director and Head of Competence Areas Division
VINNOVA, Swedish Agency for Innovation Systems
SE-101 58 Stockholm

Email: eva.lindencrona@vinnova.se

United Kingdom

-

16.2 Abbreviations

ACR	Army of the Czech Republic
BCRD	French civil budget for research and development
BMBF	German Federal Ministry of Education and Research
BMBWK	Austrian Federal Ministry for Education, Science and Culture
BMI	German Federal Ministry of the Interior
BMLV	Austrian Defence Ministry
BMVg	German Federal Ministry for Defence
BMVIT	Austrian Federal Ministry for Transport, Innovation and Technology
BNSC	British National Space Centre
BSIA	British Security Industry Association
CBRN	Chemical, biological, radiological and nuclear
CEA	French Research Centre for Atomic Energy
CMI	Finnish Crisis Management Initiative

CNES	French National Research Centre for Space
COT	Institute for Safety, Security and Crisis Management, The Netherlands
DERA	British Defence Evaluation and Research Agency (now split into QinetiQ and DSTL)
DLR	German Aerospace Center
DSTL	Defence Science and Technology Laboratory (United Kingdom)
DTI	Department for Trade and Industry, United Kingdom
EGL	EG-Liasion, Netherlands national contact point for FP 6
ESRP	European Security Research Programme
FFG	Austrian Research Promotion Agency
FGAN	German Federal Research Establishment for Applied Science
FhG	Fraunhofer-Gesellschaft, Germany
FMW	Swedish Defence Materiel Administration
FOI	Swedish Defence Research Agency
FP	European Framework Programme
IT, ICT	Information (and communication) technology
KBN	Polish State Committee on Scientific Research
MARIN	Maritime Research Institute Netherlands
MATINE	Finnish Scientific Advisory Board for Defence
MEYS	Czech Ministry of Education, Youth and Sports
NBC	Nuclear, biological, chemical
NIID	Netherlands Defence Manufacturers Association
NIVR	Netherlands Agency for Aerospace Programmes
NLR	Dutch National Aerospace Laboratory
OST	Office for Science and Technology, DTI, United Kingdom
PASR	Preparatory Action on the enhancement of the European industrial potential in the field of Security research
PSDB	Police Scientific Development Branch at the UK Home Office
R & D	Research and development

R & T	Research and technology
RIVM	Dutch institute for public health and environment
RPV	Remote-Piloted Vehicle
SGCI	French Prime Minister Service
SGDN	French Prime Minister Service
TDST	Transdepartmental Science and Technology Group at OST, United Kingdom
TEKES	Finnish National Technology Agency
TNO	The Netherlands Organisation for Applied Scientific Research
UKISC	United Kingdom Industrial Space Committee
VINNOVA	Swedish Agency for Innovation Systems
VTT	Technical Research Centre of Finland

16.3 Questionnaire

	Questions / topics	Explanations / Comments	Answers
	How does <country> prepare for PASR and ESRP?		
	*PASR: Preparatory Action on "The enhancement of the European industrial potential in the field of Security Research" (PASR 2004). **ESRP: European Security Research Programme		
A	Financial and organizational conditions for the (expected) main participants from <country> (as provided by the Government)		
1	Who are the expected main <country> participants of PASR/ESRP?	Universities, companies, research organisations (which ones?), ...	
1.1	How can they be categorized (in terms of funding and kind of research)?	Degree of funding from Government: fully financed – no basic funding Companies: type of industry	
1.2	Are some of these related to defence research? Respectively, do you expect institutions from defence research to take part in PASR / ESRP?	Yes / No, names of institutions or companies	

2	Is the Government trying (intending) to encourage companies to take part in PASR and ESRP?	
2.1	If “yes”, which measures are taken / resp. are planned?	Special workshops? National programmes?
3	Who is responsible for the <country> contribution to PASR and ESRP? (In regard to policy)?	Person, group, institutions
4	Does a national contact point or an equivalent exist for PASR/ESRP?	Person, group, institutions
B	Status and development of national activities concerning Security Research (Responsibilities, national strategy, research programmes, national security industry)	
1	Does a national strategy for “security research” exist? Respectively, is such a strategy in preparation?	Yes / No
1.1	Who is responsible for this strategy? (Resp. Where is the responsibility organizationally placed?)	Person, Group, Institution Main stakeholders
1.2	Which technological areas does the responsible body represent?	Aerospace, IT, Defence... ?
2	Do national research programmes exist that are explicitly dedicated to or explicitly include “Security Research”?	Yes / No, (if available number of programmes, names of programmes for future reference)
2.1	Who decides about establishing such programmes? Who decides about the budget? (Policy level) – just roughly without too much detail	Person, Group, Institution
2.2	Do separate responsibilities exist for security research on the civil side respectively on the defence side? (Policy level)	Yes, separate bodies / No (separate research budgets, too?)
2.3	(Estimated) overall budget for programmes dedicated to “security research”?	Absolute budget, <i>relative to general research budget, budget per citizen</i>
2.4	Is the budget for the mentioned research programmes coming from civil sources only?	Yes / No
2.5	Are the expected main actors in PASR/ESRP the same as in the national programmes?	Yes / No

2.5.1	Who are the (additional) main participants in the national programmes?	Universities, companies, research organisations (which ones?), ...
2.5.2	How can they be categorized (in terms of funding and kind of research)?	Degree of funding from Government: fully financed – no basic funding
2.6	What are the funding schemes within the security research programmes for the different main actors?	Amount of co-financing required from participants
2.7	Do funding schemes for these programmes differ from “ordinary” research programmes? (E.g. because R&D risks are higher? Restricted markets, different procurement procedures, ...)	Yes (in which regard?) No
2.8	Are the funding schemes going to be changed / updated in the foreseeable future?	Yes (in which regard?) No
<i>Which role is industry playing in the national programmes?</i>		
2.9	Is industry especially encouraged to take part in the national security research programmes?	Yes, by ... PR, interesting funding schemes, etc. / No
2.10	What are the funding schemes for industry participants?	Amount of co-financing required from company
2.11	Which industries (or technological areas) are the main actors in the national programmes (if relevant)?	Technological areas (IT, Aerospace, Manufacturing, Defence ...)
2.12	Do you think that a kind of national “security industry” exists in <country>? Does the Government programmes help to strengthen it?	Yes / No / Existed before In which regard?
3.	Are (new / additional) national research programmes on “Security Research” in preparation?	Yes / No?
3.1	What is the expected development in the future budgets of security research? (Comparing with today)	Increase, decrease Percentage of change
3.2	Is the responsibility for programmes or policy going to change?	Yes / No
3.2.1	Who will be responsible in the future?	Person, group, institution

C Divide between civil research and defence research

1	How strong is the separation between civil and defence research? Respectively, how closely are they coupled?	(Qualitative remarks)
1.1	Do dedicated defence research institutions exist in <country>?	Yes (which ones?) / No
1.2	What will be the future trend for the defence research institutions?	No change, stronger orientation towards civil markets, increase / decrease in employees, increased / decreased government funding?
1.3	Do mechanisms or research programmes exist to couple defence and civil research? (E.g. like the American DARPA)	Yes (which ones?) No
1.4	If programmes exist, what is their estimated budget?	(e.g. DARPA approx. 3 Billion USD per year)
1.5	How will these “mechanisms” develop in the future?	Increase/decrease in budget, new or additional programmes / mechanisms, stronger focus on dual-use-research, ...?
1.6	Do you expect that civil and defence markets will come closer together (e.g. because of budgetary reasons, dual-use products and services, ...)?	Yes / No (+ qualitative remarks)
1.7	Do you think that “Security” and “Security Research” are issues that will further such a development? E.g. further exchange of defence and civil research results? Open up the markets?	Yes / No (+ qualitative remarks) E.g. increased government spending on security services and products?

Bilaga 4.
Program för arbetsgruppens
studieresa i USA

Program för arbetsgruppens studieresa i USA

Måndag 25 oktober 2004

heldag	Homeland Security Conference: Identifying Opportunities for Cooperation between Sweden and the United States for Industry and Government (arrangerad av Exportrådet och svenska ambassaden i Washongton D.C.)
--------	---

Tisdag 26 oktober 2004

förmiddag	National Academies (Review of Innovation Policies and Military R&D) <ul style="list-style-type: none">- International Technology Security, US Department of Defense- US Department of Commerce/National Institutes of Standards and Technology- US Navy SBIR Program, US Department of Defense- Perspectives from the Congress
eftermiddag	American Association for the Advancement of Sciences (AAAS) <ul style="list-style-type: none">- Center for Science, Technology and Security Policy- R&T Science and Technology Program

Onsdag 27 oktober 2004

förmiddag	Department of Health and Human Services/National Institutes of Health <ul style="list-style-type: none">- Office of Biotechnology Activities- National institute of Allergy and Infectious Diseases- Fogarty International Center
eftermiddag	Department of Homeland Security/Information Analysis and Infrastructure Protection <ul style="list-style-type: none">- Strategic Partnerships Office- National Cyber Security Division- Infrastructure Co-ordination Division

Torsdag 28 oktober 2004

förmiddag	Center for Strategic and International Studies (CSIS) <ul style="list-style-type: none">- Homeland Security Program
-----------	---