Strategisk Forsknings- och Innovationsagenda

Säkerhet

En agenda beskrivning inom ramen för utlysningen för VINNOVAs satsning Strategiska Innovationsområden som arbetats fram av industri, akademi och institut inom säkerhetsteknisk forskning

Strategisk Forsknings- och Innovationsagenda

Säkerhet

Maj 2013

Innehåll

Sammanfattning 3

1 Varför är säkerhetsteknik viktig? 5

1.1 Samhällets behov 5

1.1.1 Grunden för marknadens efterfrågan 5

1.2 Behov av säkerhetsteknik i utvalda branscher 6

1.2.1 Telekommunikation 6

1.2.2 Energiförsörjning 7

1.2.3 Transport 7

1.2.4 Processindustri 7

1.2.5 Sjuk- och hälsovård 7

1.2.6 Skydd och övervakning 8

1.3 Behov i olika krisskeden 8

1.4 IKT finns i alla system – grunden för säkerhetsagendan 9

Teknik 9

Juridik 10

Socialt 10

2 Säkerhetsindustrin är viktig för Sverige 11

2.1 Potential i flera avseenden 11

2.2 Säkerhetsteknik – en vitt förgrenad industri 11

2.3 Mycket stor, och växande, global marknad 12

2.3.1 Definition 12

2.3.2 Storlek 12

2.3.3 Dynamik 12

2.3.4 Geografi 13

Globalt 13

Europa 14

Sverige 15

2.3.5 Teknikområden 16

Cybersäkerhet 16

Sensorer 17

Kommunikation och interoperabilitet 17

3 En smartare användning av befintliga värden 19

3.1 Nationella satsningar förutsätter och möjliggör internationellt samarbete 19

3.2 Utnyttja befintliga styrkor genom att bredda tillämpningen 19

3.3 Innovationsmiljöns position 19

3.3.1 Fokus på fyra styrkeområden 20

3.3.2 Breda aktörer 20

3.3.3 Internationell position 21

3.4 Samverkan 22

3.4.1 En lång process av nära, strategiskt samarbete 22

3.4.2 Tradition av samverkan i innovationssystem 22

3.5 Funktionsanalys 22

3.6 Funktionsanalys i praktiken – två exempel 23
3.6.1 Kameraövervakning 23
3.6.2 Vattenrening 25

4 Vad vill vi uppnå? 27
4.1 Fokus och spets för en kraftfull säkerhetsindustri 27
Sensorteknologi 27
Kommunikationsteknologi 27
Interoperabilitet 28
Cybersecurity 28
4.2 Vision och gemensamma mål 28
4.2.1 Vision 28
4.2.2 Insatser och mål för innovationssystemets funktioner 29
Marknad 29
Kompetens 29
Innovationsverktyg 29
FoI-miljöer 30

5 Innovationsprogram för säkerhetsområdet 31
5.1 Fokusområden och aktiviteter 31
5.2 Organisation 32
5.3 Nationellt säkerhetsforskningsprogram 33
5.4 Nationell mötesplats 33

6 Bilaga: ämnesbeskrivningar 35
6.1 Kommunikation 35
6.1.1 Generella trender inom området kommunikation 35
6.1.2 Trådlös kommunikation för samhällssäkerhet 36
6.2 Interoperabilitet 36
6.3 Intelligenta sensorsystem för säkerhet 37
6.3.1 Användningsområden 37
6.3.2 Nationella kompetensområden 38
6.3.3 Behovsbild 38
6.4 Cybersecurity 39
6.4.1 Mjukvarasäkerhet och metoder för "trust assurance" 39
6.4.2 Trusted Computingplattformar och övervakning av datormoln 40
6.4.3 Kryptologi 40
6.4.4 Nätverkssäkerhet och robusthet 41
6.4.5 Privacy och åtkomstkontroll 42
6.4.6 Rättsliga aspekter: spelregler, personlig integritet och legitimitet 42

Sammanfattning

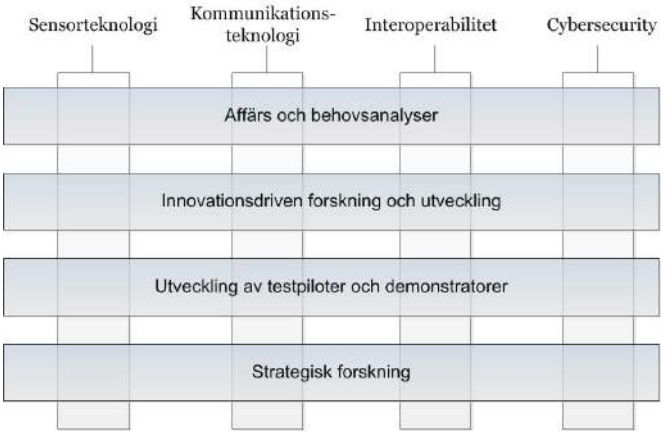
Denna agenda har sitt ursprung i den nationella forsknings- och innovationsagendan (NRIA Säkerhet), som lanserades i november 2011 på initiativ från SOFF (Säkerhet- och försvarsföretagen). Rekommendationerna formulerades då av representanter från säkerhetsområdets företag, universitet, forskningsinstitut, myndigheter och organisationer i en bred uppslutning.

Bakom denna förnyade agenda finns SOFF, Teknikföretagen, Innovationsbron, Security Link, Security Arena, Swedish ICT, agendagruppen Cyber Security and Trustworthy ICT och agendagruppen för IKT. Tillsammans representerar vi hela värdekedjan inom de fyra utpekade strategiska områdena, från stark grundforskning, ledande forskningsinstitut och innovationsmiljöer, till stark svensk exportindustri.

Det som kännetecknar säkerhetsområdet är att marknad, forskning samt branschen i sin helhet är splittrad. Det behövs fokusering och koordinering, och vår agenda föreslår en fokusering på fyra teknikområden och fyra insatsområden för att stärka vårt nationella innovationssystem.

1. Satsning på fyra strategiska tekniska säkerhetsforskningsområden där Sverige är framstående, och svensk industri har stor potential till nya produkter och tjänster: sensorteknologi, kommunikationsteknologi, interoperabilitet, och cybersäkerhet.

2. Insatser och mål för att stärka innovationssystemets centrala funktioner: Marknad, Kompetens, Innovationsverktyg, FoI-miljöer. De breda insatserna illustreras i figuren nedan.



3. Nationell samordning som koordinerar våra begränsade resurser, kortar ledtider och maximerar nyttan av nationella och internationella forskningsmedel.

Vi föreslår en interimsstyrelse för att gå vidare till en SIO-ansökan. Denna styrelse får också funktionen som ett säkerhetsforskningsråd som ska tillse att vi gemensamt effektiviserar tekniska säkerhetsforskningsprogram, tydliggör och stärker existerande centrumbildningar, och kopplar samman svensk forskning med internationell forskning (EU, USA).

1 Varför är säkerhetsteknik viktig?

Områdena samhällssäkerhet och cybersäkerhet är mycket komplexa och vitt förgrenade och därmed inte helt lätta att beskriva. En behovskarakterisering kan låta sig göras med hjälp av en betraktelse av de främsta drivkrafterna i marknadsefterfrågan för säkerhetsutrustning och system inom samhället och privat verksamhet som speglas i behoven i olika branscher[1].

1.1 Samhällets behov

1.1.1 Grunden för marknadens efterfrågan

Samhällets behov av säkerhet, som i sin tur utgör drivkrafter i marknadens efterfrågan på säkerhetsutrustning och -system, utgörs främst av:

- Den allmänna *ekonomiska aktiviteten* i samhället; ju högre aktivitet desto större krav på säkerhet.
- Den allmänna *uppfattningen om aktuella hot* mot säkerheten; när terrorister och den organiserade brottsligheten agerar på nya sätt eller när nya typer av katastrofer/kriser inträffar uppstår tillfälliga toppar i efterfrågan på säkerhet.
- *Regelverk och statliga initiativ*; utformas som en konsekvens av hot mot säkerheten, och styr efterfrågan på säkerhetsprodukter och -tjänster, exempelvis i form av minimikrav på säkerhet.
- *Teknikutveckling*; är både ett svar på marknadens efterfrågan och ett sätt att stimulera ny efterfrågan. En viktig faktor för utvecklingen av säkerhetsbranschen är företagens egenutvecklade tekniker.

Övergripande, gemensamma samhällsutmaningar, som Globalisering, Klimatförändringar, Miljöpåverkan, Urbanisering och Åldrande befolkning, innebär också nya utmaningar att hantera, även inom Säkerhet. Vidare är det en trend i samhällsutvecklingen att vårt beroende av viktiga försörjningssystem ökar. Det tillkommer risker, risker förändras, men framförallt ökar komplexiteten och systeminteraktionen i samhället samtidigt som vi varken tolererar eller har beredskap för annat än korta avbrott. Sammantaget ställer detta ökade krav på robusthet (”resiliens”) i försörjningssystemen.

Som svar på dessa utmaningar utvecklas systemen för försörjning av el, värme, vatten, livsmedel etc, liksom ny infrastruktur för transporter och IKT. I samband med förändringar och förnyelse av system finns goda möjligheter att bygga in en högre grad av robusthet om det görs i ett tidigt skede. Inom säkerhet är det oerhört viktigt att arbeta proaktivt i design, utveckling och produktion av säkra lösningar. Syftet är att brister ska kunna upptäckas i tidigare skeden, när de är mindre kostsamma att korrigera, men framförallt att inte riskera omfattande oönskade händelser med stora konsekvenser/skador.

En nationell kraftsamling för att effektivisera svensk teknisk säkerhetsforskning leder inte bara till ökad svensk export och bättre hantering av vardagskriser. Det kan också leda till

[1] Study on the Competitiveness of the EU security industry, ECORSYS, Directorate-General Enterprise and Industry, Nov 2009.

bättre lösningar för mer extrema kriser. Några exempel på händelser som har skadad oss i Sverige det senaste decenniet är följande.

- Vinterkyla och dess följder har bidragit till förseningar i tågtrafiken vintern 2010/2011, där Trafikverket uppskattar kostnaderna till 2,7 miljarder i utebliven arbetstid.
- Askmolnet 2010 som stoppade flygtrafiken under flera dygn kostade enligt EC flygindustrin 14 miljarder, och en uppskattning av kostnaderna för det svenska samhället hamnar på runt 2 miljarder.
- Utbrotten av parasiten Crytosporidium i vattenförsörjningen ledde till att 12 400 insjuknade i Östersund och 6 167 i Skellefteå.
- Under EHEC-epidemin i matförsörjningen 2011 hittades det i Sverige totalt 49 EHEC-smittade personer, varav 18 utvecklade den allvarliga njurkomplikationen HUS som ledde till minst ett dödsfall.
- I kravallerna i Göteborg 2001 grep de runt 2 500 poliserna 530 personer och omhändertog 385. Butikernas och restaurangernas kostnader i samband med kravallerna uppskattas till närmare 45 miljoner kronor.
- Stormen Gudrun 2005 slog ut energiförsörjningen, gjorde 341 000 hushåll strömlösa och stormfällde 75 miljoner kubikmeter skog. Stormen Per 2007 gjorde att 275 000 hushåll saknade ström och 12 miljoner kubikmeter skog fälldes. Kärnkraftverk stängdes, tågtrafiken stannade och telefonnätet påverkades.
- Hacker-attacken i Motala 2010 mot bostadsbolaget Platens datasystem upptäcktes först när 700 hyresgäster, ett äldreboende och ett köpcentrum blev av med värmen och människor började frysa.
- Ett datorvirus spreds till medicinsk utrustning i Skåne 2009, vilket ledde till att bland annat lagringssystem för ultraljudsbilder och övervakningssystem för förlossningar slogs ut.
- Tieto drabbades 2011 av ett haveri i ”datamolnet” som slog ut flera samhällsviktiga funktioner, så som apotek, bilprovning mm.

1.2 Behov av säkerhetsteknik i utvalda branscher

Många samhällskritiska funktioner är beroende av att infrastrukturen har hög tillgänglighet, men även att systemen går att lita på vad gäller skydd av den information som flödar i näten. Detta är inga nya aspekter utan välkända fakta. Säkerhetsteknik har därmed tillämpningar på många områden. Här belyser vi behoven i några utvalda branscher.

1.2.1 Telekommunikation

Tillförlitlig telekommunikation är fundamentalt i dagens moderna samhälle. Sverige är en världsledande nation inom produktion av telekommunikationsinfrastruktur och tillhörande tjänster. Samtidigt medför ny teknologi och ständigt nya marknadskrav förändrade förutsättningar för hur telekommunikationsnät konstrueras och driftsätts. Hänsyn måste tas både till nya teknologier och att nya roller introduceras, vilket i sig förändrar säkerhetsbilden. Denna förändrade verklighet behöver matchas med nya metoder och teknik för att ta fram robusta och säkra telekommunikationsinfrastrukturer, liksom beredskap och principer för att hantera nya hot och risker.

1.2.2 Energiförsörjning

Liksom telekommunikation är energiförsörjning en fundamental samhällsfunktion. Nätavbrott, även korta sådana, kan få stora samhällsekonomiska konsekvenser och påverkar både enskilda och hela samhällsfunktioner. Det pågår därför självklart ett ständigt arbete med att förbättra säkerheten i dagens energisystem. Samtidigt förändras energiinfrastrukturen när nya alternativa energikällor byggs ut. Detta påverkar nätens funktion och även hur de regleras. Det är därför en utmaning att säkerställa robustheten i energiförsörjningen samtidigt som energiproduktionen och nät förändras. Vidare har hoten mot energisystemen ökat under senare år på grund av att kontrollfunktionerna av näten ”öppnats upp” och sköts allt mer över Internet. Det gäller även på ”konsument”-sidan och vi förväntar oss många nya möjligheter i framtiden vad gäller kontroll av energisystem i hem och bostäder.

1.2.3 Transport

Svensk fordonsindustri är sedan decennier välkänd för sitt omfattande säkerhetsarbete med fokus på trafiksäkerhet. Säkerhet för fordon och trafik har dock många dimensioner och omfattar även exempelvis säkra transporter och IKT-säkerhet. Det transporteras stora mängder farligt gods i Sverige och övriga världen och att övervaka och hantera denna stora mängd är svårt och kostsamt. Nya sensorteknologier innebär radikalt förändrade möjligheter vad det gäller detektering av farliga ämnen samt spårning av gods. Teknikerna är dock i sin linda och behovet är stort att utveckla själva sensorteknologierna samt inte minst de system som ska hantera stora mängder sensorer och varningssystem. Utvecklingen inom IKT omdanar också fordonsteknologin som sådan. Allt fler funktioner i dagens personbilar, lastvagnar, bussar etc bygger på elektroniska komponenter och processorstöd. Vidare blir fordonen och dess olika delsystem uppkopplade och nåbara över Internet. Detta sammantaget innebär både möjligheter till ökad säkerhet, men också nya hot som måste beaktas.

1.2.4 Processindustri

En stor del av Sveriges industriella bas finns i processindustrin och vi är också mycket framgångsrika inom processautomation med en omsättning på 50 miljarder kronor per år. Den hårda globala konkurrensen inom processindustrin medför ett omfattande tryck på rationalisering, vilket i sin tur medför en större efterfrågan på effektivare automation för industriprocesser. Utvecklingen på området går också snabbt och karaktäriseras av krav på högre processeffektivitet, lägre kapitalbindning och effektivare logistik. Det finns naturligtvis en rad olika metoder och teknologier för att uppnå dessa övergripande mål, men nya sensorteknologier för att övervaka och mäta processer liksom nya kommunikationssystem är två nyckelområden. Det är mycket viktigt att denna typ av teknologier för processautomation designas för robusthet, hög IT-säkerhet och tillförlitlighet. De kompetenser som behövs för detta finns idag inte alltid inom branschen, men delvis i andra branscher och hos svenska forskare.

1.2.5 Sjuk- och hälsovård

Västvärlden står inför enorma utmaningar i fråga om fortsatt högkvalitativ sjukvård för hela befolkningen. En allt äldre befolkning medför ökade sjukvårdsbehov, som skall säkerställas av en lägre andel förvärvsarbetande och en minskande skattebas. Ett hårt effektiviseringstryck kännetecknar därför modern hälso- och sjukvård i Sverige och övriga västländer. Ett sätt att möta detta är effektivare rutiner och bättre stödfunktioner, som exempelvis nya IKT-lösningar. En allt större del av vården måste i framtiden också skötas i hemmen och av patien-

ter och anhöriga. För att detta skall fungera utan risk för liv och hälsa måste tillförlitligheten och användarvänligheten i informationssystemen förbättras avsevärt. Exempelvis kännetecknas dagens IT-system i svenska landsting av heterogenitet och de är ofta mycket svårhanterliga. Kraftigt ökad interoperabilitet och homogenitet kommer därför att bli en nödvändighet. Vidare behöver känslig medicinsk data göras tillgängliga för patienter och övriga behöriga oavsett var de befinner sig. Förverkligande av denna vision kommer att medföra stora krav vad gäller design av säkerhet och tillförlitlighet i systemen.

1.2.6 Skydd och övervakning

Det finns en stor farhåga för ett storebrorssamhälle och den ökade kontroll från samhälle och organisationer som modern övervakningsteknik möjliggör. På detta sätt är övervakning och vissa fysiska säkerhetslösningar ett direkt hot mot den personliga integriteten. Detta måste dock balanseras mot de nya möjligheter som ny teknologi och mer omfattande övervaknings- och bevakningssystem medför i form av ökad trygghet och snabbare respons vid incidenter, etc. Fysiska säkerhetssystem är ett viktigt område för denna agenda och säkerhetsbranschen som sådan är starkt växande och med ökande betydelse för svensk industri. Med rätt utnyttjande av kärnkompetenser inom svensk forskning, så som sensorteknologier, sensorsystem och IKT-säkerhet, kan vi se till att svensk industri kan konkurrera globalt inom området. Genom att ta fram teknologier som ger högt skydd av den personliga integriteten kan vi också bidra till att värna om den etiska dimensionen.

1.3 Behov i olika krisskeden

Brister eller avsaknad av säkerhet kan få stora konsekvenser och leda till kriser. Omvänt kan säkerhet utgöra förmågan att avleda eller hantera en krissituation. Ett sätt att strukturera behovet av säkerhetskunskap och -teknik är att studera vilka behov som uppkommer i olika skeden av en kris. Kraven på insatser varierar med skede i krisen, men en effektiv krishantering behövs både före, under och efter en krissituation.

KRISSKEDE	BEHOV	IINSATSER
Före	Det måste finnas en beredskap, som gör att man i det längsta kan undvika att det överhuvudtaget blir en kris. Skulle en kris ändå inträffa är tidig varning av avgörande betydelse.	Utbilda, förebygga, förbereda, produktutveckla, upptäcka.
Under	Om och när en kris är ett faktum ska vi kunna hantera den.	Leda/samverka, resurshantera, avveckla.
Efter	Det måste finnas mekanismer som ser till att vi inte bara observerar utan också ”lär oss läxan” så att vi står ännu bättre förberedda nästa gång.	Återställa, återföra erfarenheter, uppdatera.

Fig. 1 Säkerhetsbehov och -insatser relaterade till olika krisskeden

1.4 IKT finns i alla system – grunden för säkerhetsagendan

Teknikanvändningen påverkar samhället och utvecklingen gör att nya tekniska säkerhetslösningar måste tas fram eller anpassas för att produkter och tjänster skall kunna användas tryggt. Dessutom kan existerande säkerhetstekniker behöva överges på grund av att ny kunskap tillkommer, eller att teknik blir allmänt tillgänglig, och därmed sätter existerande skyddsmekanismer ur spel. Det medför behov av ny kunskap, inte bara för att utveckla ny säkerhetsteknik utan också för att kunna anpassa existerande produkter så att de förblir säkra.

Vårt moderna informationssamhälle bygger på, och är i behov av, pålitlig och säker teknik. Kommunikationssystem baserade på informations- och kommunikationsteknik (IKT) kan i allt större utsträckning betraktas som kritisk infrastruktur, både i sig själva och som en del av andra system. Dagens IKT-system är helt enkelt en integrerad del av vår vardag, såväl i näringslivet som i myndigheter och bland medborgare. De utgör en grund för utveckling av nya tjänster och produkter, men utsätts också kontinuerligt för olika typer av attacker. Detta illustreras tydligt av konsekvenserna av brister och icke adekvat säkerhet, hackerattacker och cyberbrottslighet. I USA enbart beräknas att industrin 2008 kan ha förlorat upp till 1 billion US Dollar på grund av immateriell stöld och datastöld.[2] Man kan urskilja följande strukturer som driver behoven av utveckling inom IKT.

Teknik

- Strategier för att hantera *stora integrerade system* – utvecklingen går mot nya metoder för att hantera säkerhetsrisker vid användandet av stora integrerade system, eller vad som ofta refereras till som ”system av system”.
- Förbättrad *interoperabilitet* – är en förutsättning när vi integrerar system till större system. Samtidigt behöver vi kunna kombinera olika tekniska kompetenser och lösningar, som exempelvis röntgen och biometriska applikationer, för att samtidigt identifiera både varor och personer.
- Betoning på *mjukvara* – hantering och bearbetning av information, exempelvis ökningar av detaljgraden i information, olika typer av information, eller mängden information som finns tillgänglig för beslutsprocesser, blir allt viktigare. Som en följd blir mjukvaran, jämfört med hårdvara, allt viktigare i säkerhetsutrustning och system.

[2] http://www.dhs.gov/st-centers-excellence

- Ökad användning av *automatiserade system* – för vissa säkerhetslösningar vill man undvika utrustning och system som hanteras direkt av människor. Att ersätta mänskliga operatörer kan vara ett svar på krav på reducerade (arbets-) kostnader, men kan ibland också styras av att man vill undvika att personer blir sårbara om de kan identifieras.

Juridik

- *Reglering inom IKT* – insikten om den strategiska betydelsen av exempelvis kommunikationsinfrastruktur har både inom och utanför EU lett till ökade krav på övervakning och styrning av kommunikationsinfrastruktur. Regleringar påverkar samspelet mellan den enskilde och samhället, och användning och utveckling av teknik.
- *Privacy och integritet* – teknikutvecklingen leder till nya behov och krav som den enskilde ställer när det gäller privacy och den personliga integriteten, exempelvis skydd mot identitetsstölder och kommersialiserande av känslig och privat information.

Socialt

- *Oönskade bieffekter av säkerhetssystem* – många säkerhetssystem påverkar eller inkräktar på ”normala” aktiviteter i vardagen och kan även ge oönskade kostnader, exempelvis förseningar som skapats av säkerhetsrutiner, eller har konsekvenser för personligt beteende och friheter, exempelvis lämpligheten av kroppsscannrar. I detta avseende är frågan om allmänhetens syn på tekniken av stor betydelse, i synnerhet för att skapa en acceptabel balans mellan säkerhetsnivåer och de intrång som tekniken skapar i det offentliga och privata livet.

Just nu ökar kraven på säkerhet inom IKT-världen, både ur ett tekniskt, regulatoriskt och socialt perspektiv. Syftet är dels att skydda kritisk infrastruktur och kunna erbjuda tillförlitliga och robusta system, dels att användare ska kunna känna sig trygga att utnyttja de tjänster som erbjuds. Dessa aspekter sammantagna medför att säkerhet för IKT alltmer utvecklas som ett tvärvetenskapligt område.

För tillämpning av säkerhet på IKT-system krävs nya innovativa lösningar för att säkra produkter, plattformar och tjänster i utvecklingsprocessen och en ökad användning av metoder för försäkring (assurans) av tillförlitligheten i olika system. Även mjukvarusäkerhet och mekanismer för att stå emot olika cyberattacker måste beaktas som en integrerad del i utvecklingen av IKT-system. Utvecklingen inkluderar även legala och sociala aspekter.

De forskningsområden som har speciellt innovationsvärde för säkerhet och IKT är mjukvarusäkerhet och metoder för assurans, ”trusted computing”-baserade plattformar och ”management” av datamoln, kryptologi, nätverkssäkerhet och robusthet, privacy och åtkomstkontroll samt legala aspekter såsom personlig integritet, övervakning och legitimitet. Tillsammans med behov och drivkrafter för säkerhet är behov av forskning och innovation inom dessa områden grunden för agendan.

2 Säkerhetsindustrin är viktig för Sverige

2.1 Potential i flera avseenden

Sverige ligger långt framme, både inom övergripande säkerhetstänkande och inom forskning och framtagning av säkerhetslösningar av olika slag. Som vi har visat i det tidigare finns det starka skäl att fortsätta att utveckla svensk forskning och innovation inom området säkerhetsteknik. Dels för att stärka konkurrenskraften i de verksamheter som är beroende av säkra system, dels för att utveckla säkerhetsindustrin som sådan, och den exportpotential som den rymmer.

En vital säkerhetsforskning och säkerhetsindustri bidrar också till att göra Sverige attraktivt. En internationellt erkänd förmåga att hantera kriser är ett viktigt bidrag till att höja Sveriges anseende ytterligare på den internationella säkerhetsarenan, vilket samtidigt ökar Sveriges attraktivitet i nödvändiga internationella forskningssamarbeten.

2.2 Säkerhetsteknik – en vitt förgrenad industri

Det finns idag en omfattande svensk säkerhetsteknikindustri som adresserar den svenska och internationella säkerhetsmarknaden. Den förser produkter och tjänster generellt med säkerhetsfunktionalitet i syfte att höja deras kvalitet, eller för att säkerställa kundernas behov av säkerhet.

I arbetet med en National Research Agenda (NRA) för säkerhetsområdet 2009 definierades säkerhetsindustrin 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 organiserad brottslighet och krigshandlingar). I en studie, som Chalmers då genomförde som underlag för NRA-arbetet, bedömdes hur stor andel av svensk IT-industri som då adresserade säkerhetsmarknaden. Tillväxtpotentialen betraktades som stark i alla sektorerna, främst sensorteknologi, komplexa system och IT-säkerhet. Säkerhetssektorn som helhet i Sverige ansågs då omfatta 830 företag med 67 000 anställda. Samtidigt är säkerhetsindustrin, liksom säkerhetsmarknadens, storlek en definitionsfråga. Idag har denna sektor blivit större i Sverige och säkerhetsmarknaden i och utanför Sverige växer snabbt.

Utgångspunkten för vårt förslag till en forsknings- och innovationsagenda på säkerhetsområdet är att tillämpa en bred definition, och därmed adressera den potential som ligger i att fler företag får, och tar, möjligheten att uppmärksamma den stora säkerhetsmarknaden.

Följande är några exempel på framgångsrika företag som lyckats väl internationellt. De visar också på hur säkerhet kan vara en marknad som omfattar betydligt mer än krisberedskap.

• *Axis Communication* ökade antalet anställda till 679 personer (20 % ökning) mellan 2011 och 2012. Vinsten dubblades från 325 MSEK till över 650 MSEK.

• *Securitas* är ett av de två största vaktbolagen i världen, och ett av Sveriges största företag i antal anställda (272 425). Företaget har en omsättning på 64 miljarder och en vinst på 2,5 miljarder.

• *Assa Abloy* har 41 000 anställda, en omsättning på 42 miljarder och en vinst på 4,5 miljarder.

I en marknadsanalys[3] som gjorts parallellt med detta initiativ listas de 26 största företagen på den europeiska marknaden, deras huvudområden (t.ex. lås, kommunikation, IKT, mjukvaru-utveckling, identitetskort, CCTV, detektorer, konsulttjänster etc.), deras hemland, anställda och omsättning. I rapporten listas också de 45 ledande aktörerna i Sverige på samma sätt, med kort summering av deras huvudsakliga verksamhet.

2.3 Mycket stor, och växande, global marknad

2.3.1 Definition

Analyser av säkerhetsmarknaden använder ofta det engelska ordet *'security'*, som syftar på samhällssäkerhet och -skydd och krisberedskap. Det rör funktioner som är kritiska för att skydda samhällets trygghet och stabila funktion, ex.vis säkerhet för flygplatser, kärnkraft, polis, ambulans och brandkår, transportsystem och cyberverksamhet. I det fortsatta används begreppet *civil säkerhet*, eller bara säkerhet.

Eftersom det saknas en enhetlig definition av säkerhetsindustrin varierar marknadernas storlek beroende på hur de har avgränsats i olika analyser, ex.vis vilka delbranscher som inkluderas och om man räknar in både varor och tjänster. Produktionen av säkerhetsprodukter hamnar under en mängd olika kategorier, som inte skiljer på om verksamheten är kopplad till säkerhet eller ej. Det finns heller ingen statistisk datakälla på europeisk nivå som branschen själv tagit fram.[4]

2.3.2 Storlek

Inför arbetet med denna agenda har SCB, Exportrådet och företag själva fått uppskatta marknaden. Svaret är att marknaden är mycket svårdefinierad, men att utvecklingen är positiv och att det kan handla om en tillväxt lika med, över eller mycket över BNP-ökningen.[5]

Några talar om en total världsmarknad inom civil säkerhet om 71,5 miljarder USD (2011) med en årlig tillväxt på 7,5 %.[6] Andra beskriver en världsmarknad om 197,9 miljarder USD 2012 med 3,55 % tillväxt fram till 2022.[7] Skillnaderna i uppskattningen av marknadsstorlek kan räknas i mer än hundra miljarder dollar. Differensen är troligen en konsekvens av olika definitioner och avgränsningar av begreppet 'security'.

2.3.3 Dynamik

Den allmänna uppfattningen om faktiska eller sannolika säkerhetshot styr både den totala efterfrågan och betalningsviljan vad gäller säkerhetsteknik och -funktioner. Marknaden upp-

3 E. Olsson, P. Mattsson, M. Kastman Sjöstedt: Kartläggning av Security-branschen, Skill, 4 feb 2013

4 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:SV:PDF

5 E. Olsson, P. Mattsson, M. Kastman Sjöstedt: Kartläggning av Security-branschen, Skill, 4 feb 2013

6 EOS Security Market Evaluation March 2011 och Frost & Sullivan.

7 The Global Homeland Security Market 2012-2022, Marketresearch.com

visar i hög grad ett reaktivt mönster med en efterfrågan som ofta är ett svar på specifika händelser. Efterfrågan kan komma mycket snabbt efter en ny ”händelse”, men följs också ofta av en relativt snabb nedgång när det specifika hotet uppfattas som mindre. Detta mönster av ”reaktiv” efterfrågan är förutsägbart. Specifika ”händelser” är dock till sin natur i hög grad oförutsägbara, varför efterfrågan över tid är mycket svår att bedöma. En tydlig trend är dock att vi i framtiden inte har något normalläge i samhället. Kraven på snabb anpassningsförmåga är en central aspekt i både efterfrågan och utbud.

För den svenska civila säkerhetsindustrin är den avgörande förutsättningen för deltagande i teknik- och kunskapsutvecklingen att industrin har förmåga att utveckla och producera produkter och tjänster som motsvarar behoven på en global marknad. En stor del av den inhemska efterfrågan styrs av internationella regelverk som innebär att forskning och produkter i Sverige kan fungera även på exportmarknader.

Den globala marknaden för säkerhetsteknik har en potential vad gäller lönsamhet, men kräver stora resurser för implementering, vilket kan verka bromsande på marknadstillväxten. De höga initialkostnaderna har lett till att många länder väljer mer arbetsintensiva lösningar, eller väntar med att fatta beslut om investeringar.[8]

2.3.4 Geografi

Globalt

Den globala prognosen för statliga investeringar inom civil säkerhet är att de förväntas förbli prioriterade och starka, trots ekonomiskt svåra tider, även om vissa marknader planar ut medan andra ökar sina utgifter.[9] Civila marknader för den svenska säkerhetsindustrin återfinns framför allt i USA, som också är den största marknaden för säkerhetslösningar. Department of Health and Human Services, Department of Homeland Security, National Science Foundation, och inte minst jordbruks- resp. försvarsdepartementens egna säkerhetsforskningsprogram, är stora aktörer. Samtidigt är det svårt att etablera sig som en betydelsefull aktör på denna marknad. Amerikanska företag bedöms ha fördelar genom:

- att de är marknadsledande inom teknologisk utveckling
- att den amerikanska marknaden är en vital hemmamarknad som utgörs av ”en harmoniserad rättslig ram”
- ett väl erkänt amerikanskt varumärke

Under det kommande decenniet förväntas marknader i Kina, Indien, Förenade Arabemiraten och Saudiarabien växa fram starkt.[10] Inom ett par år väntas Kina överta platsen från USA som världens största marknad för ”homeland security och public safety”. Enligt en prognos kommer den kinesiska marknaden att uppnå 10 miljarder USD 2020 och redan idag lägger Kina större resurser på civil säkerhet än på försvaret. Det finns därmed starka incitament för utländska investeringar på den kinesiska marknaden.[11]

De största vinsterna förväntas stå att finna i tillväxtmarknader i delar av Asien, Östeuropa,

8 http://finance.yahoo.com/news/market-research-report-global-homeland-080800648.html

9 www.visiongain.com

10 The Global Homeland Security Market 2012-2022, Marketresearch.com

11 http://www.homelandsecurityresearch.com/2012/09/china-homeland-security-public-safety-market-2012-2020/

Afrika och Mellanöstern, där marknaden för civil säkerhet är underutvecklad.[12] Faktorer som driver denna tillväxt antas vara generellt starka ekonomiska miljöer, nya företagsformationer, utländska investeringar, ökad urbanisering, växande medel- och överklass samt upplevd ökad risk för kriminella aktiviteter.

Europa

Enbart inom EU sysselsätter säkerhetsmarknaden ca 180 000 personer (2011) och marknadsvärdet uppskattas till 26-36,5 miljarder euro. Många av EU:s tekniska säkerhetsföretag tillhör de främsta i världen inom säkerhetssektorn. Emellertid finns det prognoser, både oberoende och branschens egna, som visar att företagens andelar av världsmarknaden kan falla med en femtedel till 2020, från 25 % till 20 %, om inte åtgärder vidtas för att förbättra konkurrenskraften. De främsta utmaningarna är att:

- EU-företag ofta har högre produktionskostnader jämfört med konkurrenterna från andra delar av världen – därmed blir det allt viktigare med tekniska fördelar.
- asiatiska företag är på väg att hinna ikapp det tekniska försprång som EU-företag har
- EU saknar ett ”EU-varumärke”, vilket kan vara avgörande på de stora framväxande marknaderna i Asien, Sydamerika och Mellanöstern.
- produkter och teknik, snarare än tjänster, förväntas bli utsatta för global konkurrens eftersom dessa svarar för den största exportpotentialen.

Nuläget kännetecknas av följande[13]:

Marknadsfragmentering (uppdelning av nationella och regionala gränser)

- medlemsländer ger inte gärna upp sina ”nationella befogenheter”
- de facto 27 separata marknader, som i sin tur består av egna separata säkerhetsmarknader
- avsaknad av harmonisering, ex.vis i certifieringsförfaranden och standarder
- negativ inverkan på både utbudssidan (industrin) och efterfrågesidan (offentliga och privata köpare av säkerhetsteknik)
- stora hinder för marknadstillträde
- mycket stora eller möjliga hinder för att åstadkomma stordriftsfördelar
- brist på konkurrens mellan leverantörer, offentliga medel används inte optimalt

Marknadens institutionella karaktär

- stort avstånd mellan forskning och marknad
- stora svårigheter att bedöma om en ny teknik slutligen lanseras eller alls kommer ut på någon marknad
- risk att potentiellt lovande forskningskoncept inte vidareutvecklas och allmänheten går därmed miste om teknik som skulle förbättra deras säkerhet

Samhällsdimensionen

- säkerhetsteknik berör djupa frågor om integritet och respekt för det privata och är därför ett känsligt område

12 World Security Equipment: Industry Study with Forecasts for 2014 & 2019

13 E. Olsson, P. Mattsson, M. Kastman Sjöstedt: Kartläggning av Security-branschen, Skill, 4 feb 2013

- industrin riskerar att förlora investeringar i teknik som sedan allmänheten inte godtar
- uppköpare kan välja produkter som inte fyller säkerhetskraven lika bra, men som är mindre kontroversiella, i syfte att få allmänhetens acceptans

EU-kommissionen har tagit fram en handlingsplan för att öka konkurrenskraften för den egna säkerhetsindustrin.[14] En väl fungerande hemmamarknad är, enligt handlingsplanen, det bästa sättet att främja nödvändig konkurrens, innovation, harmonisering och ett ”EU-varumärke”. Man pekar på att en samarbetsvilja inom EU, såväl politisk som mellan marknadens aktörer, är nödvändig för att lyckas övervinna fragmentiseringen av EU:s säkerhetsmarknader. För att förbättra konkurrenskraften på tillväxtmarknader för europeiska företag inom säkerhetsindustrin finns följande övergripande strategier:

- öka konkurrens och innovation inom EU
- sänka produktionskostnader genom att utnyttja stordriftsfördelar
- underlätta för små och medelstora företag att komma in på framväxande marknader

Mer i detalj vill kommissionen påskynda standardiseringsarbetet och verka för ett harmoniserat certifieringssystem på EU-nivå. Ett EU-varumärke som liknar den märkning som används för produktsäkerhet har föreslagits. Andra utmaningar handlar om att utnyttja synergier mellan säkerhets- och försvarsteknik för att minska fragmentering och öka stordriftsfördelar.[32]

Kommissionen har även föreslagit kraftigt ökad forskning och innovation som ett sätt att förbättra EU:s konkurrenskraft och tillväxt. EU:s FoU-program Horizon 2020 är tänkt att löpa under perioden 2014 till 2020, med en föreslagen budget på omkring 80 Mdr euro.[33] Kommissionen föreslår vidare att särskilda regler kring immateriella rättigheter ska ge nationella myndigheter möjligheter att mer direkt och snabbt kunna utnyttja resultaten av sådan EU-forskning och på så sätt föra forskningen närmare marknaden. Ett ytterligare steg i den riktningen är att sammanföra industri, offentliga myndigheter och slutanvändare från början av ett forskningsprojekt som ett sätt att minska avståndet mellan forskning och marknad.

Sverige

Analyser visar att den inhemska svenska civila säkerhetsmarknaden är liten för alla sektorer, men att det finns en tillväxtpotential, speciellt genom ökat cyberhot och kritiskt beroende av IKT. Som påtalats tidigare är det svårt att avgränsa området till en specifik marknad eftersom marknaderna, både geografiskt och tekniskt, går in i varandra. Det är också svårt att avgöra hur mycket av produktion och export som kan hänföras till Sverige, främst beroende på att många stora aktörer har bolag i flera länder.

Det finns uppenbara gränssnitt mellan säkerhet och andra branscher och kontakten med SCB visar tydligt att det är svårt att identifiera specifika varor för att kunna mäta exporten inom civil säkerhet. Många företag exporterar produkter inom säkerhetsområdet men klassa i många fall inte som säkerhetsföretag då de har en annan huvudverksamhet. Civil säkerhet kan

14 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:SV:PDF

inte heller enkelt delas in i varugrupper då det inte finns specifika varukoder för varor och tjänster inom området.[15]

Exportrådet har gjort en grov skattning av hur mycket svenska företag exporterar just nu inom säkerhetsområdet och har kommit fram till ca 4-5 Mdr SEK årligen. Resultaten indikerar också en stark tillväxt. De grenar som är starka är IKT-system, cybersäkerhet, sensorteknologi och brandsäkerhet. Som ett exempel räknar Actea med 20 % ökning per år och sannolikheten för detta resultat bedöms till 75 %.[16] SAAB har minskat den totala omsättningen för hela företaget med 1 miljard samtidigt som omsättningen för civil säkerhet har ökat med 50 MSEK.[17] Securitas uppger att, om både bevakning och rena teknikföretag räknas in, så var omsättningen 143 Mdr SEK med en förväntad ökning om 2 % årligen. Eltel Networks uppskattar marknaden inom sin del av civil säkerhet till 0,5-1 Mdr SEK. Frost & Sullivan räknar med en ökning av efterfrågan i Norden med 6 % per år de kommande åren. I samtliga fall bygger siffrorna på hur marknaden definieras.[18]

2.3.5 Teknikområden

Tekniska lösningar som används i säkerhetsprodukter tenderar att ha en rad olika användningsområden, för andra syften och i andra sektorer. Av den anledningen är säkerhetsföretag ofta aktiva på flera marknader, exempelvis inom försvar, industriell automatisering och informations- och kommunikationsteknik för att nämna några. Det innebär också att, om man breddar perspektivet till exempelvis cybersäkerhet i vid mening, så är världsmarknaden än större. Här, liksom med många IKT-produkter, används säkerhet i produkter som själva inte klassas som säkerhetsprodukter. Det gör att statistiskt material inte fullt ut karaktäriserar hela potentialen av den marknad som adresseras. Nedan ges några exempel på hur marknaden utvecklas för de teknikområden som prioriteras i denna agenda.

Cybersäkerhet

Marknaden för cybersäkerhet har vuxit kraftigt det senaste decenniet och förväntas fortsätta att växa. Statliga och militära utgifter inom cybersäkerhet beräknades globalt till 8,12 Mdr USD år 2009. En rad attacker på senare år har lett till ökat fokus på marknaden. Visiongain bedömer att USA är den klart viktigaste nationella marknaden för cybersäkerhet. I mindre utvecklade länder är däremot viljan att investera i cybersäkerhet måttlig. Dessutom sker utvecklingen av produkter inom cybersäkerhet så snabbt att vissa länder väntar med att införskaffa dem tills de anses vara mogna nog för användning.[19] En marknadsrapport (2011 av HIS Jane's) om forskning och utveckling inom cyberverksamhet uppskattar den årliga tillväxttakten till över 10 % för tidsperioden 2011-2020. Rapporten antyder även att tillväxttakten för cybermarknaden som helhet mycket väl kan bli högre än så.

---

15 Infrastat helpdesk på SCB

16 http://www.allabolag.se/5565925053/Actea_Consulting_AB

17 http://www.saabgroup.com/Global/Documents%20and%20Images/About%20Saab/Investor%20relations/Financial%20reports/Saab%20AB%20year-end%20report_2011.pdf

18 E. Olsson, P. Mattsson, M. Kastman Sjöstedt: Kartläggning av Security-branschen, Skill, 4 feb 2013

19 www.visiongain.com. Cyberwarfare Market 2010-2020. "4. Leading National Cyberwarfare Markets"

Sensorer

Tillväxten för den globala sensormarknaden förväntas vara stark. BBC Market uppskattar omsättningen år 2016 till 91,5 Mdr USD, med en årlig tillväxttakt på 7,8 %.[20] Hur stor andel som gäller säkerhetsprodukter anges inte, men flera källor ger vid handen att rörelsesensorer och bildsensorer förväntas ha en särskilt stark tillväxt med en årlig takt på 20,3 % resp. 10,2 %. Marknaden räknas i båda fallen i flera tiotals miljarder USD.

Kommunikation och interoperabilitet

Marknaden för kommunikation och interoperabilitet har kallats för en av de snabbast växande sektorerna inom civil säkerhet. Enbart för marknaderna i Europa och USA tillsammans beräknades det totala värdet för tidsperioden 2008-2012 till 72,3 Mdr USD och den genomsnittliga tillväxttakten till 18,6 % per år.[21]

[20] http://www.bccresearch.com/report/sensors-technologies-markets-ias006d.html

[21] Enligt en prognos av Homeland Security Research publicerad 200. De senaste prognoserna är inte kostnadsfria.

3 En smartare användning av befintliga värden

3.1 Nationella satsningar förutsätter och möjliggör internationellt samarbete

När det gäller civil säkerhet har ett flertal utredningar och rapporter (ESRIF, ESRAB ECORYS m.fl.) visat att samhället är i stort behov av ny kunskap och teknik för att skydda samhällets trygghet och stabila funktion. En god beredskap minskar samhällets totala kostnader för kriser. En del av denna beredskap kan vi hantera genom att ta till oss lösningar utifrån, men vi behöver också nationella satsningar för att utveckla teknik och kunskap som är anpassad till våra egna beredskapsbehov. För att dessa nationella satsningar skall bli framgångsrika krävs att vi deltar i internationellt samarbete, samtidigt som satsningarna är vår inträdesbiljett till sådana samarbeten.

De industriella förmågor som Sverige under en lång följd av år har utvecklat inom området civil säkerhet är den bas från vilken en fortsatt utveckling bör ske. Till dessa förmågor ska läggas utveckling av områden och kunskaper som har strategisk betydelse som komplement för att kunna genomföra de satsningar som presenteras här.

3.2 Utnyttja befintliga styrkor genom att bredda tillämpningen

Denna agenda har sitt ursprung i den nationella forsknings- och innovationsagendan (NRIA Säkerhet) som lanserades i november 2011 på initiativ av Säkerhets- och försvarsföretagen (SOFF). NRIA Säkerhet lämnade förslag på hur vi i Sverige kan stärka både svenskt säkerhetsarbete och förmågan hos svensk säkerhetsteknisk industri att konkurrera globalt genom att vidareutveckla vårt industriella kunnande inom säkerhetsteknikområdet. Rekommendationerna formulerades i en bred uppslutning av representanter från säkerhetsområdets företag, universitet, forskningsinstitut, myndigheter och organisationer.

Aktörerna vill nu bredda NRIA Säkerhet, framförallt på IKT-sidan och inom området cybersäkerhet. Skälet är att det finns många produkter och tjänster som inte karaktäriseras som en säkerhetsprodukt i sig, men där säkerheten är en viktig komponent, exempelvis 4G mobilsystemet eller patientjournalsystem. Det innebär att tillämpningsområdena för säkerhetsteknik är väsentligt större än rena säkerhetsprodukter. Breddningen innebär också att sociala och legala ramverk beaktas som en del i teknikutvecklingen, då dessa ramverk i hög grad berör och påverkar marknadsförutsättningarna för säkerhetsteknik.

Denna forsknings- och innovationsagenda kompletterar därför NRIA Säkerhet med en konkretisering av de fyra prioriterade forskningsområdena, och ger även konkreta förslag för hur kunskapsutvecklingen kan koordineras och nyttiggöras effektivare.

3.3 Innovationsmiljöns position

Säkerhetsområdet är ett breddområde för forskning och industriell verksamhet. Det spänner från verksamhet inom civil och nationell säkerhet till verksamhet knuten till IKT-produkter eller IKT-baserade tjänster och även sociala nätverk. Flera av de svenska industriella styrkeområdena ligger centralt inom säkerhetsområdet. Ett strategiskt innovationsområde för säker-

het kan positionera Sverige i de framväxande europeiska och amerikanska säkerhetsforskningsprogrammen. Och därmed bidra till både den gemensamma säkerheten och till innovation, konkurrenskraft och tillväxt på en snabbt växande, global marknad.

3.3.1 Fokus på fyra styrkeområden

Det finns flera svenska styrkeområden, som ligger långt framme internationellt, och som kan bidra till tekniska lösningar för att undvika, eller hantera, sådana kriser som nämndes inledningsvis. Den svenska IKT-verksamheten karaktäriseras som mycket stark, vilket skapar bra förutsättningar för att kunna förse IKT-produkter med säkerhetslösningar.

Exemplen nedan representerar de fyra styrkeområden som vi vill fokusera vår agenda på, med några exempel på hur tekniska lösningar skulle kunna ha mildrat eller förhindrat konsekvenserna av de svenska händelser som beskrevs tidigare

- *Sensorteknologi* – kemiska sensorer (elektroniska ”näsor” och ”tungor”) finns idag för att detektera en rad olika föroreningar i dricksvatten och bakterier i mat. En sådan sensor i färskvattenledningarna kan ge varningar innan bakterierna når ut till konsumenterna.

- *Kommunikationsteknologi* – robust kommunikation gör det svårare eller omöjligt att störa ut polisradion, vilket var en av huvudorsakerna till att kravallerna i Göteborg fick en sådan omfattning. Vidare kan ett robust mobilnät bättre klara stormar, översvämningar och kyla, och bidra till mer tillförlitlig tågtrafik.

- *Interoperabilitet* – svensk industri är mycket duktig på att bygga system av system där avancerade ledningssystem är en stor exportprodukt. Det finns dock fortfarande många områden där det saknas inhemska produkter.

- *Cybersecurity* – cybersäkerhetsforskningen ligger långt framme i Sverige, och det finns förutsättningar att förhindra hackerattacker och virus i central infrastruktur.

Det är av stor vikt att vi inom dessa områden kan bidra till att de starkaste forskargrupperna och aktörerna får möjlighet att *lägga större fokus på säkerhetstillämpningar* än vad som är fallet idag. Det menar vi är det centrala i att använda befintliga värden smartare. Vid sidan av de områden som här föreslås finns en rad andra där svenska företag kan ha starka intressen. Vår bedömning är emellertid att Sverige inte kan, eller bör, sprida ut de begränsade resurser som finns att tillgå, på alltför många områden. En utgångspunkt för de medverkande aktörerna har varit att det krävs en koncentration kring ett fåtal särskilt angelägna områden för statens och industrins gemensamma satsningar.

3.3.2 Breda aktörer

Sverige har en relativt god spridning geografiskt och ämnesmässigt av forsknings- och innovationsmiljöer som svarar mot olika behov. En prioritering av forsknings- och innovationsområden och en koordinering av olika aktörers insatser (forskare, företag, myndigheter) blir ett viktigt sätt att utnyttja tillgängliga resurser och uppbyggda värden på ett smartare sätt.

Det finns breda branschorganisationer och institut som stöttar utvecklingen. Starka aktörer är:

- SOFF (Säkerhets- och försvarsföretagen) med 63 medlemsföretag
- SACS (Swedish Association of Civil Security) med 19 medlemmar
- Swesec och Swelarm
- Forskningsinstituten i Swedish-ICT har Security som ett verksamhetsområde, med fokus på sensorer och IT-säkerhet.
- SP Sveriges Tekniska Forskningsinstitut.

Det finns också ett tiotal centrumbildningar inom säkerhetsområdet, från norr till söder.

- Kriskompetenscenter KKC (Luleå tekniska universitet)
- Center for CBRNE[22] (Umeå universitet)
- Crisis Research Center CRC (Mittuniversitetet)
- Center for Natural Disaster Science CNDS (Uppsala universitet)
- CRISSMART (Försvarshögskolan)
- Security Link (Linköpings universitet)
- URBSEC (Göteborgs universitet, Chalmers)
- Security Arena (Lindholmen Science Park)
- Baltic Maritime Science Park (Blekinge Tekniska Högskola)
- LUCRAM (Lunds universitet)

Dessa centrumbildningar har till största delen olika inriktningar och icke-överlappande agendor. Inom området tekniska säkerhetslösningar är Security Link och Security Arena centrala, med ungefär samma verksamhetsområden, men med fokus på olika ’technology readiness levels’ (TRL).

På ett antal lärosäten finns också betydande undervisningsverksamhet knuten till säkerhet i form av program, kurskedjor och skolor där säkerhetsaspekter är en viktig ingrediens.

3.3.3 Internationell position

Svensk industri, med komplexa systemlösningar uppbackade av en väl utvecklad infrastruktur, är väl positionerad på den internationella arenan. Sverige ligger också relativt sett långt framme internationellt i termer av starka forskningsmiljöer.

Modern säkerhetsteknik bygger till stor del på landvinningar inom IKT-området och Sverige är internationellt ledande inom detta område. En indikator på detta är resultatet av den internationella utvärderingen som gjordes inför regeringens satsning på strategiska forskningsområden (SFO). Av de 20 forskningsområden som definierades var IKT ett. Inom detta område fick tre miljöer (Stockholm, Linköping/Lund och Göteborg) högsta betyg, d.v.s ”världsledande miljö”. De flesta av de övriga områdena hade inga ansökningar som fick detta betyg.

Sverige har vidare varit framgångsrikt i ansökningarna till European Security Research Programme och inom program som Security in Energy and Transport och ICT for Trust and Security.

[22] Chemical (C), biological (B), radioactive (R), nuclear (N) and explosive (E) materials

3.4 Samverkan

3.4.1 En lång process av nära, strategiskt samarbete

Föreliggande agenda är resultatet av en lång process, från NRA 2009, via NRIA 2011. De svenska aktörerna har nu noga analyserat och värderat förutsättningar och möjligheter kring ett begränsat antal prioriterade satsningar inom säkerhetsteknikområdet. Genom samverkan mellan företag, myndigheter och akademi kring dessa satsningar kan industriella lösningar tas fram med utgångspunkt i både nationellt definierade behov och en efterfrågan från den globala marknaden. Erfarenheten av sådana nära samarbeten pekar entydigt på fördelar för både samhälle och industri, såväl i form av lägre utvecklingskostnader och en bättre anpassning till marknadens behov.

3.4.2 Tradition av samverkan i innovationssystem

Det finns också en lång tradition av samverkan mellan aktörerna i innovationssystemets olika funktioner. I Sverige utgår Myndigheten för samhällsskydd och beredskap (MSB) från sex kunskaps-/teknikområden:

- Teknisk infrastruktur
- Transporter
- Farliga ämnen
- Ekonomisk säkerhet
- Skydd, undsättning och vård

Inom varje område är innovationssystemet funktioner tydliga: forskning och utveckling, policyinsatser, utbildning, upphandling etc, som syftar till att ge olika aktörer, privata och offentliga, förutsättningar att svara mot samhällets behov och efterfrågan vad gäller säkerhet.

Vidare visar portföljanalyser av säkerhetsforskning att universitet och högskolor och institut visserligen dominerar bland de sökande av medel till säkerhetsforskning, men att företag deltar i majoriteten av projekt och med relativt god spridning mellan de olika sektorerna i säkerhetsindustrin. En majoritet av svenska universitet, högskolor och institut är involverade i projekten, med FOI som dominerande part, och antalet företag som deltar i olika projekt kan räknas i flera hundra.

3.5 Funktionsanalys

För att kunna formulera lämpliga mål och identifiera rätt insatser för att stärka det svenska innovationssystemet på säkerhetsområdet har vi också gjort en avgränsad funktionsanalys. Syftet med en sådan analys är att analysera innovationssystemets styrkor och svagheter, och vilka eventuella blockeringar som hindrar en god funktionalitet.

Vi har konstaterat att delar av innovationssystemet behöver förstärkas och är särskilt angeläget vad gäller funktionerna Marknad, Kompetens, Innovationsverktyg och FoI-miljöer. Analysen presenteras i förenklad form i tabell 1 nedan, och mynnar ut i ett antal insatser och mål (se kap. 5), som vi bedömer krävs för att stärka innovationssystemet som helhet.

Innovation handlar per definition om något som har nått och utnyttjats av marknaden, varför vi har sett det som särskilt angeläget att granska marknadsförutsättningarna. Vi refererar också till Bergek, Jacobsson m.fl. (2008), som i sin artikel om innovationssystemens funktionella dynamik diskuterar hur framväxande innovationssystem ibland kan lida av underutvecklade marknader. I artikeln studerar de det svenska innovationssystemet kring mobil data, och konstaterar bl.a. att den inhemska marknaden har en viktig roll att spela i innovationssystemets utveckling. På grund av flera faktorer, bl.a. bristande standardisering och stor osäkerhet kring nuvarande och framtida efterfrågan har utvecklingen hindrats.

Generellt menar de att det är centralt för ett innovationssystems utveckling att identifiera vilken mognadsfas marknaden befinner sig i, om det finns institutionella incitament för marknadsutveckling eller om sådana måste tillkomma, samt vilka köparna är tänkta att vara och hur deras inköpsprocesser ser ut. Utifrån denna kunskap kan sedan rätt mål och rätt insatser utformas.

3.6 Funktionsanalys i praktiken – två exempel

3.6.1 Kameraövervakning

Kameraövervakning är ett mycket effektivt sätt att minska olika risker i samhället. Första generationens övervakningssystem hade en monitor till varje kamera och en videokabel som förbindelse. Företaget Axis insåg tidigt fördelen med IP och TCP-kablar, och vilken flexibilitet och effektivitet det medförde för operatörerna. Axis blev snabbt marknadsledare, men de agerar ensamma på den internationella marknaden från ett svenskt perspektiv på näringskedjan.

Vad blir nästa stora steg i utvecklingen? Tekniskt kan man göra kamerorna trådlösa med robust och säker kommunikation. Man kan integrera informationen i större system (interoperabilitet). Men för att öppna en större marknad så måste man komma åt marknadsblockeringar. Dessa består främst av följande:

1. Regulatoriska begränsningar
2. Acceptans hos allmänhet och politiska beslutsfattare kopplat till personlig integritet

Vad kan göras? Konkreta exempel på åtgärder kan inspireras av jämförelse med andra exempel, t.ex. genom att jämföra med de åtgärder som vidtogs med de ”nakenkameror” som infördes vid säkerhetskontroller för några år sedan. Två insatser löste upp integritetsproblemen kring första generationens system:

- Teknik: Man avbildade detektionerna av främmande föremål på en generisk, avpersonifierad kropp.
- Psykologi: Man placerade monitorn fullt synlig för alla passagerare för att undvika [misstanke om] missbruk.

Tabell 1. Avgränsad funktionsanalys av innovationssystemet Säkerhet

Värdering (+/-)	Blockering	Insats
MARKNAD		
+ Nya lösningar kan snabbt skapa efterfrågan (t.ex. vattensensorer) + Sverige bra anseende internationellt + Stora, internationella företag - ”Tryggt samhälle” Låg riskupplevelse i Sverige - Reaktiv marknad. Tillfällig och situationsbetingad efterfrågan	Exportrestriktioner till vissa länder Brist på klustring Nationella certifieringskrav Integritet (övervakningslösningar betraktas ofta som ett hot)	Koordinering/ klustring
KOMPETENS		
+ Väldigt bra IKT-utbildningar + Utlysningar på nationell och EU-nivå (incitament till utveckling) - Svag koppling till Security	Brist på samordning mellan IKT och Security	Koordinering av kompetensområ-den/utbildningar
INNOVATIONSVERKTYG		
+ Starka inkubatorer och innovationsmiljöer + Tävlingsarenor (cybersecurity) - Saknas testbäddar (ex.vis övervakning) - Brist på såddfinansiering	Smala akademiska meriterings-incitament	Affärscoacher Open innovation Etablera testbädd
FoI-MILJÖER		
+ Mycket starka, världsledande IKT-miljöer + Forskarskola i security med tvärprofil + Revinge ”Katastrofstaden” + Institut med inriktning mot Security +/- Många (okoordinerade) centrumbildningar, - Ingen koppling till Security i Univ-miljöerna	Brist på mötesplatser	Koordinering Systemtänk Securitykonferens

Vad kan man göra inom området kameraövervakning? I princip liknande insatser som i det ovan nämnda exemplet:

1. Man kan avidentifiera individen på olika sätt. Ansikten kan bytas ut mot generiska accepterade konturer. Man kan presentera information på ännu högre nivå som objekt som representerar individer och grupper.
2. Man kan göra informationen allmänt tillgänglig, tex. på Internet.

Sverige skulle kunna vara ett föregångsland genom en översyn av lagstiftning och regler, och genom samarbete inom hela området.

3.6.2 Vattenrening

Sverige har världsledande tekniska lösningar för att detektera föroreningar i kritiska tillflöden. Det finns också en ledande svensk leverantör av vattenrening, Envac AB.

Men marknaden är inte färdigutvecklad utan rymmer många fler möjligheter. Sverige skulle genom exempelvis regleringar kunna sätta en ny standard genom att kräva att all vattenförsörjning övervakas med tillförlitliga och effektiva sensorer och instrument.

Sverige har kompetens för att ta fram en sådan helhetslösning i form av:

- detektorer och sensorer,
- robusta trådlös kommunikation av data,
- integration av information i större ledningssystem,
- cyber-security i alla led.

Finansiering av demonstratorer och testmiljöer efterföljt av rekommendationer och lagstiftningar skulle kunna vara insatser för att skapa en marknad som löser ett befintligt problem från konkreta hot.

4 Vad vill vi uppnå?

Att Sverige ska vara med och utveckla egen teknik och kunskap betonades av Regeringen i propositionen 2008/09:50 *Ett lyft för forskning och innovation*. Där står att: ”… en teknisk och operativ förmåga att värna samhällets säkerhet förutsätter en avancerad kunskaps- och teknikutveckling på säkerhetsområdet. Detta behov kan mötas genom satsningar på utveckling av teknik inom sådana fält som ledningssystem, inklusive varningssystem, insamling av information, kommunikation och beslutsstöd, liksom inom simulering, informationssäkerhet och sensorteknologi.”

4.1 Fokus och spets för en kraftfull säkerhetsindustri

Våra fyra föreslagna prioriterade forsknings- och innovationsområden utgör snittet mellan Sveriges industriella förmågor och de samhälls- och marknadsbehov vi kan identifiera, särskilt inom de branscher som adresserades i kap. 1.2. På dessa fyra områden ser vi goda möjligheter till innovation och potential för svensk industri att på kort och lång sikt kunna tillfredsställa samhällets behov och skapa konkurrenskraftiga produkter och tjänster för den globala marknaden. Det är följaktligen dessa områden som vi menar att Sverige bör prioritera i för staten och industrin gemensamma satsningar. Områdena beskrivs mer i detalj i bilaga 6.

Sensorteknologi

Teknik för att kunna registrera händelser med hjälp av exempelvis sensorer för farliga ämnen (CBRNE), optoelektroniska sensorer och radarsensorer. Fokus ligger på:

- Nya sensorteknologier
- Sensor- och informationsfusion
- Klassificering och anomalidetektion
- Bildbehandling
- Visualisering

Kommunikationsteknologi

Det moderna samhället är beroende av infrastruktur för kommunikation, och i synnerhet trådlös kommunikation. Trådlös kommunikation är också en förutsättning, och i många tillämpningar den enda möjliga tekniska lösningen, för krishantering och infrastrukturskydd. Till exempel möjliggör trådlösa anslutningar mobilitet och flexibilitet för personal och system på samma gång som det eliminerar behovet av förinstallerad infrastruktur. Fokus ligger på:

- Robust trådlös kommunikation
- Tekniker mot illegal störsändning
- Tekniker för ökad kapacitet och interoperabilitet
- Sensornätverk

Interoperabilitet

De flesta tekniska system är idag informationssystem. Kraven på flexibel integrering av informationssystem ökar ständigt. Den som inte har en klar strategi för systemintegration riskerar att system blir oanvändbara i framtida verksamhetskritiska samarbeten, eller får leva med mycket stora integrationskostnader under hela systemens livscykel. Felaktigt genomförda integrationer, som kopplar ihop system tekniskt men misslyckas med att kommunicera praktiskt användbar information, kan i värsta fall orsaka farliga och dyra missförstånd under kritiska operationer. Fokus ligger på:

- Sömlöst informationsutbyte mellan system
- Informationshantering
- Teknik för samhällsviktiga funktioner och för samverkan

Cybersecurity

Med det närmast universella genomslag som kommunikationsteknologi, både fast och trådlös, haft på senare år, har kraven på mjukvarukvalitet och säkerhet i hemelektronik och inbyggd utrustning ökat. Nya användningsområden, som molntjänster, RFID-teknologi och sensornätverk ställer krav på dedikerade algoritmer anpassade för den specifika tillämpningen. Vidare är sekretess och skydd av personuppgifter mot missbruk centrala för att användare ska kunna känna sig trygga att använda IKT-baserade produkter och tjänster. Samtidigt leder exempelvis hacktivism till att regeringar och regulatorer ökar kraven på övervakningen av IKT-infrastruktur, vilket kan påverka den personliga integriteten. Fokus ligger på:

- Mjukvarusäkerhet och metoder för ”trust assurance”
- ”Trusted computing” plattformar och kontroll av datormoln
- Kryptologi
- Nätverkssäkerhet och robusthet
- Sekretess och åtkomstkontroll
- Rättsliga aspekter: spelregler, personlig integritet och legitimitet

4.2 Vision och gemensamma mål

4.2.1 Vision

Svensk säkerhetsforskning och -industri år 2020:

- ger väsentliga bidrag till ökad säkerhet i Sverige och omvärlden och bidrar till att de länder där beställarna finns rankas högt vad gäller säkerhet och trygghet.
- har hög status i internationella nätverk.
- har ett globalt högt renommé som kombinatörer av IKT och säkerhet inom fyra områden: sensorteknologi, kommunikationsteknologi, interoperabilitet och cybersäkerhet.
- bidrar till hållbar tillväxt genom fler företag och en ökad andel av världsmarknaden inom området säkerhetsteknik.

4.2.2 Insatser och mål för innovationssystemets funktioner

Marknad

Insatser kan vara att definiera branscher och marknader för att mer specifikt kunna analysera var Sverige står idag på olika marknader (Europa, USA, Asien m.fl.), dels inom de fyra fokusområdena, dels i förmågan att skapa säkerhet i ”system av system”. Undersökningar kan också inkludera hur nyckelaktörer ser på den svenska värdekedjan och hur högt de värderar den. En förnyad undersökning kan göras efter några år för att se om värderingen har förändrats. Behovet är också stort att utveckla kluster som kan representera hela kedjan av säkerhet för ”system av system” och som kan möta behov och efterfrågan med den kapacitet och paketering av produkter/tjänster, som den starkt ökande och alltmer komplexa marknaden kommer att kräva.

Målet är att bättre kunna matcha svenskt kunnande med specifika marknaders behov och efterfrågan och öka Sveriges omsättning och andelar på växande marknader. Svenska företag konkurrerar framgångsrikt på särskilt utvalda marknader och vinner en ökande andel av öppna anbudsförfaranden. Svenska produkter och tjänster har bidragit till ökad säkerhet och krishanteringsförmåga i Sverige, vilket har vunnit internationell ryktbarhet, och ingår också ofta i större internationella säkerhetslösningar.

Kompetens

Insatser kan vara att arbeta för en koordinering av kompetensområden/utbildningar inom IKT resp. säkerhet. Insatsen ligger i linje med agendans kärnfråga: att bredda säkerhetsområdet från ren säkerhetsteknik till IKT, och vice versa, då en breddning dels ökar marknadens storlek, dels drar nytta av Sveriges starka renommé på IKT-området. Koordineringen ska fokusera på de fyra områden som agendan har pekat ut: sensorteknologi, kommunikationsteknologi, interoperabilitet och cybersäkerhet och särskilt bereda förståelse och kompetens vad gäller ”system av system”.

Målet är att få en god tillströmning till de utbildningar som formas i linje med agendan, liksom adekvata karriärvägar och en god kompetensförsörjning i stora företag, SME och myndigheter.

Innovationsverktyg

Insatser kan vara att identifiera lämpliga affärscoacher med förståelse för säkerhetsområdet och dess marknader och främja organisering och finansiering av sådan kompetens på strategiska platser i innovationssystemet, exempelvis med lämplig geografisk spridning i befintliga FoI-miljöer, eller i en klusterorganisation för säkerhetsområdet. Särskilt som säkerhetsområdet som innovationssystem ännu inte har kommit in i en mognadsfas kan det också finnas skäl att arrangera arenor för open innovation och andra typer av möten mellan forskare, kunder, entreprenörer och finansiärer. Även testbäddar/demonstratorer kan behövas för att testa och illustrera komplexitet och integritet när det gäller säkerhet i ”system av system”, liksom nationell upphandling, exempelvis i form av innovationsupphandling inom de sex kunskaps-/teknikområden som ingår i svenskt samhällsskydd och beredskap: Teknisk infrastruktur, Transporter, Farliga ämnen, Ekonomisk säkerhet, Skydd, Undsättning och vård. Syftet är att legitimera produkter och tjänster och underlätta för kunder globalt att investera i svenska säkerhetslösningar.

Målet är att få ett ökat intresse för möjligheterna på marknaden för säkerhet så att nya företag, patent, produkter och tjänster utvecklas och att ett större riskkapital attraheras av den svenska innovationsmiljön. Fler svenska företag utvecklar innovationer inom säkerhetsområdet och den svenska portföljen innehåller flera produkter och tjänster med världsrykte. Sverige leder, genom egna initiativ, standardiseringen inom flera strategiska områden.

FoI-miljöer

Liksom för funktionen Kompetens handlar behovet här om insatser för en koordinering av FoI-miljöer inom IKT resp. säkerhet i syfte att bredda tillämpningen av kunskapen och därmed bättre svara mot behoven, och främja efterfrågan på kunnande. Koordineringen ska fokusera på de fyra områden som agendan har pekat ut: sensorteknologi, kommunikationsteknologi, interoperabilitet och cybersäkerhet, och särskilt visa på hur ”system av system” kan utvecklas och hanteras. En konkret insats är också att skapa internationella mötesplatser/konferenser för Security.

Målet är att öka den internationella synligheten och attraktiviteten för svensk FoI inom säkerhetsområdet och främja tillströmningen av kapital och talang till de svenska FoI-miljöerna. De mötesplatser/konferenser som skapas ska vara av hög status. Svenska företag, institut och universitet och högskolor har tagit en ledande position inom strategiskt viktiga områden inom EU:s och USA:s säkerhetsforskningsprogram, bl.a genom fler beviljade gemensamma ansökningar. Tidigare och nya FoU-investeringar har utnyttjats på ett effektivt sätt. Sverige får uppdraget att forma en KIC inom säkerhetsområdet. Fler ansökningar har lämnats in och fler ansökningar har beviljats inom de styrkeområden som är mindre mogna och som därför kräver mer grundläggande forskning. Antalet citeringar ökar i särskilt utvalda internationella publikationer.

5 Innovationsprogram för säkerhetsområdet

Som vår genomgång visat är behoven av nya lösningar och produkter inom säkerhetsområdet stora. Ny teknologi är av avgörande betydelse för att svensk industri skall kunna hävda sig i den internationella konkurrensen. Men mycket av behoven handlar också om att omvandla existerande teknologier och/eller att anpassa dem. Sverige genomför forskning av hög internationell klass inom flertalet av de områden som är vitala för säkerhetsindustrin men har svårigheter (i likhet med flera andra teknikområden) med att överbrygga gapet mellan grundforskning och produktutveckling. Ett annat problem är att slutanvändarnas verkliga behov inte ger tillräckligt avtryck i prioriteringarna av forskningsresurser. Det är dessa två problem vi vill adressera med ett nytt innovationsprogram för säkerhetsområdet. Den generella modell vi ser framför oss för att förändra svenskt innovationsklimat inom säkerhetsområdet är illustrerad i Figur 3 nedan med breda ingångar där centrala aktörer inom området kan ta ansvar för olika TRL-nivåer (’technology readiness levels’).

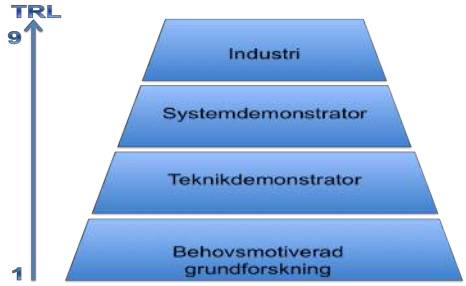


Fig. 3 Modell för att organisera forskning och innovation inom säkerhetsområdet

Om resurser och projekt allokeras enligt denna modell säkerställs det att det finns bryggor mellan de olika TRL-nivåerna och de olika aktörerna så som universitet, forskningsinstitut, etablerad industri samt små och medelstora företag har möjlighet att gå in på den nivå där de har mest att tillföra och störst kompetens. Modellen kräver att varje aktör är aktiva inom minst två nivåer för att säkerställa kunskapsöverföring och nyttiggörande av forskningsresultat.

5.1 Fokusområden och aktiviteter

Det övergripande målet om ökad innovationstakt och utveckling av säkerhetsteknologier är svårt att nå utan gemensam nationell kraftsamling och ett ökat samarbete mellan forskningsutövare, säkerhetsindustri och dess slutanvändare. Vad som behövs i praktiken är ett antal satsningar på *flera* olika TRL-nivåer. Vidare behövs också djupare förståelse av behoven och inte minst analys av affärsmodeller och praxis inom säkerhetsområdet. Detta för att kunna göra rätt avgränsningar och prioriteringar i satsningarna. Sammantaget föreslår vi ett nytt innovationsprogram med fyra olika typer av aktiviteter:

- Affärs och behovsanalyser
- Innovationsdriven forskning och utveckling
- Utveckling av testpiloter och demonstratorer

- Strategisk forskning

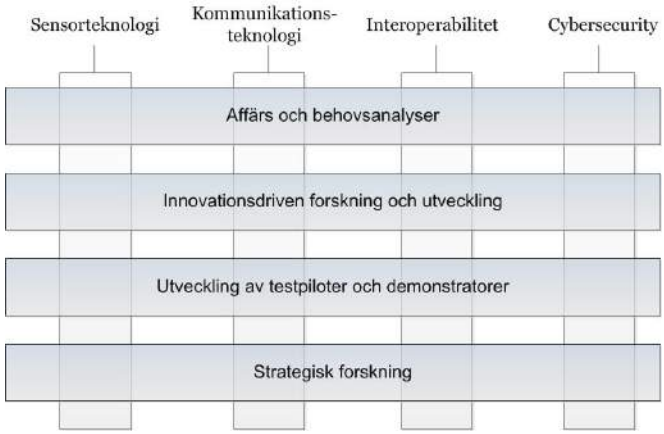


Fig. 4 Aktiviteter och deras relation till de identifierade fokusområdena.

Dessa fyra olika typer av aktiviter är oberoende av de strategiska fokusområden vi identifierat och är tillämpbara på samtliga områden vilket illustreras i figur 4. Utöver dessa så har vi i Sverige en lång erfarenhet av att arbeta med utveckling av standarder och certifiering, såväl för produkter som tjänster, personer och ledningssystem. Genom att arbeta med utveckling av kravställning både på produkter och system i sig (genom standarder och upphandling) parallellt med kravställning på implementering och hantering av system (genom krav på personer och ledningssystem) erhålls en god effekt av satsningar på innovationer. Certifiering är ett sätt att precisera och säkerställa krav- och kvalitetsnivåer, men principen för att introducera och kvalitetsäkra nya lösningar på en marknad är densamma även utan den formella hanteringen av certifikat.

5.2 Organisation

Vi föreslår att en ny organisation för att styra och stödja svensk innovation inom säkerhetsområdet inrättas. Vi ser två faser för denna, en initial första fas under 2013 där en interim-organisation sätts upp och en senare fas (2014 och framåt inom ramen för en SIO) där en permanent organisation finns på plats. I den initiala fasen bildar vi en interimsstyrelse som fungerar som arbetsgrupp för att ta fram ett fullständigt innovationsprogram för säkerhetsområdet baserat på denna agenda. Målet är att ombilda denna temporära organisation i nästa fas till en mer permanent organisation med en styrelse som fungerar som katalysator för att ta fram skarpa innovationsprojekt.

Styrelsen i interim-organisationen föreslås bestå av representanter från ledande organisationer inom området och från arbetet med innovationsagendorna, exempelvis Saab, Ericsson, Axis Communications, Securitas, Assa Abloy, SOFF, Swedish ICT, FOI (interim ordförande), Linköpings universitet/Security Link, Chalmers/Security Arena, Lunds universitet.

Det första uppdraget för denna styrelse blir att ta fram en SIO-ansökan för säkerhetsområdet. Målsättningen är att i ett senare skede omvandla denna interim-styrelse till permanent styrelse för programmet med en av industrirepresentant som ordförande.

Styrelsen ska också agera som ett nationellt råd för att skapa väsentligt bättre förutsättningar för samverkan mellan alla de forskningsinitiativ som i dag bedrivs under rubriken säkerhet. Målet är att effektivisera svensk forskning inom området och säkerställa att finansiering nyttjas på ett för samhället effektivt sätt, för att exempelvis undvika dubbelarbete och nå kortare ledtider från idé till produkt.

5.3 Nationellt säkerhetsforskningsprogram

I förlängningen skall vårt föreslagna säkerhetsforskningsprogram vara väl etablerat både inom relevant svensk högskoleforskning och säkerhetsbranschen i stort och dess organisationer så som SOFF och SACS. Det nya programmets styrelse är ansvarig för programmet som huvudsakligen kommer att består av följande:

- Löpande program för att stimulera forskningsbaserade innovationer inom utpekade områden.
- Årliga utlysningar.
- Möjlighet till särskild inriktning mot angelägna problemställningar, SME-deltagande etc
- Fokus på verksamheter med hög "TRL-gradient", och att ge tydligt demonstrationsvärde för slutanvändare.

5.4 Nationell mötesplats

Det finns ett fåtal nationella mötesplatser med olika inriktning, exempelvis TAMSEC och Säkerhetsmässan i Kista, men ingen mötesplats med långa traditioner. Det finns idag en lång rad exempel på lyckade inomvetenskapliga nationella konferenser inom IKT-området. Dessa hålls vanligen vartannat år, exempelvis inom radiovetenskap, robotik, reglerteknik, mekanik och bildbehandling. Men, som bl.a NRIA Säkerhet konstaterar, finns det ett stort behov för en tvärvetenskaplig mötesplats inom säkerhetsområdet.

Mötesplats samhällssäkerhet kommer att arrangeras av Kistamässan vartannat år, och ska bli den naturliga mötesplatsen för industri, användare och beslutsfattare. Vårt förslag är att låta detta bli en mötesplats också för forskare.

6 Bilaga: ämnesbeskrivningar

6.1 Kommunikation

Kommunikation avser här teknologi för att kunna överföra information mellan slutanvändare/människor samt mellan enheter såsom exempel datorer, mobiltelefoner, surfplattor, flygplan och bilar eller andra fordon, sensorer i ett nätverk, givare och reglerdon eller RFID-taggar.

Det moderna samhället förlitar sig mer och mer på infrastruktur för kommunikation, och speciellt trådlös kommunikation. Detta är en utveckling som kommer att fortsätta. Informationsteknologi, och i synnerhet kanske mobil kommunikation och Internet, har förändrat människors liv över hela världen. Nationellt är området av stor betydelse, både för exportindustrin och infrastruktursektorn då Sverige har världsledande företag och institut inom telekombranschen. Kommunikationssystem är dessutom en vital komponent i komplexa system, till exempel flygindustrin, och inom försvaret. Parallellt med detta, så tillkommer helt nya tillämpningsområden. Ett exempel är trådlösa sensornätverk, bestående av små sensorer som kommunicerar via radio och som rapporterar mätningar, eller ljud- och videoupptagningar av olika slag. Tillämpningar av sensornätverk finns inom säkerhet, övervakning, miljö (environmental monitoring), inom sjukvården och i processindustrin. I processindustrin är man typiskt intresserad av ersätta kablage på rörlig utrustning (robotar, till exempel) med trådlösa länkar. Många av dessa tillämpningar ställer extrema krav på tillförlitlighet och på de tidsfördröjningar i kommunikationen som man kan tolerera.

6.1.1 Generella trender inom området kommunikation

Trådlös kommunikation och speciellt mobilt bredband är en fundamental möjliggörare för alla moderna IKT-tillämpningar, inklusive sociala nätverk, “cloud computing” och maskin-till-maskin kommunikation. Den fundamentala flaskhalsen för mobilt bredband är den begränsade tillgängligheten för radiospektrum. Den nuvarande tillväxttakten är inte hållbar, om inte radikala innovationer görs som förbättrar effektiviteten med vilken spektrum används och minskar nivåerna på den utsända effekten. Helt ny teknik behöver uppfinnas och utvecklas här. En av de mest lovande riktningarna är massiva flerantennsystem, som möjliggör helt nya ingenjörslösningar som helt enkelt inte betraktades som möjliga alls med konventionell teknologi: stora, potentiellt delvis dolda, gruppantenn som förser tiofalt fler användare med bredband i samma frekvensspektrum och med en utstrålad effekt hundra gånger lägre än vad en konventionell basstation använder.

En annan riktning där vi bara har sett början, både i termer av teknikutveckling och i termer av tillämpningar, är storskalig användning av trådlösa sensorer. RFID är ett exempel, som trots dess vitt spridda användning i logistik-tillämpningar bara befinner sig i sin barndom och har en enorm latent potential att utnyttjas i en helt annan skala än vad som görs idag. Den teknologiska flaskhalsen är förmågan att överföra tillräckligt med effekt trådlöst för att förse sensorn/RFID-taggen med ström, och förmågan att urskilja flera RFID-taggar inom samma område och på samma avstånd. Massiva gruppantenner kommer bli en fundamental möjliggörare för att förbättra denna teknik tio eller hundrafalt, både i termer av räckvidd, livslängd för sensorerna och möjligheten att urskilja flera samlokaliserade taggar eller sensornoder.

Nya frekvensband börjar användas hela tiden för trådlös kommunikation, speciellt högre frekvenser i mm-vågsbandet, och denna utveckling påskyndar de trender som beskrivs ovan. Sverige har en ledande roll inom radio-access teknologi och är väl positionerat att ta en ledande roll inom denna utveckling.

6.1.2 Trådlös kommunikation för samhällssäkerhet

Trådlös kommunikation är också en förutsättning för effektivt fungerande samhällssäkerhet och specifikt för krishantering och infrastrukturskydd. I många av dessa tillämpningar är trådlös kommunikation den enda möjliga tekniska lösningen. Till exempel möjliggör trådlösa anslutningar mobilitet och flexibilitet för personal och system på samma gång som det eliminerar behovet av förinstallerad infrastruktur. Särskilt relevanta exempel på användningsområden är kommunikationslänkar för räddningsmanskap och annan utryckningspersonal i krissituationer, sensornätverk för infrastrukturskydd, säkerhets/övervakningskameror och larmsystem.

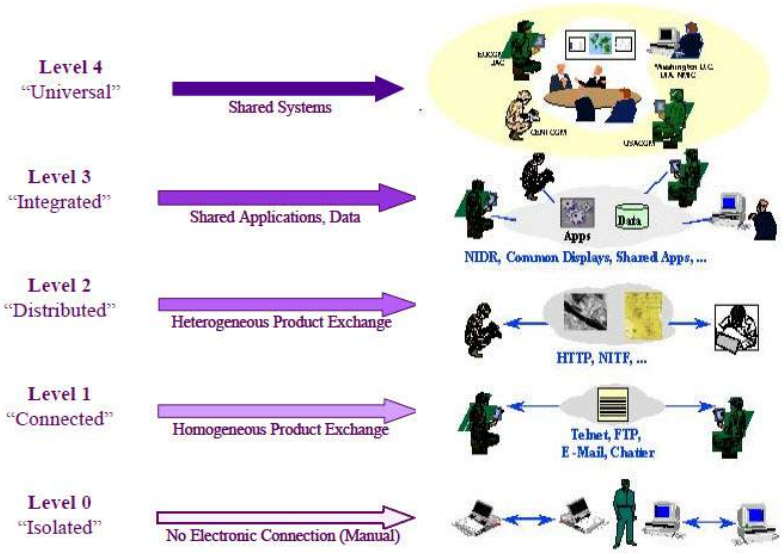
Många länder har liksom Sverige valt TETRA-standarden för trådlös kommunikation i nödsituationer. Det är idag allmänt känt att TETRA har begränsad robusthet mot störningar, begränsad kapacitet och lider av interoperabilitetsproblem länderna emellan. Aktörer som kan bidra med lösningar på dessa problem kommer att vinna marknadsandelar och bidra till ekonomisk tillväxt. En viktig forskningsfråga är hur mobiltelefoni, GSM, 3G och LTE, kan användas som ytterligare nätverk för att hantera kapacitetsbehov och interoperabilitetsproblem, samtidigt som hög robusthet bibehålls. En annan viktig fråga är hur framtida TETRA-standarder kan vidareutvecklas för att öka robusthet och kapacitet. Sverige har en lång tradition av spetsforskning inom telekommunikation och har möjlighet att öka marknadsandelarna även inom kommunikation för insatspersonal.

Frekvensspektrum är en begränsad resurs och antalet användare kommer bara att öka. Därför är det enda möjliga sättet att öka robusthet/kapacitet att dra nytta av spatial diversitet. Följaktligen kommer mångantennsystem att vara ett grundläggande verktyg för att förbättra kommunikation vid räddningsinsatser.

6.2 Interoperabilitet

IEEE definierar interoperabilitet som “the ability of two or more systems or components to exchange information and to use the information that has been exchanged”. De flesta tekniska system är idag informationssystem. Kraven på att flexibelt integrera med andra informationssystem ökar ständigt. Den som inte har en klar strategi för systemintegration riskerar att system blir oanvändbara i framtida verksamhetskritiska samarbeten eller får leva med mycket stora integrationskostnader under hela systemens livscykel. Felaktigt genomförda integrationer som kopplar ihop system tekniskt men misslyckas med att kommunicera praktiskt användbar information kan i värsta fall orsaka farliga och dyra missförstånd under kritiska operationer.

Interoperabilitet är centralt i många discipliner, såsom logistik (internationella distributionskedjor med civila aktörer), medicin (tex sammanslagning av journalsystem), och försvar (samverkan mellan länder och mellan stridskrafter ökar kraven på interoperabilitet, både vad avser materiel och förband). Ledningssystem för civil säkerhet har samma utmaningar inom interoperabilitet, och här är SAAB en stor och viktig aktör.



Interoperabilitet kan delas upp i följande delar:

- Syntaktisk interoperabilitet för utbyte av data. Här spelar standarder stor roll.
- Semantisk interoperabilitet för att tolka information. Det här är ett utmanande område där svensk forskning ligger långt framme (FOI, LiU).

En nivåindelad referensmodell beskrivs i US DoD C4SIR Framework Architecture och kallas för Levels of Information Systems Interoperability (LISI). I denna modell finns fem nivåer (se figuren ovan). Den lägsta nivån, nivå 0, avser system som är helt isolerade, d.v.s. systemen består av helt disjunkta och icke-interoperabla enheter. Nästa nivå är parvis sammankopplade system, och nivå 2 omfattar distribuerade system inom en viss begränsad domän. På nivå 3 kan systemen dela på både data och applikationer t.ex. för att uppnå en gemensam lägesuppfattning. Slutligen, på nivå 4, samverkar systemen globalt och är fullständigt interoperabla.

6.3 Intelligenta sensorsystem för säkerhet

När samhället ställer upp mål som att vi skall ha ett gott skydd för individer och den kritiska infrastrukturen, att vi snabbt skall ha ett välgrundat beslutsunderlag för krisinsatser eller att vi skall kunna hantera räddningsinsatser eller pandemier effektivt så är ofta nyckeln till kostnadseffektiva lösningar ny sensorteknik. Här har vi valt att fokusera på intelligenta sensorsystem där målet är att kunna gå från personaltunga och relativt långsamma eller oprecisa system till automatiska system med stor förmåga att hitta det vi söker. Texten är till största delen baserad på kunskapsöversikter inom områdena sensorsystem och sensordatafusion, framtagna av FOI och LiU som underlag inför MSB:s inriktningsarbete 2010.

6.3.1 Användningsområden

I dagsläget är de viktigaste delområdena där ny kunskap och teknik krävs:

1. Snabba och portabla/distribuerade detektorer för farliga ämnen som giftiga kemikalier, bakterier eller virus
2. Kostnadseffektiva sensorsystem som kan upptäcka hot i form av dolda människor, vapen, explosivämnen mm
3. Automatiska övervakningssystem för kritisk infrastruktur som fungerar dygnet runt i alla väder
4. Portabla sensor- och positioneringssystem för krishantering och räddningsinsatser efter olyckor, naturkatastrofer eller attentat

5. Fjärranalyssystem med förmåga att i realtid detektera t ex stormskador (skog, infrastruktur) skogsbränder, översvämningar och föroreningar liksom säkerhetsrelaterade hot kring hav och gränser

Alla områdena ovan inkluderar hela kedjan från de enskilda detektorerna och sensorerna via sensornät, sensordatafusion och identifiering av onormala händelser till alarmfunktioner och kopplingen till operatörer och beslutsfattare.

6.3.2 Nationella kompetensområden

Sverige ligger långt framme kunskapsmässigt inom flera centrala områden.

- Biologiska sensorer och detektorer för farliga ämnen.
- Radarteknik och radarsystem för övervakning av stora områden.
- Radiobaserade positionering och identifieringssystem.
- Sensornätverk, inkluderande distribuerade beräkningar och minimal kommunikationsbehov för energisnåla och skalbara lösningar.
- Sensorfusion för systembyggande och extraktion av information från flera sensorer av olika slag.

Inom dessa områden finns en stark akademisk kompetens, stora företag med stark export såväl som små avknoppningsbolag nischade till säkerhetsområdet.

6.3.3 Behovsbild

Sverige och svenskarna påverkas allt mer av den globala utvecklingen och vi påverkas därför också i ökande grad av de förändrade risker, hotbilder och den ökade sårbarhet som det medför. Som exempel på förändringar som påverkar behovet av intelligenta sensorsystem kan nämnas;

• Klimatförändringen som medför högre medeltemperatur och förändrade vind- och nederbördsmönster vilket kan ge ökande risker för stormskador, erosion, översvämningar och stora skogsbränder. Det finns därför ett behov av fjärranalyssystem (på satelliter, flygplan eller obemannade flygplan) som kan ge en snabb information om hur läget utvecklas.

• Ökande flyktingströmmar och brottslighet ställer nya krav på övervakning av gränser. Kontinuerlig övervakning av EU:s yttre gräns över hav har högsta prioritet och behov av att kunna upptäcka och följa små snabba båtar och flygplan på låg höjd kräver nya tekniska lösningar. Nya samverkande system på olika plattformar (satellit, flygplan, fartyg etc) med realtidsförmåga och 24/7-tillgänglighet behöver utvecklas för att lösa uppgiften.

• Det snabbt ökande internationella resandet medför en snabb spridning av pandemier. Det finns därför ett behov av portabla eller distribuerade instrument som snabbt kan identifiera smittämnen. Sveriges åtagande internationellt medför också att svensk räddningspersonal bör ha tillgång till mobila sensor- och positioneringssystem som ger en aktuell lägesbild samt därutöver sensorer för att räddningspersonal skall kunna hantera problemen på plats (t ex att detektera människor i rasmassor, upptäcka farliga smittämnen eller farliga kemikalier mm).

• En alltmer globaliserad ekonomi gör att alltmer råvaror transporteras vilket medför ökande risker för olyckor eller attentat med allvarliga konsekvenser i våra stadskärnor. Det finns därför ett behov av nya övervakningssystem i stationsområdena samt sensorer som hjälper insatsledningen efter en händelse t ex genom att ge en möjlighet att i realtid följa hur ett gasmoln rör sig och vilka halter av farliga ämnen som det innehåller.

• En alltmer centraliserad energi- och vattenförsörjning gör samhället sårbart för olyckor och attentat. Det finns därför ett behov av förbättrade övervakningssystem för allt ifrån kraftverk och transformatorstationer till fjärrvärmeanläggningar och vattenförsörjningssystem.

• Sveriges ökande internationella engagemang förändrar hotbilden för terrorism i Sverige. Detta gör att vi måste förbättra områdesbevakning och inpasseringskontroll vid kritisk infrastruktur och kanske också ta fram portabla säkerhetssystem för stora evenemang.

• De öppna gränserna leder till en ökad internationell grov brottslighet. Detta gör att övervakningen vid t ex hamnar eller måste förbättras liksom möjligheten att snabbt identifiera explosivämnen mm.

• Kollektiva transportsystem för både gods och människor ökar i betydelse vilket medför en ökad sårbarhet för individer och samhälle vid olyckor eller attentat. För att minska riskerna måste förbättrade sensorsystem för övervakning och personskanning utvecklas som både löser uppgiften samtidigt som de inte påverkar flödet av människor eller gods negativt.

Flera av områdena ovan saknar idag praktiskt taget helt nödvändiga tekniska hjälpmedel för att kunna bilda en relevant lägesbild på lokal eller övergripande nivå. För alla områdena gäller att ökande kostnader för manuell bevakning gör nya tekniska lösningar som automatiserar så mycket som möjligt av bevakning och kontroll synnerligen angelägna.

De behov som driver den globala marknaden är snarlika de svenska behoven ovan, givetvis med regionala skillnader beroende på klimat, kultur, samhällsutveckling, geografiska förutsättningar med mera. Sverige har ett etablerat kunnande avseende såväl tekniska system inom sensorområdet som förmåga att utnyttja nya landvinningar för att möta behoven. Det finns således goda förutsättningar för svenska aktörer att agera på den globala sensor-marknaden, vilken bedöms ha en tillväxt på ca 7.8 % årligen, enligt en marknadsprognos från BBC market.

6.4 Cybersecurity

Cyber säkerhet är ett mycket brett område som berör säkerheten kring ICT användning. De sex områden som nämns har utöver deras industriella betydelse också en stark forskningsanknytning i Sverige hos forskningsinstitut, universitet, och företag.

6.4.1 Mjukvarasäkerhet och metoder för "trust assurance"

Med det närmast universella genomslag kommunikationsteknologi, båda fast och trådlös, haft de senare åren, har kraven på mjukvarukvalitet höjts signifikant. Detta inkluderar tillförlitlighet, feltolerans, och alla aspekter av säkerhet, både funktionell säkerhet, ”privacy” och integritet, samt it-säkerhet i traditionell mening. Mjukvara är i ständigt ökande grad en nyckeldifferentiator och en central komponent i industriella produkter. Förmågan att leva upp till ständigt höjda kvalitetskrav är därför en betydelsefull strategisk fråga för att Svensk industri kan behålla och stärka sin konkurrenskraft. Om detta ska åstadkommas är utbildning och träning av utvecklarkunskaper inom områden relaterat till mjukvarukvalitet såsom programmering, testning, verifikation, och validering av stor betydelse, men det finns även stor potential till utveckling av nya verktyg, metoder, och produkter inom områden som säkra mjukvarukomponenter, säkra programmeringsspråk, säkerhetstestning, programanalys, och formell verifiering.
Vetenskapliga framsteg under de senaste 10-15 inom dessa områden visar på nya möjligheter. Många säkerhetsluckor orsakas av dåligt konstruerade programmeringsverktyg och språk. Välkända exempel är ”buffer overflows” och bristen på ”array bounds checking” i C och C++. Bättre stöd inom programmeringsspråk, API design, och verktyg för analys och avlusning behövs. Automatiska och halvautomatiska analysverktyg har förbättrats i mycket hög grad på grund av framsteg inom de grundläggande algoritmerna. Detta har gjort att tröskeln

för användning av formella metoder i industriell skala har sänkts betydligt. Exempel är framstegen inom låg-nivå mjukvaruverifiering i seL4 och Microsoft's Hyper-V projekt. Dessa indikerar att säkra och formellt certifierbara exekveringsplattformer är inom räckhåll i ett 5-10 års perspektiv.
Andra ”trust assurance” teknologier är av lika stor betydelse, inklusive körtidsmonitorering och sårbarhetstestning, inklusive ”fuzzing”. Båda är ovärderliga verktyg inom produktion av högkvalitativ mjukvara, men mycket kunskap behövs fortfarande, inom exempelvis "coverage" estimering, val av testfall, och modellrekonstruktionstekniker.

6.4.2 Trusted Computingplattformar och övervakning av datormoln

Virtualisering, trusted computing, övervakning

Säkerhet har blivit en viktig del i utformningen av hemelektronik, såsom mobila eller smarta telefoner, mediespelare, hemroutrar och olika nätverkssensorer samt SCADA-system. Säkerhetsfrågor gällande inbyggda system varierar från driftsäkerhet, som hög tillgänglighet, robust utförande, nätverksåtkomst etc. till skydd mot mjukvarubaserade attacker såsom virus och trojaner. I en del hårdvaruplatformar används virtualisering som en teknik för att skapa säkrare system. I ett virtualiserat system kör en hypervisor på den mest privilegierade nivån och med hjälp av hårdvaruskydd åstadkommer den både säker isolering och övervakningstjänster av operativsystem och program. Detta är mycket värdefullt eftersom det låter både tillförlitliga och icke tillförlitliga program dela samma hårdvara utan störningar. I denna säkra exekveringsmiljö är kraven på isolering mellan program kritiska. Hypervisorn måste inte bara skydda mot slumpmässiga och oavsiktliga fel och felaktiga konfigurationer som potentiellt kan bryta isoleringen, utan den måste även skydda mot riktade attacker. På så sätt erbjuder virtualisering en metod som täcker behovet av kostnadseffektiva säkra exekveringsmiljöer på off-the-shelf-hårdvaruplattformar. Andra metoder inkluderar dedikerad hårdvara och att dra nytta av säker lagring och moduler för säkra exekveringsmiljöer.

Virtualisering är dessutom en hörnsten i den nuvarande trenden inom IT-drift idag för att konsolidera IT-system på gemensamma plattformar. Infrastructure as a Service (IaaS) är en snabbt växande affärsmodell som bygger på virtualisering. Virtualiserad beräkningsinfrastruktur erbjuder många ekonomiska och administrativa fördelar. Dock hindras realiseringen av dessa av bristen på säkerhet för de tjänster som erbjuds. I synnerhet finns det ett behov av lösningar som garanterar konfidentialitet och integritet av data och som kan verifieras av tjänstens användare. Detta är särskilt utmanande i stora infrastrukturnät med en enorm mängd gemensamma datorresurser och dynamisk schemaläggning av virtuella maskiner (VM) på dessa resurser. De strategiska kraven i dessa områden kommer både från befintliga svenska företag som erbjuder dator och kommunikationsinfrastruktur som Ericsson och TeliaSonera, men även från offentliga organisationer som är på väg att flytta tjänster till molnet och som behöver riktlinjer för vilka säkerhetskrav som ska ställas på leverantörerna av en molntjänst.

6.4.3 Kryptologi

Molntjänster, Kvantdatorer, Lättviktskryptologi

De senaste 15 åren har vi sett tre världsomspännande projekt med syfte att identifiera nya och starka kryptografiska algoritmer. Dessa är AES-tävlingen, SHA-3-tävlingen och eSTREAM. Dessa projekt har identifierat starka blockchiffer, strömchiffer och hashfunktioner, men nya användningsområden ställer krav på dedikerade algoritmer som är anpassade för den specifika tillämpningen. Kryptering för molntjänster och kryptering i extremt begränsade miljöer är viktiga tillämpningar. Ett annat viktigt område som fått ökat fokus är kvantdatorer och det är därför också viktigt att förbereda sig för en eventuell framtid med dessa.

Vid användning av molntjänster vill man ofta kunna göra beräkningar på krypterad data i molnet. För att detta ska fungera behövs algoritmer med homomorfiska egenskaper. Denna

typ av algoritmer finns, men användandet kräver så stora resurser att det inte är praktiskt tillämpbart. Mer forskning krävs inom detta område för att människor, företag och organisationer ska kunna utnyttja molntjänster även för känslig och viktig data.

En ökad användning av t.ex. RFID-teknologi och sensornätverk, som båda bidrar till att förverkliga det som ofta kallas Internet of Things, ställer också stora krav på säkerhet. Kryptografiska algoritmer särskilt anpassade för små inbyggda system, med stora krav på energieffektivitet och kretsstorlek, kommer krävas för att garantera säkerheten i dessa system. Det kommer också ställas stora krav på implementationskostnaden för att ekonomiskt motivera användandet av dessa algoritmer. Samtidigt som det har bedrivits en hel del forskning inom detta område, så har denna forskning varit väldigt fokuserad på konfidentialitetsskydd, medan meddelandeautentisering inte alls har fått samma uppmärksamhet. Vidare är det tydligt att algoritmer mer fokuserade på den direkta applikationen kan göras mer effektiva. I en värld med 50 miljarder uppkopplade enheter är även små energibesparingar viktiga, då det bidrar till ett mer hållbart samhälle.

Kvantdatorer och kvantberäkningar har fått mycket uppmärksamhet. Det är en utbredd missuppfattning att kraftfulla kvantdatorer automatiskt gör kryptering verkningslös. Däremot finns det effektiva algoritmer beskrivna för kvantdatorer som skulle knäcka några av de mest kända och använda asymmetriska algoritmerna, t.ex. RSA och DSA. En sådan kvantdator skulle försätta samhället i en mycket svår situation just på grund av den utbredda användningen av dessa algoritmer. Samtidigt finns det algoritmer baserade på asymmetrisk kryptografi som verkar mycket svåra att knäcka även med en kraftfull kvantdator, t.ex algoritmer baserade på kodningsteori. Dessa algoritmer är dock inte lika effektiva som RSA och DSA och att bara byta ut algoritmerna skulle därför vara mycket kostsamt. Mer forskning för att effektivisera dessa algoritmer är därför nödvändig som ett steg i att garantera säker informationsöverföring i en värld med kvantdatorer.

6.4.4 Nätverkssäkerhet och robusthet

Software defined networks, virtuella nät, cyber crime

Med nätverkssäkerhet och robusthet avses den förmåga av kommunikationsnätverk att motstå negativ yttre påverkan av mänsklig såväl som naturens ursprung. Områdets betydelse sammanfaller med den som beskrevs för kommunikationsområdet. Men teknologimässigt så finns det skillnader framförallt genom betraktelse av nätverkskommunikation som brukar olika kommunikationsteknologier, överlagringsnätverk och Software Defined Networks (SDN).

Förutom en starkt ökad användning av mobil teknik för ett växande antal kommunicerande enheter så börjar vi se användningen av molnteknik för att skapa så kallade molnbaserade tjänster. Inom den traditionella telekommunikationsindustrin ser man här möjligheter till att skapa så kallade Telco moln. Genom ett Telcomoln eller SDN i allmänhet kan man erbjuda dedikerade nätverk för specifika organisationer och som för sina fysiska förverkliganden kan använda sig av olika typer av IKT-tekniker. Parallellt med de uppenbara fördelarna med bättre utnyttjande av resurser, följer många säkerhetsproblem som behöver åtgärdas och där vi idag endast känner dellösningar. Utöver dessa frågor så vill man åstadkomma robusta nätverk som kan hantera ökade dataflöden. Denna fråga blir synnerlige tydlig om man tittar på problem orsakade av hacktivsm och cyberattacker, men är också uppenbar när man tittar på skador från t.ex. brand och naturkatastrofer. Insikten om betydelse av kommunikationsnätverk har på senare tid givet upphov till ökad kommersiell och regulatoriskt styrd kravställning på säkerhet.

Förutom att dessa frågor är viktiga för tillit i nätverk och deras styrsystem i allmänhet och hur dessa nätverk används, så banas här en väg för användning av kommersiell kommunikationsteknik, t.ex. mobilt bredband, av myndigheter som behöver bättre stöd för informationsspridd-

ning i nödsituationer, teknik för övervakning, upptäckt av avvikelser och övervakning av kritisk IKT-beroende infrastruktur. Det medger också möjligheter till bättre metoder och system för robust och säker krishantering.

Vidare kommer morgondagens allmänna nätverk vara uppbyggd med hjälp en behovsstyrd sammanlänkning av heterogena kommunikationssystem som förmodligen ägs av olika intressenter. Att förse dessa nätverk med adekvata skydds- och säkra kontrollmekanismer kommer vara en stor utmaning med många kommersialiseringsmöjligheter.

6.4.5 Privacy och åtkomstkontroll

Inom ramen för IT-och IKT-säkerhet så berör privacy skydd av personuppgifter mot missbruk, dvs informativ integritet. Informativ integritet är relaterad till personens rätt att avgöra när, hur och i vilken utsträckning information om honom eller henne överförs till andra [F. Westin, Privacy and Freedom, 1967] och är en grundläggande rättighet som garanteras i Europeiska unionen. Det ingår i europeiska kommissionens direktiv som beskriver hur personlig information behandlas och lagras i fråga om öppenhet, syfte och proportionalitet. Principen om nödvändigheten av insamling och behandling, vilket är en av de viktigaste integritetsskyddskraven, bestämmer att insamling och behandling av personuppgifter endast bör tillåtas om det är nödvändigt för de arbetsuppgifter som hör till ansvarsområdet.
Industrin måste beakta genomförandet av teknik som förbättrar skyddet av privatliv och data när det är möjligt. Till exempel måste tjänsteleverantörer ta skyddskrav för privacy och integritet i beaktande vid outsourcing av bearbetning eller lagring av kundernas data till molnbaserade plattformar.

Eftersom det finns ett starkt samband mellan integritet och åtkomstkontroll (mekanismer för åtkomstkontroll kan användas för att begränsa tillgången till information) så krävs vid framtagning av digitala tjänster och system att det skapas strategier för åtkomstkontroll, t.ex. att begränsa åtkomsten av data i sociala nätverksprofiler. Dock kan metoder för åtkomstkontroll bli bakvända och svåra att hantera för många användare. Här återstår mycket arbete att göra.

6.4.6 Rättsliga aspekter: spelregler, personlig integritet och legitimitet

Lagstiftning, integritet, legitimitet

De rättsliga aspekterna av cybersäkerhet har flera dimensioner. Dels handlar det om ett grundläggande behov av tydlighet – vad det är som ska gälla i termer av reglering av marknadsförhållanden och relation till individer och andra aktörer – och dels kan det handla om att vissa värden av lagstiftaren anses vara mer skyddsvärda än de åtgärder som man avser att införa. Ett sådant värde kan vara skyddet för individens integritet, som då måste balanseras mot exempelvis övervakning. Man ska även lyfta fram ytterligare en nivå av relevans för utfallet av cybersäkerhet, dvs att även teknisk implementering som berör människor är beroende av den sociala kontext den utförs i. Här bör man fokusera en åtgärds legitimitet, dvs. hur den uppfattas av de som den berör, inte minst med hänsyn till att åtgärder som inte uppfattas som legitima tenderar att kringgås eller rentav motarbetas.

Spelregler
Om man diskuterar det första fallet i termer av åtgärder som aggregerar trafikdata eller användarbeteende på något sätt så kan man exempelvis fråga sig vem som äger de data som produceras. Man kan fråga sig om det ur något perspektiv faktiskt är den som genererar informationen, dvs kör runt i sin uppkopplade bil, surfar runt på internet eller använder sin mobiltelefon. Detta skulle i så fall påverka spelreglerna för hur informationen kan hanteras, tex om den kan säljas vidare. Här finns det även en utmaning i det alltmer digitalt framväxande och geografiskt gränslösa i mötet med de olika geografiskt anknutna jurisdiktioner som rätten traditionellt sätt verkar inom. Eventuella luckor i regleringen mellan stater kan verka negativt för cybersäkerhetsfrågor. Det finns också klara indikationer på att den rättsliga regleringen

ofta släpar efter samhälls- och teknikutvecklingen, inte minst i hur rätten ”förstår” världen, vilket gör att även de rättsliga begreppen kan bli inaktuella.

Personlig integritet
När det gäller ansamling av trafik- eller användardata i relation till individers integritet, måste man först fråga sig vad man faktiskt kan göra med de data som lagras, om man kör den mot kartdata, mot annan konsumentdata, bostadsregister etc. Detta leder till frågan vem som kommer/kan/bör ha tillgång till data. Här kan paralleller dras till upphovsrättsindustrins ideliga kamp om att få tillgång till identitetsinformation från ISPer. Om det finns känsliga delar i den information som sparas som kan vara förmånlig för vissa aktörer så kommer denna fråga att aktualiseras och rentav politiseras, dvs det kommer att bli en principfråga. Kan den läcka, kan den säljas, bör den skyddas etc? Vem äger data?
Här måste frågan om eventuella övervakningsmöjligheter lyftas. Som systemutvecklare kan man inte förutsätta att alla förvaltare av systemet bara kommer att ha goda avsikter med användningen. I vilken mån kan man övervaka individer? Om informationen skulle utgöra en förmånlig komponent i övervakning bör man nog även fundera över skillnaden i ”privacy by policy” och ”privacy by design”, dvs att i vissa lägen kanske inte ens ett rättslig skydd är speciellt starkt, medan ett designat skydd kan vara mycket mer verkningsfullt.

Legitimitet – och dess potential för innovation
När det gäller legitimitetsaspekter kring cybersäkerhet så är detta fält kanske det minst tekniska och samtidigt det som kräver ett brett tvärvetenskapligt betraktelsesätt som samtidigt innehåller en stor innovativ potential. I vilken mån vet, vill eller kan exempelvis konsumenterna eller de som berörs av en implementering påverka? Oavsett om vad den som designar systemen ser fördelar så är det inte säkert att den publik som är tänkt att ta emot det har samma uppfattning. Detta kan leda till en rad oförutsedda konsekvenser som man kan förbereda sig på i större eller mindre grad. Dvs. systemen implementeras i en socio-kulturell kontext och är beroende av hur dessa uppfattas av dess adressater. Några exempel att fundera på här är DRM-skydd på exempelvis DVDer, som ledde till en massiv hackningsverksamhet, och ”jailbreakade” mobiltelefoner där konsumenter vill ha större frihet att påverka användandet av produkten de köper.
Det kan röra frågor om hur folk beter sig i relation till i övrigt robusta och säkra system, vilka normer och attityder de omfattas utav, men även hur säkerhetsfrågor uppfattas och därmed tas emot av olika grupper i samhället. Dessa något mer svårfångade faktorer avgör hur framgångsrik en säkerhetsteknisk implementering blir. Å ena sidan bör man inte undvika att inkludera dessa faktorer bara för att de kan tyckas svårfångade, och å andra sidan är detta ur ett svenskt innovationsperspektiv en breddande aspekt som gör att mer tvärgående projekt också är troligare att lyckas uppnå säkrare system.
Detta är rimligen en utmaning för de ofta teknikorienterade vetenskaperna att förhålla sig till uppfattningar, normer och attityder, men samtidigt ur ett svenskt innovationsperspektiv en brett inbjudande fråga. Sverige är lyckligtvis inte bara bra på teknikrelaterad innovation utan även på social innovation där tekniken måste placeras i en samhällelig kontext. Här handlar det därmed i viss mån om ett breddat perspektiv där ”säkerhetsteknik” i cybersammanhang behöver vidgas till att inbegripa ”säkerhetsfrågor” överlag. Vilket innebär ett breddat löfte för svensk innovationskraft.