Strategisk utblick 7

Närområdet och nationell säkerhet

Cecilia Hull Wiklund, Daniel Faria, Bengt Johansson och Josefin Öhrn-Lundin (red.)

FOI-R--4454--SE

Oktober 2017

FOI

Strategisk utblick 7:
Närområdet och nationell säkerhet

Cecilia Hull Wiklund, Daniel Faria,
Bengt Johansson och
Josefin Öhrn-Lundin (red.)

Oktober 2017

FOI-R--4454--SE

ISSN 1650-1942
Tryckt i Stockholm 2017 av Totalförsvarets forskningsinstitut, FOI
Omslagsbild: Anton Balazh/shutterstock.com
FOI-R--4454--SE
Godkänd av Lars Höstbeck

Innehåll

Förord

Sedan den första *Strategisk utblick* gavs ut 2009 har det säkerhetspolitiska omvärldsläget förändrats på ett sätt som i allt större grad satt närområdet i centrum. Samtidigt pågår en snabb teknikutveckling inom både det militära och civila området som skapar nya möjligheter, men också sårbarheter och utmaningar för dagens beslutsfattare.

För att kunna skapa ett tryggt och säkert samhälle krävs djup kunskap om ett brett spektrum av frågor inom exempelvis försvars- och säkerhetspolitik, försvarsplanering, militär teknik, kritisk infrastruktur, informationssäkerhet och CBRN-skydd. FOI:s uppgift är att tillhandahålla sådan kunskap till relevanta samhällsaktörer. FOI har genom många års forsknings- och utvecklingsarbete byggt en kompetens med såväl djup som, i det närmaste unik, bredd och utgör en central resurs för samhället. *Strategisk utblick*, som är en av FOI:s profilpublikationer, har som syfte att spegla denna kompetens på ett lättillgängligt sätt men med bibehållen vetenskaplig kvalitet. Min förhoppning är att årets utgåva ska vara intressant och värdefull läsning för såväl beslutsfattare som den intresserade allmänheten.

För att återspegla omvärldsläget har årets *Strategisk utblick* temat *Närområdet och nationell säkerhet*. Artiklarna reflekterar på olika sätt de säkerhetsutmaningar Sverige kommer att ställas inför under de närmaste åren. Utblickens inledande artikel lyfter fram de utmaningar som Sverige möter i omställningen till att fokusera på nationell säkerhet, inte minst vad gäller resurstilldelning och förhållningssätt. Artikeln följs av en försvarsekonomisk analys som pekar på ett högt, omedvetet, politiskt risktagande i försvars- och säkerhetspolitiken. Den geostrategiska kontexten behandlas i två säkerhetspolitiska analyser. Den första berör Östersjöområdet, som är av särskild geostrategisk betydelse i interaktionen mellan Ryssland och Nato. Den andra beskriver förutsättningarna för samarbete mellan Sverige och Tyskland, den mest betydande Natomedlemmen i Östersjöområdet.

I och med det ökade fokuset på nationell säkerhet har totalförsvaret och territoriellt försvar fått allt större betydelse i försvarspolitiken. Denna *Strategisk utblick* diskuterar totalförsvar ur två perspektiv. En artikel lyfter nyckelfaktorer för att kunna bygga ett modernt totalförsvar med maximal försvarseffekt: vilken försvarskritisk verksamhet som ska bedrivas av Försvarsmakten respektive det civila försvaret,

hur organiseringen av statliga myndigheter bör se ut samt behovet av långsiktigt beslutsunderlag. En annan behandlar det psykologiska försvaret, av central betydelse för att kunna motstå informationspåverkan och bygga försvarsvilja.

Den snabba utvecklingen av informationstekniken skapar nya utmaningar inom försvars- och säkerhetsområdet. Detta speglas i fyra artiklar i rapporten. Digitalisering och samhällsviktig verksamhets användning av internet skapar nya möjligheter men också nya beroenden. Inhämtning av underrättelser, påverkansoperation samt dolda militära operationer lyfts fram i en artikel som områden där internet har en ny betydelse som militärt verktyg. En annan artikel lyfter fram hur produkter i allt större grad är kopplade till internet (*Internet of Things*), vilket ökar risken för cyberangrepp som kan skapa allvarliga störningar hos samhällsviktiga system. Elsystemet är ett exempel på ett sådant system och ytterligare en artikel visar hur så kallade smarta elnät förstärker sårbarheten för attacker. Den fjärde artikeln lyfter fram hur den ökade tillgängligheten till geografiska data, underlättad av den pågående digitaliseringen, kan skapa betydande effektiviseringar i samhället men också riskerar att skyddsvärd information sprids på ett oönskat sätt.

Teknisk utveckling leder till mer avancerade vapensystem som det svenska försvaret behöver både kunna nyttja och möta. Flera artiklar i årets strategisk utblick behandlar detta frågekomplex. En av dem undersöker vilken betydelse närvaron av långräckviddiga vapen i närområdet ska ges i en bedömning av Sveriges försvarsbehov; en annan lyfter fram behovet av en svensk försvars- och säkerhetsstrategi för rymdfrågor. I ytterligare en artikel diskuteras de besvärliga beslutsproblem svenska beslutsfattare kan ställas inför vid en allvarlig kontaminering av livsmedel som en följd av ett kärnvapenanfall.

Rapporten avslutas med tre artiklar med en inriktning som är ny för årets *Strategisk utblick*. I två av dem har författare från Norge och Finland inbjudits att presentera reflektioner kring respektive lands försvarsplanering. Detta skapar en värdefull relief till de tidigare artiklarna som har utgått från ett huvudsakligen svenskt problemperspektiv. I den avslutande artikeln diskuteras slutligen den betydelse försvarsforskningen har för svensk säkerhet, det vill säga den faktor som är den huvudsakliga orsaken till FOI:s existens.

Den strategiska utblicken har involverat författare från FOI:s samtliga forskningsavdelningar. Förutom ett stort tack till författarna själva vill jag även rikta ett tack till de fyra redaktörerna som möjliggjort denna 7:e strategiska utblick.

Stockholm i oktober 2017

Jan-Olof Lind
Generaldirektör
Totalförsvarets forskningsinstitut, FOI

1. Nationell säkerhet och närområdet – Sverige backar hem

Robert Dalsjö och Michael Jonsson

Under det gångna decenniet har den säkerhetspolitiska situationen i Sveriges närområde påtagligt försämrats. Ett alltmer hotfullt Ryssland har gjort att fokus har förflyttats från förhållanden i fjärran länder till närområdet. Nationell säkerhet och nationellt försvar står nu återigen på agendan, men ännu präglas både resurstilldelning och förhållningssätt av de många åren då fred och säkerhet kunde tas för givna. Därtill är statsskutan ett trögt skepp att vända. Givet de kända brister som finns inom både Försvarsmakten och totalförsvaret är behovet av kraftfulla åtgärder stort. Analys och policyutformning försvåras också av oviljan att öppet diskutera svenska nationella intressen och de växande hoten mot dessa. Den svenska nationella säkerhetsstrategin som publicerades tidigare i år behöver snabbt kompletteras med tydligare mål, ökade finansiella medel och skarpare metoder, för att åtgärda de sårbarheter som är ett resultat av många års önsketänkande, underfinansiering och bristande säkerhetsmedvetande.

Från solsken till stormvarning

Decennierna efter Berlinmurens fall var den rosiga optimismens tid. När Ryssland inte längre var hotfullt och farligt så behövdes inte längre militär makt i Europa, trodde man. Västeuropa rustade ner, USA tog hem nästan alla sina förband, och Nato ställde om till fredsoperationer i fjärran länder.

Så gjorde också Sverige. Det militära försvaret radikalbantades till en liten styrka för internationella insatser, medan de civila delarna av totalförsvaret helt enkelt lades ner. Beredskapshänsyn i samhällsplaneringen försvann eftersom de ansågs dofta vadmal och naftalin, viktiga funktioner avreglerades och privatiserades, allt i fredlogikens och affärsmässighetens namn.

Själva säkerhetsbegreppet breddades och gjordes post-modernt, staterna och deras suveränitet skulle minska i betydelse. I stället skulle fokus ligga på mänsklig säkerhet, liv, hälsa och välfärd. I den mån man vid denna tid alls såg några hot så var dessa av en ny sort, och icke-militära och icke-statliga, såsom klimatförändringar, pandemier, stora migrationsflöden eller terrorism.

Rysslands mer aggressiva signaler från 2007 och dess krig i Georgien 2008 borde ha fungerat som väckarklockor, men Sverige och resten av västvärlden tryckte på snooze och somnade om. I 2009 års försvarsbeslut kläddes visserligen vår post-moderna säkerhetsagenda på med handfasta mål och uppgifter som fokuserade på statens säkerhet, suveränitet och handlingsfrihet mot yttre hot. Försvarsmakten gavs också uppgiften att ”hävda Sveriges suveränitet, värna suveräna rättigheter och nationella intressen”, och beredskapskrav ställdes åter. Men styrsignalerna togs då inte riktigt på allvar av en förvaltning som fortfarande var inställd på låga kostnader och fredsmässig drift. Att denna hållning även delades av regeringen visades av att statsministern i januari 2014 förklarade att ett mellanstatligt krig i Europa inte längre var tänkbart.

Det blev följaktligen ett brutalt uppvaknande när Ryssland mindre än två månader därefter invaderade och annekterade Krim. Plötsligt tvingades Sverige inse att världen var farlig igen. Ryssland hade förkastat den europeiska säkerhetsordningen och försökte med hot och våld att karva ut en egen maktsfär. Snart blev det också klart att om det skulle komma till ett krig mellan Ryssland och Nato så vore Baltikum Natos svagaste punkt. Östersjöområdet hade blivit det nya kalla krigets brännpunkt, och om det blev ett krig här så skulle Sverige obönhörligen dras in. Som lök på laxen kom så 2016 Brexit och valet av Donald Trump till USA:s president, vilket gjorde att tvivel uppstod om Nato och EU kunde räknas med som pålitliga motvikter mot Ryssland.

Den höjda spänningen till trots så är ännu sannolikheten för ett öppet krig liten, men redan i dag – i formell fred – pågår en kamp om makt och inflytande i regionen. Ryska storövningar, hotfulla närflygningar och nya vapensystem bör inte främst ses som krigsförberedelser, utan som ett ”säkerhetspolitiskt kroppsspråk” där budskapet är att grannländerna är små och svaga, Ryssland är stort och farligt, och att USA bör hålla sig borta. Detta budskap understöds också av en påfallande skicklig psykologisk krigföring som via olika digitala medier sprider misstro mot västliga beslutsfattare och försöker underminera västlig sammanhållning. Än så länge har dock sammanhållningen hållit och den ryska kampanjen verkar ha fått motsatt effekt, i och med att länderna i närområdet nu stärker sina försvarsmakter samt att USA och de stora västmakterna ägnar vårt närområde betydligt mer uppmärksamhet.

Det sårbara Sverige

Efter Krimkuppen framstod Sverige som väldigt illa skyddat och den post-moderna säkerhetsagendan från 00-talet som passé. Nationell säkerhet kunde inte längre tas för given och vi blev smärtsamt varse hot och sårbarheter som vi tidigare struntat i. Det var inte bara det militära försvarets svaghet eller det faktum att Ryssland hade nya vapen. Det var också det civila försvarets obefintlighet och samhällets radikalt ökade sårbarhet för elavbrott, cyberangrepp och andra störningar.

Således behövde den mentala kartan justeras rejält, säkerhetsagendan skrivas om och nya prioriteringar göras. Man skulle kunna säga att Sverige snabbt rasslade ner i Maslowtrappan, från världsförbättrande till att säkra egen säkerhet och överlevnad.

Detta blev mycket tydligt i 2015 års försvarsbeslut och i den process som föregick den. Allmänheten såg kanske mest att försvarsanslagen ökade något och att Gotland återigen skulle försvaras med trupp på plats. Men viktiga styrsignaler var också att begrepp som rikets försvar, suveränitet, krigsduglighet och mobilisering återkom, att operativ förmåga sattes i högsätet, och att värnplikt och totalförsvar skulle återinföras. Hänsyn till behov under krig och beredskap skulle åter tas i samhällsplaneringen.

I början av 2017 presenterade regeringen så en ”nationell säkerhetsstrategi”, utarbetad inom regeringskansliet, i vilken svenska nationella intressen spelade en framträdande roll. Som strategi betraktat, liksom som styrdokument för förvaltningsmyndigheterna, har dokumentet brister i och med att det bitvis ger intryck av en önskelista av saker som ska uppnås, utan inbördes prioritering eller indikation om hur dessa mål ska uppnås. Detta sagt så är ändå strategin den första både officiella och offentliga sammanställningen av svenska nationella intressen.

Svenska nationella intressen

Svensk politik och förvaltning har länge haft ett problematiskt förhållande till begreppet nationella intressen. Begreppet är sprunget ur den ”realistiska” tankeskolan inom internationell politik, en kyligt kalkylerande tradition som sätter egenintresset i högsätet och skyr alla former av idealism. Därför sågs också begreppet som pestsmittat av det utrikespolitiska etablissemanget under de decennier när svensk utrikespolitik skulle formas av progressiva värderingar och fylla en global roll. Trots detta så fortsatte den praktiska politiken i hög grad

präglas av nationella intressen, som den hade gjort sedan tidigt 1800-tal.

Det var nämligen det nationella intresset av att inte hamna i krig med Ryssland som låg bakom den försiktiga neutralitetspolitiken som förts sedan 1812. Likaså var det nationella intresset av att ha en motvikt mot det ryska inflytandet som låg bakom den diskreta – och tidvis mycket hemliga – återförsäkringspolitiken gentemot västmakterna. Det var det nationella intresset som motiverade de avsteg från neutraliteten som höll oss utanför det andra världskriget. Och när den svenska blandekonomiska modellen kraschade så var det behovet av en fungerande ekonomi som plötsligt gjorde EU-medlemskapet till ett nationellt intresse.

En fördel med nationella intressen som analytiskt redskap och ledstång för praktisk politik är att en intresseanalys inte sällan lyfter fram djupstrukturer och andra förhållanden som ofta tas för givna, men som kan behöva omvårdnad för att bestå. Som exempel kan för svensk del nämnas systemet med frihandel och fri sjöfart som är en förutsättning för vårt välstånd, att det finns spärrar mot en åternationalisering av Europeisk säkerhet, och att den amerikanska kärnvapenstödda säkerhetsgarantin till Europa består.

Nationella intressen är således ett användbart begrepp för både bedrivandet av praktisk politik och för analys, men samtidigt är det också på flera sätt problematiskt. Förespråkarna utmålar gärna nationella intressen som objektivt existerande och som närmast oemotsägliga. De kanske de också är, men då bara på en sådan hög abstraktionsnivå att de också blir oanvändbara för att styra policy. För att kunna styra policy behöver man ur dessa grundläggande intressen också härleda svar på *hur* och *med vad* dessa mål ska säkras. Här kommer ofrånkomligen ett mått av subjektivitet in, inte minst eftersom det kan finnas flera alternativa vägar till ett och samma mål.

Ett annat problem är var gränsen mellan värderingar och intressen bör dras. I en del fall verkar det finnas ett mått av överlappning, där för nationens självbild centrala värden eller värderingar också ses som nationella intressen. Samtidigt är det inte ovanligt att värderingar och intressen kommer i konflikt med varandra – att så varit fallet på senare tid är uppenbart, exempelvis vad gäller frågorna om ett globalt kärnvapenförbud, om vapenexport och om svensk politik gentemot arabvärlden.

Slutligen så måste olika nationella intressen kunna vägas mot varandra. Exempelvis kan ekonomiska intressen tala för att köpa rysk gas eftersom den är billig, men säkerhetsintressen kan tala emot. Då måste en rangordning eller en avvägning mellan olika intressen göras. Svaret på sådana frågor kan ofta vara situationsberoende. I ett lugnt läge kan det te sig som rätt problemfritt att säga ja till en rysk gasledning, men om läget är hotfullt kan prioriteringen bli en annan.

Det är bland annat detta fenomen som förklarar omsvängningen i svensk säkerhetspolitik under senare år, med dess kritik av ryskt maktspråk, dess uppvärdering av försvaret och dess betoning av militärt och säkerhetspolitiskt samarbete med grannländerna, USA och Nato – en förändring som av medierna döps till Hultqvistdoktrinen, men som uppenbarligen stöds också av statsministern.

Från önskelista till realistisk strategi

Trots att viktiga steg har tagits de senare åren för att påbörja anpassningen till en mer hotfull och farlig omvärld, inklusive den uppgörelse om försvarsanslagen 2018-2020 som presenterades nyligen, så framstår ännu omställningen som påfallande ofullgången, halvhjärtad, och utan någon större känsla av att det kan vara bråttom. Fortfarande så har en stor del av regeringens nationella säkerhetsstrategi karaktären av en önskelista. Fortfarande så är merparten av våra strukturer, system, tankemönster och attityder formade av de decennier då vi antog att inga större faror fanns. IT-outsourcing till utlandet på Transportstyrelsen och Fortifikationsverket, att Karlskrona kommun satt upp en webkamera som visade när örlogsfartyg löpte in och ut, och Karlshamns vägran att säga nej till den ryska gasledningen, är bara några exempel som visar på att säkerhetsmedvetandet ännu inte är särskilt högt eller att frågorna tas särskilt mycket på allvar. Flera artiklar i denna *Strategisk utblick* lyfter fram möjliga hot mot vår nationella säkerhet och visar att strategierna för att hantera dessa risker fortfarande är få.

Regeringen säger nu att rikets försvar är en prioriterad kärnuppgift för staten och att man satsar på säkerheten. Men trots vissa anslagshöjningar så ligger anslagen till det militära och det civila försvaret fortfarande och hovrar runt en procent av BNP. Inga höjda ambitioner ska finansieras; bara de värsta hålen i 2015 års försvarsbeslut ska fyllas – och detta vid en tidpunkt när statens budget spås gå med rekordöverskott. Vore det på allvar, och vore det bråttom, skulle man väl kunna ha väntat sig något mer?

Nationell säkerhet kostar pengar och nationell säkerhet är jobbigt, i och med att det gör många uppgifter mer komplicerade att lösa. Under de gångna decennierna har Sverige medvetet och omedvetet underfinansierat det militära försvaret och lagt ner det övriga totalförsvaret (se exempelvis artikeln *Försvarsförmågan och försvarsanslaget* i denna publikation. Samtidigt har de säkerhetspolitiska aspekterna av exempelvis elförsörjningen och beroendet av internet inte tagits på allvar, vilket skapat betydande sårbarheter som en angripare kan exploatera i såväl krig som kriser. Idag tycks medvetenheten om den förändrade hotbilden äntligen ha börjat sjunka in, medan finansieringsviljan och förändringsviljan fortsatt dröjer.

Kanske lika viktigt som ökade resurser är att det behövs ett tydligt skifte i svenskt strategiskt tänkande, som till fullo tar höjd för vilka krav som en osäkrare omvärld ställer på det svenska samhället. För att navigera dagens och morgondagens spända geopolitiska läge är det centralt att svenska beslutsfattare har en tydlig bild av vilka Sveriges vitala nationella intressen är, hur dessa vid behov ska vägas mot varandra, samt vilka medel och metoder som är nödvändiga för att kunna slå vakt om dessa.

För vidare läsning

Robert Dalsjö, "Hubris, Nemesis and the Search for Kryptonite: Why Eternal Peace Lasted Only 25 Years", inlägg 19/1 2017 på bloggen *Försvar och Säkerhet* , www.kkrva.se.

Robert Dalsjö, och Thomas Hultmark, "Hur uppnå verkan i kris och gråzon", *Kungl. Krigsvetenskapsakademiens Handlingar och Tidskrift* Nr 2/2017

Robert Dalsjö, *Trapped in the Twilight Zone. Sweden Between Neutrality and Nato,* 2017, Finnish Institute of International Affairs.

Robert Dalsjö, *Brännpunkt Baltikum,* 2016, FOI-R--4278--SE.

Robert Dalsjö, *Nationella intressen och Sverige,* FOI Memo 5470, november 2015.

2. Försvarsförmåga och försvarsanslaget – en avvägning mellan behov och pengar

Peter Nordlund och Mikael Wiklund

I Sverige har det under lång tid funnits en politisk acceptans för en viss risk i försvarsförmåga till fördel för finansiering av andra politikområden. När nu omvärldsläget hastigt försämras minskar snabbt den politiska riskacceptansen. Tidigare politiska beslut och problem med de beräkningar som ska kompensera försvaret för inflation har dock skapat en obalans mellan kraven på militär förmåga och tilldelningen av resurser. Forskningen visar exempelvis att en betydande del av den nu förda ekonomiska politiken på försvarsområdet inte förs på grund av politiska beslut, utan styrs av oavsiktliga och teknisk-ekonomiska begränsningar om vilka den politiska medvetenheten är låg. Det finns därför ett fortsatt högt, omedvetet, politiskt risktagande i försvars- och säkerhetspolitiken. För att minska det politiska risktagandet krävs anslagshöjningar som bättre matchar de politiska ambitionerna men också att kompensationsberäkningarna ses över.

Minskningen av försvarets köpkraft

Försvarsmaktens köpkraft, det vill säga storleken på Försvarsmaktens ekonomiska medel och vad Försvarsmakten kan få för dem, har under lång tid minskat. Köpkraften har minskat med cirka 19 miljarder kronor mellan 1999 och 2014 – sett till den årliga tilldelningen av ekonomiska medel. För att uppnå samma köpkraft 2014 som 1999 skulle Försvarsmaktens anslag ha behövt vara cirka 61 miljarder kronor (jämfört med de faktiska 42).

Ett sätt att förhålla sig till utvecklingen av försvarets köpkraft, utöver att se till tilldelningen av ekonomiska medel, är att relatera försvarsanslagen till andelen av BNP. BNP anger främst vilken (relativ) uppoffring i andel av samhällets resurser som försvarsanslagen utgör i olika länder. BNP-andelen kan vara något missvisande då det inte säger något om de egentliga behoven av militär förmåga och bör normalt inte vara styrande för en anslagstilldelning. Måttet kan däremot vara en lämplig utgångspunkt för att jämföra fördelningen av den ekonomiska bördan i en allians mellan vänner i Europa eller medlemmar i Nato. Detta för att länderna ska bidra i relation till ekonomisk förmåga. Ett exempel på detta är Natos rekommendation att två procent av medlemsländernas BNP ska läggas på försvaret. Förändringar av försvarsutgifterna i absoluta tal över tid ger

troligtvis en bättre bild av den militära förmågeutvecklingen än vad försvarsanslagens andel av BNP kan ge. I tabellen nedan framgår försvarsutgifternas utveckling mellan olika regioner och länder sedan millennieskiftet.

Tabell 1. Försvarsutgifternas utveckling år 2000-2015. Källa: SIPRI. Fasta priser USD.

Område/Land	Försvarsutgifternas utveckling
Världen	+ 55 %
Europa	+ 16 %
Norden (exkl. Sverige)	+ 19 %
Ryssland	+ 216 %
USA	+ 44 %
Sverige	- 14 %

Det svenska försvaret har således sedan millennieskiftet, både i absoluta som relativa ekonomiska medel, fått en kraftigt minskad köpkraft. Utvecklingen av de svenska försvarsutgifterna är en tydlig indikation på en avsevärt försämrad relativ försvarsförmåga.

Anledningarna till den försämrade köpkraften är flera:

För det första har politiska ställningstaganden förändrat Försvarsmaktens uppdrag, och därmed omfattningen av verksamheten. Dessa ställningstaganden går hand i hand med en minskning av de anslag som har tilldelats Försvarsmakten. Detta kan till exempel observeras i budgetpropositioner och efterföljande styrning av Försvarsmakten.

För det andra har köpkraften påverkats av mer tekniska omständigheter som handlar om hur försvarets kostnader utvecklas och hur Försvarsmakten kompenseras för detta. Detta omfattar en blandning av:

- kostnadsutvecklingen rörande försvarets så kallade *insatsvaror* (exempelvis personal, lokaler och materiel)
- hur effektivitet/produktivitet utvecklas i försvaret
- den årliga omräkning av anslagen som sker för att kompensera för hur priserna på insatsvarorna utvecklas.

Pris- och löneomräkning inom försvaret sker med ett eget index – det så kallade Försvarsprisindex (FPI). FPI består av olika officiella och icke-militära index, som ska kompensera Försvarsmakten

för inflation. Syftet med omräkningen är att säkerställa att det är politiska beslut och deras ekonomiska konsekvenser som styr Försvarsmaktens verksamhet snarare än oförutsägbara ekonomiska växlingar såsom fluktuationer i valutakurser eller inflationen i andra länder.

Den problematiska omräkningen och kraven på försvaret

I en ideal situation ska FPI säkerställa att försvaret vare sig över- eller underkompenseras för att marknadspriserna på Försvarsmaktens insatsvaror ändras.[1] Forskning visar dock att FPI kraftigt har underkompenserat Försvarsmakten för pris- och löneförändringar. Cirka hälften av köpkraftsurholkningen mellan åren 1999 och 2014 har berott på underkompensationen. Oavsiktliga ekonomiska begränsningar i hanteringen står alltså för cirka halva den förda ekonomiska politiken på försvarsområdet.

Ett tydligt exempel på pris- och löneomräkningens betydelse kan ses i effekterna av att beräkningsprinciperna i FPI ändrades år 2012. Beräknat på perioden fram till 2015 resulterade denna tekniska förändring i en årlig minskning av anslagen på cirka 1,3 miljarder kronor (sett till 2015). Det motsvarar drygt 6 till 7 miljarder i förlorad finansiering per efterföljande försvarsbeslutsperiod. Försvarsbeslutet 2015 uttryckte den politiska ambitionen att tillföra försvaret drygt 10 miljarder kronor under perioden 2016 till 2020. På grund av den tekniska förändringen av FPI försvinner dock större delen av den politiskt aviserade ekonomiska förstärkningen, vilken i realiteten landar runt endast 3 till 4 miljarder kronor.

Kompensationen och försvarets verkliga förutsättningar har mycket lite gemensamt och det är i slutänden möjligheterna och förmågan till politisk styrning som blir lidande. Ett grundproblem är att FPI utgår från civila officiella index. Detta innebär att Försvarsmaktens tilldelning av resurser, och därmed synen på effektivitet/produktivitet, i stora drag utgår från utvecklingen av priser och effektivitet på de marknader som dessa civila index representerar. Dessutom finns det ett avdrag inbyggt i FPI vilket ska motsvaras av en löpande intern effektivisering i försvarsstrukturerna – det så kallade produktivitetsavdraget. Även detta bygger på en civil konstruktion, produktivitetsutvecklingen i privat tjänstesektor.

Trots att förutsättningarna för produktivitet är sämre på försvarsområdet drabbas ofta Försvarsmakten av dubbla produktivitets- och effektivitetskrav. Detta inträffar när politikerna i anslagsbesluten

1 Undantaget är det inbyggda så kallade produktivitetsavdraget vilka syftar till att skapa ett visst effektivitetstryck på försvaret. Mer om detta längre ner i artikeln.

ålägger Försvarsmakten nya uppgifter utan att skicka med finansiering, med hänvisning till att Försvarsmakten kan finansiera de nya uppgifterna med rationaliseringar. En annan variant är att man minskar anslaget utan att samtidigt minska uppdragen genom att hävda att Försvarsmakten kan genomföra rationaliseringar. Vad politikerna inte alltid tar hänsyn till är det inbyggda produktivitetskravet i FPI. Försvarsmakten får på så sätt två överlagrade produktivitetskrav riktade mot sig, ofta utan inbördes hänsynstagande och då uppstår dubbla produktivitetskrav. Det inbyggda årliga produktivitetskravet har legat på ca 0,9-2,0 procent och motsvarar i antal anställda ca 200-400 kontinuerligt eller 300-400 tidvis tjänstgörande i rationalisering per år – detta ska då ske utan att försvarsförmågan påverkas.

Det finns en mängd orsaker till varför Försvarsmaktens kostnadsutveckling kan avvika från de civila antaganden som omräkningen står för. En särskilt viktig orsak är att försvarsområdet är förknippat med svåra förutsättningar att löpande effektivisera verksamheten. Detta exempelvis på grund av att

- varu- och tjänstesammansättningen i försvaret ser annorlunda ut än för valda index
- exponeringen mot olika valutor skiljer sig åt relativt vad FPI förutsätter
- marknaderna där Försvarsmakten hämtar insatsvaror präglas av monopol och oligopol
- verksamheten präglas av stora fasta kostnader och få möjligheter att byta materielsystem eller personal, vilket leder till en trögrörlighet i att ställa om produktionen
- Försvarsmakten behöver ta hänsyn till politiska förhållanden som lägger restriktioner på dess agerande (exempelvis var i Sverige verksamheten är lokaliserad, vilka materielsamarbeten som kan genomföras med främmande makt, osv).

De centrala skillnaderna utgörs av att Försvarsmakten ofta använder unika resurser för att ta fram lika unika, och ofta svårbedömda, produkter och effekter. Konsekvenserna av att inte leva upp till kravet i bland annat omräkningen kan bli allvarliga. Krympande resurser tvingar Försvarsmakten till neddragningar i verksamheten och i förlängningen en lägre försvarseffekt. Detta är inte intentionen bakom omräkningen.

Ett exempel på skillnaderna mot de civila marknaderna som försvaret jämförs med är kostnadsutvecklingen på försvarsmateriel. Forskning tyder på att det sker en mycket snabb kostnadsutveckling

för försvarsmateriel i förhållande till den allmänna prisutvecklingen. En försiktig uppskattning pekar på en ökningstakt med cirka tre till fyra procent utöver konsumentprisindex. Detta innebär att beståndet av försvarsmateriel, med dagens storlek på försvarsorganisationen, kommer att minska snabbt om anslagen endast ökar i takt med den allmänna prisutvecklingen. Anslag som endast justeras i takt med den allmänna inflationen gör det därför omöjligt att bibehålla en oförändrad materielstock och storlek på insatsorganisationen.

Ett underfinansierat försvarsbeslut?

Försvaret har under lång tid fått en successivt minskad förmåga genom minskade ekonomiska resurser. Försvarsbeslutet 2015 utgjorde dock ett trendbrott då det för första gången på ett kvartssekel gav uttryck för höjda försvarsutgifter och ökad köpkraft. Problemet är att utgångsläget inför beslutet 2015 var en långsiktig underfinansiering av föregående försvarsbeslut på cirka 4 till 6 miljarder kronor[2] (sett till årlig anslagsnivå).

Risken för att försvarsbeslutet 2015 var underfinansierat, i förhållande till den politiska ambitionen som uttrycktes, var stor. Detta berodde dels på ovanstående ”skuld” från föregående försvarsbeslut, dels på att det var osäkert om ambitionshöjningarna var fullt ut finansierade och dels på att risken att den bristfälliga omräkningsmekanismen FPI fortsatte vidga gapet genom strukturell underkompensation.

Överbefälhavaren har, i samband med budgetunderlaget för 2018, pekat på ytterligare behov av drygt sex miljarder kronor under innevarande försvarsbeslutsperiod. Detta behov beror framför allt på de okompenserade prishöjningarna. En del av dessa kommer av valutaeffekter knutna till anskaffningsbeslut såsom JAS 39 Gripen E. Uttalandet kan ses som en indikation på att så länge som FPI inte följer Försvarsmaktens faktiska pris- och kostnadsutveckling riskerar alltid den ekonomiska resurstilldelningen att hamna på efterkälken och därmed aldrig komma ifatt behovet. Politikerna kommer således fortsatt att behöva leva med valet mellan att konstant skjuta till extra medel till Försvarsmakten eller att Försvarsmaktens leveranser aldrig motsvarar den politiska beställningen. En ny försvarsöverenskommelse träffades också underhand, i augusti 2017. Den täcker den brist, under den resterande delen av försvarsbeslutsperioden fram till år 2020, som Försvarsmakten flaggade för i budgetunderlaget. Detta förbättrar den kortsiktiga situationen men löser inte grundproblemen som en lång period av försämrade ekonomiska förutsättningar har skapat. Samtidigt riskerar FPI också att skapa nya hål i försvarsanslagen genom fortsatt underkompensation.

2 Fasta, inflationsjusterade, priser.

Försvarets resurser – en fråga om risktagande

Politiskt beslutfattande rörande försvarets ekonomiska resurser handlar i slutändan om ett val av nivå på risktagande. Säkra kostnader, det vill säga de medel som tilldelas försvaret, måste ställas mot osäkra kostnader – "kostnaden" för att inte kunna hantera allvarliga framtida hot eller händelser. Vilka risker är acceptabla i förhållande till vad politiken är villig att betala? Problemet ligger i att militär förmåga måste byggas upp innan allvarliga händelser sker för att vara meningsfull. Det betyder att politikerna måste avdela resurser för att hantera – ofta svåranalyserade och hypotetiska – *potentiella* hot och risker på bekostnad av *reella* behov på andra politikområden. Lockelsen i att underskatta risker, och på så sätt frigöra resurser till annat, är uppenbar. Liknelsen med en hemförsäkring är tydlig. Den tecknas därför att det *kan* komma att brinna, men försäkringspremien som måste betalas tar resurser från faktiska och omedelbara behov.

Den politiska kalkylen, och därmed risktagandet, handlar om hur stora konsekvenser av allvarliga händelser som kan accepteras relativt hur stora resurser som riskminskning får kosta.

Idealet är att denna process av prioritering och risktagande är en medveten process vilken är underkastad explicita politiska beslut. Om försvarets köpkraft minskar så ska det vara en funktion av att politikerna anser att a) riskerna har minskat; eller b) att man är villig att ta större risker. Forskning visar dock att stora delar av det verkliga beslutsfattandet är överlämnat till automatiska tekniska mekanismer för omräkning av anslagen. Stora delar av det politiska risktagandet ligger alltså utanför direkt politisk och parlamentarisk kontroll. När detta dessutom tenderar att systematiskt underkompensera relativt den faktiska pris- och kostnadsutvecklingen inom försvaret så blir följden att risktagandet överstiger de uttalade politiska avsikterna. Det borde därför vara angeläget att förutom att höja anslagsnivån också se över konstruktionen av pris- och lönekompensationen i FPI i syfte att göra den mer följsam till den faktiska pris-, kostnads- och löneutvecklingen i försvaret.

Bristande försvarsförmåga innebär att politikerna måste räkna med att risker manifesteras i oönskade händelser i en högre utsträckning samtidigt som dessa händelser blir allvarligare. Även om det är svårt att sätta en prislapp på detta så är det att betrakta som en kostnad (i värsta fall även en nationellt existentialistisk sådan) vilken över tid kommer att behöva betalas. Kostnader för hantering av en försvarsrelaterad risk sker i termer av kronor och statsbudget. Kostnader för att lämna en sådan risk utan åtgärd sker i termer av minskad politisk handlingsfrihet, minskat inflytande för demokratiska fri- och rättigheter, svagare internationellt system,

hot mot nationell existens och tillkortakommanden rörande medborgarnas liv och hälsa. Om kostnaden för riskhantering understiger kostnaden för att lämna risker icke-adresserade är det samhällsekonomiskt rationellt att omfördela medel till en ökad försvarsförmåga. Denna värdering måste kunna göras trots att kostnadsposterna skiljer sig år.

Till syvende och sist handlar det försvarsekonomiska vägvalet om att få krav på förmåga och tilldelning av ekonomiska medel att gå i takt. Historiskt har det funnits en tendens till att resurserna släpar efter cirka ett försvarsbeslut sett till ambitionen. Även denna gång står det klart att en anslagsförstärkning kommer att behövas, kanske redan under innevarande försvarsbeslutsperiod trots att de nyligen tillskjutna medlen förbättrat Försvarsmaktens ekonomiska situation. Framförallt behövs en rejäl anslagsförstärkning i nästa försvarsbeslut för åren 2021 till 2025. Annars är det osannolikt att politikerna får den försvarsförmåga den tänkt sig, med de politiska riskerna det innebär.

För vidare läsning

Peter Nordlund, Erik Lundberg och Bernt Öström, *Mindre försvarsmateriel och organisation för pengarna,* 2016, FOI-R--4250--SE

Peter Nordlund, Peter Bäckström, Karsten Bergdahl och Janne Åkerström, *Försvarsmaktens ekonomiska förutsättningar* 2014, FOI-R--3901--SE

Peter Nordlund, Janne Åkerström, Bernt Öström och Helge Löfstedt, *Kostnadsutvecklingen för försvarsmateriel*, 2011, FOI-R--3213--SE.

3. Östersjöområdet – en ny geopolitisk brännpunkt

Mike Winnerstig

Östersjöområdet har hamnat i geopolitiskt fokus. De baltiska länderna är små och svårförsvarade, och även en begränsad attack mot dem skulle innebära att Ryssland skulle kunna splittra Nato och utmana det amerikanska ledarskapet globalt. Sannolikheten för detta är låg, därför att riskerna för Ryssland är höga. Detta särskilt sedan Nato våren 2017 började framgruppera allierade förband till de baltiska länderna och Polen. Styrkorna omfattar inte mer än en bataljonsstridsgrupp per land, men utgör en effektiv "snubbeltråd" mot ryskt agerande. Sveriges centrala placering i Östersjöområdet kommer naturligen dra in vårt territorium i en eventuell konflikt. Att förstå hur den geopolitiska dynamiken fungerar i vårt grannskap bör därför vara av högsta vikt för svenska beslutsfattare.

Östersjöområdet i strategiskt fokus

Sveriges närområde, särskilt Östersjöländerna, har de senaste åren hamnat i ett militärstrategiskt fokus. Detta utgör en skillnad mot situationen under det kalla kriget, där brännpunkten var centralfronten mitt i det numera enade Tyskland. Östersjöområdet saknade inte dramatik för svensk del även under denna period, men geopolitiskt var det något av ett bakvatten.

Idag är Östersjöområdet snarare en brännpunkt för den ökande konfrontationen mellan Ryssland och västvärlden. Den främsta grunden till detta är den ryska aggressionen mot Georgien 2008 och Ukraina 2014 och framåt vilken tjänstgjort som alarmklockor för alla mindre länder i Rysslands närområde, inklusive Sverige och Finland. Till detta kommer den informationskrigföring som Ryssland länge bedrivit särskilt mot de baltiska staterna. Ryska aktörer har i destabiliseringssyfte spridit budskap bland annat om att de baltiska länderna inte är trovärdiga som stater, att deras politiska etablissemang ägnar sig åt förföljelser av de rysktalande minoriteterna, och att de har ett "fascistiskt" förflutet som avspeglar sig i deras politik idag. Detta bidrar till bilden av en rysk revanschism i närområdet som, tillsammans med den betydande ryska militära upprustningen de senaste tio åren, väcker farhågor om framtida ryskt militärt agerande.

Brännpunkt Baltikum

De baltiska staterna är små både till yta och befolkning, saknar strategiskt djup och har begränsade försvarsmakter utan eget flygvapen. Detta gör dem till de potentiellt mest utsatta av de Nato-allierade staterna om den ryska geopolitiska revanschismen skulle ta sig nya uttryck. Vore Ryssland på allvar villigt att utmana västvärlden och det amerikanska globala ledarskapet militärt skulle detta enklast kunna ske genom en begränsad attack mot en del av något baltiskt land.

Ett sådant agerande skulle ställa USA och övriga Nato-medlemmar inför valet att antingen aktivt inleda ett krig mot Ryssland – vilket teoretiskt sett relativt snart skulle kunna övergå till ett kärnvapenkrig i någon form – eller att gå Ryssland till mötes genom någon form av förhandlingslösning. Det senare alternativet skulle effektivt underminera USA:s ledarskap över hela världen och med stor sannolikhet också leda till en upplösning av Nato eftersom alliansen då misslyckats med sin huvuduppgift: att försvara ett medlemslands territorium. I många västliga huvudstäder framstår inget av dessa alternativ som aptitligt.

Helhetsbilden är dock inte så dyster som den initialt kan verka. Sannolikheten för att Ryssland utan provokation skulle vilja riskera att gå i krig mot hela västvärlden är inte särskilt stor. Militärgeografin är relativt gynnsam för de baltiska staterna; mycket av gränslandet mot Ryssland och Vitryssland består av sjöar, träsk och liknande terräng som är relativt lättförsvarad om det finns gripbara markstridsförband i området. De baltiska länderna har därtill gjort stora försvarssatsningar de senaste åren. Estland lägger sedan länge något mer än 2 procent av BNP på försvaret och både Lettland och Litauen kommer att ha uppnått denna nivå senast 2018. I Estland och Litauen planeras för närvarande för arméstridskrafter om två brigader vardera, vilket är samma nivå som det svenska försvaret inriktar sig mot. Kvarstår gör dock det faktum att ingen av de baltiska staterna klarar sig själva mot en rysk motståndare under någon längre tid. Att lösa sitt försvarsproblem genom integration i både EU och Nato har därför varit en självklar lösning för de baltiska länderna ända sedan de återtog sin självständighet för mer än 25 år sedan.

USA och försvaret av Östersjöområdet

USA är i ett Östersjöperspektiv den enda västliga makt som på allvar kan balansera en rysk militär revanschism. Detta förhållande har inte alltid varit tydligt i Washington, DC. Alla amerikanska presidenter från det kalla krigets slut och

framåt har inlett sina mandatperioder med att säga sig vilja skapa en bättre relation till Ryssland. Ett särskilt tydligt exempel var Barack Obama, som initierade den så kallade återställningspolitiken gentemot Ryssland 2009 – trots att rysk militär året innan militärt ockuperat stora delar av det lojala amerikanska partnerlandet Georgiens territorium. Så sent som 2012 fattade Obama beslut om att halvera antalet permanent stationerade amerikanska armébrigader i Europa, och att dra bort USA:s alla tunga stridsvagnar från kontinenten. Det ryska agerandet under senare år – särskilt vad gäller Ukraina 2014 – gjorde Ryssland ånyo till en strategisk motståndare till USA i Obama-administrationens ögon. Att Trump-administrationen från 2017, särskilt president Donald Trump själv, har en explicit agenda för att förbättra relationen till Ryssland är i detta ljus bara en variant av ett tidigare mönster.

Trumps politiska ambition har dock redan nu överflyglats av de militära realiteterna. Det amerikanska försvarsdepartementet implementerar fortfarande de planer som Obama-administrationen fattade beslut om vad gäller att förstärka försvaret av de mest utsatta europeiska allierade. Inom ramen för *European Reassurance Initiative* (ERI) görs nu märkbara militära framflyttningar av amerikansk trupp och materiel. Syftet är inte bara att återförsäkra de europeiska allierade staterna om amerikanskt stöd, utan också att aktivt avskräcka Ryssland för att agera militärt mot något Nato-land. Det amerikanska Europakommandot har återfått tunga förband, inklusive stridsvagnar, som samtränar med och bygger upp förmåga hos både de baltiska länderna och Polen. EUCOM har också återfått statusen som ett ”krigförande” kommando, efter att under lång tid sedan det kalla krigets slut huvudsakligen haft understödjande uppgifter.

Under Obamas sista år fyrdubblades de finansiella satsningarna på ERI. I Trump-administrationens första budget för 2018 föreslås att de ska öka med ytterligare 40 procent. Det är alltså fullt möjligt att hävda att även om presidentens retorik är anmärkningsvärt Rysslandsvänlig, så går Pentagons resurser dit de geopolitiska problemen finns. För Europas del innebär det Östersjöområdet.

Det finns flera orsaker till detta. Den mest uppenbara är att ett framgångsrikt ryskt utmanande av Nato och Nato-fördragets artikel 5 (om gemensamt försvar) kraftfullt skulle underminera amerikanskt globalt ledarskap. Den andra är att centrala aktörer i Trump-administrationen – som försvarsminister James Mattis, utrikesminister Rex Tillerson och den nationelle

säkerhetsrådgivaren H.R. McMaster – inte är naiva vad gäller Ryssland utan gör realistiska, geopolitiska analyser av landets agerande och vilka amerikanska motdrag som behövs.

President Trumps egen inställning i frågan är i dagsläget oklar. Han har uttalat betydande förståelse för Ryssland, särskilt dess president Vladimir Putin, samtidigt som han riktat stark kritik mot de europeiska Nato-allierade för deras bristfälliga satsningar på sina försvarsmakter. Han har dock inte minskat de amerikanska militära satsningarna på Europa och försvaret av små europeiska stater mot potentiell rysk aggression – tvärtom föreslår han som sagt att den amerikanska budgeten för detta ökas. Det går att tolka hans kritik mot de europeiska Nato-allierade som en del av ett förhandlingsspel, där Trump genom sin relativa ovilja att uttala villkorslöst stöd för Nato-alliansen som sådan, vill tvinga de europeiska länderna att öka sina försvarsutgifter. De flesta Nato-länder betalar idag klart mindre än de 2 procent av BNP som alliansen – när Obama var president – definierat som en miniminivå. Trumps retorik och kritik bör därför möjligen i mindre utsträckning ses som en del av hans Rysslandssyn och mer som en ny amerikansk strategi för att öka försvarssatsningarna i Europa, vilka i många fall är inriktade just på att möta en möjlig rysk aggression.

Nato och enhanced Forward Presence

I kontrast mot det kalla krigets situation är en majoritet av strandstaterna runt Östersjön Nato-medlemmar, och därmed delaktiga i alliansens gemensamma försvarsplanering. Under lång tid efter de baltiska ländernas officiella upptagande i Nato-kretsen 2004 genomförde Natos militära strukturer ingen försvarsplanering för dessa länder. Det dröjde ända fram till 2010 innan Nato som helhet började ta Östersjöområdet på allvar ur ett militärstrategiskt perspektiv. Man utvidgade då den befintliga försvarsplaneringen för Polen – som blivit Nato-medlem 1999 och då både krävt och fått sådan planering – till de baltiska staterna. Detta var kontroversiellt inom alliansen vid denna tid, eftersom flera inflytelserika Nato-länder initialt var helt emot att en sådan planering skulle genomföras. Motivet var att det automatiskt skulle utmåla Ryssland som den enda tänkbara fienden, vilket tyska och andra befattningshavare ansåg skulle provocera Ryssland i onödan.

Efter Rysslands aggression mot Ukraina och den illegala annekteringen av Krim 2014 blev det emellertid enklare att argumentera för att det inte bara behövdes planer utan reella resurser till de nya så kallade ”frontstaterna” – främst de baltiska länderna och Polen. Vid Natos toppmöte i Warszawa

2016 beslöts därför att en *enhanced Forward Presence* (eFP) skulle inrättas. Detta innebar att allierade förband under längre perioder skulle baseras i ”frontstaterna”, för att genom sin närvaro och sin faktiska stridsförmåga utgöra ett väsentligt bidrag till dessa länders försvar. Konceptet operationaliserades till en manöverbataljon per land, plus stödförband från ytterligare Nato-länder. Man beslöt dessutom att implementera detta relativt fort, med början redan tidigt 2017.

Under sommaren 2017 har konceptet materialiserats i alla frontstaterna. I Estland har en brittisk tung infanteribataljon grupperats, tillsammans med ett franskt mekaniserat infanterikompani. I Lettland finns nu en kanadensisk motoriserad infanteribataljon, ett spanskt mekaniserat infanterikompani och ett polskt stridsvagnskompani, tillsammans med mindre understödsförband från Italien, Slovenien och Albanien. I Litauen har Tyskland baserat en mekaniserad infanterbataljon, som understödjs bland annat av ett norskt infanterikompani och enheter från den nederländska armén. I Polen har USA baserat en bataljonsstridsgrupp från den motoriserade brigad som USA har permanent baserad i Tyskland. Därutöver bidrar även Storbritannien och Rumänien med moderna stridande enheter inom ramen för den polska delen av eFP.

Totalt deltar nu mer än ett dussin Nato-länder i det direkta försvaret av de baltiska länderna och Polen. Truppstyrkan rör sig om drygt 1100 soldater per land, vilket innebär att hela insatsen omfattar ungefär en brigads storlek (knappt 4500 man). Ur militär synvinkel är detta givetvis mest ett så kallat snubbeltrådsförband. Med detta menas att styrkan inte är tillräckligt stor för att ensam kunna avvärja ett militärt anfall från en stormakt av Rysslands typ, men i händelse av ett sådant anfall kommer angriparen att direkt hamna i krig med halva Nato samtidigt och indirekt med hela västvärlden. Den avskräckande effekt som får anses ligga i detta torde kunna betraktas som mycket stor. Att styrkan inte är större än en bataljonsstridsgrupp per land, innebär också att det inte går att hävda att den skulle kunna få offensiva uppgifter. Till det är den alldeles för liten.

Givet de militärgeografiska realiteterna och de växande baltiska försvarsmakterna kan emellertid styrkorna efter erforderlig samträning också direkt bidra påtagligt till de baltiska ländernas försvar. Beroende på förvarningstiden och på hur stora resurser som en angripare skulle avdela, kan de baltiska och polska försvarsmakterna – tillsammans med de allierade förbanden –

agera som en reell bromskloss också mot ett substantiellt ryskt militärt angrepp. Som ytterligare resurser har Nato också sedan tidigare inrättade snabbreaktionsstyrkor, exempelvis *NATO Response Force* (NRF) och *Very High Readiness Joint Task Force* (VJTF). NRF (maximalt 40 000 soldater) och VJTF (runt 5000 soldater) är inte permanent baserade någonstans utan sätts ihop efter beslut i särskilt ordning.

Genom dessa åtgärder kan Nato ha hittat en rimlig balans mellan avskräckning och provokation. Ryska företrädare och rysk media utmålar dock hela processen som destabiliserande för regionen, vilket i huvudsak torde bero på att den minskar den ryska handlingsfriheten vad gäller militärt agerande.

Konsekvenser för Sverige

Sverige har i relativt bred politisk enighet de senaste två decennierna successivt ersatt sin traditionella neutralitetspolitik med en solidaritetspolitik, som Försvarsberedningen kallar det. Sverige är inte med i någon militär allians men har förpliktelser – av ännu inte helt definierat slag – till alla EU-länder genom EU:s Lissabonfördag (artikel 42:7), och har dessutom sedan 2009 uttalat en så kallad solidaritetsförklaring till alla EU- och nordiska länder. Varje tänkbar militär konflikt i Östersjöområdet innebär också att svenskt territorium kommer att bli mycket eftertraktat av de krigförande parterna, särskilt vad gäller operationer i Baltikum.

Allt detta innebär att även Sverige med all sannolikhet mycket fort skulle dras in i konfliktförloppet. Det säkerhetspolitiska läget i Östersjöområdet har idag fler likheter med det kalla kriget än någonsin efter 1991, men utan någon stark ideologisk dimension. Geopolitiskt och militärstrategiskt har däremot konfliktens brännpunkt kommit avsevärt närmare Sverige. Detta är något som svenska beslutsfattare och det svenska försvaret nu tvingas att hantera. En god insikt i den geopolitiska dynamiken i vårt grannskap är en nödvändig grund för detta.

För vidare läsning

Robert Dalsjö, *Brännpunkt Baltikum*, 2016, FOI-R--4278--SE.

Fredrik Lindvall, Mike Winnerstig, *Väpnad solidaritet - USA:s militära närvaro i Europa fram till 2020*, 2017, FOI-R--4428--SE.

Mike Winnerstig (ed.), *Tools of Destabilization. Russian Soft Power and Non-military Influence in the Baltic States*, 2014, FOI-R--3990--SE.

4. Tyskland – en ny bundsförvant för Sverige i Europa?

Eva Hagström Frisell och Anna Sundberg

Tysklands betydelse för Sverige och säkerheten i svenskt närområde har ökat under de senaste åren. Tyskland och Sverige har även visat ett nytt intresse för att fördjupa sitt bilaterala försvarssamarbete. Förutsättningarna för ett fördjupat försvarssamarbete är vid en första anblick goda. En analys av de säkerhetspolitiska inriktningsdokument som länderna nyligen har antagit visar dock på grundläggande skillnader i synen på hur den nationella säkerheten bäst ska främjas. Tyskland och Sverige har därtill olika roller att spela i Europa. Medan Tyskland utgör en centralt placerad stormakt som spelar en framträdande roll inom europeisk säkerhetspolitik är Sverige en medelstor stat med ett mer regionalt fokus på säkerhet och stabilitet.

Nya förutsättningar för samarbete

På grund av det försämrade säkerhetsläget i närområdet och de utmaningar som idag finns mot sammanhållningen i Europa befinner sig både Tyskland och Sverige på jakt efter nya samarbetspartners.

Tyskland har länge varit Europas ekonomiska stormakt, men har under senare tid även klivit fram som en av Europas säkerhetspolitiska ledare. Det finns gott om utmaningar som måste hanteras och omvärldens förväntningar på ett tyskt ledarskap har ökat efter den ryska aggressionen mot Ukraina, men också efter valet av Donald Trump i USA och Brexitomröstningen i Storbritannien. Därtill är Europas traditionella stormakter när det gäller försvar och säkerhet – Storbritannien och Frankrike – i hög grad upptagna med annat. Storbritannien måste hitta sin roll utanför EU och kämpar samtidigt med landets interna sammanhållning medan Frankrike framför allt är inriktat på terrorismhantering både på hemmaplan och internationellt.

Sedan ett par år finns det även en ökad vilja från den tyska regeringen att svara upp mot förväntningarna utifrån. Att Tyskland är redo att ta ett större ansvar för internationell säkerhet är ett återkommande budskap i politiska deklarationer och avspeglas även i handling. Ett exempel är att Tyskland har tagit ledningen för den bataljonsstridsgrupp som inom ramen

för Natos framskjutna närvaro placerats i Litauen. Ur ett tyskt perspektiv handlar det emellertid om ett ansvarstagande inom vissa ramar och det tyska engagemanget får inte riskera att uppfattas som alltför dominant. Den tyska säkerhets- och försvarspolitiken fortsätter därför att utformas i nära samarbete med andra och det är Nato och EU-samarbetet som utgör den tyska säkerhets- och försvarspolitikens grundpelare.

Även Sverige har ett starkt intresse av att bidra till stabilitet och säkerhet, särskilt i närområdet, och under de senaste åren har den nationella försvarsfrågan hamnat högre upp på den politiska dagordningen. Men tvärtemot de tyska beslutsfattarna fortsätter den svenska regeringen att hänvisa till den militära alliansfriheten som en viktig princip och utesluter såväl ett Nato-medlemskap som ett fördjupat säkerhets- och försvarspolitiskt samarbete inom EU. Istället fokuserar Sverige på att stärka de bilaterala samarbetena med andra stater. Relationen till USA intar en särställning. Därutöver har Sverige lagt särskild vikt vid att utveckla det operativa militära samarbetet med Finland. Den svenska solidaritetsförklaringen omfattar därtill alla medlemsländer i EU samt de nordiska länderna. Bland dessa har Sverige ambitionen att främst utöka samarbetet med de övriga nordiska och baltiska länderna. Bilaterala samarbetsavtal på försvarsområdet har dessutom slutits med Storbritannien och Polen.

Precis som Tyskland påverkas Sverige av de förändrade säkerhetspolitiska förutsättningarna. Sverige måste ersätta Storbritannien som nära partner inom EU och kan komma att behöva en annan säkerhetspolitisk bundsförvant än USA. Den politiska och ekonomiska stormakten Tyskland ligger då nära till hands. Den svenska regeringen har också uttryckt att Tyskland spelar en viktig roll för stabiliteten i svenskt närområde och ser därmed en direkt koppling mellan just Tyskland och svensk säkerhet. Under 2016 inledde Sverige och Tyskland en diskussion om ett fördjupat försvarssamarbete och i juni 2017 undertecknade ländernas försvarsministrar en gemensam avsiktsförklaring om samarbete. Ur ett säkerhetspolitiskt perspektiv kan dock inte ett samarbete med Tyskland ge samma tyngd som relationen med de militära stormakterna USA och Storbritannien, vilka har en större förmåga att agera militärt i svenskt närområde.

Nyligen definierade nationella intressen

Tyskland och Sverige har nyligen definierat sina respektive nationella intressen, vilka återfinns i Tysklands och Sveriges säkerhetspolitiska inriktningsdokument. Tyskland presenterade

i juli 2016 en ny vitbok för tysk säkerhetspolitik och framtida inriktning av försvarsmakten och i januari 2017 lade den svenska regeringen fram en nationell säkerhetsstrategi.[3] Att definiera nationella intressen på detta sätt har tidigare varit politiskt känsligt och det har i båda länderna funnits en ovilja att positionera sig och låsa fast sig i dessa frågor.

Även om de två dokumenten skiljer sig åt i karaktär och omfång så ger de ledtrådar om förutsättningarna för ett fördjupat bilateralt samarbete. Båda dokumenten är antagna av regeringen, vilket ger dem en större tyngd och relevans än om de hade varit en produkt från respektive försvarsdepartement. Att Tysklands tre största partier står bakom dokumentet ökar vidare sannolikheten för att inriktningen håller över tid. Den tyska vitboken arbetades dessutom fram genom en inkluderande process som erbjöd delar av samhället en möjlighet att bidra. Syftet var att förankra och förklara tysk säkerhetspolitik och bidra till debatt.

I Sverige sker vanligen den bredare politiska förankringen av säkerhets- och försvarspolitiken inom ramen för Försvarsberedningens arbete. Den svenska säkerhetsstrategin togs däremot fram inom regeringskansliet utan direkta förhandlingar med oppositionen. Statsminister Stefan Löfven har dock uttryckt en förhoppning om att den nationella enighet som brukar finnas kring svensk säkerhetspolitik också ska gälla implementeringen av den nya strategin. Ministrar och statssekreterare inom det nyligen inrättade Säkerhetspolitiska rådet ska ha ett särskilt ansvar för att följa upp strategin.

Samsyn kring hot och säkerhet

De nationella inriktningarna har således tagits fram på olika sätt, men dokumenten uppvisar lika fullt många likheter. Tyskland och Sverige företräder båda en bred syn på säkerhet. Detta återspeglas i att den nationella säkerheten betraktas som en angelägenhet för hela samhället, men också i att de identifierade säkerhetsutmaningarna spänner över ett brett spektrum.

Tyskland och Sverige delar även många geostrategiska förutsättningar och dessa likheter återspeglas i deras respektive hotupplevelse. Båda länderna målar i dokumenten upp en

3 Die Bundesregierung, *Weissbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr (*dokumentet finns även i engelsk översättning: *White Paper 2016 On German Security Policy and the Future of the Bundeswehr*) och Regeringskansliet, Statsrådsberedningen, *Nationell säkerhetsstrategi,* januari 2017.

likartad bild av den säkerhetspolitiska utvecklingen i Europa. Det talas om ett försämrat säkerhetsläge där Ryssland utmanar den rådande säkerhetsordningen samtidigt som Europa står inför betydande interna utmaningar och dess södra grannskap präglas av konflikter.

De identifierade säkerhetsutmaningarna är också i stor utsträckning desamma i de båda länderna, även om det i praktiken förekommer skillnader i den nationella säkerhetspolitiska debatten. Tyskland har redan sedan flera år haft ett större fokus på terrorism, vilket nu även blivit en central fråga i Sverige. Den svenska nationella debatten har i större utsträckning än den tyska fokuserat på det ryska hotet i närområdet. I båda dokumenten presenteras dock en bred lista av utmaningar och hot som spänner från incidenter med militära maktmedel, påverkansförsök, cyberattacker och terrorism till organiserad brottslighet, klimatförändringar och pandemier. Bägge länderna betonar därtill vikten av bevarandet av en stark transatlantisk länk och USA:s betydelse för europeisk säkerhet samtidigt som de uttalar sitt stöd för en stärkt integration i Europa.

En direkt jämförelse av de nationella intressen som finns uppräknade i de respektive dokumenten visar att de dessutom i stort sett är desamma i de två länderna. På två viktiga punkter skiljer de sig dock åt (se tabellen nedan). För det första lyfter den tyska vitboken fram en stark tysk ekonomi och en fri världshandel som ett eget säkerhetsintresse, medan motsvarande skrivningar i den svenska strategin kopplas till främjandet av en regelbaserad multilateral världsordning. För det andra inkluderar de tyska säkerhetsintressena skyddet av allierade och ett starkt transatlantiskt samarbete. I den svenska strategin anses istället främjandet av stabilitet och säkerhet i närområdet vara av nationellt intresse.

Tysklands säkerhetsintressen	Sveriges nationella intressen
• Skydd av befolkningen, suveräniteten och den territoriella integriteten i Tyskland • Skydd av befolkningen, suveräniteten och den territoriella integriteten hos allierade • Vidmakthållande av den rättsbaserade världsordningen • Säkerställande av befolkningens välstånd genom en stark tysk ekonomi och en fri världshandel • Främjandet av ett ansvarsfullt användande av bristvaror och knappa resurser • Fördjupad europeisk integration • Konsolidering av det transatlantiska partnerskapet.	• Att tillgodose invånarnas trygghet, säkerhet och hälsa • Att säkra försörjning och skydd av samhällsviktiga funktioner • Att upprätthålla grundläggande värden: demokrati, rättsstat, mänskliga fri- och rättigheter • Att under alla omständigheter försvara Sveriges frihet, säkerhet och rätt till självbestämmande • Att främja stabilitet och säkerhet i vårt närområde • Att samarbete, solidaritet och integration inom EU bevaras och stärks • Att främja en regelbaserad multilateral världsordning.

Avgörande skillnader i prioriterade samarbeten

En samsyn kring vad som hotar och utmanar samt behovet av ett helhetsgrepp för att ta sig an dessa utmaningar ter sig som en bra grund för ett fördjupat bilateralt samarbete mellan Sverige och Tyskland. Vid en djupare analys framträder emellertid uppenbara olikheter. Den stora skillnaden ligger i prioriteringarna mellan olika säkerhets- och försvarspolitiska samarbeten. För Tyskland har Nato och EU högsta prioritet, medan Sverige snarare betonar bilaterala försvarssamarbeten.

Tysklands säkerhet är nära sammanbunden med dess allierade inom Nato. Försvaret av allierades territorium framhålls i vitboken som ett centralt säkerhetsintresse. Nato är dessutom det viktigaste ramverket för många bilaterala tyska initiativ. Genom att ta ledning som ramnation (*Framework Nation*) söker Tyskland knyta till sig andra länder som bilateralt integrerar styrkor eller förmågor i den tyska försvarsmakten. Tyskland ser det därutöver som sin uppgift att driva på ett fördjupat säkerhets- och försvarspolitiskt samarbete inom EU; det långsiktiga målet beskrivs som en försvarsunion. Tyskland har uttryckt sitt stöd för att tillsammans med en mindre grupp länder skapa ett så kallat permanent strukturerat samarbete på

försvarsområdet (*Permanent Structured Cooperation, PESCO*), vilket framförallt syftar till att skapa en ny grund för initiativ och samarbetsprojekt för att främja förmågeutveckling i EU-länderna.

Den svenska regeringen har understrukit att det inte är aktuellt för Sverige att gå med i Nato. Försvarsminister Peter Hultqvist har varit tydlig med att en ansökan om ett medlemskap skulle få långtgående konsekvenser för inrikespolitiken, grannlandet Finland och stabiliteten i närområdet. Samtidigt har partnerskapet med Nato gradvis utvecklats och 2016 ratificerade riksdagen det så kallade värdlandsavtalet, vilket reglerar möjligheterna för Natos medlemsländer att verka på svenskt territorium. Sverige delar inte heller Tysklands vision för det europeiska försvarssamarbetet och har ställt sig tveksam till flera av de initiativ som Tyskland har stått bakom. För den nuvarande svenska regeringen tycks EU främst ses som ett forum för utrikes- och säkerhetspolitiskt samarbete och i mindre utsträckning ett försvarspolitiskt verktyg.

Möjligheter till ett fördjupat samarbete

En jämförelse av Tysklands och Sveriges nya inriktningsdokument ger få konkreta detaljer om möjliga samarbetsområden. På ett övergripande plan indikerar de allmänt hållna formuleringarna en samsyn mellan länderna vad gäller hot och säkerhet. Trots att denna typ av dokument sällan brukar vara positionerande pekar de emellertid på avgörande skillnader mellan länderna vad gäller prioriterade säkerhetspolitiska samarbeten.

Medan den svenska nationella säkerhetsstrategin identifierar Tyskland som en viktig partner, saknas i den tyska vitboken en motsvarande skrivning om Sverige. Detta innebär dock inte att Tyskland är negativt inställd till bilaterala samarbeten i sig. Under senare år har Tyskland initierat en rad militära samarbeten med stater i Europa, till exempel med Nederländerna, Polen, Norge, Tjeckien och Rumänien. Ur ett svenskt perspektiv kan det dock vara problematiskt att dessa samarbeten framför allt sker i en multilateral kontext och då främst inom Nato. För Tyskland utgör dessa samarbeten en viktig arena för att legitimera stormaktsrollen, men de är också betydelsefulla för att säkerställa tillgången till olika förmågor.

Sverige och Tyskland delar flera brister i den militära förmågan. Båda länderna har under lång tid minskat försvarsutgifterna och de höjningar som nu är föreslagna är långt ifrån tillräckliga för att överkomma bristerna på egen hand. De har problem med personaluppfyllnad, tillgänglighet till materiel samt låg

beredskap och begränsad övningsverksamhet i förbanden. Dessa kapacitetsluckor skulle kunna utgöra en möjlig grund för samarbete. Det kan handla om fördjupat operativt samarbete i Östersjöområdet eller vid internationella insatser, men även om gemensam förmågeutveckling vad gäller materiel eller övningar.

Avslutningsvis är framtidsutsikterna för ett närmare samarbete mellan Tyskland och Sverige också avhängiga utvecklingen i Europa och resten av världen. Flera faktorer – däribland resultatet av Brexit-förhandlingarna, utvecklingen av president Trumps politik, det fortsatta ryska agerandet samt händelseutvecklingen i Europas södra närområde – kan skapa en ny dynamik i de säkerhets- och försvarspolitiska samarbetena i Europa. Dessa kan utvecklas i flera olika riktningar. Det kan exempelvis handla om ett närmare samarbete mellan en begränsad grupp av länder, stärkta bilaterala relationer eller fördjupad integration inom Europa. Det är dock inte säkert att Sverige och Tyskland kommer att dra samma slutsatser kring vilken samarbetsform som bäst gynnar den nationella säkerheten.

För vidare läsning

Eva Hagström Frisell, och Anna Sundberg, *En försiktig balansgång: Tysklands nya roll inom säkerhets- och försvarspolitiken*, 2017, FOI-R--4399--SE.

Johan Eellend, Anna Sundberg och Niklas H. Rossbach, *The Russian wake-up call to Europe: French, German and British security priorities*, 2016, FOI-R--4270--SE.

Johan Eellend, *En stillastående förändring: Tysk säkerhetspolitik och dess betydelse för Östersjöområdet*, 2014, FOI-R--3912--SE.

5. Totalförsvar – vägval inför framtiden

Fredrik Lindgren och Ann Ödlund

Arbetet med att bygga upp ett modernt totalförsvar måste fokusera på att skapa maximal försvarseffekt. Ett viktigt övervägande handlar om vilken försvarskritisk verksamhet som ska bedrivas av Försvarsmakten och vad som ska levereras av det civila försvaret. Dagens organisering av statliga myndigheter och fördelningen av ansvar och roller kan också behöva omprövas för att nå bästa möjliga försvarseffekt. Slutligen behöver den civila delen av totalförsvaret ta fram ett långsiktigt beslutsunderlag för sin förmågeutveckling istället för att som i dagens krisberedskap låta utvecklingen vara händelsestyrd.

Att tänka ”krig” och förbereda sig för ett väpnat angrepp sågs länge som både onödigt och alltför dyrt. Utvecklingen inom flertalet områden i samhället, inklusive krisberedskapen, har inte tagit höjd för hot från en angripare, utan har koncentrerats till att hantera fredstida händelser i form av mindre störningar och kortare försörjningsavbrott. Utifrån ett försämrat omvärldsläge lade emellertid det försvarspolitiska inriktningsbeslutet 2015 sitt fokus på höjd beredskap och krig och prioriterade en utveckling av krigsförbandens operativa förmåga samt planering för ett sammanhängande totalförsvar.

I den här artikeln fokuserar vi på framtidens totalförsvar och presenterar några viktiga utgångspunkter och vägval för utvecklingen av totalförsvaret. Syftet är dels att visa på hur enskilda frågor kan påverka den samlade förmågan i totalförsvaret, dels att bidra med några idéer till förändringar av totalförsvarets förutsättningar.

På väg mot ett modernt totalförsvar

Totalförsvaret har börjat återuppbyggas och arbetet med detta måste inriktas så att det ger maximal försvarseffekt. I arbetet behöver bland annat prövas vilken försvarskritisk verksamhet som ska bedrivas av Försvarsmakten, vad civila aktörer ska stå för och hur totalförsvaret bör organiseras för bästa möjliga försvarseffekt. Det kan också ifrågasättas om den idag i huvudsak händelsestyrda och reaktiva utvecklingsmetod som dominerar krisberedskapen är lämplig när samhället bygger sin försvarsförmåga för höjd beredskap och krig. De system,

strukturer och förmågor som nu byggs upp kommer att styra utvecklingen av totalförsvaret även längre fram. Det är därför nödvändigt att analysera vilka krav som kommer att ställas i olika beredskapsnivåer och hur försvaret av Sverige bör utvecklas för att nå mesta möjliga försvarseffekt.

I *Strategisk utblick* från år 2015 lyfte vi fram tre utmaningar för utvecklingen av det civila försvaret:

- att hantera gråzonen och övergången från fredstid till krigsorganisering
- att integrera det civila försvaret med nuvarande system för krisberedskap
- att balansera de olika delarna av målet för det civila försvaret för att undvika en ensidig fokusering på stödet till Försvarsmakten.

Utmaningarna är fortfarande giltiga och dessutom relevanta även för totalförsvaret. Baserat på vad som har hänt sedan dess går det idag att finna nya utgångspunkter och vägval för återuppbyggnaden av ett modernt totalförsvar.

På politisk nivå finns en bred uppgörelse kring försvarspolitikens inriktning och regeringen har ökat de ekonomiska resurserna till försvaret. Myndigheternas redovisningar utifrån regeringens uppdrag om en återupptagen totalförsvarsplanering visar att det bland berörda myndigheter och aktörer finns en vilja att delta i totalförsvarsplaneringen. Inställningen till totalförsvaret har nu börjat förändras allteftersom kunskapen och medvetenheten höjs, inte minst genom utbildningsinsatser och övningsverksamhet.

MSB:s (Myndigheten för samhällskydd och beredskap) undersökning *Opinioner 2016* visar också att det mellan mätningarna 2013 och 2014 skedde en relativt kraftig ökning av andelen av Sveriges befolkning som anser att Sverige absolut bör ha ett militärt försvar – en förändring som hållit i sig under de senaste mätningarna. En stor andel av befolkningen anser dessutom enligt undersökningen att dagens beredskap att hantera och möta ett militärt angrepp är otillräcklig. Enligt DN/IPSOS 2016 anser en majoritet av svenskarna att de ekonomiska resurserna till försvaret bör öka. En slutsats av detta är att det idag finns goda förutsättningar för att bygga ett modernt totalförsvar.

Eftersom totalförsvaret har det antagonistiska angreppet i fokus och därmed ställer andra krav än krisberedskapen, är det inte förvånande att återupptagen totalförsvarsplanering inledningsvis möttes av en viss tveksamhet av berörda myndigheter. I en undersökning om krigsorganisering och resursförstärkning som FOI genomförde 2014 lyfte bevakningsansvariga myndigheter fram kunskaps- och resursbrist som hinder för att ta sig an totalförsvarsfrågorna. En uttryckt politisk vilja, kombinerat med positiva attityder och signaler från myndighetsledningar och andra beslutsfattare som når ut i organisationerna, är tillsammans av central betydelse för utvecklingen av totalförsvaret och inte minst för att förändra det tankemönster som i princip uteslutit krig som ett möjligt hot mot Sverige.

Försvarseffekt i fokus

Även om arbetet med den återupptagna totalförsvarsplaneringen redan kommit en bit längs vägen återstår fortfarande ett stort arbete med att bygga ett modernt totalförsvar. Vi menar att de åtgärder som vidtas i detta arbete måste utgå från krav på förmåga i totalförsvaret och att fokus ska ligga på den samlade försvarseffekten, det vill säga Sveriges förmåga att försvara sig mot angrepp.

Att enbart vidta åtgärder som isolerat förbättrar förmågan i delar av det militära och civila försvaret är en för låg ambition i det fortsatta arbetet. De åtgärder som vidtas och de satsningar som genomförs behöver värderas utifrån en sammanhållen bedömning av totalförsvarets olika delar. Ett exempel är att det skulle vara ett dåligt resursutnyttjande att bygga upp förmåga att ge långvarigt stöd till en annan aktörs verksamhet, om denna verksamhet enbart är dimensionerad för två veckors uthållighet.

Med begränsade resurser och stora utvecklingsbehov behöver uppbyggnaden av förmågor hos olika aktörer balanseras och prioriteras – fortfarande med försvarseffekt i fokus. Det finns behov av central styrning med morot och piska, samtidigt som hänsyn tas till den utveckling och anpassning som naturligt tenderar att uppstå när civila och militära, privata och offentliga aktörer möts, planerar och övar tillsammans. I det första fallet krävs att man kommer överens på politisk nivå om att ge centrala myndigheter förutsättningar att kunna genomföra planering. I det andra fallet ligger ansvaret främst på regionala och lokala myndigheter och aktörer att gemensamt utveckla effektiva lösningar utifrån sina specifika behov och möjligheter. Ytterst

handlar båda fallen dock om att identifiera områden som är viktiga ur en totalförsvarssynpunkt och förbereda hur och av vem fördelning av resurser inom totalförsvaret kan genomföras i ett skarpt läge.

Vi vill också peka på faran att fastna i dagens strukturer, ansvarsförhållanden och regelverk när förslag på åtgärder och satsningar föreslås och värderas. Om försvarseffekt ska stå i fokus kan de förra behöva förändras för att ge totalförsvaret de förutsättningar som krävs för det spektrum av hot som Sverige måste kunna hantera. Sedan totalförsvaret utvecklades från mitten av 1940-talet – och sedermera avvecklades från slutet av 1990-talet – har det svenska samhället genomgått stora förändringar. Detta gäller inte minst i fråga om marknadsreformer inom en rad samhällsviktiga verksamheter där offentliga aktörer tidigare hade en dominerande roll som ägare och utförare. Det moderna totalförsvaret måste därför inte bara kunna leverera nya förmågor för att möta dagens och framtidens behov, det måste också utformas utifrån andra förutsättningar i samhället.

Vägval för framtidens totalförsvar

De beslut som vi fattar idag kommer att påverka och styra förmågan i morgondagens totalförsvar. Det finns flera principiellt viktiga frågor där vägval behöver göras och nedan följer några exempel på sådana.

- Vilken försvarskritisk verksamhet ska bedrivas av Försvarsmakten och vad ska levereras av det civila försvaret?

Ansvarsfördelningen mellan det civila och det militära försvaret är inte självklar. När ansvar ska pekas ut och resurser fördelas bör ett övervägande göras avseende vilka uppgifter som bäst utförs i Försvarsmaktens egen regi och vilka uppgifter som bör åläggas civila aktörer. Exempel på områden där sådana vägval behöver göras är sjukvård och försörjning av förnödenheter som livsmedel och drivmedel till Försvarsmaktens förband. Olika alternativ bör tas fram och vägas mot varandra med bästa möjliga försvarseffekt i fokus, även om detta innebär att andra intressen kan behöva stå tillbaka. En viktig fråga gäller civila aktörers kombattantstatus inklusive skyddsnivåer och säkerhet för berörda personalkategorier och leverantörer.

Arbetet med totalförsvarsplanering och andra förberedelser kommer att resultera i att en rad konkreta civila och militära behov kopplade till höjd beredskap identifieras och de lösningar

som väljs för att möta dessa behov måste utgå från dagens avreglerade samhälle och slimmade försvarsmakt. Offentliga och privata aktörers strävan efter kostnadseffektiva lösningar har inneburit att många samhällsviktiga funktioner idag har låg eller ingen redundans annat än för mindre störningar. Detta kan fungera vid fredstida händelser genom omfördelningar, men förmågorna är sannolikt otillräckliga vid ett angrepp på Sverige. Vi tror dock inte att det är möjligt att bygga upp tillräcklig redundans för att samhället ska kunna fungera som vanligt under en krigssituation. Ur ett totalförsvarsperspektiv är olika funktioner olika viktiga – vissa förmågor måste prioriteras högre än andra. Det är även skillnader i vilka krav som ställs på olika kommuner och län beroende på deras geografiska och militärstrategiska läge.

- Hur ska totalförsvaret organiseras för bästa möjliga försvarseffekt?

Sveriges offentliga organisering utgår dels från en sektorsindelning där olika myndigheter har utpekade ansvarsområden och roller, dels från geografiska indelningar på nationell, regional och lokal nivå. Det fokus på försvar av territoriet som totalförsvaret innebär, leder sannolikt till att den geografiska dimensionen behöver bli mer framträdande och tydlig i organiseringen av samhällets totalförsvarsförmåga. Ett problem som rör både totalförsvar och krisberedskap är att olika statliga myndigheters regionala indelningar idag skiljer sig åt, vilket komplicerar samverkan på regional nivå. En högre regional nivå som omfattar flera län skulle förenkla samordning inom totalförsvaret och även inom krisberedskapen. En enhetlig indelning av statlig verksamhet på regional nivå skulle sannolikt ytterligare förenkla en sådan samordning.

Det finns flera sätt att organisera en högre regional nivå, en länsstyrelse kan till exempel ges extra ansvar och resurser inom ett större område, exempelvis motsvarande Försvarsmaktens militärregioner. MSB skulle även kunna organisera delar av sin verksamhet på ett sätt som förstärker den geografiska dimensionen i syfte att, inom ramen för sitt ansvar inom civilt försvar,[4] ge bättre och mer riktat stöd till aktörer på regional nivå, i första hand till länsstyrelserna. Det finns två sätt, det mindre genomgripande är att MSB organiserar enheter för att stötta främst länsstyrelser och kommuner i deras arbete. Det

[4]MSB ska enligt sin myndighetsinstruktion ”företräda det civila försvaret på central nivå i frågor som har betydelse för avvägningar av civila och militära behov av samhällets resurser om inte något annat följer av särskilda föreskrifter.”

lite mer genomgripande är att MSB etablerar en egen regional närvaro som speglar en högre regional nivå. Förutom stöd till den högre regionala nivån skulle en regional närvaro även förbättra MSB:s möjligheter att företräda det civila försvaret på central nivå.

Dagens bevakningsansvar, som gäller endast vissa statliga myndigheter, medför att flera för totalförsvaret viktiga myndigheter saknas i den pågående planeringen. De sex befintliga samverkansområdena som idag ligger till grund för samverkan lämpar sig dessutom dåligt för konkret planering då de täcker in för många olika verksamheter. Dessa bör i planeringshänseende ersättas med ett tydligt sektorsansvar där en myndighet har ansvar för samordning och planering inom respektive sektor i syfte att underlätta en sammanhållen planering och förmågeutveckling.

Även övergripande principer för samordning och prioritering av samhällets totala resurser behöver utvecklas – inte bara de enskilda aktörernas förmågor. Centrala och regionala register över kritiska resurser underlättar överblicken över vad som finns tillgängligt vilket kan göra det enklare att fatta beslut om fördelning av dessa resurser. Det behöver även utredas vilka lager för viktiga förnödenheter som behövs, vilka avtal som behöver skrivas eller ses över, samt vilka åtgärder som behövs för att förbereda förfogande[5] för totalförsvarets behov.

- Fungerar krisberedskapens händelsestyrda utveckling för det civila försvaret?

Utvecklingen av den fredstida krisberedskapen och därmed grunden för det civila försvaret, har de senaste decennierna framförallt varit händelsestyrd och reaktiv. Erfarenheter och analyser av allvarliga händelser och hantering av stora kriser har legat till grund för åtgärder i syfte att öka samhällets förmåga att hantera kommande kriser.

I den återupptagna planeringen för totalförsvaret är det i stället nödvändigt att utgå ifrån antaganden om möjliga krigshandlingar som kan drabba samhället snarare än ifrån egna erfarenheter av inträffade kriser. Redan idag genomförs vissa långsiktiga analyser inom krisberedskapsområdet. Det saknas alltså inte underlag för att väga in framtiden vid utvecklingen av olika förmågor, men detta behöver ställas mot totalförsvarets krav. För att undvika att det civila försvaret ska präglas av en liknande händelsestyrd utveckling som krisberedskapen,

[5]Enligt förfogandelagen

bör ett strategiskt beslutsunderlag tas fram med alternativ för vidmakthållande och utveckling av det civila försvaret med försvarseffekten i fokus. Försvarsmaktens perspektivstudier är exempel på hur en samlad framåtblickande analys kan översättas i behov av framtida förmågor.

Ökat engagemang och nya möjligheter

Vem som ska göra vad under höjd beredskap – civilt eller militärt, privat eller offentligt – är ett vägval där den största utmaningen i arbetet framöver sannolikt kommer att ligga i att komma överens om en långsiktig inriktning på politisk nivå som sedan kan slås fast på central myndighetsnivå. Principer för organisering av totalförsvaret är ett annat vägval där flera alternativ bör tas fram och analyseras, liksom om och i så fall hur det civila försvaret ska utveckla en långsiktig planeringsprocess.

Hittills har den återupptagna totalförsvarsplaneringen främst engagerat Försvarsmakten, MSB och de övriga bevakningsansvariga myndigheterna. Det finns fler myndigheter och aktörer som behöver engageras i utvecklingsarbetet, till dessa hör försvarsmyndigheter (till exempel Försvarets materielverk (FMV), Försvarets radioanstalt (FRA), Totalförsvarets forskningsinstitut (FOI), övriga centrala myndigheter, kommuner och landsting/regioner samt näringslivet. Vidare är sektorsvisa analyser och bedömningar, liksom hänsyn till geografiska förutsättningar och skillnader, centrala för att åstadkomma en fungerande och trovärdig totalförsvarsplanering.

Avslutningsvis vill vi lyfta fram att intresset för och medvetenheten om totalförsvaret har ökat de senaste åren. Dagens mer uttalade politiska prioriteringar tillsammans med ett bredare samhälleligt engagemang skapar ett möjlighetsfönster för förändring och utveckling inom totalförsvaret vilket bör utnyttjas. I den här artikeln har vi valt att visa på några viktiga vägval i den fortsatta utvecklingen av totalförsvaret. Fokus på den samlade försvarseffekten kan tyckas självklar, men olika intressen, drivkrafter och agendor (civila såväl som militära) riskerar att skymma det övergripande syftet – att bygga upp ett totalförsvar med förmåga att möta ett väpnat angrepp mot Sverige.

6. Psykologiskt försvar – avgörande för svensk försvarsförmåga

Niklas H. Rossbach[6]

Sverige utsätts idag för påverkansoperationer som kan drabba den fria åsiktsbildningen. Under en gråzonskonflikt kommer desinformation som riktas mot allmänheten och beslutsfattare att öka. För att värja sig behöver Sverige en mer samlad och tydlig organisation av landets motåtgärder och motståndsvilja. Ett modernt strategiskt psykologiskt försvar förutsätter en utpekad central aktör som kan överblicka såväl hela hotbilden som berörda myndigheters roller och förmågor. Saknas detta hamnar ansvaret mellan stolarna både mellan och inom olika myndigheter. Utan ett sammanhållet psykologiskt försvar är det mycket svårt både att stå emot försök att sprida desinformation och att skapa en försvarsvilja. Utan sådana motåtgärder kommer heller ingen annan del av försvaret att fungera.

Psykologiskt försvar och totalförsvaret

”Jag kan flyga. Jag är inte rädd” säger karaktären Stig-Helmer i den svenska filmklassikern Sällskapsresan. Precis som Stig-Helmer behöver försäkra sig om att det är rimligt att flyga behöver den svenska allmänheten försäkras om att det är meningsfullt att göra motstånd i händelse av ofred. Det gäller även i gråzonen mellan fred och krig, där en fiende försöker påverka utvecklingen utan direkta krigshandlingar. För att säkerställa den övertygelsen behövs en sammanhållen ansträngning, vilket ett strategiskt psykologiskt försvar kan bidra till.

Utan ett tillräckligt psykologiskt försvar står våra uppfattningar oskyddade mot fientlig påverkan och då kan exempelvis vilseledning påverka våra beteenden. Detta riskerar i sin tur att undergräva både civila och militära ansträngningar för att värna landets säkerhet. Det psykologiska försvaret är således ett grundläggande strategiskt område som angår hela totalförsvaret.

Det psykologiska försvaret är lika centralt för det nya totalförsvaret som det var under kalla kriget. Under de senaste decennierna har dock det psykologiska försvaret krympts

6 Artikeln baseras till del på forskning som genomförts vid universitet i Oxford med stöd av Axel och Margaret Ax:son Johnsons stiftelse.

nästan till utplåningens gräns. Inte minst mot bakgrund av den ökade säkerhetspolitiska spänningen i Sveriges närområde har det blivit nödvändigt att uppmärksamma den viktiga roll som ett psykologiskt försvar har i försvaret av Sverige.

Psykologiskt försvar – ett slitstarkt begrepp

Sveriges psykologiska försvar var från början ett svar på den psykologiska krigföring som främmande makt förväntades bedriva i händelse av krig. Begreppet psykologiskt försvar, som framförallt använts i Sverige,[7] var ett försök att röra sig bort från det snäva uttrycket propaganda som framförallt förknippades med Nazityskland och andra världskriget. Det svenska uttrycket har visat sig både hållbart och anpassningsbart, men dess genomförande har blivit otydligt i konturerna särskilt som uppgifterna angår flera myndigheter.

”Psykologiskt försvar” innefattar tre viktiga delar. Vilka uppgifter som varit de mest framträdande har dock varierat genom åren. De tre delarna är:

- att motverka vilseledning och desinformation, inklusive ryktesspridning, och propaganda, med andra ord allt det som fientlig psykologisk krigföring ägnar sig åt
- att säkerställa att myndigheterna kan få ut sitt budskap under en kris, såsom ett krig
- att bidra till att förstärka befolkningens försvarsvilja, exempelvis genom att uppmärksamma opinionen kring försvarsviljan.

Ny teknik har alltid utnyttjats inom den psykologiska krigföringen och försvaret mot detsamma. Bara lite drygt tio år efter att Nazitysklands propagandaminister Dr. Goebbels gjorde sina sista radioutsändningar i diktaturens tjänst experimenterade det svenska psykologiska försvaret, i syfte att värna demokratin, med direktsända presskonferenser i TV om sin övningsverksamhet.

Modern informations- och kommunikationsteknik ger psykologisk krigföring nya möjligheter. Falska nyheter kan spridas via sociala medier och cyberangrepp mot svensk

7 Begreppet etablerades i Sverige, som ett praktiskt svar på omvärldens förberedelser för psykologiska krigföring, i och med publiceringen av SOU 1953:27 om Psykologiskt försvar. Idag kan begreppet användas för att få ett grepp om floran av överlappande nya begrepp såsom informationsoperationer, påverkansoperationer och informationskrigföring, PSYOPS osv.

infrastruktur kan tillsammans med ryktesspridning undergräva allmänhetens förtroende för myndigheterna. Staten behöver en samlad överblick över alla potentiella kanaler där motståndaren kan bedriva propaganda och påverkansoperationer, men det är också viktigt att förstå hur hotet har förändrats sedan det kalla kriget.

Nygammal hotbild

Förutsättningarna för det psykologiska försvaret såg helt annorlunda ut under det kalla kriget då hotbilden var tydligare än idag. I dagsläget måste psykologisk försvarsverksamhet kunna hantera både statliga och icke-statliga aktörer och måste samtidigt som den motverkar operationer som pågår i fred vara förberedd på krigstida förhållanden. Likheten mellan förr och nu består i att det är samma viktiga värden som står på spel, såsom möjligheten att hålla fria val. Förr riskerade demokratin att falla offer för en ockupationsmakt. Idag kanske en främmande makt istället försöker att manipulera svenska politiska val genom olika slags påverkansoperationer.

Förr som nu är försvarsviljan – eller motståndsandan – central för ett fungerande försvar. Ett försvar kräver både vilja och förmåga, och det handlar om hela landets vilja. För att ta det till sin spets: utan en vilja att försvara Sverige, skulle all utrustning och alla mobiliserande styrkor vara av ringa värde. Men det finns fler överväganden som gör att försvarsviljan inte enbart kan vara ett ansvar för ett strategiskt psykologiskt försvar.

För att uppnå en försvarsvilja behövs insatser från flera delar av samhället och inte minst olika myndigheter. Men i sin ansträngning att stärka försvarsviljan finns risken att myndigheter, med eller utan avsikt, hemfaller åt någon form av inhemsk propaganda. Detta kan på sikt göra mer skada än nytta. Därför är stärkandet av försvarsviljan en fråga som kräver noggranna överväganden om vad staten bör göra och vad andra delar av samhället bör göra.

På 1950-talet ville Beredskapsnämnden för psykologiskt försvar (föregångaren till myndigheten Styrelsen för Psykologiskt Försvar) undvika att anklagas för någon form av manipulation av allmänheten. Sverige hade nämligen haft sin beskärda del av klumpiga och politiskt tveksamma åtgärder för att hantera opinionen under det andra världskriget och den nya verksamheten för psykologiskt försvar ville inte bli förknippad med dessa. En uppmärksammad psykologisk försvarsövning på 1970-talet påminde om riskerna uppfattades som att staten ägnade sig åt propaganda. Även på 1980-talet när fredstida

uppgifter som att upplysa om totalförsvar och säkerhetspolitik blev ett åtagandet för det psykologiska försvaret befarade beslutsfattare att det skulle uppfattas som problematiskt.

Totalförsvaret kan komma att behöva ett narrativ om vad som utgör ett trovärdigt försvar. Ett sådant berättande behöver givetvis formuleras eller åtminstone förankras på politisk nivå men är viktigt för att visa hur myndigheterna arbetar på ett meningsfullt sätt. Ett strategiskt psykologiskt försvar skulle kunna bidra till att koordinera en berättelse om vilka värden Sverige vill stå för i framförallt säkerhetsrelaterade sammanhang.

Utan ett samordnat psykologiskt försvar blir det sannolikt svårare att säkerställa en försvarsvilja. Rimligtvis behöver försvarsviljan också stärkas innan en kris brutit ut. Den behövs för att motivera byggandet och deltagandet i ett totalförsvar. Inte minst behövs försvarsviljan för att kunna rekrytera personal till civilt försvar och Försvarsmakten och för att motivera värnpliktiga. Traditionellt har försvarsviljan definierats av det kalla kriget, och antagandet om att hotet är ett väpnat angrepp av en främmande makt. När påverkansoperationer pågår i fredstid behöver kanske även försvarsviljan säkerställas i fredstid eller en ny slags försvarsvilja upprätthållas mot lågintensiva hot.

Framtidens psykologiska försvar

MSB:s psykologiska försvarsverksamhet kan ses som ”här och nu”-uppgifter i fredstid, vilket det psykologiska försvaret under det kalla kriget endast sysslade med i begränsad omfattning. Visserligen var det tidigare psykologiska försvaret strategiskt, men det bistod endast i en liten utsträckning med att förbereda befolkningen på hur den skulle agera i händelse av krig.

En del av MSB:s uppgifter härrör visserligen från det gamla psykologiska försvaret. MSB följer hur allmänhetens vilja att försvara landet utvecklas men studerar även opinionen rörande propaganda och gråzonskonflikt. Myndigheten har även ökat kunskapsspridningen om påverkansoperationer och om hur Sverige kan försvara sig. Detta kan komma att bli ännu viktigare med anledning av så kallad hybridkrigföring. Om propaganda och påverkansoperationer är tillräckliga för att motståndare ska uppnå sina målsättningar är det inget självändamål att låta en konflikt övergå till en väpnad strid. Men även en motståndare som förbereder sig på en öppen väpnad konflikt skulle vilja undergräva försvarsviljan i Sverige innan en öppen konflikt bryter ut. Kunskap är i sig dock inte tillräckligt för att stärka försvarsviljan, det krävs även en tydlig ansvarsfördelning inom staten.

Om psykologiska försvarsuppgifter blir många myndigheters ansvar riskerar psykologiskt försvar att komma att handla om vitt skilda saker och att inte bli någons ansvar. En del myndigheter kommer att se det som en teknisk uppgift, förknippad med cyber- och IT-frågor, och andra kommer att nedprioritera den. Så länge hoten är lågintensiva kan de kanske hanteras styckevis utan en sammanhållande part. Men vid en kris kan det bli uppenbart att det behövs mer än ett nätverk av myndigheter som pysslar med psykologiska försvarsuppgifter utefter egna förutsättningar.

Ett skäl till att det behövs en central och tydlig aktör – ett strategiskt psykologiskt försvar och kanske helst i formen av en egen myndighet – beror på att hotbilden har förändrats och blivit mer mångfacetterad. Det ökar behovet av en samlad syn. Påverkansoperationer kan bedrivas på flera sätt men för att framgångsrikt motverka dem är det viktigt att kunna sätta in exempelvis en informationsoperation i ett större strategiskt sammanhang.

Försvarsmakten har en viktig roll inom psykologiskt försvar och har en uppmärksammad förmåga att genomföra psykologiska operationer, så kallade PSYOPS, exempelvis inom ramen för insatser. Men detta är långt ifrån det strategiska psykologiska försvar Sverige tidigare haft. Lika litet nu som under det kalla kriget bör ett sådant försvar koordineras av Försvarsmakten. Det vore problematiskt om frågor som berör demokratins kärna, såsom den fria åsiktsbildningen, underordnades militära hänsynstaganden. Dels för att hoten redan finns i fredstid och dels för att Försvarsmakten i händelse av krig måste fokusera på psykologisk krigföring vid fronten och därför inte kan ta ansvar för hela samhället.

Ett modernt välfungerande totalförsvar skulle sannolikt tjäna på att det psykologiska försvaret fick en tydlig, samlad och central organisation – det vill säga ett strategiskt psykologiskt försvar. Det skulle innebära en kombination av den ställning psykologiskt försvar ursprungligen hade och den motverkan mot informationspåverkan som idag faller inom ramen för psykologisk försvarsverksamhet.

Ett strategiskt psykologiskt försvar behövs

För att förstå behovet av ett modernt psykologiskt försvar behöver man inte skärskåda militära scenarion. Det går även att peka på riskerna för att påverkansoperationer undergräver landets demokrati och förmåga till beslutsfattande i händelse av en kris. Idag behövs det psykologiska försvaret för att undanröja

effekten av påverkansoperationer i fred och inte bara i krig. Det psykologiska försvaret kan till och med vara ett avgörande instrument som avvärjer hotet från en motståndare som inte kan eller är beredd att gå till väpnat angrepp.

För att psykologiskt försvar ska vara effektivt behöver det vara strategiskt av flera skäl:

För det första behövs en samlad kunskap om en motståndares psykologiska krigföringsmetoder. Ett nog så skickligt bemötande av påverkansoperationer på skilda håll i samhället, såsom media och underrättelsemyndigheter, är otillräckligt. I händelse av en plötslig kris eller allvarlig konflikt kan ett samlat grepp om både förståelse för vad som utgör påverkansoperationer och hur motåtgärder ska organiseras visa sig vara avgörande.

För det andra är det nödvändigt att överväga en särställning för det psykologiska försvaret inom ramen för det nya totalförsvaret. Inte minst för att visa var det samlade ansvaret för psykologiskt försvar finns. Såväl det offentliga Sverige som allmänheten behöver veta vart de ska vända sig för att få hjälp med att känna igen vad som är psykologisk krigföring och för att få stöd kring hur de ska värja sig, oavsett om påverkan rör en kommun, en individ eller hela riket. Utan en strategisk och central ställning för det psykologiska försvaret riskerar psykologiska försvarsuppgifter att tappas bort bland eller i olika myndigheter. Ett strategiskt psykologiskt försvar bör, liksom förr, ha en tydlig civil ställning för att få en självständig roll inom ramen för totalförsvaret. Detta skulle också underlätta för samverkan på jämbördig fot med underrättelse- och försvarsmyndigheter.

För det tredje, ett strategiskt psykologiskt försvar skulle göra det lättare att samverka och visa solidaritet med andra likasinnade länder. Dessa länder skulle veta vilken myndighet i Sverige de skulle kunna samverka med vid gemensamma åtgärder och försvar mot påverkansoperationer. Ett strategiskt psykologiskt försvar skulle också underlätta för Sverige att föra fram vilka värderingar som bör prioriteras.

För vidare läsning

Rossbach, Niklas, (preliminär titel) *Fighting propaganda – The Swedish experience of psychological warfare and Sweden's psychological defence 1940-1960*, kommande, Axel och Margaret Ax:son Johnsons Stiftelse

7. Internet som militär arena – en utmaning i totalförsvaret

Mikael Wedlin och Erik Westring

Beroendet av internet för samhällsviktig verksamhet ökar idag oerhört snabbt, nya tjänster utvecklas hela tiden och ersätter gamla sätt att kommunicera. Detta har också ökat internets betydelse ur försvarssynpunkt. Inhämtning av underrättelser, påverkansoperationer samt dolda militära operationer är områden där vi har kunnat se internet användas som ett nytt militärt verktyg även i fredstid. Det digitala slagfältet är därför av stor betydelse i utvecklingen av det nya totalförsvaret och Sverige behöver därför följa med i utvecklingen, tekniskt, organisatoriskt och legalt.

Att internet kan fungera som en arena även för militär verksamhet är inte någon ny tanke. När FOI började studera IT-krigföring under andra halvan av 90-talet utgick forskningen från att detta var krigföringens framtid; kanoner och krut tillhörde historien. Speciellt oroväckande var den digitala påverkan eller utslagning av vår kritiska infrastruktur som förväntades kunna ske. Nu när internetoperationer börjat bli verklighet i pågående konflikter kan vi bättre avgöra vad som utgör en realistisk framtid. Att internet skulle få en stor del i vårt dagliga liv gissade vi rätt på, det finns idag ingen del av vårt dagliga liv som inte berörs av internetkopplade system. Internetarenans påverkan på nutida konflikter har dock inte skapat det totala digitala angrepp som slagit ut hela samhällen som tidigare befarats. Istället har vi kunnat se att det har varit i fasen före själva konflikten som användningen av internet varit som störst.

Även om vi nu börjar förstå mekanismerna för krigföring på internet så är det oerhört svårt att förutse den framtida utvecklingen. Den första svenska internetbanken startade redan 1996 men det är först under de senaste fem till tio åren som utvecklingen lett till att internet de facto blivit den främsta kommunikationsvägen för bankärenden. Nästan alla de tjänster som vi idag betraktar som självklara som Google, Facebook och Youtube har skapats under de senaste 20 åren. Vad vi med god sannolikhet kan förutspå är att internet fortsätter vara en betydande infrastruktur i alla samhällssektorer och att dess betydelse också förmodligen kommer att öka. Man skulle till och med kunna gå så långt som att påstå att internet på sikt kommer att medföra större förändringar i vår livsstil än vad den industriella revolutionen gjorde under 1800-talet.

De militära utmaningarna

Internet har framför allt fyra egenskaper som skapar försvars- och säkerhetspolitiska utmaningar och särskilda militära problem:

Eftersom det med relativt enkla medel går att dölja sin sanna identitet på internet kan operationer på internet lätt förnekas. På internet är det svårt att vara säker på att någon verkligen är den personen som den utger sig för att vara. Rättslig legitimering av militär intervention gäller bara om man kan associera en militär statsaktör till det som sker; något som i grunden kan vara svårt på internet. Ur ett militärt perspektiv är detta till fördel för den som vill agera i det dolda och till nackdel för den som ska försvara sig.

Genom internet kan operationer med militära syften genomföras även på stort avstånd. Internet är en domän helt utan nationsgränser och ”förflyttning” är i princip omedelbar och utan avstånd. Detta gör att operationer på internet kan ske varifrån som helst och i princip helt utan risk för egen personal. Gränslösheten innebär också ett oklart juridiskt och folkrättsligt läge. Använder jag annans territorium om min skadliga kod placeras på mejlservers i tredje land?

Infrastrukturen för den digitala militära arenan delas även med civila. Tidigare har militära och civila hot varit väl åtskilda. Speciellt i Sverige har vi av tradition vinnlagt oss om en extra tydlig åtskillnad. På internet flyter dock de militära och civila hoten in i varandra. Detta är särskilt så eftersom det kan vara svårt att avgöra en attacks ursprung, syfte och mål: om samtliga banker i ett land plötsligt får sina webbportaler utslagna samtidigt kan antagonisten vara en annan stat som utför en krigshandling, eller några enskilda tonåringar utan något annat syfte än att provocera. Generellt är sådana händelser svåra att värdera och analysera. Detta gör det också komplicerat att avgöra vilka lagar som gäller vid IT-angrepp, eller om det ens finns några. I stort sett alla konflikter runt mellanöstern har följts av intrång i webservrar. Är detta en del av de militära operationerna? Vem kan ställas till svars? Spelar det någon roll om avsändaren är militär? Sveriges största utmaning här är att fördela uppgifterna mellan Försvarsmakten och det civila försvaret.

Internet öppnar upp kostnadseffektiva möjligheter som möjliggör för asymmetrisk krigföring. Angrepp över internet är ofta till sin natur asymmetriska; även små, monetärt resurssvaga organisationer eller individer kan utföra aktioner över internet. Förmågan att genomföra internetattacker byggs till stor del upp av ren kunskap och det räcker med enstaka individer med rätt kompetens för att störa även relativt stora system. För att generera större störningar eller långsiktig skada behöver dock även angrepp över internet större resurser, både i form av underrättelseförmåga och gott om tid.

Ett tydligt exempel på detta är *Stuxnet*, angreppet på Irans nukleära program med hjälp av ett datorvirus mot anrikningsanläggningen för uran i Natanz. Genom att plantera in ett virus i styrsystemen fick man ett antal av deras centrifuger att gå sönder och inte producera något uran. Även om denna skadliga kod var ett av de mer avancerade som setts då det hittades, och var hopsatt av ett flertal olika typer av kod från flera olika programmerare, så kan man tänka sig att det skulle kunna ha skrivits av en enda enskild person med tillräckligt mycket kunskap och tid. För att skapa en framgångsrik skadlig kod av den här riktade typen behövs dock också ingående kunskaper om Irans nukleära program, detaljerade ritningar och tillgång till både den hårdvara och mjukvara man vill kunna angripa och de frekvensomformare som styr dessa. Det sistnämnda är nödvändigt för att kunna utveckla den skadliga kod som förstör centrifugen utan att de inbyggda skydden slår till. Tillgång till denna typ av resurser är det idag bara stater som har.

Även om internet möjliggör asymmetrisk krigföring är det osannolikt att någon med små resurser kan åstadkomma mer än mindre störningar. För att slå mot hela samhällssektorer krävs en mycket kvalificerad motståndare.

INTERNET SOM MILITÄRT MEDEL

Traditionella militära medel genererar oftast en större och mer förutsägbar effekt än ett cyberangrepp. Man kan som exempel på detta betrakta angreppet mot Ukrainas elförsörjning julen 2015. Angreppet var planerat åtminstone sex månader i förväg och åstadkom en störning med ett kortare avbrott där de första abonnenterna började återfå strömmen redan efter tre timmar. Traditionell bekämpning av Ukrainas elförsörjning hade rimligen gett mer permanenta skador, dessutom på ett mer förutsägbart sätt. Militära angrepp för att slå ut infrastruktur kommer sannolikt därför bara att vara ett komplement till traditionella förmågor.

Vi har dock framför allt kunnat se tre områden där internet är en intressant arena för militära operationer:

För underrättelseinhämtning. Internet torde vara varje underrättelseorganisations dröm. All information finns samlad på ett ställe, relativt enkelt åtkomlig i ett format som är möjligt att bearbeta maskinellt. Det är uppenbart att detta redan pågår i stor skala och att stora resurser allokeras för informationsinhämtning. Ett nästan övertydligt exempel på detta är de avslöjanden som Snowden gjorde för ett par år sedan. Det finns också ett flertal publicerade exempel på illegal övervakning av organisationer och individer av den kinesiska staten.

Som en plattform och medel för påverkansoperationer. Internet har förändrat våra medievanor och metoder för nyhetsinhämtning på ett fundamentalt sätt. Till skillnad från tidigare kan idag vem som helst på ett enkelt sätt vara producent av information och att identifiera avsändaren är näst intill omöjligt. Falsk information med syfte att påverka sprids med epidemisk effektivitet. Informationsflödet ökar lavinartat och aktörer i vårt närområde upprustar målinriktat på internet för att använda dessa nya digitala medier för sina geopolitiska syften. Ett oroväckande exempel är den påverkan som presidentvalet i USA utsattes för. Det är mycket troligt att framtida europeiska val kommer att utsättas för samma typ av påverkan. Exemplet med Ukrainas elförsörjning kan också betraktas som en påverkansoperation, vars syfte troligen snarare var att ingjuta osäkerhet hos befolkningen än att uppfylla något traditionellt militärt mål. Internet har således öppnat upp för nya effektivare metoder och verktyg inom påverkansoperationer och det finns all anledning att anta att omfattningen kommer att fortsätta öka.

Dolda operationer vid skymningsläge/gråzon. Förnekbarheten i internetbaserade operationer kan särskilt utnyttjas i de lägen man vill genomföra militära operationer utan att de uppfattas som krigshandlingar. Aktioner på internet har därför en särskild betydelse i krigsförberedande åtgärder och i så kallad förbekämpning. Det tidigare nämnda exemplet med *Stuxnet* faller typiskt in under den här kategorin. Det var en extremt avancerad och osäker operation, men vi kan anta att avsändaren inte ville eskalera motsättningen till öppen konflikt.

Sammanfattningsvis kan vi konstatera att internet som militärt medel framförallt kommer att beröra oss i fredstid.

Internationell utblick

Flera stater har numera öppet deklarerat att de förfogar över en militär internetförmåga, vilket styrker antagandet att internet kommer att vara en naturlig del av framtida militära konflikter. Ryssland har till exempel bara de senaste åren vid flera tillfällen blivit anklagade för att ha använt dataintrång som konfliktmetod. Stuxnetoperationen genomfördes sannolikt av USA och Israel, även om ingen av dem har erkänt detta. Även Iran och Kina, bland andra, har förekommit i intrångsrapporter där det är rimligt att anta att en statsaktör låg bakom intrånget.

De senaste åren har det uppdagats att stater är mycket intresserade av information avseende andra länders infrastruktur. Det finns ett antal rapporter från amerikanska myndigheter som konstaterar spår av att främmande stater har kartlagt infrastrukturen i USA. Även FRA rapporterar om 10 000 ”cyberaktiviteter” riktade mot Sverige varje månad. Enligt FRA är den övervägande delen av dessa rent spionerі och försök att komma över information, men man har också identifierat åtminstone ett försök att kartlägga svensk infrastruktur.

Efter att Estland var hårt ansatt av IT-attacker under våren 2007 bildade man något som närmast är att likna vid ett digitalt hemvärn, ”Estonian Cyber Defence League”. Syftet med detta har varit att stärka samhällets förmåga att hantera cyberangrepp samt att främja privat-offentlig samverkan.

Var står Sverige idag?

Sverige har en förhållandevis god datormognad och har arbetat aktivt med att förstärka den allmänna IT-säkerhetsnivån under de senaste 10 åren. I internationell jämförelse av risker kopplade till IT-hot ligger Sverige därför relativt bra till. Vår kritiska infrastruktur är dock inte byggd för att kunna stå emot attacker från någon med en stats resurser, varken i cyberrymden eller i den vanliga världen. Där har vi mycket kvar att göra. FOI:s IT-säkerhetsarbete har främst syftat till att höja medvetandet och att införa skydd mot de enklaste typerna av angrepp. IT-säkerhet har dock varit ett litet forskningsområde i förhållande till hur snabbt området utvecklas. Det är en utmaning att få med säkerhetsaspekterna i den snabba utvecklingen. Det finns ett stort behov av mer kvalificerad forskning.

Förändringar i omvärldsläget de senaste åren har gjort att Sverige har börjat återuppbygga det civila försvaret och totalförsvarstanken har fått ny aktualitet. De samhällsförändringar kopplade till internet som har skett sedan

Sverige senast hade en totalförsvarsorganisation ställer krav på att det nya totalförsvaret även omfattar ett försvar mot digitala hot.

Rollerna för hantering av de digitala hoten behöver klaras ut och nödvändig samverkan mellan myndigheter och andra aktörer behöver utvecklas. Vems uppgift är det att släcka bränder på internet? Om militärflyg från andra länder kränker Sveriges gränser skickar Försvarsmakten ut eget flyg för att avvisa detta. Om ett tyskt godståg med kemikalier spårar ut utanför Stenungssund är det polisen och brandkåren som hanterar detta. I internetvärlden är det annorlunda, inte minst på grund av att de civila och militära hoten flyter in i varandra.

Sveriges motståndskraft mot digitala hot kommer att vara beroende av att alla i samhället samverkar. Samverkan finns redan mellan försvarsmyndigheterna och inom krishanteringssystemet. Denna samverkan behöver utvecklas ytterligare. Här måste det till en tydligare samverkan mellan polisiära och militära myndigheter och möjligheterna utökas för Försvarsmakten att stödja Polisen. Försvarsmakten är rimligtvis ansvarig för att motverka militära attacker även via internet. Dessutom måste civila leverantörer av samhällskritiska funktioner, så som mobiloperatörer eller banker, involveras i planering och hantering av hoten. Här finns en stor utmaning för det nya totalförsvaret.

Påverkansoperationer på internet utgör ett uppenbart hot mot vår demokrati och våra politiska processer. En självklarhet under uppbyggnaden av totalförsvaret är att vi bygger kompetens samt utvecklar teknik för att förstå även dessa angrepp, så att vi effektivt kan motverka också denna typ av subtil krigföring.

För att hantera de digitala hoten behövs regleringar nationellt och internationellt. Det är dock en utmaning att reglera ett så snabbt föränderligt område. Samtidigt är det viktigt att värna om öppenheten på internet. Sverige har en roll i att stå för en öppenhet som samtidigt möjliggör ansvarsutkrävande. På samma sätt som att vi har en brandkår som rycker ut vid bränder som den enskilda inte klarar att släcka själv, borde vi kanske vid större påfrestningar ha en styrka av frivilliga IT-tekniker som redan är samövade och förberedda att agera i en krissituation på ett sätt som en enskild systemägare ensam har svårt att göra.

Behöver kanske Sverige, i likhet med Estland, ett digitalt hemvärn?

8. Internet of Things – en IT-säkerhetsmässig mardröm

Daniel Eidenskog och Farzad Kamrani

Internet of Things (IoT) är ett samlingsnamn för produkter som innehåller elektronik med någon form av uppkoppling mot andra system, vanligtvis via internet. Antalet cyberangrepp som involverar IoT-enheter har ökat under senare år, vilket tillsammans med det förändrade omvärldsläget gör att risken är överhängande för större och mer utbredda cyberangrepp där IoT-enheter är centrala. Sveriges totalförsvar bygger i stor utsträckning på motståndskraften i de normala samhällsfunktionerna. Många av dessa har internetanslutna system som till del baseras på IoT-produkter, vilket gör systemen särskilt sårbara samtidigt som samhällskritisk verksamhet utgör en tydlig måltavla för cyberangrepp. För att på sikt minska risken för allvarliga cyberangrepp med störningar i samhällskritisk verksamhet bör Sverige ha en tydlig strategi inom cybersäkerhetsområdet. Sverige bör också ta en aktiv roll i arbetet för ökad cybersäkerhet i kommersiella IoT-produkter.

En tillväxtmarknad med litet säkerhetsfokus

Internet of Things (IoT) utgör en bred marknad där produkter inom en rad olika segment ingår, exempelvis hushållsapparater, fordon, byggnadssystem och industriella maskiner. Tillväxttakten inom IoT-marknaden är hög och flera marknadsanalysföretag förutspår en global ökning från ungefär fem miljarder enheter år 2015 till drygt 75 miljarder enheter år 2025.

Marknadsanalytikerna förutspår att privatpersoner kommer äga en majoritet av dessa IoT-enheter. Privatpersoner utgör ett kundsegment där cybersäkerhet inte är ett viktigt kriterium vare sig vid inköpstillfället eller senare under produktens användning. Istället är nya funktioner och lågt pris ofta drivande faktorer. Det saknas även reglering av cybersäkerhetsaspekter och det är svårt att få tillverkare ansvarsskyldiga för sårbarheter i deras produkter. Tillverkarna har därmed generellt sett små incitament att satsa på cybersäkerhet. Detta leder därför i många fall till produkter med en säkerhetsnivå som ligger långt efter många andra IT-områden.

Även inom IoT-segment som riktar sig mot professionella användare är säkerheten ofta bristfällig. Detta har exempelvis visat sig genom omfattande säkerhetsbrister i professionella nätverksanslutna övervakningskameror. I flera fall har säkerhetsbristerna legat på

en nivå som antyder att mjukvaran utvecklats i total avsaknad av grundläggande förståelse för cybersäkerhet.

Givet den stora mängden av IoT-enheter innebär avsaknaden av säkerhetsfokus att cyberangrepp som riktar sig mot eller utnyttjar IoT-produkter riskerar att få stor omfattning. Angreppen kan därmed påverka såväl internetinfrastrukturen som potentiellt samhällsviktiga system och enskilda individer.

Totalförsvaret är beroende av internet

Sveriges totalförsvar bygger på att de normala samhällsfunktionerna kan upprätthålla ett fungerande samhälle även i händelse av kris eller krig, enligt den så kallade ansvarsprincipen. Det gäller både militära och civila funktioner där avbrott och störningar i den egna verksamheten kan påverka hela samhället och dess innevånare. Grundläggande samhällsviktiga sektorer som dricksvattenförsörjning, energiförsörjning, livsmedelsdistribution och kommunikationer är alla beroende av såväl IT-system som industriella styrsystem för sin funktion.

Många system inom kritiska sektorer har anslutningar till internet och bygger åtminstone delvis på IoT-produkter, vilket sätter systemen i riskzonen för cyberangrepp. I det förändrade omvärldsläget är risken överhängande att allt större och mer utbredda angrepp görs mot samhällskritiska funktioner, där angreppen riktas mot IoT-produkter eller där IoT-produkter används som en språngbräda för att förstärka angreppen.

Sveriges omfattande beroende av informationsteknologi innebär att samhället är utsatt för cyberrisker som knappast gick att föreställa sig för bara ett par decennier sedan. Med beroendet av internet som infrastruktur och med vitala samhällsfunktioner i riskzonen för cyberangrepp blir de potentiella konsekvenserna stora vid utbredda angrepp.

För att på sikt minska risken för allvarliga cyberincidenter med efterföljande störningar i kritisk verksamhet bör Sverige arbeta aktivt med cybersäkerheten inom IoT-området:

Sverige bör ha en tydlig strategi med syfte att öka kunskapen och beredskapen inom cybersäkerhetsområdet. En viktig del i en sådan cybersäkerhetsstrategi är att tydliggöra vikten av de system och komponenter som staten inte har kontroll över. Krishanteringens närhetsprincip är lämplig när det gäller att hantera en akut krissituation, men grundproblemet, att det är relativt enkelt att genomföra cyberangrepp oavsett var man befinner sig, går inte att hantera på lokal nivå.

Sverige bör ta en aktiv roll i arbetet för ökad cybersäkerhet i kommersiella produkter, exempelvis inom EU-samarbetet. Cybersäkerhetsfrågor är i grunden globala för alla system med koppling till internet, vilket innebär att arbetet för förbättrad cybersäkerhet måste bedrivas på både nationell och internationell nivå. Cybersäkerhetsläget på den privata marknaden påverkar samhället och måste ingå som en del av statens arbete inom cybersäkerhetsområdet.

Personlig integritet är större än personen

En annan aspekt av IoT-enheternas täta närvaro berör personlig integritet, som i förlängningen även kan påverka nationell säkerhet. Många IoT-enheters syfte är att samla in information om användaren, exempelvis i form av platser som besöks, hälsostatus, träningsvanor eller andra aktiviteter. Informationen förs i regel vidare till tillverkarens molntjänster så att användaren kan nyttja dessa för olika ändamål, samtidigt som tillverkaren får tillgång till informationen för sitt bruk.

Ett grundläggande problem är att IoT kan introducera många nya risker för den personliga integriteten, oftast i snabbare takt än rättsliga mekanismer och sociala normer kan anpassa sig. I en värld där allt fler saker är anslutna till internet sänks kostnaderna för insamling, lagring, bearbetning och delning av data dramatiskt. Integritetsriskerna sträcker sig från vardagliga och enkla problem såsom överbeskyddande föräldrars övervakning av sina barn och alltför påträngande marknadsföring till mer allvarliga fall där regeringar och statliga aktörer begränsar medborgarnas frihet eller utför angrepp mot andra länder.

Den rikedom av information som är åtkomlig genom IoT-enheter kombinerat med utökad beräkningskapacitet och effektivare algoritmer skapar stora möjligheter att identifiera, övervaka, avlyssna och spåra individer samt att kartlägga deras beteendemönster. IoT-enheter använder ofta passiva metoder för datainsamling, vilket resulterar i att användarna i regel är mindre medvetna om att de övervakas.

Personer som innehar nyckelbefattningar i samhället riskerar att bli måltavlor för riktade angrepp som bland annat kan nyttja IoT-enheter. Riktade angrepp mot individer sker oftast med hjälp av välinformerad och sofistikerad social manipulation kombinerat med tekniska angrepp. Den brittiska journalisten och människorättsaktivisten Rori Donaghy utsattes för ett sådant riktat angreppsförsök, genom en kombination av social manipulation och skadlig kod. Framgångsrik social manipulation förutsätter att angriparen har goda kunskaper om den som utsätts för attacken, något som kan uppnås genom att samla in information från flera olika källor. Genom att angripa IoT-enheter

och få tillgång till den stora mängd data som dessa potentiellt har så ökar möjligheten för en angripare att genomföra lyckade angrepp mot specifika nyckelpersoner.

Avlyssning har länge varit en välkänd metod för att samla in just den typ av information som beskrivs ovan, men ett hinder har varit svårigheten att placera lämplig avlyssningsutrustning i personernas närhet. Med den snabba tillväxten inom IoT-området sker en dramatisk ökning av antalet enheter som kan användas för avlyssning; enheter som dessutom placeras ut frivilligt av den som kartläggs. Exempel på enheter som kan användas för avlyssning är IP-kameror, datorer, smartphones, smarta klockor, trådlösa headsets och enheter för röststyrning av hem.

Stora mängder sårbarheter och angrepp

Tidigare handlade cyberattacker huvudsakligen om angrepp mot informationssystem, datanät och persondatorer. Med IoT kommer den fysiska världen i form av sensorer, ställdon, kontrollsystem och vardagliga objekt i allt större utsträckning att sammanflätas med internet, vilket möjliggör nya typer av angrepp. IoT-enheternas intåg innebär att en angripare kan ta kontrollen över de fysiska objekten och orsaka fysisk förstörelse eller till och med förlust av liv. Stuxnet-masken som riktade sig mot anrikningsanläggningar i Iran, angreppet mot det ukrainska elnätet 2015 och demonstrationer där forskare tagit total kontroll över en bil genom dess internetanslutning visar att angrepp mot IoT-enheter kan omfatta helt nya dimensioner än de som tidigare har observerats.

Säkerhetsbrister i installerade produkter åtgärdas sällan då det i många fall är en komplex procedur att installera uppdateringar och att detta måste göras manuellt av konsumenten. Dessutom är det vanligt att produkterna fortfarande används flera år efter att tillverkaren slutat släppa säkerhetsuppdateringar, något som gör det omöjligt för konsumenten att undvika säkerhetsbrister.

Överbelastningsattacker som använder IoT-enheter har ökat i antal under de senaste åren och har åstadkommit några av de kraftigaste störningarna på internet någonsin. I oktober 2016 attackerades en så kallad namnuppslagningsfunktion. Detta resulterade i att ett antal webbplatser var oåtkomliga för de flesta användare under flera timmar. Bland de drabbade webbplatserna fanns de svenska myndighetssidorna krisinformation.se och regeringen.se, men även ett antal kommersiella tjänster och nyhetsplatser såsom Netflix, Spotify, Twitter, BBC, CNN och Fox News. Detta angrepp, likväl som flera andra omfattande överbelastningsattacker, byggde på skadlig kod som infekterat stora mängder IoT-enheter.

Många angrepp leder till att angriparen får fullständig kontroll över enheten och dess information. I de fall där syftet är mer riktat mot personen eller organisationen som använder IoT-enheten kan användningen vara betydligt mer utstuderad än för exempelvis överbelastningsattacker. Det har exempelvis visats hur enkelt det är att manipulera videoströmmen som levereras av en nätverksansluten övervakningskamera för att dölja en händelse.

Delar av det ukrainska elnätet stängdes ner genom ett omfattande och avancerat IT-angrepp i december 2015. Angreppet byggde nästan uteslutande på sårbarheter i traditionella IT-system men inkluderade även angrepp mot IoT-liknande enheter. Under angreppet byttes mjukvaran ut i vissa komponenter vilket resulterade i att kommunikationen till anläggningarna inte längre fungerade. Detta medförde i sin tur att det krävdes manuella åtgärder på plats för att få igång eldistributionen och att delar av elnätet inte gick att fjärrstyra förrän den drabbade utrustningen hade ersatts.

Förstörande angrepp har även dykt upp på internet genom skadlig kod som riktar sig mot vissa IoT-enheter och gör dessa obrukbara. Det har spekulerats i vem som är det egentliga målet för dessa angrepp. En teori är att de är riktade mot tillverkarna som påverkas negativt av garantiärenden och dålig publicitet till följd av angreppen, där risken att tappa kunder och därmed förlora pengar anses kunna ge ett ökat incitament för säkrare produkter.

Angrepp där målet är att komma åt information i IoT-enheter riktas ofta mot enskilda personer eller organisationer, ofta opportunistiskt eller slumpvis valda, där information kan samlas in eller system tas över för exempelvis utpressningssyften, kartläggning eller övervakning. Uppmärksammade produkttyper är nätverksanslutna övervakningskameror och babymonitorer, som i ökande utsträckning förekommer i privatbostäder. Kända säkerhetsbrister är emellertid inte begränsade till dessa två produktkategorier utan har påvisats i ett brett spektrum av produkter såsom smarta TV-apparater, insulinpumpar, leksaker, vitvaror, industriella diskmaskiner, termostater, bilar och sexleksaker.

Det är synnerligen viktigt att IoT-leverantörer får kännedom om sårbarheter så att dessa kan åtgärdas. Det förekommer att statliga aktörer samlar kunskap om sårbarheter för egen underrättelseverksamhet istället för att rapportera dem till leverantörerna och göra dem allmänt kända, vilket är mycket oroande. Det finns inga garantier att kunskapen inte läcks och skadar allmänheten, något som även har inträffat då en läckt sårbarhet använts i ett utpressningsvirus som nått omfattande spridning.

Styrmedel för cybersäkerhet saknas

I dagsläget saknas det i princip styrmedel för att förbättra cybersäkerheten i civila produkter. Kundernas krav på cybersäkerhetsområdet är än så länge låga, speciellt för konsumentprodukter. Många typer av angrepp, exempelvis överbelastningsattacker, drabbar inte den person som äger utrustningen vilket gör att denne ofta känner liten anledning att bekymra sig om säkerheten i produkterna. Med ökande mediefokus på cyberangrepp och sårbarheter kan mycket väl konsumenternas medvetenhet om effekterna av bristande cybersäkerhet öka och därmed även de krav de ställer på tillverkarna.

Det finns diskussioner på EU-nivå om att införa en märkning, ”Trusted IoT Label”, för IoT-produkter som uppfyller vissa krav. Denna är tänkt att bygga på samma grundtanke som energimärkningen av exempelvis vitvaror, där egenskaperna presenteras på ett tydligt sätt för konsumenterna för att underlätta deras val och styra det mot säkrare produkter.

En annan väg att gå är lagstiftning och regleringar. En möjlighet är att utforma regleringen liknande systemet med obligatorisk CE-märkning av produkter som säljs inom EU. CE-märkningen lägger stort ansvar på tillverkare och importörer av produkter, något som överlag visat sig fungera bra inom exempelvis personsäkerhet hos elektriska produkter, maskiner och skyddsutrustning, även om det förekommer fusk där produkter CE-märks trots att de inte uppfyller kraven.

Så länge dagens låga incitament för producenterna kvarstår pekar alla tecken på att problematiken med bristande cybersäkerhet inom IoT-området kommer att fortsätta under överskådlig framtid. I och med att antalet installerade IoT-enheter ökar kan det antas att följdverkningarna av osäkra IoT-enheter kommer att växa.

För på vidare läsning

Farzad Kamrani, Mikael Wedlin, Ioana Rodhe, *Internet of Things: Security and Privacy Issues*, 2016, FOI-R--4362--SE.

9. Sveriges elförsörjning – hur möter vi en ökad sårbarhet?

Maria Andersson och Lars Westerdahl

Hela vårt samhälle har blivit starkt beroende av elförsörjning. Utan elektricitet slutar det mesta att fungera. Samtidigt är elförsörjningssystemet mycket sårbart och den pågående utvecklingen mot smarta elnät förstärker detta. Angripare kan redan ta sig in i dagens elnät i syfte att utföra cyberattacker. Dessa kan leda till stora störningar i samhället, vilket ett aktuellt exempel från Ukraina visar. Dessa ökade risker måste tas hänsyn till i den pågående omvandlingen av det svenska elförsörjningssystemet.

Elförsörjningssystemet som mål för cyberhot

Försvarets radioanstalt (FRA) meddelade i januari 2017 att man funnit spår av aktiviteter som misstänks ha varit förberedelser för cyberangrepp mot det svenska elnätet. I Ukraina skedde 2015 en cyberattack mot elnätet. Angreppet inleddes med att mejl med preparerade bilagor skickades till olika eldistributörer. Bilagorna innehöll skadlig kod vilket gjorde det möjligt för angriparna att ta sig förbi brandväggar och in i styrsystemet, och därifrån ta sig vidare till sitt huvudsakliga mål. Cyberattacken ledde till att hundratusentals abonnenter blev strömlösa. Efter några timmar kunde man manuellt återstarta elnätet.

Ett elförsörjningssystem i förändring

Det svenska elnätet håller på att utvecklas mot ett så kallat smart elnät. Smarta elnät karaktäriseras av en ökad användning av modern kommunikationsteknik. Data samlas in från fler aktörer, vilket skapar möjligheter till ingående analyser av olika tillstånd i elförsörjningssystemet. Analyserna kan bland annat ligga till grund för en mer kostnadseffektiv prissättning, förbättrade prognoser på efterfrågan samt en högre efterfrågeflexibilitet. Med smarta elnät finns goda möjligheter till förbättrad energi-effektivitet och minskade kostnader för elförsörjningssystemet. Men utvecklingen mot smarta elnät ökar även sårbarheten för cyberattacker.

Traditionella elnät distribuerar el i en riktning och produktionen är anpassad till ett schablonmässigt kundbehov. Elproduktionen har historiskt sett huvudsakligen skett i storskaliga elproduktionsanläggningar såsom vattenkraftverk och kärnkraftverk.

Smarta elnät kan ses som ett uppgraderat traditionellt elnät, där ny teknik installeras för förbättrad styrning och övervakning av alla delar av elförsörjningssystemet. Den nya tekniken gör det möjligt att bättre kunna balansera utbud och efterfrågan på el. Detta är en av anledningarna till att smarta elnät har en högre efterfrågeflexibilitet och bättre kan hantera variabel elproduktion från förnyelsebara energikällor såsom sol- och vindkraft. Ytterligare en drivkraft bakom utvecklingen mot smarta elnät är klimatpolitiken där klimatmålen i EU och Sverige ställer krav på att minska utsläppen av växthusgaser. Viktiga delar för att uppnå klimatmålen är att öka användningen av förnyelsebara energikällor och förbättra energieffektiviteten. Båda dessa områden gynnas av smarta elnät. Sammanfattningsvis så är det den storskaliga introduktionen av variabel elproduktion, samt krav på energieffektivisering och efterfrågeflexibilitet som skapat en efterfrågan på smarta elnät. I jämförelse med traditionella elät ställer smarta elnät större krav på att fler aktörer kommunicerar och samverkar med varandra.

Ökad sårbarhet

Elnätens styrsystem har traditionellt varit mer eller mindre isolerade från omvärlden. I takt med utveckling och prisfall på IT-komponenter har dessa i högre grad ersatt traditionella elektriska komponenter och företagsspecifika lösningar i styrsystem. Exempelvis används ofta hård- och mjukvarukomponenter samt kommunikationsprotokoll som från början har utvecklats för vanliga kontorssystem i de styrdatorer som används i elnätet. Denna utveckling har resulterat i att kontrollsystem och kontorssystem kan kommunicera med varandra. För affärsverksamheten i en organisation har detta inneburet en potentiellt ökad tillgång till mer aktuell information över vad som produceras. Denna information kan exempelvis användas i syfte att debitera kunden mer korrekt.

Sammankopplingen av system skapar inte bara ett ökat kommunikationsbehov utan ökar även exponeringen av produktions-, transmissions- och distributionssystem mot en miljö som de inte är designade att hantera. Ett ökat internt kommunikationsbehov ökar komplexiteten hos elförsörjningssystemet, samtidigt som en ökad exponering mot internet medför en öppning mot antagonistiska hot. En antagonist, det vill säga en medveten angripare som vill stjäla information, hindra tillgång till system eller utnyttja dem för egna intressen, är något som inte tidigare i någon större utsträckning behövts ta hänsyn till.

Säkerhetsfunktioner som är korrekt införda i ett system är i dagsläget svåra att ta sig förbi. Detta har medfört att angripare istället ger sig på människor genom exempelvis nätfiske (eng. *phishing*) och riktat nätfiske (eng. *spear phishing*). Dessa angrepp syftar till att lura personen som sitter vid en dator i målorganisationen att öppna en preparerad bilaga eller att klicka på en länk till en preparerad webbsida. Om angreppet lyckas, det vill säga användaren öppnar bilagan eller klickar på länken, har angriparen kommit förbi brandväggen och är inne på nätverket. Utifrån ett sådant fotfäste kan en angripare ta sig vidare mot sitt huvudsakliga mål. Elavbrottet i Ukraina 2015 är ett exempel på de sårbarheter som finns hos elförsörjningssystemet.

Behovet av strukturerat säkerhetsarbete

Risken för sårbarheter är större i komplexa system med flera aktörer. I en sådan miljö krävs ett strukturerat säkerhetsarbete mellan aktörer för att uppnå ett fullgott skydd för hela elnätet. Målet med säkerhetsarbetet är att ett system ska kunna bidra till verksamheten även om antagonister försöker angripa systemet. Detta uppnås med en kombination av utbildade människor, administrativa åtgärder och tekniska lösningar.

Ett kontinuerligt säkerhetsarbete blir särskilt angeläget för kontrollsystem med tanke på att de oftast har en lång livslängd, ibland upp till 20 år, och höga krav på tillgänglighet. Detta kan jämföras med kontorsbaserade IT-system, vilka ofta omsätts i intervallet 3–5 år. Varje aktör måste också därför arbeta systematiskt med säkerhetsfrågor för de egna systemen under hela dess livslängd.

Ett system designas för att kunna hantera kända sårbarheter. Efter hand som systemet underhålls och förvaltas kan nya sårbarheter tillkomma, till exempel genom en ökad exponering. Det innebär att ett system som inte förvaltas ur ett säkerhetsperspektiv försämras över tiden. Säkerhet är inte en produkt som tillförs ett system vid ett tillfälle, utan resultatet av ett långsiktigt och kontinuerligt arbete.

Säkerhetsanalys

Infrastruktursystem såsom elförsörjningssystem utvecklas sällan av en enskild systemägare. Flera aktörer interagerar i elförsörjningssystemet och systemet består av flera delsystem som behöver ta hänsyn till varandra. Förändringar i dessa delsystem sker inte samtidigt, vilket medför att nya och gamla delsystem behöver kunna utbyta information med varandra, och kan även ha beroenden mellan sig.

Att bygga IT-system för en miljö där det finns flera system med olika ägare ställer stora krav på gränsytorna mellan systemen för att kommunikation ska vara möjlig. Varje aktör måste säkerhetsställa sitt delsystems funktion samt identifiera vilka risker delsystemet utsätts för. Det är därför viktigt att delsystemägare har en gemensam syn på den hotbild deras system ska verka under. När ett nytt system ska införas blir säkerhetsanalysen ett viktigt verktyg för att identifiera vilka säkerhetsfunktioner som behövs och vilka rutiner som behöver stödja dessa.

Säkerhetsarbetet upphör dock inte när systemet tas i bruk, eftersom säkerheten i ett system kommer att försämras med tiden. IT-system innehåller svagheter som upptäcks efter hand och korrigeras genom uppdateringar (så kallad *patchning*). Om dessa uppdateringar inte installeras kommer systemet att innehålla kända svagheter.

Ett system som förvaltas förändras kontinuerligt vilket medför att nya säkerhethetsanalyser behöver genomföras kontinuerligt. Den funktionalitet som tillförs ett system efter att det tagits i bruk behöver granskas lika noggrant som nya funktioner görs under systemets utveckling.

Att förebygga cyberattacker

De grundläggande förutsättningarna för säkerheten i ett system skapas under systemets utveckling och genom underhållsarbete. Därutöver behövs ett aktivt säkerhetsarbete under systemets användning, med förebyggande och uppföljande aktiviteter över tiden. Ökad säkerhet uppnås med hjälp av tekniska lösningar, administrativa rutiner och en stödjande organisation.

Administrativa rutiner ger struktur åt säkerhetsarbetet. Det strukturerade säkerhetsarbetet fokuserar dock inte enbart på den funktionalitet som systemet ska leverera, utan även den funktionalitet som systemet faktiskt har. Det innebär att systemägaren måste känna till vad som finns installerat i systemet och vårda all funktionalitet alternativt ta bort sådant som är onödigt. Kontroll av underhållsarbetet, exempelvis installerade uppdateringar, är en del av säkerhetsarbetet.

I samverkande system, till exempel i elnäten där det finns flera aktörer, blir det ännu viktigare att aktivt övervaka de egna nätverken. De säkerhetsfunktioner som har tillförts i utvecklingsfasen är designade att hantera den hotbild om fanns när systemet togs fram. För ett system som varit i drift ett tag kan nya hot ha uppstått, vilka de gamla säkerhetslösningarna

inte alltid kan upptäcka eller hantera. Det blir därför viktigt att exempelvis vara uppmärksam på förändringar i kommunikationsmönster i de egna nätverken. För att upptäcka otillåten aktivitet på nätverket behövs övervakning, som exempelvis loggning, intrångsdetekteringssystem och antivirusprogram, men också personal som kan följa upp loggar och larm.

Att hantera cyberattacker

Ett upptäckt angrepp behöver hanteras, oavsett om det syftar till informationsstöld, att förhindra åtkomst eller att utnyttja systemfunktioner för egna syften. Hur denna hantering ska gå till beror på vilken typ av funktionalitet som systemet levererar. I ett informationssystem utan hårda tidskrav kan man välja att ta systemet ur drift för att åtgärda intrånget. Men för ett system som stödjer kritisk infrastruktur, såsom elnät, är detta inte alltid möjligt. I sådana fall får angreppet hanteras samtidigt som systemet fortsätter att stödja organisationens verksamhet.

Nyckeln till att hantera ett angrepp effektivt är förberedelser. En etablerad krisgrupp baserad på ett antal nyckelpersoner med god kännedom om verksamheten och med ett stort kontaktnät är en viktig resurs i ett sådant läge. Gruppen måste vara förberedd genom att i förväg ha gått igenom ett antal möjliga fall och ha upprättat handlingsplaner, kontaktlistor, med mera. En sådan grupp behöver inte enbart finnas till för att hantera cyberattacker utan kan vara en tillgång som ”allmän brandkår” inom en organisation.

Större organisationer kan etablera en fast grupp med hög teknisk kompetens för att hantera IT-problem, ett så kallat *Computer Emergency Response Team* (CERT). Dess uppgift är i första hand att så snabbt och effektivt som möjligt återställa ett angripet system och i andra hand att se till att samma problem inte uppstår igen. En CERT är kostsam att ha så dessa tenderar att vara branschsamarbeten eller nationella funktioner. Som externa resurser kan de stödja mindre organisationer med teknisk kompetens och kunskap om kända hot.

Smarta elnät innebär en högre exponering av styrfunktionalitet vilket ger en större angreppsyta mot systemen. Angreppsytan behöver dock inte medföra att det ställs krav på andra säkerhetsfunktioner i systemet. Däremot kan högre krav ställas på förmågan att upptäcka intrång i de egna systemen jämfört med tidigare, samt att kunna hantera incidenter. Ett ökat antal aktörer inom elförsörjningssystemen ställer dessutom högre krav på samordning av säkerhetsfrågor.

Det nya elförsörjningssystemet kräver både nya och gamla säkerhetslösningar

Det finns flera starka drivkrafter bakom utvecklingen mot smarta elnät, och utvecklingen kan komma att gå snabbt. Det är viktigt att inleda ett både intensifierat och strukturerat säkerhetsarbete redan i utvecklingsfasen, och att arbetet fortgår under elnätens hela livslängd. Ett aktivt säkerhetsarbete – där människor, administrativa rutiner och teknik samverkar – är en nödvändighet för IT-system med långa livslängder. Det medför att ett aktivt säkerhetsarbete är viktigt så länge systemet är operativt.

Angreppet mot elnätet i Ukraina 2015 exemplifierar väl detta behov. Även om bortfallet av el bara var några timmar hade angreppet pågått i flera månader. Det är vanligt att cyberattacker förblir oupptäckta i flera månader, ibland år, beroende på angriparens mål. I Ukrainafallet inleddes angreppet med en riktad nätfiskeattack i syfte att få ett fotfäste i nätverken. Därefter vidtog en lång period av spaning i nätverken i syfte att hitta en väg från den inledningsvis övertagna datorn till det faktiska målsystemet. Det är under denna period som ett aktivt säkerhetsarbete med övervakning skulle kunna ha upptäckt angreppet.

Det svenska elnätet, likt mycket annan kritisk infrastruktur, består av flera aktörer. Det är därför viktigt att incidenter kan rapporteras till en organisation där en överblick kan uppnås.

Händelserna i Ukraina påvisar också en annan viktig lärdom – att det är fortfarande viktigt med manuella återställningsfunktioner. För att få igång eldistributionen igen var teknikerna tvungna att tillfälligtvis återgå till manuella funktioner.

För vidare läsning

Admund Gudmunsson Hunstad, och Martin Karresand, *Monitorerings- och övervakningssystem*, 2017, FOI-R--4420--SE.

Jessica Johansson, *Litteraturstudie – Risk- och sårbarhetsanalyser i smarta elnät*, 2013, FOI Memo 4500.

10. Geografisk information – en vital resurs i förändring

Ulf Söderman, Simon Ahlberg och Gustav Tolt

Den pågående digitaliseringen av samhället leder till att vem som helst kan få tillgång till detaljerade geografiska data. Detta är en försvårande omständighet i svensk kris- och försvarsplanering som behöver uppmärksammas och som ställer krav på nya förhållningssätt. Att en betydligt större mängd data än tidigare kan bli allmänt tillgängliga ökar exempelvis behovet av kontroll över skyddsvärd information. Det antagonistiska perspektivet bör beaktas parallellt med den tekniska utvecklingen så att framtida panikåtgärder och obehagliga överraskningar kan undvikas. Geografisk information är en vital resurs i förändring och det finns ett behov av att utveckla en strategi och ett förhållningssätt till den.

En revolution avseende geografisk information

Tillförlitlig geografisk information är en förutsättning för effektiv krishantering och försvarsverksamhet. Informationen används för planering, övning och inte minst vid genomförande av insatser. Historiskt sett har geografisk information över det egna territoriet, till exempel topografiska kartor, varit en strategisk och noga kontrollerad resurs. Kunskap om lokala förhållanden som har kunnat ge fördelar gentemot potentiella motståndare har använts vid försvarsplanering och haft en begränsad spridning.

Idag pågår en mindre revolution avseende geografisk information. Med digitaliseringen av samhället kommer nya tekniska system för insamling av data, förbättrad infrastruktur för lagring, bearbetning och distribution samt nya system för presentation av resultat. Vi kan se en ökad användning och spridning av detaljerad geografisk information samtidigt som vi plötsligt inte längre har kontroll över och exklusiv tillgång till denna information. Att enskilda dataset i sig blir mer tillgängliga behöver dock inte utgöra säkerhetsrisker, men en helt annan situation kan uppstå om flera informationsmängder sammanförs eller tolkas med rätt bakgrundskunskap.

Digital geografisk information för alla

Noggrann geografisk information är inte längre förbehållen begränsade grupper och dess spridning är inte lika noga

kontrollerad som tidigare. I den pågående digitaliseringen av samhället finns inte bara en tydlig trend mot ökad användning och spridning av detaljerad geografisk information. Allt fler röster hörs också med krav på att fritt få använda och distribuera sådan data, exempelvis för att främja nyföretagande. Detta gäller särskilt om informationen är offentligt finansierad.

Bakom detta finns en kraftfull teknisk utveckling. Med nya sensorsystem kan stora mängder detaljerade data enkelt samlas in. Digitala kameror ger skarpa bilder, radarsensorer mäter på långa avstånd och ser genom moln, och positioneringssystem gör att insamlade data enkelt och noggrant går att knyta till geografiska positioner. Sensorerna blir dessutom allt billigare och finns snart överallt – i allt från mobiltelefoner till drönare och i våra fordon. Flera stora kommersiella aktörer, men också nischade hightechbolag i både Sverige och utlandet, bygger upp enorma mängder allmänt tillgänglig geografisk information. Det finns även initiativ där användare går samman för att samla in och organisera geografiska data som sedan tillhandahålls gratis. Ett exempel på detta är OpenStreetMap, som erbjuder alla intresserade öppen kartdata.

Samtidigt utvecklas också en digital IT-infrastruktur i rasande tempo med nya kraftfulla system för att hantera stora mängder data. System baserade på artificiell intelligens lär sig känna igen företeelser, hitta mönster och blixtsnabbt anpassa information efter våra önskemål. Till detta utvecklas också nya presentationssystem för att snabbt och enkelt åskådliggöra resultat. Ett aktuellt exempel är så kallade VR-glasögon som gör det möjligt att på ett helt nytt sätt ta till sig 3D-representationer av omvärlden.

Geografisk information skapar samhällsnytta

Vad en konstant tillgång till aktuella nationella data kommer att innebära för utvecklingen av nya tjänster kan vi idag bara sia om. Detaljerade data som till exempel Lantmäteriets nya höjddata, vilka baseras på bearbetning av flygbilder, kan ligga till grund för en mängd olika tillämpningar inom vitt skilda områden. De kan till exempel användas för att planera skogsbruk, bestämma var solpaneler ska placeras eller analyseras för att se hur landskapet och olika miljövärden förändras över tid. Givetvis kan den också användas i militär verksamhet. Många nya tjänster och produkter kommer även att dra nytta av de allt bättre och mer detaljerade data för att hjälpa oss i vår vardag, till exempel navigera självkörande bilar eller visualisera tänkta byggprojekt i en så kallad förstärkt verklighet (*augmented reality,* AR).

Även om den tekniska utvecklingen öppnar för många nya innovativa tillämpningar hänger mycket på tillgängligheten till data. Bland utvecklare och slutanvändare ökar intresset för så kallade öppna data – data som är fri att använda, återanvända och distribuera. Där finns också en stark drivkraft att främja innovation och företagande för ekonomisk tillväxt både på det lokala och det nationella planet. Sammantaget kan stora samhällsekonomiska vinster göras såväl i form av nya produkter och tjänster som i effektivisering av befintlig verksamhet.

Ett exempel på utvecklingen med öppna geografiska data är Helsingborgs kommun, som nyligen gjort en stor del av sina data allmänt tillgängliga på internet. Förutom grundläggande geografisk information finns även händelseinformation från väktare, polis och brandförsvar samt driftinformation bestående av felanmälningar och synpunkter från medborgarna. Data kan laddas ned till egen dator eller nås direkt via internet. Flera appar har redan sett dagens ljus i spåret av detta initiativ. Helsingborg är dessutom inte ensamt – flera andra kommuner arbetar redan med liknande projekt.

På nationell nivå pågår en liknande utveckling. Lantmäteriet har under flera år drivit frågan och en del av myndighetens data finns idag fritt att hämta och använda, bland annat väg- och terrängkartor. Flera andra myndigheter har också öppnat delar av sina data. Lantmäteriet vill gå vidare och göra ytterligare data fritt tillgängliga men hindras för närvarande av att en väsentlig del av myndighetens finansiering förväntas komma från avgifter för den geografiska informationen. Lantmäteriet har redovisat analyser av nytta med öppna geografiska data och gjort framställan till departementet med önskemål om förändringar. Med en fortsatt utveckling i denna riktning kan stora delar av Lantmäteriets nationella geografiska information komma att göras tillgänglig som en öppen och enkelt tillgängliga resurs.

Öppna data kan bli ett säkerhetshot

Givet den ökade tillgången till geografisk information och den ökade efterfrågan på ännu mer data, vilka blir konsekvenserna ur ett försvars- och krishanteringsperspektiv? Vad händer om vem som helst kan sammanföra data i helt nya kombinationer? Är det möjligt – eller ur ett samhällsutvecklingsperspektiv ens önskvärt – att försöka strypa den pågående trenden med den ökande tillgången till geografisk information? Detta är svåra frågor som bör hanteras på nationell nivå. Sverige är av tradition ett högteknologiskt och innovationsvänligt land. Nya tekniska framsteg anammas snabbt och i strävan att exploatera och kapitalisera på ny teknologi håller varken

lagstiftning eller riskhantering jämna steg. Då blir det lätt en överreaktion och krav ställs på förbud eller kraftiga inskränkningar i användningen av ny teknik. En liknelse kan göras vid den snabba utvecklingen av obemannade flygande farkoster och de möjligheter som dessa erbjuder. Då riskerna uppenbarades med flygande farkoster och då användningen av ombordkameror stod i strid med rådande integritetslagstiftning kom ett domstolsavgörande som effektivt hindrade företag från att använda sådana farkoster i sin verksamhet. Det behöver inte vara så. Om det antagonistiska perspektivet beaktas i utvecklingen så kan förebyggande åtgärder, lagstiftning och användning utvecklas parallellt.

Öppen och lättillgänglig geografisk information är även lätt tillgänglig för nya grupper av antagonister och det är inte svårt att föreställa sig hur den underlättar för planering av fientliga aktioner. Möjliga framryckningsvägar kan analyseras, platser lämpliga för landstigning eller luftlandsättning kan identifieras och målkoordinater för precisionsbekämpning kan bestämmas med mycket god noggrannhet. I ett värsta scenario kan en person eller grupp med fientliga avsikter genomföra all planering inför en aktion helt och hållet utan att behöva besöka platsen och därmed riskera att dra till sig uppmärksamhet som kan avslöja planerna. Attentat kan också i framtiden tänkas ske med autonoma farkoster som programmeras att agera helt eller delvis självständigt. Utifrån detaljerad geografisk information kan deras förflyttning och slutdestination ges med väldigt hög noggrannhet.

Mycket talar för att vi ur ett försvars- och krishanteringsperspektiv behöver uppmärksamma och fundera över hur vi på bästa sätt bör förhålla oss till den nya spelplan som växer fram. I ett militärt scenario kan en motståndare ha minst lika detaljerad information som vi och utnyttja den väl så effektivt. Vi behöver analysera vilka risker det medför och hur det påverkar vår försvars- och krisplanering. I det sammanhanget bör såväl skydd som användning av informationen beaktas.

Öppna och privata data i okända händer

Det är också viktigt att ta med i beräkningen att teknikutvecklingen fortsätter och situationen kan bli ännu mer svårbemästrad. Så länge det är frågan om öppna geografiska data eller andra typer av allmänt tillgängliga data och tjänster finns fortfarande möjligheten att ha kännedom om vad en motståndare kan tänkas ha tillgång till. Problemet blir annorlunda när nya tillämpningar utvecklas där olika aktörer också kombinerar allmänt tillgängliga information med egen

insamling av data och underrättelser. När det gäller nationer med stora resurser är detta ingen ny utveckling – så har det alltid varit och kommer fortsätta vara. Skillnaden är att vi idag står på tröskeln till en utveckling där allt fler kommersiella aktörer blir involverade. Både användning och tillgång till data hamnar alltmer utanför vår kontroll. Behovet att ha kontroll över skyddsvärd information kommer därför med stor sannolikhet att öka.

Ett konkret exempel är den snabba utvecklingen av självkörande bilar. En vital komponent i den utvecklingen är en databas med mycket detaljerad geografisk information. På varje fordon kommer det att finnas flera sensorer som analyserar den omedelbara omgivningen. Resultatet läggs ihop med information om en lite större omgivning från en databas för att på ett säkert sätt köra bilen mot målet. Insamlade sensordata skickas också till databasen så att den kan uppdateras med den senaste informationen längs den aktuella färdvägen. Med hjälp av data från hundratusentals fordon blir databasen snabbt en dynamiskt föränderlig, otroligt detaljerad 3D-karta med stora mängder aktuell information om både trafikläget och infrastrukturen för i stort sett hela trafik- och vägmiljön.

Informationen krävs för att få trafiken att flyta bättre. Trafikstockningar rapporteras snabbt och andra trafikanter kan omgående få hjälp med att omplanera sin färdväg så att stopp kan undvikas. Men hur kan man hindra att en efterlyst person inte får hjälp av systemet att komma undan? Om polisen efter till exempel ett attentat stoppar kollektivtrafik och upprättar vägspärrar påverkas trafikflödet omedelbart. Databasen och systemet som programmerats för att upprätthålla ett flöde och hjälpa trafikanter omplanerar och hjälper nu istället den efterlysta med uppgifter om aktuella avspärrningar och ger råd om alternativa vägar för att komma fram på enklast och snabbaste sätt.

En nationell strategi behövs

I förlängningen av exemplet med de självkörande bilarna finns ett scenario där den som förfogar över databasen kommer att kunna ha tillgång till mer detaljerad och aktuell information över trafik- och vägmiljön än ansvariga kommuner och myndigheter. Även för många andra syften kommer geodata av olika slag att samlas in och sannolikt lagras i flera olika databaser placerade utanför nationsgränsen. Vem äger alla dessa data? Kommer ett privat konsortium av biltillverkare att godtyckligt kunna sälja och distribuera information om svensk väginfrastruktur till vem som helst? Kommer det att

innebära att vi till slut inte vet vem som har tillgång till och kan använda aktuell och detaljerad geografisk information om vårt eget territorium? Vilken kontroll över detaljerad geografisk data kommer vi då själva att ha i en förlängning? I frågan om samtalsinformation finns möjlighet att få ut denna från mobiltelefonoperatörer vid misstanke om grova brott. På liknande sätt skulle frågor avseende lagstiftning och regelverk kring behandling av geografiska data kunna utredas.

Utvecklingen ger upphov till en rad komplicerade frågor som måste besvaras. Geografisk information är en vital resurs i förändring och vi behöver uppmärksamma detta och utveckla en strategi och ett förhållningssätt för att motta förändringen på bästa sätt. Det är inte minst viktigt som en del i arbetet att bygga ett fritt, öppet och samtidigt tryggt och säkert samhälle.

11. Hotet från långräckviddiga vapen

Erik Berglund, Martin Hagström och Anders Lennartson

Vapensystem med lång räckvidd för bekämpning av mark-, sjö- och luftmål får allt mer uppmärksamhet. Det kan handla om amerikanska och ryska kryssningsrobotar mot mål i Syrien, ryska ballistiska robotar i vårt närområde eller amerikanskt missilförsvar i Korea. Förekomsten av långräckviddiga vapnen har potentiellt en stor inverkan på säkerhetspolitiken. Till viss del kan denna ses som överdriven. En bidragande orsak är att det finns en tendens att förenkla de möjliga effekterna av långräckviddiga vapen genom att betrakta de olika vapnens nominella räckvidder ur ett rent geometriskt perspektiv. Detta återspeglar sällan det faktiska hotet mot framför allt rörliga mål. Försvars- och säkerhetspolitiska överväganden måste bygga på realistiska hotbedömningar och därför är det av stor vikt att göra korrekta hotanalyser baserade på tekniska fakta.

Vapen med lång räckvidd utgör i många fall såväl en taktisk som strategisk fördel i en konflikt. Lång räckvidd betyder att en aktör kan projicera ett hot från en egen skyddad position utan att själv utsättas för motståndarens direkta hot. Samtidigt tvingas motståndaren anpassa sitt taktiska uppträdande och vidta olika skyddsåtgärder.

Begreppet långräckviddiga vapen syftar oftast på robotar. Robotar kan vara avsedda att träffa olika typer av mål – fasta eller rörliga – och kan skjutas iväg från marken, flygplan eller fartyg. Beroende på mål, syfte och konstruktion benämns robotar på olika sätt. Kryssningsrobotar och ballistiska robotar används mot fasta mål på marken. Ballistiska robotar skjuts med hög hastighet upp till hög höjd och får sedan falla mot ett förutbestämt mål i en ballistisk kastbana. Ballistiska robotar har traditionellt använts för att nå mål på marken mycket långt bort, exempelvis på andra kontinenter. Kryssningsrobotar är ofta konstruerade för att flyga långsammare än ballistiska robotar och på låg höjd. De navigerar och har en motor som driver fram roboten under hela färden.

Sjömålsrobotar och luftvärnsrobotar är exempel på robotar som används mot rörliga mål. För att en robot ska kunna träffa ett rörligt mål krävs en målsökare, det vill säga en sensor med syfte att styra in roboten mot målet. Sjömålsrobotar är

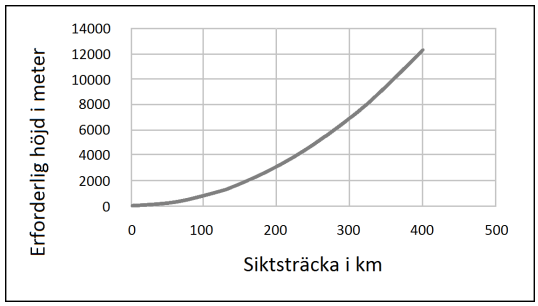
kryssningsrobotar som utrustas med en målsökare för att kunna träffa fartyg. Luftvärnsrobotar skjuts från marken eller fartyg mot rörliga luftmål, såsom flygplan eller andra robotar.

Under det senaste decenniet har robotsystem med lång räckvidd blivit vanligare i vårt närområde. Ryssland har exempelvis stationerat markroboten *Iskander* och luftvärnsroboten *S-400* i Östersjöområdet. Därutöver finns kryssningsroboten *Kalibr* på fartyg i Östersjön. Finland och Polen har anskaffat vapen med lång räckvidd i form av den signaturanpassade kryssningsroboten *JASSM*. Tyskland har sedan några år kryssningsroboten *Taurus KEPD 350*. I Sverige uppgraderar försvaret sina sjömålsrobotar. Även i andra delar av världen är kryssningsrobotar och ballistiska robotar aktuella vapen. I Syrien har såväl USA som Ryssland gjort insatser med kryssningsrobotar och i Nordkorea sker ständigt mer eller mindre lyckade uppskjutningar av till synes allt mer avancerade ballistiska robotar.

Den faktiska hotbilden mot rörliga mål

Det finns en avgörande skillnad i hotet från robotar som används mot fasta respektive rörliga mål. Ett rörligt mål som varierar sin bana måste ständigt mätas in. Rörligheten är därmed ett skydd i sig och teknikövertaget är fortfarande hos målet. För fasta mål har dock teknikutvecklingen medfört ett överläge för kryssningsrobotar och ballistiska robotar gentemot målet.

Det Ryska luftvärnssystemet S-400 har uppmärksammats mycket i Sverige. Med en räckvidd om uppemot 400 km kan S-400 nominellt nå svenskt territorium. Den faktiska räckvidden för ett luftvärnssystem har emellertid flera praktiska begränsningar. En uppenbar begränsning är jordytans krökning, vilket illustreras i figuren nedan. Ur figuren kan man läsa ut att ett flygplan måste flyga på höjder över 12 000 meter för att kunna synas ovan horisonten från marken på 400 km avstånd. Eller vice versa, för att se marken på 400 kilometers avstånd måste en observatör befinna sig på 12 000 meters höjd. Ett flygplan som flyger på låg höjd syns alltså inte på långt avstånd. På stora avstånd skulle ett luftvärnssystem i klass med S-400 kunna skjuta ner exempelvis ett trafikflygplan som flyger rakt fram på marschhöjd (11 km). Mot ett manövrerande stridsflygplan på låg höjd är däremot den faktiska räckvidden för S-400 snarare mellan 0 och 20 km, beroende på terrängen.



Figur 1. Erforderlig höjd i meter för att kunna se ett mål på marken (siktsträcka).

En annan begränsning är robotens flygtid. Tiden det tar för en luftvärnsrobot att färdas 400 km är cirka tio minuter. Under samma tid hinner ett stridsflygplan förflytta sig över hundra kilometer. För att en långräckviddig luftvärnsrobot ska ha en chans att träffa ett snabbt och manövrerande mål som ett stridsflygplan måste den därför under flygningen mot målet få uppdaterad information om målets aktuella läge och hastighet flera gånger. Målet måste alltså mätas in med flygande eller fasta radarstationer. Dessa måste vara placerade så att de har fri sikt till målet och data om målet måste kunna sändas till roboten via en datalänk.

Exemplen ovan illustrerar att en enskild luftvärnsenhet därför endast utgör ett begränsat hot mot stridsflyg. För att ett luftvärnssystem ska vara riktigt effektivt krävs att det utgörs av ett nätverk av sensorer och vapenplattformar. Verkan på stora avstånd kräver dessutom flygburen radar. Effekten av ett luftvärnssystem är således ofta beroende av kopplingen till komplexa sensorplattformar och informationssystem.

Hotet från ett luftvärnssystem i exempelvis Kaliningrad eller på Gotland kan alltså inte beskrivas med enkla resonemang baserade på nominell räckvidd där luftvärnet antas ha samma effekt inom hela denna räckvidd. Ett flygplan som startar från en flygbas i Sverige kan inte heller i startögonblicket skjutas ner av ett luftvärn baserat på andra sidan Östersjön, främst beroende på luftvärnsrobotens flygtid till målet. För att bekämpa rörliga mål krävs en kvalificerad kedja av sensorer, ledningsfunktioner, vapenbärare och vapen. Detta ställer stora krav på både inmätningsnoggrannhet och snabbhet. I dagsläget är det troligen endast USA som har tillräckliga resurser för att använda långräckviddiga markmålsvapen mot rörliga eller starkt tidskritiska mål.

Ett hot främst mot fasta mål

Insatser mot fasta markmål kan ske med system med lång räckvidd utan hjälp av komplexa sensorsystem eftersom målens position är känd. Kryssningsrobotar och ballistiska robotar för insatser mot markmål är därför hot som svenska försvaret måste beakta.

Insatser med ballistiska robotar eller kryssningsrobotar kan med dagens navigeringsteknik göras med god precision förutsatt att målet kan upptäckas, identifieras och mätas in. Mot fasta mål som byggnader, flygbaser och delar av elkraftnätet kan inmätningen göras i förväg, eventuellt via flygspaning eller satellitbilder.

Ballistiska robotar som kan utgöra ett hot mot Sverige finns främst i Ryssland. *Iskander* har en räckvidd som ofta anges som 400-500 km och kan därmed nå delar av Sverige. *Iskander* har kort flygtid – mindre än tio minuter från andra sidan Östersjön – samt god precision. Den kan inte användas mot rörliga mål, men den korta flygtiden gör att den kan användas mot viktiga mål av tillfällig karaktär som större lednings- och omlastningsplatser.

Utvecklingstrender

Utvecklingen av högteknologiska långräckviddiga vapen ser ut att fortsätta. Den pågående utvecklingen inom främst navigeringsområdet i kombination med en allmän teknologispridning gör att kryssningsrobotar som kan användas mot fasta markmål blir billigare. Detta innebär att kryssningsrobotar som hittills varit dyra potentiellt kan bli ett mängdhot och dessutom tillgängliga för en växande mängd aktörer, även ickestatliga sådana. Att ickestatliga aktörer kan få tillgång till kryssningsrobotar kan vidga hotbilden från att vara ett militärt hot till att även utgöra ett terrorhot.

En högteknologisk utvecklingstrend är system med en ökad samverkan mellan sensorer och robotar, det vill säga nätverk av sensorer, vapenplattformar och vapen. Samverkan mellan delsystemen syftar i första hand till att bygga en tillräckligt god lägesbild för att genomföra en insats. Vidare syftar den till att ge roboten tillräckligt aktuella måldata för träff och att göra det möjligt för flera robotar att komma samtidigt till målet. Här är sensorer med god prestanda och säkra datalänkar av avgörande betydelse. USA är ledande inom utveckling av samverkande bekämpningssystem, främst för bekämpning av markmål. I Sverige pågår i princip ingen egen utveckling av samverkande bekämpningssystem.

Robotar med höga hastigheter är en annan trend. Med höga hastigheter menas här farter på 3000 km/h eller mer. Genom korta bantider minskar målets möjligheter att vidta motåtgärder som att manövrera undan eller skjuta tillbaka. Höga hastigheter är också viktiga för att minska tiden som den anfallande roboten kan utsättas för luftförsvar i målets närhet. Ett exempel på höga hastigheter är den rysk-indiska sjömålsroboten *BRAHMOS* som kan flyga med ungefär 3000 km/h och den kommande *BRAHMOS II* som är tänkt att nå farter över 5000 km/h.

Skydd mot långräckviddiga robotvapen

Under det kalla kriget utgjorde fientligt bombflyg och sabotage det främst hotet mot fasta installationer. Det var möjligt att försvåra inmätning av målpositioner genom avspärrningar, maskeringar och begränsning av informationsspridning. Fientligt bombflyg skulle vara tvunget att komma relativt nära för att kunna sätta in sina vapen och kunde därmed utsättas för hotet från motverkande luftvärn. Idag är det svårt att motverka inmätning av fasta installationer eftersom satellit- och flygfoto är lätt tillgängligt även för aktörer utan egna spaningssystem.

Luftvärn kan användas mot både kryssningsrobotar och ballistiska robotar, men det finns en påtaglig obalans i att försvarsvapnen ofta är dyrare än de anfallande robotarna och att den yta som luftvärnet kan skydda är liten. Kryssningsrobotar flyger lågt och kan utnyttja terrängen för att undgå upptäckt, medan ballistiska robotars höga fart gör att luftvärnsrobotarnas effektiva räckvidd begränsas. I praktiken innebär dessa begränsningar att ett avancerat luftvärnssystem med en nominellt lång räckvidd endast kan skydda en yta som motsvarar en flygbas eller en medelstor stad. Med avancerade sensorsystem kan en större yta skyddas men sådana system är tekniskt avancerade och kostsamma. Sensorutrustade spaningsflygplan som flyger på hög höjd kan öka förvarningstiden för luftvärnssystem från sekunder till minuter. Detta kräver emellertid en konstant närvaro i luften och i praktiken en stor flotta av sådana spaningsflygplan. Sverige har för närvarande två spaningsflygplan av denna typ.

Utvecklingen har skapat ett tekniskt överläge för hotsystemen mot fasta mål men även en obalans i kostnader mellan hot- och skyddssystem. Detta illustrerades nyligen då Israel avfyrade två Patriot-robotar, som kostar omkring 30 miljoner kronor styck, för att skjuta ner en drönare över Syrien. Om utvecklingen fortsätter och kryssningsrobotar i framtiden utgör ett mängdhot innebär det att kostnaderna för att skydda sig med dagens luftvärnssystem blir mycket höga.

Ett sätt att motverka både luftvärnsrobotar och robotar avsedda för fasta mål är att slå ut robotarna innan de skjuts upp. Utöver långräckviddiga vapen kräver detta god underrättelseinformation om robotarnas placering. Kravet på sådan underrättelseinformation blir extra stort om en angripare använder rörliga avfyringsramper. Ett sätt att skydda sig mot robotar som är beroende av navigeringssystem är att störa ut dessa, vilket reducerar risken för träff i målet. En sista åtgärd är fysiskt skydd, exempelvis att fasta mål placeras i bergrum. Skyddsåtgärder som maskering och skenmål är högst relevanta.

När det gäller skyddet av rörliga mål har duellen inte förändrats lika dramatiskt. För att en motståndare ska träffa ett rörligt mål måste målet mätas in. Motståndarens sensorbärare för målinmätning kan vara sårbara, både för fysiska angrepp och för så kallade telemotmedel. Dessutom krävs att motståndaren har en snabb och välfungerande kedja av sensorer, ledningsfunktioner och vapen för att kunna bekämpa ett rörligt mål.

En korrekt teknisk bedöming är nödvändig för rätt typ av skydd

Robotsystem med lång räckvidd är mycket kraftfulla vapensystem och de spelar en allt större roll för bekämpning av mark-, sjö- och luftmål i många stridssituationer. Den tekniska utvecklingen har medfört att kryssningsrobotar och ballistiska robotar kan nå mål långt bort från avfyringsplatsen med stor precision. Särskilt mot rörliga mål är dock skillnaden mellan den nominella effekten av långräckviddiga vapen och det faktiska hotet mycket stor.

Skyddsåtgärder och motmedel skiljer sig åt för rörliga respektive fasta mål. Motmedel och skydd är mycket kostsamma och bör sättas in där de får störst effekt. Därför är det av stor vikt att analysera hotet från långräckviddiga vapen utifrån tillgängliga fakta och teknisk kunskap för att avgöra vad som utgör de största faktiska hoten mot olika typer av skyddsvärda mål, och hur skyddet av dessa mål bäst bör utformas. Försvars- eller säkerhetspolitiska åtgärder mot ett övervärderat hot kan vara mycket kostsamma. Att övervärdera hotet kan därmed potentiellt vara lika skadligt som uteblivna åtgärder mot ett undervärderat hot.

12. Behovet av en svensk försvars- och säkerhetsstrategi för rymden

Sandra Lindström och John Rydqvist

Sverige är inom vissa områden en avancerad rymdnation. Den svenska militära rymdverksamheten är dock liten och det är idag framförallt civila och kommersiella intressen som driver det svenska rymdengagemanget. Detta reflekteras i det förslag på en svensk rymdstrategi som kom ur 2015 års Rymdutredning. Beroendet av rymdtjänster ökar i takt med större användning. Det gäller även militär rymdverksamhet som får ökad betydelse. Om inte de försvars- och säkerhetspolitiska aspekterna av rymdverksamheten på ett tydligare sätt beaktas i svensk rymdpolitik riskerar Sverige att stå sämre förberett för att kunna utveckla det framtida nyttjandet av rymdtjänster, samt att möta de hot och risker som kan uppkomma när andra aktörer flyttar fram sina positioner inom området. Detta kan på sikt innebära en risk för vår nationella säkerhet.

Rymdens betydelse i ett försämrat säkerhetsläge

Sveriges säkerhetspolitiska situation har försämrats sedan 2008. Som småstat, med intresse av att värna och främja de normer och överenskommelser som det rådande internationella systemet grundar sig i, har Sverige vidtagit ett antal åtgärder för ökad gemensam säkerhet. Förutom med EU utvecklas särskilt viktiga säkerhetspolitiska partnerskap också med USA, Finland, Norge och försvarsalliansen Nato. Åtgärder som stärker möjligheterna till gemensamt agerande i händelse av kris och krig kompletteras med förmågor och bättre samordning, lägesbild, informationsdelning och säkrad infrastruktur för totalförsvaret.

Rymdsystem och rymdtjänster har för många stater ända sedan 60-talet varit viktiga för att förstärka förmågan att förebygga risker och hot, samt för att öka förmågan att kunna försvara sin stat. Idag använder många stater rymdbaserade navigeringstjänster, satellitövervakning och satellitbaserad kommunikation, både civilt och militärt. I flera fall är det samma system som nyttjas av båda sektorerna och rymden är en av de arenor där denna typ av dubbelanvändning är mest tydlig. Det sker också en snabb teknisk och konceptuell utveckling inom rymddomänen. Rymdbaserade system bedöms därför spela en ännu större roll för försvar och säkerhet i framtiden.

Sverige har varit sen med att göra en koppling mellan säkerhetsarkitekturen i rymden och försvars- och säkerhetspolitik. En av huvudanledningarna är att den svenska rymdverksamheten i huvudsak varit en akademisk och industriell fråga, vilket har lett till att utvecklingen av den civila rymdverksamheten varit helt dominerande. Samtidigt använder Sverige dagligen rymdtjänster inom försvars- och säkerhetssektorn. Denna användning kommer sannolikt att öka i takt med att utbudet av rymdtjänster växer och får ökad kvalitet. Hittills har den militära utvecklingen på rymdområdet skett inom olika parallella verksamheter, som ett resultat av kortsiktiga operativa behov, snarare än som ett resultat av en långsiktig övergripande strategi.

Rymdtrender och framtida rymdhot

Resultatet av den globala utvecklingen i rymddomänen är att även Sverige har blivit mer produktivt och effektivt. Exempelvis nyttjas satellitkommunikation för att få ut krisinformation vid större olyckor när mobilnätet har slagits ut eller överbelastats. Satellitnavigering gör att vi sparar pengar vid vägbyggen och det bidrar till en mer bränslesnål lastbilstrafik. För börser, banker och tradingbolag är den exakta tidsangivelsen som GPS-satelliterna levererar nödvändig för att kunna bedriva verksamheten. Detta skapar samtidigt beroenden i samhället som i sin tur leder till ett antal konkreta hot och risker som Sverige måste kunna hantera. Internationellt diskuteras tre övergripande hot och risker, med bäring på försvar och säkerhet, i rymdsammanhang:

För det första ökar många stater sin militära förmåga med hjälp av satellittjänster, både via egna system men även via det ökande utbudet av kommersiella tjänster. Det finns även exempel på icke statliga aktörer, till exempel rebell- och terroristgrupper som nyttjar rymdtjänster. Tillgången till rymden säkras genom fler självständiga nationella program för utveckling av uppskjutningsraketer, en teknik som även kan användas för att utveckla ballistiska robotar. Iran och Nordkorea har numera uppskjutningskapacitet. Pakistan och Turkiet har pågående program.

För det andra leder den militära logiken till att koncept och planer utvecklas för att förhindra en potentiell motståndare att få tillgång till rymdtjänster i händelse av en konflikt. Detta är en konsekvens av att rymdsystem för flera stormakter är helt avgörande för att kunna hantera breda nationella säkerhetsfrågor liksom för militär verksamhet. Här är beroendena av rymdsystem och rymdtjänster särskilt tydliga och med dessa

beroenden följer behovet av att säkra och skydda sina system. USA, Ryssland och Kina har exempelvis på olika sätt fortsatt att utveckla anti-satellitteknik.

För det tredje ökar mängden rymdskrot drastiskt. I takt med att rymden nyttjas mer frekvent och av fler aktörer ökar både mängden satelliter och okontrollerbara föremål i omloppsbana. Detta leder till en förhöjd risk för kollisioner mellan rymdskrot och satelliter. Det finns idag inte något effektivt sätt att samla in föremålen och det finns inte heller en internationell samsyn på hur problemet ska hanteras. Dessutom kan det ta lång tid innan skrotet faller ner och försvinner, ibland hundratals år. Det finns scenarier där skrotmängden på grund av flera på varandra följande kollisioner ökar exponentiellt och till slut gör rymden obrukbar. Samma effekt skulle en medveten attack mot en satellit kunna resultera i.

En begränsad svensk rymdstrategi

Även om Sverige har blivit mer produktivt och effektivt i och med den allt bredare användningen av rymdtjänster så finns det stor förbättringspotential för att uppnå en starkare och mer konkurrenskraftig svensk rymdverksamhet. Behovet av en sammanhållen strategi för utvecklingen på rymdområdet har därför uppmärksammats på senare år. Resultatet blev att regeringen tog initiativ till en rymdutredning som skulle lämna förslag på en sådan strategi.

År 2015 utkom utredningsbetänkandet *En rymdstrategi för nytta och tillväxt*. Texten är främst formulerad utifrån civila och kommersiella intressen. Målsättningen med strategin är att svensk rymdverksamhet ska bidra till tillväxt och ökad sysselsättning, vilket avspeglar det traditionella sättet att bedriva rymdverksamhet i Sverige.

Givet de försvars- och säkerhetspolitiska risker som diskuterats ovan är inriktningen i detta betänkande problematiskt. Förvisso lyfts frågan om behovet av bättre civil-militär samordning, men i stort saknas ett försvars- och säkerhetsperspektiv. Det är en brist i ett dokument som ska ligga till grund för en nationell rymdstrategi och det leder till ett antal frågor, exempelvis:

- Finns det en tillräcklig förståelse för säkerhetsimplikationerna med befintliga och framtida rymdsystem, och är den svenska användningen genomtänkt?
- Finns det tillräcklig kunskap, rätt kapacitet och samordning för att kunna bedöma motståndare och möta eventuella antagonistiska hot?

- Hur använder vi den kunskap och erfarenhet som finns civilt när medvetenheten om rymdens betydelse i ett försvars- och säkerhetspolitiskt sammanhang blir mer påtaglig?
- Vilka risker för det med sig om det försvars- och säkerhetspolitiska perspektivet inte får genomslag i en nationell rymdstrategi?

Rymdverksamhet bedrivs generellt i fyra olika sektorer: den civila, den kommersiella, den militära och underrättelsesektorn. Den nationella rymdstrategin skulle tydligare än vad som framkommit i utredningens förslag kunna koppla an till alla dessa fyra sektorer genom att staka ut hur Sverige kan bibehålla och utveckla befintliga styrkor i sin rymdverksamhet, samt föreslå hur försvars- och säkerhetspolitiska aspekter av utvecklingen i högre grad ska kunna beaktas som komplement till och förstärka närings- och utbildningsaspekterna. Rymdstrategin skulle på ett mer visionärt sätt kunna identifiera vilka möjligheter som finns på längre sikt i försvars- och säkerhetssektorn i och med den snabba utvecklingen inom rymdområdet.

Rymdens möjligheter för svenskt försvar

Sverige är inom vissa områden en avancerad rymdnation. De internationella trenderna inom rymdområdet sammanfaller delvis med det som sker här hemma, men det finns också annat som tillsammans med den nationella utvecklingen gör att det framträder nya möjligheter. Till exempel skulle utvecklingen av små satelliter kopplade till billigare alternativ för uppskjutning kunna ge Sverige möjligheter att i framtiden själv bygga, skjuta upp, driva och använda nationella satelliter utan insyn och utan begränsning från andra stater.

Andra områden som kan vidareutvecklas och förstärkas samt bli till nytta inte bara för den civila och kommersiella sektorn utan speciellt för den svenska statens försvars- och säkerhetsbehov är exempelvis:

- drivmedel för ballistiska missiler och rymdraketer
- övervakning och inmätning av rymdobjekt
- robusthetshöjande teknik för såväl satellitkommunikation som rymdbaserad PNT (positionering, navigering, tidssynkronisering)
- rymdrelaterad telekrigföring
- övervakning och spaning från rymden.

Möjligheterna till egenutvecklad nationell förmåga, såväl för forskning och teknikutveckling som operationell förmåga är många. Exempelvis skulle en akademisk forskning kring rymdskrotsproblematiken kunna initieras. De statliga svenska satelliterna som skjuts upp bör även sömlöst kunna nyttjas för försvars- och säkerhetsforskning.

Ökad kunskap om hur vi själva och omvärlden nyttjar och utvecklar rymdtjänster för försvar och säkerhet ökar möjligheterna att bedöma en motståndares förmåga men är också en viktig del i att prioritera svensk utveckling av rymdprodukter och rymdtjänster. Den nationella förmågan för såväl forskning och teknikutveckling som operationella tjänster kan utvecklas exempelvis för att tydligare belysa dubbelanvändningsperspektiv. En bred svensk förståelse för och acceptans av rymddomänens många och komplementära användningsområden kan också bereda väg för mer djupgående och omfattande internationella samarbeten inom försvars- och säkerhetsområdet. En förstärkt militär rymdverksamhet skulle sannolikt också leda till flera möjligheter för samarbeten med den redan starka svenska rymdindustrin och rymdakademin.

EN MER KOMPLETT SVENSK RYMDSTRATEGI

Enligt rymdutredningen utgör idag den svenska militära rymdverksamheten ungefär fyra till fem procent av statens totala satsningar på rymdverksamhet. Militär rymdverksamhet är dock en tydlig framtidsbransch och rymdarenans betydelse för svenskt försvar och säkerhet är stadigt ökande. Enligt *The Space Report 2016* investerar USA cirka 53 procent av den totala statliga rymdbudgeten på försvar och säkerhet medan övriga världen tillsammans spenderar uppskattningsvis cirka 33 procent av den totala statliga rymdbudgeten på försvar och säkerhet. En svensk rymdstrategi har alla möjligheter att formuleras så att alla fyra sektorer: civil, kommersiell, militär och underrättelse, förs fram på ett mer balanserat sätt än i nuvarande betänkande. Exempelvis går det att tydligare beakta synergier mellan civila och militära intressen. Ett annat förslag är att lyfta fram vilken forskning och högteknologisk produktutveckling som behövs initieras nu för att tillgodose eventuella försvars- och säkerhetsbehov i ett längre perspektiv. Den strategiska inriktningen skulle kunna formuleras så att svensk rymdverksamhet även ska bidra till en ökad militär förmågehöjning, ett stärkt svenskt försvar samt ett säkrare Sverige. Detta genom att både bygga på de styrkor vi redan har och genom att identifiera de områden där det finns möjligheter till utveckling.

Den föreslagna nationella rymdstrategin behöver därför kompletteras med en dedikerad försvars- och säkerhetsstrategi för rymdfrågorna. Antingen som ett fristående dokument eller integrerat med den civila strategin. En försvars- och säkerhetsstrategi för rymdfrågorna skulle på ett heltäckande sätt kunna ta hänsyn till alla operativa myndigheters behov, materielförsörjning, regelverk och tillstånd, exportfrågor, utbildningsbehov samt forskning och teknikutveckling kopplat till svensk militär rymdverksamhet och säkerhetspolitik. Den skulle ta hänsyn till både styrkor, svagheter, möjligheter och risker med rymdverksamhet. Alla berörda totalförsvarsmyndigheter skulle inkluderas och ges en tydlig roll.

Avsaknaden av en långsiktig försvars- och säkerhetsstrategi för rymdfrågorna i Sverige har hittills försvårat ett effektivt nyttjande av rymdtjänster när det gäller nationell säkerhet. Idag förlitar vi oss på kommersiellt tillgängliga rymdtjänster eller internationella samarbeten för försvars- och säkerhetssektorn. Vi är beroende av andra stater och därmed mer sårbara. Om frågorna inte på ett tydligare och bredare sätt beaktas står Sverige sämre förberett. Det gäller framtida nyttjande och utvecklingsmöjligheter likväl som att möta de hot och risker som kan uppkomma mot staten Sverige när andra aktörer flyttar fram sina positioner och stärker sin förmåga inom rymdområdet.

Med strategisk utblick mot framtiden

Sverige är sedan länge en rymdaktör och det svenska samhället har ett starkt beroende av olika rymdsystem och rymdtjänster, både civilt och militärt. Exempelvis är vi så beroende av det amerikanska GPS-systemet att det inte är ekonomiskt eller praktiskt möjligt att ens i ett medellångt till långt perspektiv övergå till att förlita oss enbart på EU:s nya satellitnavigationssystem GALILEO, ett system som Sverige har varit med och kravställt samt även finansierat i och med vårt medlemskap i EU. Avsaknaden av en långsiktig och övergripande plan är troligen en starkt bidragande orsak till varför vi befinner oss i denna situation.

I omvärlden går utvecklingen inom rymdområdet snabbt. Antalet nya stater med satelliter har nästan fördubblats under 2000-talet. Även mindre tekniskt avancerade länder satsar på egna satellitsystem eftersom tekniken numera är lättillgänglig och billigare. Det är även ett sätt för dessa stater att parallellt och i samverkan med andra utveckla sin inhemska forskning, industri och stärka sitt försvar. Beroendet av rymdtjänster leder även till att denna tillgång behöver skyddas. De stora

rymdaktörernas utveckling med anti-satellitprogram är särskilt oroande. I värsta fall står vi inför att rymden blir den nya konfliktarenan.

I förslaget till en sammanhållen svensk rymdstrategi är det positivt att man lyfter fram behovet av ökad civil-militär samverkan. Problemet är att förslaget inte tillräckligt tydligt visar på möjligheterna att uppnå sådan samverkan. Förslaget avspeglar snarare hur Sverige traditionellt har bedrivit rymdverksamhet. Frågor eller verksamhet som direkt kan utveckla och bidra till nationellt försvar och samhällets säkerhet lyfts knappast alls.

Sverige är ett litet land med begränsade resurser. Det är orealistiskt att tro att det ska gå att bedriva en bred och allomfattande civil och militär rymdverksamhet och rymdutveckling. Samtidigt har Sverige behov av att fortsätta utveckla sitt nyttjande av rymden inom alla sektorerna. Ett första steg för att hitta en balans i statens satsningar är att ta fram en försvars- och säkerhetsstrategi för rymdfrågorna. En sådan kan tillsammans med den civila strategin ligga till grund för framtida statliga prioriteringar och beslut kring inriktningen av svensk rymdforskning och rymdverksamhet.

För vidare läsning

Christer Andersson, och Sandra Lindström, *Den nationella rymdutredningen och Försvarsmakten,* 2015, FOI Memo 5564.

Sandra Lindström, *FOIs inspel till Rymdutredningen*, 2015, FOI--2015--287.

Sandra Lindström (red), *Omvärldsanalys RYMD 2014 Trender, möjligheter och hot för militär förmågeutveckling*, 2014, FOI-R--3985--SE.

13. Livsmedelsförsörjning efter radioaktivt nedfall – fem limpor och en hel befolkning

Niklas Brännström, Torbjörn Nylén och Henrik Ramebäck

Sverige har förlorat delar av sin förmåga att hantera kriser där radioaktivt nedfall är en komplicerande faktor. I en situation där det otänkbara skulle inträffa och Sverige blir militärt angripet med taktiska kärnvapen skulle detta ställas på sin spets och påfrestningarna på alla delar av samhället bli stora. Ett angrepp med taktiska kärnvapen skulle, utöver direkt förstörelse och skadeutfall, få stora konsekvenser för svensk livsmedelsförsörjning. Därför måste förmågan att förutse var nedfallet hamnar, mäta aktiviteten av deponerade radionuklider, bestämma upptaget i livsmedel samt beräkna vilken stråldos detta skulle ge ifall det kontaminerade livsmedlet konsumerades stärkas avsevärt. Beslutsfattare måste i förväg våga tänka tanken att detta är ett möjligt scenario, och när tanken väl är tänkt fråga sig vilka beslutsunderlag som kommer att krävas för att kunna agera. Förmågan att hantera situationen behöver därefter säkerställas genom lämpliga åtgärder, utbildning och övning.

En handelsberoende livsmedelsförsörjning

I dagsläget importerar Sverige ungefär hälften av all mat som konsumeras i landet. För enskilda produkter såsom kaffe och te förlitar vi oss helt på import. Det samma gäller en stor del av frukt och grönt samt drygt hälften av allt kött. Andelen importerade mejeriprodukter och spannmål är å andra sidan liten. Om handeln med andra länder förändras kommer det påverka utbudet i livsmedelsbutikerna. Detta märktes inte minst under köldknäppen som drabbade medelhavsområdet vintern 2016. Plötsligt saknades vissa grönsaker i våra grönsaksdiskar och för många av de som salufördes hade priserna ökat markant.

Frukt och grönt har kort hållbarhet och går inte att lagerhålla om tillgången tillfälligt skulle minska. För många andra råvaror kan lagerhållning helt lösa ett tillfälligt produktions- eller importbortfall. Under kalla kriget hade Sverige en jordbrukspolitik som gjorde oss nästan självförsörjande med mat. Dessutom fanns det lager med livsmedel i krisberedskapssyfte. Jordbrukspolitiken reformerades i början av 1990-talet till att bli marknadsstyrd och de sista livsmedelslagren avvecklades i början av 2000-talet.

Lagerhållning är dyrt, både för stater och butiksägare, och det är effektivt och lönsamt att sälja varan direkt då den levereras till butiken. Nackdelen är att systemet blir sårbart; när leveransen uteblir är livsmedlet slut. Men om varken nationen eller livsmedelsbutikerna har några lager, vem ska då ha ett lager för att klara en kortare störning? Under våren 2017 genomförde Myndigheten för samhällsskydd och beredskap (MSB), tillsammans med länsstyrelserna och kommunerna, en informationskampanj för att stärka svensk krisberedskap. Alla medborgare uppmanades att hålla ett eget lager, en krislåda, för att klara en kortare tids avbrott i exempelvis livsmedelsimporten.

Köldknäppar eller transportstrejker i all ära, men det finns allvarligare hot. Vad blir till exempel effekten av krig i svenskt närområde kombinerat med radioaktivt nedfall över svenska jordbruk? Hur länge räcker medborgarens matvarulager i en sådan situation? Och vad gör vi sedan, innan saneringsåtgärder och omläggning av produktion åter möjliggör inhemsk livsmedelsförsörjning?

Ett försämrat säkerhetspolitiskt läge

Det säkerhetspolitiska läget i närområdet har försämrats och konflikterna i Georgien och Ukraina visar att tröskeln för att ta till väpnat våld också har minskat. Till bilden av ett allmänt försämrat säkerhetspolitiskt läge ska läggas att USA och Ryssland bedriver förmågeutveckling kring sina kärnvapensystem. Också Frankrike och Storbritannien använder stora resurser för att bibehålla sin förmåga. Även om det finns ett omfattande provstoppsavtal för kärnvapen (som i formell mening inte trätt i kraft) finns inget avtal som förbjuder användning av kärnvapen för att uppnå taktiska eller strategiska mål i en väpnad konflikt. Användning av kärnvapen ingår i rysk försvarsdoktrin som ett verktyg på både taktisk och strategisk nivå. Ryssland genomför regelbundna övningar med sina kärnvapenförband och det är rimligt att utgå från att en rationell kärnvapenstat tänker använda sig av kärnvapen om situationen kräver det. Ett angrepp med taktiska kärnvapen i regionala eller lokala konflikter är ett reellt hot som dessutom kan komma att öka. Detta har bland annat påpekats i Försvarsmaktens och MSB:s gemensamma grundsyn för en sammanhängande planering för totalförsvaret.[8] Även i Militärstrategisk doktrin från 2016 diskuteras hotet från taktiska kärnvapen och det konstateras att vårt försvar måste förbereda sig för ett sådant hot. Det är därför viktigt att sådana situationer omhändertas inom ramen för kris- och försvarsplanering.

8 *Sverige kommer möta utmaningarna*, FM2016-13584:3/MSB2016-25.

Om det ofattbara inträffar

Låt oss betrakta ett läge där ett begränsat anfall med fjärrstridsmedel sker mot militära och logistiska mål i Sverige. Krigslyckan för Sveriges motståndare har snabbt vänt och därför känner de sig pressade att garantera effekten av angreppet. Vid dessa mål detonerar därför förutom konventionella vapen även ett fåtal taktiska kärnladdningar. Utöver den initiala strålningen, stöt- och värmevågor samt efterföljande eldstormar, kommer en stor del av marken att kastas upp och en mängd radioaktiva partiklar av olika storlek att bildas. Beroende på partiklarnas storlek kommer vissa av dem att ramla till marken nära detonationsplatsen medan andra kommer att transporteras längre med vinden. Vissa partiklar kommer att kastas högt upp i atmosfären och tillbringa decennier där innan de når markytan igen.

Ett anfall av denna typ skulle försätta Sverige i följande situation:

- Importen av livsmedel är nästan helt strypt på grund av konflikten och dess inverkan på logistiken.
- Lokalt har människor svåra skador från effekterna av kärnvapendetonationen. Att ta hand om dessa slukar en betydande del av samhällets resurser.
- Stora delar av den övriga befolkningen har hunnit söka provisoriska skydd i någon källare. En del av dessa har hörsammat MSB:s uppmaning om att ha ett förråd av livsmedel hemma. De står därmed rustade för att klara de första dygnen.
- Inrikestransporter av livsmedel och andra förnödenheter försvåras på grund av brist på transport- och drivmedel, samt skadad infrastruktur. Även strålningsnivåerna i drabbade områden kan ställa till med problem. Inte ens under hotet om förestående svält kommer all åkermark att kunna användas. I närheten av detonationsplatserna kommer stråldoserna att vara så höga att det inte går att vistas där. Bonden kan inte bruka sina åkrar.

Man tager vad man haver

Lagerhyllorna står tomma och den del av befolkningen som inte har hörsammat MSB:s uppmaning, eller som inte normalt lagerhåller torra livsmedel i skafferi, går hungrig. Snart kommer hela befolkningen att stå inför en hungersituation. Den inhemska matproduktionen drabbas av radioaktivt nedfall i olika grad och frågorna är många: Hur stor andel av jordbruket överlevde anfallet och går drabbad åkermark att använda? Finns

det tjänligt foder till djuren? Går det att äta spannmålet och köttet? Kan man dricka mjölken?

Med anledning av att stora delar av importen, av logistiska skäl, har strypts kommer det i de svenska livsmedelsbutikerna efter ett tag bara att finnas svenska råvaror. En del av dessa kommer inte ens att vara andra klassens prima för att parafrasera författaren Michail Bulgakov när han i klassikern Mästaren och Margarita beskriver livsmedlens kvalitet i efterkrigstidens Sovjetunionen. Grödan som växer (om den växer) på åkrarna kommer vara så kontaminerad att den inte får saluföras eller användas som foder enligt de gränsvärden EU tänker sig införa efter ett radioaktivt nedfall. Däremot skulle den kanske kunna vara tjänlig inför hotet om svält. Dessutom skulle den kanske kunna saneras från ytkontamination och lagras medan de radioaktiva ämnen som har kort halveringstid sönderfaller.

Svåra val kräver bra beslutsunderlag

I detta läge har beslutsfattaren att bestämma vilka stråldoser från mat som är acceptabla. Svensk strålskyddsberedskap och strålningsmedicin har en viss kapacitet att kartlägga nedfall och mäta stråldoser till människan samt att utföra laboratoriemätningar på prover från bete, råvaror och livsmedel efter ett reaktorhaveri. Denna kapacitet är med all sannolikhet inte tillräcklig för att klara ett kärnvapenscenario där både underlag i form av kontaminationsmätningar och stråldosberäkningar, samt medicinska undersökningar för prioriteringar av medicinsk behandling, krävs. Även kapaciteten att utföra mätningar för att avgöra om kontaminerat livsmedel ligger under gränsvärden, så kallad *friklassning*, är otillräcklig då drabbade människor kommer att prioriteras före livsmedelsmätningar.

Någon nationell plan för att snabbt iordningställa en tillräckligt stor kapacitet för att mäta radioaktiva ämnen i livsmedel existerar inte idag. Detta beror på att det fredstida ansvaret att visa att livsmedlet ligger under EU:s gränsvärden vilar på den som saluhåller eller saluför livsmedlet. Man kan anta att om det råder svårigheter att i en konfliktsituation importera livsmedel så torde även annan import, till exempel av mätutrustning vara drabbad. Att bygga upp nya kvalificerade mätlaboratorier med både personal och mätutrustning som klarar av grundläggande mättekniska kvalitetskrav är ingen enkel uppgift. Hög mätteknisk kvalitet är nödvändig för att beslutsfattare, och i slutändan befolkningen, ska kunna lita på de mätresultat som ska ligga till grund för beslut att åter nyttja mark som inte längre bedöms vara farlig att bruka.

Avsaknaden av en nationell plan leder till att de få resurser som skulle stå till buds sannolikt skulle användas för att göra stickprov på livsmedel, råvaror och mark. Främst skulle syftet vara att validera beräkningar av halter i råvaror, livsmedel och den resulterande interna stråldosen till befolkningen. På grund av att kärnvapenhotet länge bedömts som lågt finns de teoretiska metoderna för sådana beräkningar bara delvis nationellt och metoderna har inte satts samman för att fungera i ett scenario som detta. Detta trots att det sannolikt kommer att vara just beräkningarna som ger beslutsfattarna det fylligaste underlaget för planering av motåtgärder och mätinsatser.

Den begränsade kapaciteteten att både förutse och faktiskt bestämma stråldos i föda skulle efter ett kärnvapenanfall leda till svårigheter att bedöma ett livsmedels tjänlighet. Troligtvis skulle hälsovådligt kontaminerade livsmedel konsumeras samtidigt som ätbara matvaror av misstag kasseras. Det kommer att vara en mycket grannlaga uppgift för de ansvariga att fatta beslut om tillfälliga gränsvärden som kan komma att vara avsevärt högre än vad konsumenten tidigare upplevt. Det är viktigt att det finns en mental beredskap i samhället för en situation liknande denna. Det är även nödvändigt att finna vägar för hur situationen ska kunna hanteras, och sätta resurs- och kvalitetskrav för att kunna genomföra nationella mätningar, samt utveckla prognosverktyg och principer för att kunna fatta beslut. Den avvägning som måste kunna göras är mellan konsekvenserna av undernäring och svält samt konsekvenserna av höga internstråldoser från föda. En rimlig önskan är att kunna lägga dessa avvägningar på bordet i god tid för att vara förberedda om dagen skulle komma.

Fem limpor och en hel befolkning

Även om samhället skulle besluta sig för att tillföra medel för att bygga förmågan att ta fram bra beslutsunderlag återstår flera utmaningar. Bland annat måste riskerna på ett förtroendeingivande sätt kunna kommuniceras till befolkningen och livsmedel fördelas mellan dem. Om detta misslyckas är risken stor att allt från livsmedelsbrist till svält kommer att leda till en förtroendeklyfta gentemot myndigheter och andra beslutsfattare. I värsta fall kan detta leda till folkvandring, från stad till landsbygd, och till inre spänningar mellan de som har och de som inte har.

För vidare läsning

Martin Goliath, Torbjörn Nylén, Daniel Sunhede och Mattias Waldenvik, *Kärnvapenhot och civilt försvar – en kunskapsöversikt*, 2017, FOI-R--4444--SE.

Stina Holmgren, Annika Tovedal, Oscar Björnham och Henrik Ramebäck, 'Time optimization of ^{90}Sr measurements: Sequential measurement of multiple samples during ingrowth of ^{90}Y', 2016, *Applied Radiation and Isotopes*, Volym110, s. 150-154.

Pontus von Schoenberg, Jonas Boson, Håkan Grahn, Torbjörn Nylén, Henrik Ramebäck och Lennart Thaning, 'Atmospheric dispersion of radioactive material from the Fukushima Daiichi nuclear power plant', 2014, i *Air Pollution Modeling and its Application XXII* Steyn et al, (Red.), Springer: Dordrecht

14. Ett norskt perspektiv på försvarsplanering

Alf Christian Hennum och Tore Nyhamar (Forsvarets forskningsinstitutt, FFI)

I försvaret av det norska territoriet är Nato ett avgörande instrument. Norsk försvarsplanering behöver därför utformas på ett sådant sätt att den säkrar hjälp från Nato vid ett militärt angrepp. Den behöver också trygga en förmåga att säkra och ta emot sådan assistans. För att möjliggöra detta behöver Norges långsiktiga försvarsplanering balansera nationella behov med Natos. Norge skräddarsyr därför sina egna förmågor så att det blir möjligt att genomföra uppgifter som gynnar alliansen och det egna territoriet. De strategiska prioriteringar som görs vad gäller såväl anskaffning av materiel som utplaceringen av den norska försvarsmaktens resurser ska ses i ljuset av detta.

Det försvarspolitiska utgångsläget

Den norska försvarsmaktens huvuduppgift är att säkerställa Norges självständighet och politiska handlingsfrihet. Nato har, sedan Norges undertecknande av det nordatlantiska fördraget – Atlantpakten – år 1949, varit en hörnsten i den norska försvars- och säkerhetspolitiken. Under kalla kriget, precis som idag, byggde Norges strategi på tillgången till allierades militära förstärkningar. Nato har däremot utvecklats sedan kalla krigets slut. Antalet medlemsstater har ökat samtidigt som många medlemsstater numera uppfattar hotbilden som en kamp om politiskt inflytande snarare än om att förhindra militär erövring. Detta har i sin tur lett till en större mångfald av strategiska perspektiv och prioriteringar inom alliansen. Som en konsekvens av detta har antalet situationer som självklart skulle leda till att artikel 5 utlöses kommit att minska. Nato har därmed gradvis förändrats från sin tidigare roll som traditionell försvarsallians till att bli en politisk säkerhetsorganisation med en militär förmåga. Exakt var alliansen står på denna skala är inte givet utan kommer att variera för varje enskild utmaning som dess medlemmar ställs inför. Av vikt i vårt resonemang är att den nuvarande norska försvarsplaneringen måste säkerställa de allierades hjälp om Norges försvarsstyrkor ställs inför en alltför krävande situation.

Efter kalla krigets slut kom Nato att prioritera sina internationella insatser (”*out of area or out of business*”). Norge deltog i dessa insatser, särskilt i Afghanistan, för att säkerställa

alliansens fortsatta relevans. Till skillnad från Danmark övergav dock inte Norge principen om att försvaret av det egna territoriet kvarstod som försvarsmaktens huvuduppgift. Att Nato sedan 2014 återigen kommit att fokusera på de allierades egna territorium (”*coming home*”) har från norsk synvinkel varit en välkommen utveckling, inte minst eftersom det kom som ett svar på Rysslands ökade förmåga. Det nuvarande hotet mot Norge har utvecklats från det rent existentiella hot som Sovjetunionen tidigare har utgjort mot landet. Dagens Ryssland uppfattas förvisso som det enda landet med en förmåga, och i viss mån ambition, att använda militära maktmedel mot Norge, men Rysslands förmåga är fortfarande avsevärt mindre än dåvarande Sovjetunionens. Dessutom skulle en eventuell konflikt mellan de två länderna idag snarare uppstå som en följd av Rysslands strävan efter politiskt inflytande, än den territoriella erövring som hade varit målet under kalla kriget, och som Norges försvarsplanering var dimensionerad för att kunna avvärja.

Avskräckande åtgärder

Begreppet avskräckning (eng. *deterrence*) är numera centralt inom försvarsplanering. Även om begreppet först på senare tid har kommit att användas i offentlig skrift är avskräckning ett koncept med rötter i teorier från så långt bakåt som 1960-talet och har implicit kommit att vara en del av norsk försvarsplanering sedan dess. Idag, när såväl hot som garantier blivit allt luddigare, har begreppet kommit att bli föremål för en uttrycklig diskussion.

Avskräckning består delvis av en kognitiv – eller ”upplevd” – aspekt och delvis av en rent fysisk aspekt. Vad gäller den kognitiva delen är målet med avskräckning att övertyga potentiella angripare att påtryckningar eller angrepp mot Norge inte kommer att löna sig. Den fysiska avskräckningen består av tillräckliga militära medel, kombinerat med uppdaterade och välövade planer för att använda dem effektivt, i händelse av att annan form av avskräckning misslyckas. Nato är det viktigaste avskräckande medlet mot en militär attack mot Norge. På senare tid har norska avskräckande strategier därför inkluderat åtgärder som säkerställer att den norska Försvarsmakten arbetar på ett sådant sätt att det otvivelaktigt utlöser militär förstärkning från Nato.

De tre viktigaste försvarsåtgärderna för norsk säkerhet är därmed att säkerställa att en attack mot Norge *utlöser* assistans från Nato, samt att Norge har förmågan att *säkra* och *ta emot* förstärkningar från alliansen. Försvarsgrenarnas struktur och

försvarskoncept är en del av detta. Utöver vapensystem är uppdaterade och inövade planer för hur hjälp ska kunna tas emot av yttersta vikt. Detta inkluderar övningar som Trident Juncture 18. Norsk försvarsplanering prioriterar även att kunna bidra till Natos förmåga och vilja att agera som en allians. Till exempel måste Norge ha militära styrkor att bidra med till Natos snabbinsatsstyrkor, så som Natos Response Force och alliansens stående stridskrafter inom marin och flygvapen.

Norges långsiktiga försvarsplanering

En stor utmaning för den långsiktiga försvarsplaneringen efter kalla kriget har varit att etablera en tydlig koppling mellan å ena sidan säkerhetsutmaningar och politiska ambitioner, och å andra sidan rekommenderade strukturer för försvarsgrenarna. Vad – specifikt – ska våra styrkor kunna utföra och vilka plattformar och enheter behövs för detta?

En viktig del av den norska försvarsplaneringen har varit de så kallade Försvarsstudierna initierade av Överbefälhavaren (*Forsvarssjefen*). Metoden som har använts för att genomföra dessa utredningar har varierat, men utredningarna har i allt väsentligt varit den huvudsakliga drivkraften bakom den krävande, men nödvändiga, förändringen av det norska försvaret.

Sedan 2014 har försvarsplaneringen på Försvarsdepartementet skett löpande. Detta innebär att nödvändiga analyser kan genomföras och beslut fattas även under perioderna mellan de traditionella försvarsplanerna som tas fram vart fjärde år. Innan försvarsplanerna tas fram presenterar *Forsvarssjefen* sina militära råd (*Fagmilitære råd* eller FMR) för hur han anser att det norska försvaret borde utvecklas. Traditionellt sett har dessa råd haft stort inflytande över de politiska försvarsplanerna, men de är trots detta fortfarande enbart rekommendationer till ministern, och det är Försvarsdepartementet som själva formulerar innehållet i försvarsplanerna innan dessa lämnas till Stortinget för beslut.

Som en del i processen med att formulera försvarsplanerna genomförs en *strategisk analys*. Denna analys har förmågor som utgångspunkt och grundar sig på högnivåförmågor. I den senaste försvarsplanen, med titeln *Kampkraft og bærkraft* (2016) lades särskilt fokus på balansen mellan uppgifter, försvarsstruktur och kostnader. De huvudprioriteringar som angavs var att stärka Norges nationella försvar genom:

- bibehållen situationsmedvetenhet och krishantering
- ökad beredskap, stridskraft och överlevnadsförmåga
- ökad förmåga att ta emot allierad förstärkning
- ökad militär närvaro
- mer regelbundna övningar och utbildningar.

Beslutet att öka förmågan att ta emot allierad förstärkning är av stor betydelse, eftersom Norges system för värdlandsstöd hade fallit ur bruk och inte uppdaterats sedan kalla krigets slut. Systemet för värdlandsstöd finns fortfarande kvar, men planerna måste uppdateras för att möta förändrade förutsättningar efter år 2020.

I utredningsfasen av försvarsplaneringsprocessen ligger fokus för analysen på de stridande enheterna och hur dessa borde utvecklas. Det finns flera fördelar med denna utgångspunkt: de stridande enheterna är de som faktiskt ska lösa försvarsuppgifterna, och själva analysen är enklare att genomföra för dessa enheter än för supportenheter och infrastruktur. Syftet med stridande enheter är oftast tydligt, och det är enkelt att ange en ambitionsnivå för ett uppdrag. Supportenheter å andra sidan har oftast en mer komplex roll i samspelet med andra försvarsenheter, och det är därmed svårare att bedöma vilken inverkan förändringar hos dessa enheter kommer att ha.

Norges långsiktiga försvarsplanering har kämpat med skenande kostnader, framförallt när det gäller militärt materiel. Traditionellt sett har detta inte tagits med i beräkningarna när nya budgetar ska förhandlas fram. Resultatet är en försvarsstruktur som är för stor i förhållande till sina anslag och som därmed misslyckas med att producera den militära stridsförmåga som förväntas. Svårigheterna med att analysera förhållandet mellan stridande enheter och supportenheter försvårar problemet ytterligare. Detta problem, som inte är unikt för Norge, har äntligen tagits hänsyn till i den senaste planen. I det fall planen kan förverkligas kommer det att resultera i en försvarsstruktur med tillräckliga anslag och som är hållbar över tid.

Prioritering mellan Norges och Natos behov

Den långsiktiga planeringsprocessen har huvudsakligen fokuserat på nationella behov. Natos försvarsplaneringsprocess (NDPP) har uppmärksammats, men norska nationella scenarier och försvarsstrukturer har dominerat planeringsprocessen.

Beroendet av alliansen är varken bortglömt eller negligerat, men tar sikte på en mer långsiktig utveckling bortom det mer omedelbara målet att täppa till hålen i Natos förmågor. Som en av de mindre medlemsstaterna kan Norge inte på egen hand göra mycket åt dessa luckor.

Norge betonar vikten av investeringar i försvarsförmågor som kan bidra till alliansen samtidigt som de är relevanta för det egna försvaret. En strategisk prioritering är förstärkningen av Norges markbaserade luftvärn, där det befintliga medelräckviddiga missilsystemet Norwegian Advanced Surface-to-Air Missile II system (NASAMS) ska uppgraderas och förbättras genom att tillföra missiler med förlängd räckvidd. Till detta tillkommer nya system med missiler och sensorer med lång räckvidd. Även om luftvärn är en uppenbart nationell kapacitet för nationella behov, så blir det ändå tydligt hur alliansen prioriteras genom hur dessa system är tänkta att användas. Både NASAMS II och de nya långräckviddssystemen kommer att koncentreras kring de två flygbaserna Ørland och Evenes, som är kritiska inte enbart för Norges egna styrkor, utan även som potentiell samlingsplats för allierad förstärkning. Anskaffningen av F-35 Lightning och de planerade anskaffningarna av nya ubåtar är andra exempel på förmågor som ger Norge möjlighet att bevara sin närvaro och, om nödvändigt, agera både för sig själva och för alliansen.

Norge är det enda Natoland som delar havs- och landsgräns med Ryssland (i området som på norska refereras till som *Nordområdene*[9]). Detta gör Norges territorium avgörande för Natos närvaro i det arktiska området vad gäller övervakning, underrättelseinhämtning och försvar. Norges införskaffning av nya maritima spaningsflyg – fem stycken P-8 Poseidon för att ersätta de allt äldre P-3 Orion – är ett typexempel på en kapacitet som möter behoven hos alliansen. Prioriteringen av dessa förmågor visar på de ansträngningar som gjorts för att ge Norge ett trovärdigt försvar genom att bidra med situationsmedvetenhet och underrättelser för både egen del och för Natos. Å ena sidan kan den här typen av avancerade förmågor upplevas som ett hot av Ryssland, men å andra sidan är det mindre problematiskt för Ryssland att dessa aktiviteter – som varje suverän stat har rätt till – genomförs av Norge som enskild stat snarare än av alliansen eller USA. Sammantaget bidrar dessa satsningar till Norges förmåga inom krishantering, såväl enskilt som en del av Nato.

9 En precis definition av begreppet saknas men omfattar för det mesta havsområdena, och tillhörande landområden, norr om Norge och upp till Nordpolen.

Det föråldrade systemet för värdlandsstöd är fortfarande på plats, men det kräver löpande övningar och har dessutom ett behov av att uppdateras för att bättre svara mot aktuella hot i och med uppehållet under Natos satsningar på internationella insatser. Därför satsar Norge nu på att vara värd för övningar tillsammans med relevanta allierade, med fokus på snabba insatser och territoriellt försvar. I dagens läge, när mer avgränsade och politiska hot är huvudfokus för planeringen, är det beredskap och responstider som prioriteras, både för Norges egna militära styrkor och vid övningar med dess allierade. Den ökade övningsaktiviteten inom USA:s marinkår, som mer eller mindre fortlöpande övar i Norge, är ett typexempel på den nya satsningen på mindre men snabbare svarsinsatser i samarbete med allierade.

En balanserad försvarsplanering

Norges långsiktiga försvarsplanering måste balansera de behov som finns nationellt och de som uttrycks hos Norges allierade. Att bidra till förmågan inom alliansen är ett sätt att göra det på. Ännu viktigare är dock att Norge skräddarsyr sina egna förmågor för att kunna genomföra uppgifter som gynnar hela alliansen såväl som försvaret av det egna territoriet. Den prioritet som ges till *Nordområdena* och området runt Arktis ska ses i ljuset av detta. Med det sagt kvarstår dock Norges strategiska utmaning med att hålla militära styrkor i norr, långt bort från landets populationscentra. Norska försvarsmakten möter färre utmaningar när de agerar i övriga delar av landet.
Norsk försvarsplanering är inte enbart en fråga om försvarsstrukturer. Tillräckliga anslag för relevanta övningar med allierade samt uppdaterade doktriner är också strategiska prioriteringar. Slutligen syftar de grundläggande prioriteringarna av det nationella försvaret också till att säkra förmågan att ta emot förstärkningar från allierade och kunna agera sida vid sida med dem.

15. Problematiken inom finsk försvarsplanering

Jyri Raitasalo (Finska försvarsministeriet)

Sedan slutet på kalla kriget har finsk försvarspolicy och principer för försvarsplanering kommit att förändras, främst som ett resultat av förändringar i den internationella säkerhetsmiljön. Viktigt att notera är dock att i en europeisk jämförelse har finsk försvarsplanering snarare karaktäriserats av kontinuitet än förändring. Detta särskiljer Finland från de flesta andra västerländska stater som de senaste 25 åren genomfört grundläggande omställningar av sin syn på internationell säkerhet, försvarsplanering och användningen av militärt våld. Insikt i faktorerna som ligger bakom Finlands försvarspolitiska kontinuitet är avgörande för att förstå och analysera Finlands senaste försvarspolitiska redogörelse, framlagd till det finska parlamentet i februari 2017.

> Det kalla krigets slut och den förändrade hotbilden skapar nya utmaningar för Finlands försvar. Hotet om ett omfattande krig har ersatts av förekomsten av regionala kriser som riskerar att eskalera. I takt med att kriser i allt högre grad blir interna frågor för enskilda stater eller på annat sätt områdesspecifika händelser, är vi skyldiga att anpassa våra väpnade styrkors struktur och våra genomförandeplaner för att möta dessa kriser. Sammantaget har bilden av framtidens krigföring kommit att förändras väsentligt.
> *Uttalande från finska riksdagens försvarsutskott till utrikesutskottet, 1997*

Arvet

Försvarsplanering är en samling militärpolitiska aktiviteter som syftar till att definiera (politiskt acceptabla) militära hot mot den nationella säkerheten. Försvarsplanering definierar därmed även de huvuduppgifter som de väpnade styrkorna måste vara dimensionerade för. Försvarsplanering bör alltså ses som en politiskt styrd process som sätter prioriteringar för, och fördelar resurser till, de militära styrkornas underhåll, utveckling och användning.

Hur försvarsplaneringen genomförs beror till stor del på den strategiska kontext som den berörda aktören befinner sig i. Eftersom stater har såväl olika historiska erfarenheter

som geostrategisk placering råder stor variation vad gäller föreställningar om vilka hot staten måste vara beredd att möta, vem eller vad som måste skyddas från dessa hot och vilka militära medel som anses effektiva eller acceptabla att använda. Med andra ord kommer olika aktörers föreställningar om krig – dess art, sannolikhet och mål – att påverka hur de organiserar sin försvarsplanering.

Under det kalla kriget baserades den finska försvarsplaneringen på den säkerhetspolitiska principen om neutralitet och att undvika att dras in i den konfrontation mellan stormakterna som karaktäriserade tidsepoken. En bibehållen kapacitet att skydda landets territoriella integritet mot militära hot – utan att direkt namnge potentiella angripare – utgjorde fundamentet för den finska försvarspolicyn och dess principer under kalla kriget.

I och med slutet på stormaktskonfrontationen och den snabba upplösningen av det bipolära internationella systemet under tidigt 1990-tal, fann sig stater och andra internationella aktörer i en situation där de gamla spelreglerna ifrågasattes och nya eller ändrade regler för systemet behövde formuleras. Dock var den här förändringsprocessen av spelreglerna inte av formell karaktär. Snarare handlade det om en process på såväl aktörs- som systemnivå, där olika föreställningar om det kalla krigets plötsligt slut och det nya internationella systemets karaktär gav upphov till ett behov av ny politisk inriktning för att främja de olika aktörernas intressen i detta nya – fortfarande vagt formulerade – internationella system. Samtidigt utvärderade aktörer framtida policyalternativ och presenterade visionära uttalanden och principer för att på så vis kunna vara med och forma det nya system som började växa fram i en riktning som skulle ligga i linje med deras intressen. Tiden direkt efter kalla krigets slut sågs som en övergångsperiod men utan en tydlig slutpunkt för denna förändringsprocess. Politiska ledare skapade historia, men inte under förutsättningar som de själva hade valt.

Det efterlängtade slutet på kalla kriget blev därmed början av en process – såväl implicit som explicit – där själva logiken bakom det internationella systemet, den typ av krig som förekommer i det, och kraven på militär förmåga skulle komma att omdefinieras. Med andra ord; slutet på det kalla kriget tvingade fram en förändring i den underliggande logiken utifrån vilken stater baserar sin försvarsplanering och hur de underhåller, utvecklar och använder sina militära förmågor.

Efter kalla kriget

Med slutet på det kalla kriget kom Finland snabbt att "röra sig mot Väst". Medlemskapet i den Europeiska Unionen och deltagandet i Natos Partnerskap för fred-samarbetet blev konkreta uttryck för skiftet i Finlands säkerhetspolitiska synsätt; från neutralitet till militär alliansfrihet. Under perioden sedan kalla krigets slut har finsk försvarspolitik och dess principer för försvarsplanering därigenom kommit att utvecklas med nära kopplingar till – eller praktiskt taget inom – det västerländska säkerhetssamfundet, om än utifrån nationellt unika utgångspunkter.

Under 1990-talet, och det efterföljande årtiondet, följde finsk försvarsplanering – och utvecklingen av den finska försvarsmakten – logiken om en långsam utveckling, baserad på det förhållandevis gynnsamma säkerhetsläget under perioden efter kalla krigets slut. Finland följde därmed den globala trenden att nyttja det ekonomiska andrum som uppstod då Försvarsmakten kunde dimensioneras utan ett omedelbart krigshot. Försvarsmakten kom därför att effektiviseras både vad gäller fredstida organisation, infrastruktur och personal, samt beredskapsnivåer och storlek på truppstyrkorna i krigstid.

Fokus för den finska försvarspolitiken var dock även fortsättningsvis att kunna förhindra alla potentiella militära hot mot nationen genom att bibehålla en tillräcklig militär förmåga för att kunna slå tillbaka alla typer av angrepp, till och med en storskalig konventionell militär attack. Detta skedde samtidigt som de flesta västeuropeiska stater förändrade sina riktlinjer för försvarsplanering i en mer "revolutionerande" anda – med ett yrkesförsvar avsett främst för internationella insatser utanför Natomedlemmarnas territorium.

Under 2000-talets första årtionde började klyftan mellan principerna i finsk försvarsplanering och motsvarande principer hos de flesta andra västerländska (europeiska) länder gradvis att öka och kom snart att leda till en diskussion om huruvida en generell manlig värnplikt och vidmakthållande av ett territorialförsvar mot potentiella storskaliga militära attacker var en bra utgångspunkt för utvecklingen av försvarsförmågan.

I efterhand kan man hävda att den USA-ledda omvandlingen av de väpnade styrkorna i västvärlden, med utgångspunkt i konceptet *Revolution in Military Affairs*, och den övergång som skett från värnplikt till frivilligbaserade professionella militärer i många länder under det senaste årtiondet, gjorde det tydligt att Finland började komma "ur fas" med andra västländer på

försvarsområdet. Finland var angeläget att delta i utvecklingen av den europeiska försvarssfären, med fokus huvudsakligen på militär krishantering, men gjorde detta baserat på militära förmågor som hade utvecklats enbart för att klara av kraven på territoriellt försvar mot externa och statsbaserade militära hot. Därmed började en nationell ”identitetskris” växa fram under det första decenniet på det nya årtusendet. Senare händelser, framförallt i Georgien (2008) och Ukraina (2014-), kom dock snart att dämpa de tveksamheter som hade vuxit sig starka under perioden från millennieskiftet och framåt.

Vid analyser av skillnaderna mellan finsk och mer generell västerländsk försvarsplanering, exempelvis inom Nato, är det av yttersta vikt att hänsyn tas till såväl geografiska som historiska förhållanden med avseende på kopplingen till Ryssland. Trots det faktum att Ryssland hade stora svårigheter att bibehålla den inhemska freden var landet, i alla fall ur en militär synvinkel, fortfarande att betrakta som en stormakt direkt efter kalla krigets slut. Dessutom har Ryssland och Finland en gemensam gräns som sträcker sig mer än 1000 kilometer på land. Finländare minns fortfarande händelserna under kriget med Sovjetunionen 1939–1945 och de politiska och militära påtryckningar som Sovjet utövade på Finland under det kalla kriget. Även om säkerhetsläget i Finland har genomgått en klar förbättring jämfört med de decennier som följde andra världskriget har det potentiella hot som Ryssland utgör inte helt försvunnit i och med det kalla krigets slut.

> Hotet mot Finland definieras av landets geopolitiska läge… Det enda realistiska hotet som kan uppstå är det från öst, det vill säga från Ryssland.
> *Generallöjtnant (pensionerad) Ermei Kanninen 1994*

> Trots att vi kanske inte betraktar Ryssland som ett hot i politisk bemärkelse, måste Finland ändå utveckla sin försvarsförmåga så att vi kan hantera alla former av tänkbara utvecklingar, inklusive en förändring i det politiska läget i Ryssland.
> *Statsminister Paavo Lipponen 2004*

> Ryssland försöker återta så mycket som möjligt av sin tidigare roll som ledare, vilket påminner om det inflytande Sovjetunionen hade i Eurasien.
> *Finsk säkerhets- och försvarspolicy 6/2004*

Mellan slutet av det kalla kriget och 2012 genomgick den finska Försvarsmaktens fredstida organisation flera omgångar av nedläggningar av baser och mängden avlönad personal minskade från omkring 20 000 personer till färre än 15 000. Krigsorganisationen skars under samma tid ner från 540 000 till 350 000 soldater. Detta var en följd av att det gynnsamma internationella säkerhetsläget möjliggjorde en lägre ambitionsnivå vad gäller underhåll och utveckling av försvarsförmågan. Utöver de potentiella riskerna kopplade till Rysslands framtida utveckling identifierades inga betydande militära hot som behövde bemötas av den finska försvarsmakten. Även om militär krishantering började bli rutinuppdrag, så var truppernas storlek och kostnaderna kopplade till dessa insatser små i förhållande till Försvarsmaktens organisation i krigstid och den nationella försvarsbudgeten. Beslut för materialanskaffning gjordes fortsatt med utgångspunkt i nationellt territorialförsvar.

Överraskningen

Rysslands "varningsskott" i Georgien (2008) bortsågs ifrån, eller glömdes snabbt bort, inom de flesta delarna av det västeuropeiska säkerhetssamfundet. Ur Finlands synvinkel kom händelserna istället att rättfärdiga grunden i dess försvarsplanering. En tillräcklig nationell försvarsförmåga för att kunna försvara sitt territorium och vitala samhällsfunktioner visade sig fortfarande ha en plats i världen, kanske till och med i Europa. Trots allt hade kriget i Georgien inträffat mindre än sex månader efter att ett Nato-toppmöte mynnat ut i ett vagt formulerat löfte om att Georgien och Ukraina skulle kunna ansluta sig till alliansen någon gång i framtiden.

Under ekonomisk press, och främjad av det till synes goda internationella säkerhetsläget, togs trots detta under åren 2011–2012 ett antal regeringsbeslut för att genomföra en försvarsreform till år 2015, samtidigt som försvarsbudgeten skars ner med omkring tio procent. Som ett resultat av detta kom nivån på materielinvesteringar (anskaffning) att störtdyka, omfattningen av den dagliga verksamheten minskades, antalet avlönad personal i Finlands försvarsmakt sänktes till 12 000 personer, och storleken på försvarsstyrkan i krigstid sänktes från 350 000 till 230 000 soldater. Samtidigt togs administrationsnivån "militära provinser" bort från Försvarsmaktens organisation och en rad processer och funktioner hos Försvarsmakten kom att förnyas. Sammantaget anpassades arbetssätt och ambitionsnivå efter den ansträngda finansiella situation som den globala finanskrisen hade medfört sedan 2008. Det enda som inte förändrades var fokus för finsk försvarsplanering, som även fortsättningsvis var att försvara

territoriet och vitala samhällsfunktioner mot statsbaserade militära hot.

Samtidigt som processen med försvarsreformen genomfördes bröt krisen i Ukraina ut. Till många västländers stora förvåning invaderade Ryssland Krimhalvön, med efterföljande annektering. Mindre än sex år efter kriget i Georgien hade Ryssland lyckats modernisera delar av sina väpnade styrkor – både i fråga om utrustning och hur man utförde militära insatser. Utöver detta startade Ryssland en militär konflikt – praktiskt taget ett proxykrig – i östra Ukraina. Sedan dess har relationerna mellan Väst (EU och Nato) och Ryssland blivit extremt ansträngda. Till och med kommunikation mellan de inblandade parterna, vilket är fundamentet inom diplomati, har blivit besvärligt och nästintill omöjligt.

Finsk försvarspolicy idag

Det är mot ovan nämnda bakgrund som den försvarspolitiska redogörelse som presenterades 2017[10] måste förstås och utvärderas. Rapporten drar upp de försvarspolitiska riktlinjerna för hur den finska försvarsförmågan ska upprätthållas, utvecklas och användas fram till 2030. För första gången sedan kalla krigets slut uppmärksammas i dokumentet den försämring av säkerhetsläget och ökande militära spänning som finns i Finlands närområde.

I den försvarspolitiska redogörelsen noteras att de resurser som tilldelats det militära försvaret är otillräckliga under rådande omständigheter och att försvarsförmågan behöver utvecklas mer än vad som gavs utrymme för i den försvarsreform som genomfördes 2012. Framför allt tilldelar regeringen Försvarsmakten ytterligare medel till anskaffning av materiel – en kumulativ årlig ökning till år 2020, som innebär ytterligare 150 miljoner euro perår – samt för beredskapsåtgärder (55 miljoner euro perår). Utöver detta meddelade regeringen att två framtida projekt för att utveckla strategisk förmåga kommer att tilldelas ytterligare resurser utöver grundbudgeten – ersättandet av jaktflygplanet F-18 Hornet samt en uppgradering av marinen genom ”Squadron 2020”-projektet. Den beräknade kostnaden för dessa två projekt ligger på 8,2 – 11,2 miljarder euro.

Vad gäller principerna för den nu rådande försvarsplaneringen introducerar 2017 års försvarsredogörelse inte några betydande konceptuella förändringar. Finland kommer även

10 *Statsrådets försvarspolitiska redogörelse*, Statsrådets kanslis publikationsserie 6/2017, Helsingfors 2017

fortsättningsvis att underhålla och utveckla sin försvarsförmåga för att kunna förhindra att statsbaserade militära hot uppstår, och om nödvändigt kunna bekämpa sådana hot. Utöver detta kommer Finland att fortsätta fördjupa sina internationella försvarssamarbeten och har bibehållit möjligheten att ansöka om Nato-medlemskap. Det pågående bilaterala samarbetet med Sverige anses nu av regeringen vara av högsta betydelse – precis som samarbetet med USA. Samtidigt tar regeringen bort ett antal legala hinder vad gäller möjligheten att ta emot och ge internationell militär hjälp.

Sammantaget har förändringarna i det internationella säkerhetsläget sedan Krimkrisen resulterat i anpassningar av det finska försvarssystemet. Dessa anpassningar kan dock inte sägas innebära några större avsteg från det synsätt och de principer som har vuxit fram gällande Finlands försvarspolicy under perioden sedan det kalla krigets slut. Den överraskning som Rysslands agerande under 2014 och framåt har inneburit för analytiker och ledare i västvärlden – även i Finland – har inte medfört något behov av att omvärdera synsättet på finsk försvarspolitik eller de principer som styr hur försvaret upprätthålls och utvecklas. Huruvida detta beror på den strategiska kompetensen hos beslutsfattarna inom finsk försvarspolitik eller på saktfärdighet och tröghet i den beslutsfattande processen under de senaste 25 åren är en fråga för framtida analys och politisk debatt.

16. Försvarsforskningens betydelse för att främja nationell säkerhet

Katarina Wilhelmsen och Mikael Wiklund

Nationell säkerhet handlar i grund och botten om våra svenska intressen, hot mot dessa och samhällets förmåga att möta hoten. Försvars- och säkerhetsforskningen spelar en central roll i att bygga den förmåga och beredskap som krävs för att säkerställa vår nationella säkerhet eftersom tillgänglig kunskap är gränssättande för såväl militär operativ förmåga som samhällets allmänna beredskap. Trots detta har den statliga finansieringen av försvarsforskningen minskat med mer än 50 procent de senaste tio åren. I takt med att omvärldsutvecklingen har försämrats har de långsiktiga konsekvenserna av att minska försvarsforskningen blivit allt mer uppenbara och akuta. 2016 års försvarsforskningsutredning föreslog därför en ökning av forskningsmedlen. Om resultaten av mer forskningsmedel ska kunna ge effekt för förmågan att hantera hot mot den nationella säkerheten redan inom nästa försvarsbeslutsperiod behöver sådana ökningar påbörjas omgående.

Nationell säkerhet

Regeringens nationella säkerhetsstrategi konstaterar att de externa hoten mot samhället är komplexa och att det inte går att förutse exakt vilka hot som kommer att uppstå. Därför måste en fortsatt långsiktig kunskapsuppbyggnad, forskning och teknikutveckling säkerställas för att stärka samhället. Forskning är alltså centralt för den nationella säkerheten.

Ett sätt att se på begreppet nationell säkerhet är frånvaron av hot mot våra värderingar och vår möjlighet att som stat själv diktera hur vårt samhälle utvecklas. Därtill kan läggas frånvaron av rädsla att våra värderingar och livsförutsättningar ska attackeras. Nationella säkerhetsfrågor måste därför omfatta strategier för att minska sådana hot, samt för att kunna återgå till ett normalläge efter att en hotfull händelseutveckling – exempelvis naturkatastrofer, terrorangrepp, militära handlingar eller olika former av ekonomiska och diplomatiska påtryckningar – har inträffat.

Politiskt sett är nationell säkerhet ofta svårt att förhålla sig till. Detta beror på att frågor av betydelse för nationell säkerhet sällan renodlat kan hänföras till det nationella säkerhetsområdet.

Denna typ av frågor inleder istället ofta sin bana som försvars-, infrastruktur-, eller utrikespolitiska frågor och får sin betydelse för nationell säkerhet när de senare möter de andra politikområdena. Ett exempel vi sett i närtid är att nationell säkerhet kan handla om utlokalisering av IT-drift. Forskning som stödjer nationell säkerhet återfinns därför inom en bred uppsättning områden, där försvars- och säkerhetsforskning har en framträdande roll.

Utmaningar knutna till nationell säkerhet och forskningens roll

I grund och botten handlar nationell säkerhet om våra värderingar och intressen, samt hot mot dessa och samhällets förmåga att möta hoten. Detta innebär särskilda utmaningar, där forskning är en väsentlig del av lösningen:

- Samhällets förmåga att skapa nationell säkerhet definieras relativt hotbilden. Om hoten ökar samtidigt som samhällets kapacitet är statisk så nedgår förmågan. Det räcker således inte bara att bibehålla tidigare landvinningar för att förmågan ska kvarstå.

- Samhällets förmåga att möta hot utvecklas med en tydlig tidsfördröjning. Beslut om att utveckla rätt förmåga måste oftast fattas lång tid innan den ska vara tillgänglig. Att önska sig en bättre beredskap och förmåga när behovet redan uppstått är lönlöst.

- Beslut om önskad framtida förmåga fattas därför under osäkerhet. Planering och förmågeutveckling inom försvar och säkerhet sker gentemot en okänd och svårbedömd framtid. Strukturer för att verka under osäkerhet är därför av central betydelse.

- Samhällets förmåga att skapa nationell säkerhet omfattar mycket mer än Försvarsmaktens förmåga eller brist på densamma. Nationell säkerhet är ett sammanhang mellan flera olika politikområden och kan inte hanteras av försvaret allena.

Försvarsforskningen spelar en avgörande roll i att tillfredsställa olika kunskapsbehov av betydelse för att hantera utmaningar förknippade med nationell säkerhet. Det mest uppenbara perspektivet handlar om att skapa mer och djupare kunskap inom identifierade förmågeområden för att bibehålla eller öka en förmåga över tid. Det handlar om avancerad forskning av hög kvalitet som för forskningsfronten framåt och skapar ledande experter inom olika ämnesområden. Forskningsresultaten är av vital betydelse för ökad förmåga inom respektive område.

Men forskning är också ett verktyg för att skapa handlingsfrihet inför idag okända utmaningar och hantera osäkerhet. Sådan forskning behövs eftersom forskning inriktad mot kända förmågebehov inte är tillräcklig för att förbereda oss för okända hot. Denna forskning kan inte ske mot tydligt definierade behov eftersom osäkerheten i sig medför att det inte går att besluta om exakt vad som behöver utvecklas. Forskningen handlar istället om att utveckla tillräckligt bra kunskap på utvalda områden för att det, när behov uppstår, ska vara möjligt att gå vidare till att utveckla förmåga.

Båda dessa forskningsperspektiv är viktiga för förmågeutvecklingen och behöver finnas samtidigt.

Forskning sker också ur ett tredje perspektiv, där forskningens syfte snarare är att skapa en avskräckningsförmåga eller tröskeleffekt än att skapa kunskap, forskningsresultat och förmåga till problemlösning i sig. Forskningen handlar ur detta perspektiv om att skapa en trovärdig bild av vilken operativ förmåga man möjligen har eller har möjlighet att utveckla inom en viss tidsrymd. Stark forskning och ett avancerat kunskapsläge gör troligt att en förmåga kan utvecklas, eller kanske redan finns.

Försvarsforskningens roll för att utveckla skyddet mot militära hot är uppenbar, men försvarsforskningens betydelse för övriga dimensioner av nationell säkerhet blir allt tydligare också i gränserna mellan det civila och militära. Detta framträder tydligt inom exempelvis informations- och cybersäkerhet där det civila samhället blir mer och mer uppkopplat och beroende av internet för sin dagliga funktion samtidigt som internet också utvecklas som militär arena. Flera artiklar i denna utgåva av *Strategisk utblick* belyser också dessa och närliggande frågeställningar.

Försvarsforskningens särskilda förutsättningar

Försvarsforskningen har långa traditioner. När den tekniskt-naturvetenskapliga försvarsforskningen utvecklades under nittonhundratalet rekryterades forskare inom ämnen såsom kemi, fysik och matematik från de akademiska miljöerna. Dessa forskare skapade tillsammans forskningsmiljöer där de nya forskningsområdena för att tillgodose försvarets kunskapsbehov utvecklades.

Idag är försvarsforskningen specialiserad mot områden som vanligen inte täcks av andra forskningsutförare, exempel på detta är krigsvetenskap, operationsanalys, underrättelse-

analys, forskning kring vapen och telekrig. Detta gör att försvarsforskningen får en särskild betydelse för nationell säkerhet, eftersom den utvecklar insikt på områden där samhället inte har andra källor till kunskap.

På samma sätt som den civila forskningens innehåll förändras i takt med nya rön sker en ständig utveckling av forskningen inom försvarsområdet. Exempel på aktuella nya områden inom försvarsforskningen är cyber- och påverkansoperationer samt utvecklingen av obemannade farkoster för den militära arenan. Försvarsforskningen är integritetskritisk eftersom den syftar till utveckling av operativ förmåga och den är ofta omgärdad med sekretess. Sekretessen beror på krav avseende förmågeutveckling men också på att det handlar om kunskap som inte är lämplig att sprida, exempelvis av säkerhetsskäl. Inom vissa forskningsområden, av stor vikt för försvaret, sker en betydande kunskapsutveckling civilt samtidigt som det finns försvarsspecifika behov som inte kan täckas av civila utförare. Detta beror dels på integritets- och säkerhetsskäl men också på behovet av *domänkunskap*. Domänkunskap, det vill säga kännedom om den miljö och den verksamhet där resultaten ska användas och skapa nytta, är i många fall avgörande för att forskningen ska generera effekt. Specialiserade kunskapsområden, integritet och domänkunskap är skäl till varför betydande delar av försvarsforskningen behöver ske i särskilda forskningsmiljöer.

Forskning – en kunskapsberedskap

Forskning skapar effekt genom att resultaten, det vill säga den nya kunskap och de nya verktyg som över tid skapats genom forskningen, omsätts i en verksamhet. Resultaten skapar inte en singulär, enstaka effekt utan leder till flera effekter på olika platser och olika tider. Effekterna av viss forskning är omedelbart uppenbara, medan det i andra fall kan ta år, eller till och med årtionden, innan det verkliga värdet framträder. Det finns inga enkla förutsägelser om potentiella effekter eller utfall, och inget enda mått på effekt. Forskningen skapar en bank av kunskap, eller en kunskapsberedskap, som kan användas för att lösa olika problem vid olika tidpunkter. Med detta synsätt kan forskningen ses som en beredskap eller försäkring för att kunna lösa framtida problem, och därmed innebär minskade satsningar på forskning också ett ökat framtida risktagande.

Det är inte ovanligt att nyttjande av forskningsresultaten förväxlas med själva forskningen i sig. Man skapar sig bilden att forskaren som löser ett problem här och nu sysslar med forskning när hen istället tillämpar sin expertis. De två aktiviteterna är

besläktade men de är inte desamma, och den ena, forskningen, är en förutsättning för den andra, problemlösningen. Problem uppstår och kan lösas här och nu genom den kunskapsberedskap som byggts upp under lång tid. Om kunskapsberedskapen inte finns kan heller inte problemen lösas.

Om aktiviteterna förväxlas ligger det alltså nära till hands att tro att expertis här och nu kan prioriteras på bekostnad av långsiktig forskning. Den långsiktiga kunskapen riskerar då att utarmas med ett framtida risktagande som följd. Forskningens långsiktighet innebär också att det tar lång tid innan effekterna av minskningar blir synliga.

Urholkningen av framtidens beredskap

Tidscyklerna för forskning är annorlunda än de politiska tidscyklerna. Beslut avseende (försvars)forskning fattade inom en försvarsbeslutsperiod, i en säkerhetspolitisk kontext, når sannolikt full effekt först i en senare försvarsbeslutsperiod. Den svenska försvarsforskningen har under de senaste decennierna genomgått stora neddragningar, flera av dessa har vi sett konsekvenserna av medan andra ännu inte nått full effekt.

Försvarsbeslutet år 2000 innebar en övergång från ett invasionsförsvar till ett insatsförsvar. Regeringen bedömde att den grundläggande positiva säkerhetspolitiska situationen i Sveriges närområde kvarstod, även om det fanns en osäkerhet angående Rysslands politiska utveckling. De grundläggande förbättringarna av det säkerhetspolitiska läget innebar att försvarsutgifterna kunde minska samtidigt som försvarsförmågan upprätthölls. Inriktningen stärktes i nästa försvarsbeslut när det också beslutades att ytterligare skära ner på utgifterna för det militära försvaret bland annat genom neddragningar på de försvarsgemensamma myndigheterna inklusive forskningen. Kraftiga besparingar beslutades inom forskning och teknikutveckling för försvaret.

Försvarsbeslutet 2009, som kom till efter Georgienkriget, innebar ökade krav på operativ förmåga och att resurser skulle frigöras för detta ändamål. Detta innebar även ytterligare nedskärningar av medel för forskning och utveckling. Även budgetpropositionerna för 2012 och 2013 föreslog neddragningar avseende medel för forskning och utveckling.

Sammantaget har nedskärningarna inneburit att forskning och utveckling inom försvarsområdet har minskat med mer än 50 procent sedan år 2005 och att den långsiktiga forskningen, som är grunden för utvecklingen av framtida operativ förmåga,

skurits ned kraftigt till förmån för operativ förmåga här och nu. Att det alls har varit möjligt att, trots de kraftiga minskningarna, kunna ge kunskapsstöd till utvecklingen av den operativa förmågan beror på forskningens långsiktiga karaktär. Den kunskap som idag ligger till grund för förmågeutvecklingen har betydande inslag av forskning som skett i tidigare perioder.

Dagens läge

Det har skett omfattande förändringar i omvärlden sedan år 2000. Hoten har utvecklats och vi ser idag både en avancerad militär förmåga liksom förmåga till cyber- och påverkansoperationer i vårt närområde som vi måste förhålla oss till. Den försvarspolitiska inriktningen anger att det enskilt viktigaste under den kommande inriktningsperioden är att höja den operativa förmågan i krigsförbanden och öka den samlade förmågan i totalförsvaret. Försvarsmakten ska kunna försvara Sverige mot väpnat angrepp och anslagen till försvaret har ökat. Ökningarna har fram till augusti 2017 emellertid inte gällt forskningsanslagen, vilka under det senaste decenniet snarare drabbats av stora neddragningar.

En ökning av försvarets operativa förmåga och Sveriges möjlighet att möta andra hot mot den nationella säkerheten innebär också behov av ökade satsningar på forskning. Försvarsforskningsutredningen skriver att det, i ljuset av omvärldsutvecklingen, behövs ökade resurser till försvarsforskningen och att totalt minst 400 miljoner kronor bör tillföras den försvarsrelaterade forskningen i nästa försvarsbeslutsperiod för att stärka Försvarsmaktens operativa förmåga och den samlade förmågan i totalförsvaret. Utredningen öppnar samtidigt för att ökningen kan behöva tidigareläggas om omvärldsutvecklingen försämras ytterligare.

Vad behövs för att minska det svenska risktagandet?

Omvärldsutvecklingen har knappast förbättrats den senaste tiden och om nya forskningsresultat ska kunna nå full effekt för förmågeutvecklingen under nästa försvarsbeslutsperiod behöver ökningen därför påbörjas snarast. I den överenskommelse som träffades i augusti 2017 om ökning av försvarsanslagen aviseras också åtgärder kopplade till anslagen för forskning och utveckling inom försvarsområdet. I ett första steg häver överenskommelsen de senaste aviserade neddragningarna på forskningen. Den öppnar också upp för att från 2018 börja återhämta tidigare neddragningar.

Ökade satsningar på forskning handlar om att skapa hållbara forskningsmiljöer som ges den tid som krävs för att utveckla

ny kunskap inom försvarsspecifika områden. Ökad produktion av kunskap och forskningsresultat kan inte ske ögonblickligen, lika lite som det går att öka antalet lärare, officerare eller poliser utan att sådana först utbildats och tränats.

Forskning handlar om att utveckla ny kunskap, att bryta ny mark inom ett område och det finns dessvärre inga genvägar. Samarbeten kan bidra till en snabbare kunskapsutvecklingsprocess och ge värdefull tillgång till en större kunskapsmängd, men det tar tid att skapa bärkraftiga forskningsmiljöer. Resultaten ska sedan omsättas i den militära förmågeutvecklingen som, precis som forskningen, är kvalificerad verksamhet som inte heller denna uppstår ögonblickligen.

Därför måste en ökning av försvarsforskningen ske hållbart med utgångspunkten att det behövs utrymme för kunskapsutveckling innan effekterna av satsningen blir fullt synliga. Avsaknad av synliga effekter inom något eller några år innebär inte att dessa inte kommer att uppstå, utan beror på de inneboende tidsperspektiven i forskning.

För att befintlig kunskap inte fortsatt ska utarmas, med ett säkerhetsmässigt risktagande på långt sikt som följd, måste därför den ökning av anslagen för forskning och utveckling inom försvarsområdet som nu aviserats fortsätta och ske med ett långsiktigt och hållbart perspektiv.

Författare

Simon Ahlberg är civilingenjör i datateknik och förste forskare vid FOI:s enhet för Sensorinformatik. Där arbetar han inom bland annat geoinformatik och verksamhetsutveckling avseende Försvarsmaktens användning av geografisk information. Han har även forskat kring militär modellering och simulering, med tonvikt på snabb framställning av omvärldsmodeller genom automatisk bearbetning av data från flygburna sensorplattformar.

Maria Andersson är förste forskare vid FOI:s enhet för Sensorinformatik. Hon har en doktorsexamen i energisystem vid Linköpings universitet. Hennes expertområden är metoder för automatiskt detektion av kritisk information i stora datamängder samt energisystemanalys. Hon arbetar i nationella och internationella projekt med fokus på olika övervakningstillämpningar, där sensordata samlas in och analyseras.

Erik Berglund är överingenjör vid FOI:s enhet för Systemteknik. Hans expertområden är robotsystem, luftvärn och analys och värdering av vapensystem. Erik är för närvarande tjänstledig för arbete vid Försvarsdepartementet och har tidigare arbetat vid Organisationen för förbud mot kemiska vapen (OPCW) och Frontex.

Niklas Brännström är tillförordnad enhetschef för FOI:s enhet Hot, Spridning och Radioaktiva ämnen. Hans expertområde är atmosfäriska spridningsberäkningar. Niklas har disputerat i matematik vid University of Warwick i Storbritannien.

Robert Dalsjö är forskningsledare vid FOI:s enhet för Strategi och policy, med fokus på aktuella politisk-militära frågor, vilket för närvarande betyder nationella intressen, tröskelförsvar/avskräckning och Östersjösäkerhet inklusive A2/AD (fysiska avreglingszoner). Han har tidigare tjänstgjort som analysstöd/rådgivare vid Försvarsdepartementet och vid Natodelegationen.

Daniel Eidenskog arbetar som forskare vid FOI:s enhet för Informationssäkerhet och IT-arkitektur. Han arbetar huvudsakligen med forskning och expertstöd inom informations- och IT-säkerhet åt såväl Försvarsmakten som civila myndigheter. Daniel är Tekn. Dr. i datorteknik och har en bakgrund inom utveckling av IT-säkerhetsprodukter avsedda för Försvarsmakten. Delar av Daniels forskning sker inom NCS3, nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet.

Martin Hagström är forskningsledare vid FOI:s enhet för Systemteknik. Hans expertområde är autonoma system, flyg och obemannade farkoster och han har under de senaste åren forskat om autonoma vapensystem. Han ansvarar för FOI:s stöd till inriktningen av Försvarsmaktens forskning inom vapen och skydd. Martin har tjänstgjort i många roller vid FOI och deltagit i flera internationella forskningsprojekt.

Eva Hagström Frisell är forskningsledare vid FOI:s enhet för Säkerhetspolitik. Hennes expertområde är europeisk säkerhet och internationella insatser. Hon har nyligen publicerat rapporter om Tysklands och Polens säkerhets- och försvarspolitik. Eva har tidigare tjänstgjort som analysstöd vid Försvarsdepartementet och som strategisk rådgivare vid Myndigheten för samhällsskydd och beredskap (MSB).

Alf Christian Hennum har arbetat som forskare vid Forsvarets Forskningsinstitutt (FFI) i Norge sedan år 2003. Han har en masterexamen i teoretisk kemi från Oslo universitet. Vid FFI har han arbetat som operationsanalytiker, huvudsakligen med inriktning mot långsiktig planering på en strategisk nivå. Under utvecklingen av den senaste försvarsplanen samordnade han FFI:s stöd till det norska Försvarsdepartementet.

Michael Jonsson är förste forskare vid FOI:s enhet för Strategi och policy. Hans expertisområde är inomstatliga konflikter och icke-militära säkerhetshot. Han har nyligen publicerat rapporter om Somalia, Nigeria och Syrien, samt bidragit till en studie om säkerhets- och försvarspolitik i norra Europa. Michael har disputerat i statsvetenskap och har tidigare tjänstgjort som konsult för Internationella Valutafonden (IMF) och operationsanalytiker vid Försvarshögkvarteret.

Farzad Kamrani jobbar som forskare vid FOI:s enhet för Beslutsstödsystem. Han har arbetat flera år med modellering och simulering och forskar inom området artificiell intelligens och maskininlärning. Han är även intresserad av datasäkerhet och personlig integritet. Han har en magisterexamen i datavetenskap från Göteborgs universitet och en teknologie doktorsexamen inom elektronik- och datorsystem från KTH.

Anders Lennartsson är forskningsledare vid FOI:s enhet för Systemteknik. Hans expertområde är flyg- och rymdteknik, inklusive robotvapen i form av ballistiska robotar, kryssnings- och jaktrobotar, samt missilförsvar. På uppdrag av UD är han ordförande i den tekniska arbetsgruppen inom Missile Technology Control Regime, en av fyra exportkontrollregimer.

Fredrik Lindgren var tidigare forskningsledare vid FOI:s enhet för Samhällets säkerhet, med fokus på krisberedskap, civilt försvar och totalförsvar. Han har under de senaste åren varit projektledare för flera av FOI:s projekt om civilt försvar och även arbetat med analyser och studier av samhällets krisberedskap på nationell nivå. Fredrik är för närvarande tjänstledig från FOI och arbetar åt Länsstyrelsen Uppsala. Han har tidigare arbetat på Försvarsdepartementet.

Sandra Lindström är förste forskare vid FOI:s enhet Marina system där hon för närvarande är tjänsteförättande enhetschef. Hon har arbetat på FOI i 15 år och har huvudsak koordinerat och lett arbetet för rymdgruppen. Sandra har lett olika rymdprojekt för kunder som Försvarsmakten, Försvarets Materielverk (FMV) och Utrikesdepartementet. Hon har en civilingenjörsexamen i rymdteknik från Luleå tekniska universitet.

Peter Nordlund verkar vid FOI:s enhet för Försvarsekonomi. Han bär titeln överingenjör men är trots denna ekonom från Handelshögskolan. Han leder projekt med stor försvarsekonomisk bredd där den ekonomiska analysen ofta har en tydlig verksamhetskoppling. Peter har under 17 år arbetat inom bank- och finanssektorn i olika chefspositioner.

Tore Nyhamar har sedan år 2001 arbetat på Forsvarets Forskningsinstitutt (FFI) i Norge, som projektledare och forskare. Han har doktorerat på statsvetenskapliga institutionen vid Oslo universitet där han innehade olika positioner mellan 1989 och 2001. I sitt arbete vid FFI har han lett organisationens arbete kring internationella insatser. Hans nuvarande forskning handlar huvudsakligen om små staters framtida militär operationer och skyddet av civila vid militära operationer.

Torbjörn Nylén tillhör FOI:s enhet för Hot, spridning och radioaktiva ämnen. Han är filosofie doktor i radioekologi och verkar som kompetensområdesledare för forskningen inom radioaktiva ämnen vid FOI. Hans expertområde är intern dosimetri samt upptag och omlagring av radioaktiva ämnen i människa och miljö.

Jyri Raitasalo, Övlt är senior tjänsteman vid planeringsenheten (strategisk planering) vid Finska försvarsdepartementet. Jyri har disputerat i statsvetenskap och innehar en docenttitel i strategi och säkerhetspolitik vid Försvarshögskolan i Finland. Han har varit befälhavare vid Helsingfors luftfvärnsregemente (Pansarbrigaden), universitetslektor i strategi vid den finska försvarshögskolan, militärassistent till finska Överbefälhavaren och stabsofficer (strategisk planering) i finska Försvarsmaktens huvudstab (J5). Jyri är medlem i den svenska Krigsvetenskapsakademin.

Henrik Ramebäck är forskningschef vid FOI:s enhet för Hot, spridning och radioaktiva ämnen. Hans expertområde är identifiering, mätning och karaktärisering av radioaktiva ämnen och kärnämnen. Henrik innehar även en adjungerad professur i kärnkemi vid Chalmers tekniska högskola.

Niklas H. Rossbach är förste forskare vid FOI:s enhet för Säkerhetspolitik med amerikansk och europeisk säkerhetspolitik som sin främsta inriktning. Han har återkommande skrivit om Brexit men även om de strategiska följderna av ny amerikansk energiutvinning. Han har doktorerat i historia vid Europeiska universitetsinstitutet och med stöd av Axel och Margaret Ax:son Johnsons Stiftelse forskat om psykologiskt försvar vid universitet i Oxford.

John Rydqvist verkar vid FOI:s enhet för Säkerhetspolitk och hans expertområde är säkerhetspolitiska och militärstrategiska förändringar i Öst-, Syd-, och Västasien. Han har särskilt fokuserat på hur strategiska vapensystem påverkar regional och global säkerhetsarkitektur. För tillfället studerar han kärnvapenstrategi i de Euroatlantiska relationerna. John är projektledare för de försvarspolitiska studierna på FOI. Mellan 2006 och 2015 ledde han projektet ”Asiens och Mellanösterns säkerhetspolitik”.

Anna Sundberg är förste forskare vid FOI:s enhet för Säkerhetspolitik där hon fokuserar på europeiska staters säkerhets- och försvarspolitik. Hon har nyligen publicerat rapporter om Tyskland och Polen. Tidigare har hon även skrivit flera rapporter om EU. Anna har arbetat på Försvarshögskolan och även tjänstgjort vid det franska forskningsinstitutet Fondation pour la recherche stratégique och som analysstöd vid Försvarsdepartementet.

Ulf Söderman är forskningsledare vid FOI:s enhet för Sensorinformatik. Ulf arbetar huvudsakligen med geoinformatik med inriktning mot ny geografisk information i 3D och dess tillämpningar för Försvarsmakten. Han har tidigare forskat kring 3D-kartering och framställning av digitala 3D-landskapsmodeller med data från flygburna sensorplattformar. Han har en civilingenjörsexamen i Datateknik och en doktorsexamen i Datalogi från Linköpings tekniska högskola.

Gustav Tolt är förste forskare och projektledare vid FOI:s enhet för Sensorinformatik. Gustav arbetar huvudsakligen med utveckling av analysmetoder för 3D geografisk information och data från 3D-avbildande lasersensorer. Han har en civilingenjörsexamen i Teknisk Fysik från Chalmers Tekniska Högskola och en doktorsexamen i Industriell Mätteknik från Örebro Universitet.

Lars Westerdahl är forskare vid FOI:s enhet för Informationssäkerhet och IT-arkitektur. Hans expertområde är informationssäkerhet. Han koordinerar sedan tre år enhetens arbete inom Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3), vilket är en del av MSB:s program för ökad säkerhet i industriella informations- och styrsystem. Lars har tidigare arbetat med åtkomstkontroll samt informationssäkerhetsfrågor för IT-system under utveckling och nyttjande.

Erik Westring är forskningsingenjör vid FOI:s enhet för Informationssäkerhet och IT-arkitektur. Hans expertområde är informationssäkerhet för samhällsviktig verksamhet. Han är aktiv i och har publicerat rapporter för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NSC3) i samarbete med Myndigheten för samhällsskydd och beredskap (MSB). Han är med och organiserar samt genomför större nationella/internationella IT-säkerhetsövningar.

Mikael Wedlin är forskningsledare vid enheten för Informationssäkerhet och IT-arkitektur på FOI. Hans huvudämne är IT-vapen och IT-krigföring med främst ett tekniskt perspektiv. Han har även studerat sårbarhetsaspekter på vår kritiska infrastruktur samt svarat för en stor del av enhetens verksamhet inom utvecklingen av en träningsanläggning för IT-säkerhet på en teknisk nivå, CRATE.

Katarina Wilhelmsen är forskningsdirektör vid FOI. Hennes arbete vid FOI rör bland annat inriktning och utvärdering av forskning. Hon har också arbetat med liknande frågor inom Försvarsmakten. Under 2016 var hon sekreterare i utredningen *Forskning och utveckling på försvarsområdet*. Katarina disputerade i fysik vid Chalmers, är docent vid Stockholms universitet och har varit adjungerad professor vid Chalmers.

Mikael Wiklund är förste analytiker vid FOI:s enhet för Strategi och Policy. Hans expertområde är strategisk myndighetsstyrning med fokus på försvarspolitik, försvarsekonomi och underrättelsetjänst. Han har nyligen arbetat med strategiutveckling och riskhantering inom försvarsmyndigheterna. Mikael tjänstgör för tillfället som operationsanalytiker inom Försvarsmaktens högkvarter men har även tidigare varit utredningssekreterare och expert i en statlig utredning om försvarsstrukturer.

Mike Winnerstig, Dr, är forskningsledare vid FOI:s enhet för Säkerhetspolitik. Hans forskning har under lång tid fokuserat på amerikansk utrikes-, säkerhets- och försvarspolitik samt Nato och andra transatlantiska säkerhetsfrågor. Sedan 2010 har han också studerat Östersjöområdets säkerhetsproblem, särskilt de baltiska ländernas försvars- och säkerhetspolitik. Inom ramen för sin tjänstgöring på FOI har han också tjänstgjort som analysstöd på Försvarsdepartementet.

Ann Ödlund är förste forskare vid FOI:s enhet för Strategi och policy. Ann har en utbildningsbakgrund inom beteendevetenskap och organisationspsykologi. De senaste åren har hon genomfört studier främst inom totalförsvar och civilt försvar och har publicerat flera rapporter i ämnet.

Redaktion

Daniel Faria är förste analytiker vid FOI:s enhet för Marina system och medredaktör för *Strategisk utblick 7*. Han ansvarar för forskningsprojekt inom rymdsäkerhet och militär rymdrelaterad förmågeutveckling, samt är teknisk expert åt Utrikesdepartementet inom rymdområdet. Daniel har en magisterexamen i fysik och en doktorsexamen i astrofysik från Lunds universitet. Innan han påbörjade sin nuvarande position vid FOI arbetade han inom operationsanalys och forskningspolitik.

Cecilia Hull Wiklund är projektledare och huvudredaktör för *Strategisk utblick 7*. Hon är förste analytiker vid FOI:s enhet för säkerhetspolitik och programansvarig för FOI:s Afrikastudier. Cecilia har tidigare tjänstgjort som analysstöd vid Försvarsdepartementet med fokus på internationella insatser och Afrika. Hon har även arbetat med erfarenhetshantering på Försvarsmaktens insatsstab och med insatsutvärdering på FN.

Bengt Johansson är forskare vid FOI och docent i miljö- och energisystem vid Lunds universitet. Hans expertområde är energi- och klimatpolitik och han har på senare år bland annat intresserat sig för hur energisäkerheten påverkas av den pågående omställningen av energisystemet. Bengt har tidigare under flera år arbetat med energi- och klimatpolitiska frågor på Naturvårdsverket.

Josefin Öhrn-Lundin är en av redaktörerna för *Strategisk utblick 7*. Hon arbetar som analytiker vid FOI:s enhet för Försvarsekonomi. Josefin har en MSc i innovations- och tillväxtekonomi från Kungliga Tekniska Högskolan.

ISSN1650-1942

www.foi.se