Strategisk utblick 8

Totalförsvarets tillväxt – utmaningar och möjligheter

Niklas H. Rossbach, Josefin Öhrn-Lundin, Daniel K. Jonsson, Anna Sundberg, Sofia Olsson, Jakob Gustafsson och Camilla Trané (red.)

FOI-R--4773--SE

Maj 2019

FOI

FOI

Strategisk utblick 8

Totalförsvarets tillväxt – utmaningar och möjligheter

Niklas H. Rossbach, Josefin Öhrn-Lundin
Daniel K. Jonsson, Anna Sundberg,
Sofia Olsson, Jakob Gustafsson
och Camilla Trané (red.)

Maj 2019

FOI-R--4773--SE

ISSN 1560-1942
Tryckt i Stockholm 2019 av Totalförsvarets forskningsinstitut, FOI
Omslagsbild: Trons / TT
FOI-R--4773--SE
Godkänd av Lars Höstbeck

Innehåll

Totalförsvarets tillväxt – utmaningar och möjligheter

Förord

I år är det tio år sedan den första Strategisk utblick gavs ut men årets är den första med huvudsakligt fokus på totalförsvaret. Kapitlen ger ett smakprov på den breda kompetens som FOI besitter och kan bidra med.

Utvecklingen av Sveriges nya totalförsvar är en central uppgift för samhället. Totalförsvaret är nödvändigt för att förbereda Sverige för olika typer av störningar, konflikter och ytterst krig. Det är förstås det försämrade säkerhetspolitiska omvärldsläget som har aktualiserat behovet av en återstart.

Även om begreppet totalförsvar ibland för tankarna till det civila försvaret så omfattar totalförsvarets verksamhet också Försvarsmakten. Det militära försvaret har ytterst till uppgift att försvara Sverige mot incidenter och väpnat angrepp.

Till det civila försvarets uppgifter hör att värna civilbefolkningen, upprätthålla de viktigaste samhällsfunktionerna och stödja Försvarsmakten. Till skillnad från Försvarsmakten består det civila försvaret inte av en enda myndighet. Istället utgörs det av samma verksamheter som får vårt samhälle att fungera till vardags, exempelvis livsmedels- och energiförsörjning, bank- och betalningssystem, sjukvård, polis samt kommunala verksamheter, inklusive räddningstjänst. Det civila försvaret ska bygga på den fredstida krisberedskapen, men under högsta beredskap utgörs totalförsvaret av den samhällsverksamhet som då behövs.

Strategisk utblick 8 pekar även på nödvändigheten för det civila försvaret att hantera olika former av icke-militära angrepp. Ett exempel är påverkansoperationer, som inte behöver vara en del av en öppen väpnad konflikt. Med andra ord kan sådana angrepp äga rum i gråzonen mellan krig och fred.

För att kunna skapa ett ändamålsenligt totalförsvar krävs djupa kunskaper i flera olika områden såsom försvars- och säkerhetspolitik, krisberedskap, militär teknik, samhällskritisk infrastruktur, informationssäkerhet och skydd mot farliga ämnen. FOI:s uppgift är att tillhandahålla sådan kunskap.

Under många års forsknings- och utvecklingsarbete har FOI byggt upp en kompetensbas som utgör en central resurs för hela samhället. 2019 års upplaga av Strategisk utblick speglar såväl FOI:s forskning som kunskap om totalförsvarsfrågor. Jag hoppas

att rapporten ska vara tankeväckande och värdefull läsning för berörda beslutsfattare och andra som är verksamma inom totalförsvaret, likväl som för den intresserade allmänheten.

Författarna diskuterar olika aspekter av totalförsvaret. Kapitlen 1 till och med 3 bildar en bakgrund till övriga avsnitt. Här visas hur globala trender har lett till behovet av ett totalförsvar anpassat för vår tid, och vikten av att både tänka nytt och tillvarata erfarenheter från 1990-talet, vilket var den senaste tid då Sverige hade en omfattande totalförsvarsplanering. Trots snabba förändringar i vår omvärld kommer det att ta tid att återstarta totalförsvaret.

Kapitlen 4 till och med 6 berör förutsättningarna för att totalförsvaret ska fungera väl under de kommande åren. Det handlar bland annat om motivation för att medborgare ska bidra till totalförsvaret, det som brukar kallas försvarsvilja. Dessutom behövs fungerande samverkan myndigheter emellan. Om samarbeten förbereds i fred, fungerar de som regel bättre vid en kris.

Kapitlen 7 och 8 handlar om olika ekonomiska aspekter på totalförsvaret. Kapitel 7 visar hur Sverige liksom andra länder brottas med att lägga försvarsbudgeten på rätt förmågor, det vill säga de som behövs i framtiden. Kapitel 8 handlar om samarbete mellan näringsliv och myndigheter med fokus på försörjning.

Kapitel 9 är det första av de mer renodlade naturvetenskapliga kapitlen och behandlar hur den syntetiska biologin kan stärka försvaret av Sverige, men också hur syntetisk biologi i orätta händer kan ge upphov till nya hot. Kanske kommer området om några år att bli lika omtalat som digitaliseringen är idag.

Kapitlen 10 till och med 14 handlar om olika perspektiv på det som i den allmänna debatten associeras med IT-frågor, och allt oftare med digitalisering eller cyber. De handlar exempelvis om vikten av att öva cyberförsvaret. Kapitlen tar också upp betydelsen av att även skydda hårdvaran för att samhället ska kunna fungera vid en kris. Utöver detta belyses den artificiella intelligensens (AI) betydelse för totalförsvaret och hur fejkade nyhetsbilder kan underminera försvarsviljan.

Kapitel 14 är dessutom plats för årets gästspel. I årets Strategisk utblick har Fortifikationsverket bjudits in för att ge sitt perspektiv på hur Sverige kan skydda information i säkra miljöer, till exempel bergrum. Kapitlet tydliggör att ett sådant skydd inte kan byggas i en handvändning.

Slutligen visar kapitel 15 hur FOI kan bidra till ett stärkt totalförsvar genom att introducera en ny kunskapsmodell. Efter det senaste försvarspolitiska inriktningsbeslutet om att återuppta

totalförsvarsplaneringen har delar av FOI:s verksamhet successivt anpassats i syfte att möta uppdragsgivarnas kunskapsbehov avseende totalförsvaret.

En av FOI:s stora styrkor är att myndigheten har en djup kunskap om och insikt i både den civila och den militära delen av totalförsvaret. Denna förståelse ger en unik möjlighet att bidra till utvecklingen av många olika delar av totalförsvaret. Att identifiera områden av betydelse för totalförsvaret där FOI kan hjälpa till är viktigt för att få till stånd en långsiktig dialog med våra uppdragsgivare om behov och möjligheter till kunskapsuppbyggnad. Det är något som gagnar såväl totalförsvaret som ett tryggt och säkert Sverige.

Rapporten har involverat författare från FOI:s samtliga forsknings-avdelningar. Förutom ett stort tack till författarna vill jag även rikta ett tack till redaktörerna och deras fantastiska insats som möjliggjort vår åttonde Strategiska utblick.

Stockholm, maj 2019

Anna-Lena Österborg
Vikarierande generaldirektör
Totalförsvarets forskningsinstitut, FOI

1. Sveriges totalförsvar, globala trender och nya utmaningar

Samuel Bergenwall och Carina Gunnarson

Sveriges försvars- och säkerhetspolitik står inför stora utmaningar under de närmaste fem till tio åren. Den positiva säkerhetspolitiska utvecklingen som följde på det kalla krigets slut har brutits. Samtidigt som den sociala och ekonomiska utvecklingen i världen fortsätter i positiv riktning, finns trender som pekar på ökad instabilitet och osäkerhet såväl globalt som i Sveriges närområde. Denna negativa omvärldsutveckling ställer högre krav på Sveriges militära och civila försvar. Det nya totalförsvaret behöver anpassas för att kunna bemöta nya utmaningar i en föränderlig omvärld.

Säkerhetsläget i världen har försämrats

Mot bakgrund av Rysslands illegala annektering av Krim och pågående aggression mot Ukraina har spänningarna ökat i Östersjöregionen. Storbritanniens utträdesprocess ur EU och Trumpadministrationens säkerhetspolitik har bidragit till oförutsägbarheten avseende den säkerhetspolitiska utvecklingen globalt och i Europa. Mellanöstern och Nordafrika, EU:s sydliga närområde fortsätter att vara instabilt, vilket påverkar Europas politik och sammanhållning.

Utöver detta tillkommer växande spänningar i Asien – en region som har en allt viktigare roll för den globala ekonomin och säkerheten. Ökade spänningar och konflikter bortom Europa, mellan stater såsom USA, Kina och Ryssland påverkar multilaterala organisationer som EU, NATO och FN. Detta får återverkningar också i Sveriges närområde. Kinas militära upprustning och strävan efter större politiskt inflytande såväl regionalt som globalt har även säkerhetspolitiska konsekvenser för Sverige.

Den regelbaserade världsordningen, demokratin och globaliseringen är utmanad

Den gradvisa maktpolitiska tyngdpunktsförskjutningen från väst till Asien har åtföljts av större utmaningar för internationella regler och normer. USA:s dominerande roll i det internationella systemet, som etablerades efter andra världskriget och förstärktes efter kalla krigets slut, håller på att förändras. Osäkerheten har ökat om USA:s globala roll, stöd för den regelbaserade världsordningen och fortsatta engagemang för Europas säkerhet. Samtidigt försöker framväxande regionala och globala stormakter samt icke-statliga aktörer att utmana internationella normer och underminera den västledda och regelbaserade världsordningen.

Stormakter försöker återigen att etablera intressesfärer medan etablerade multilaterala institutioner försvagas.

Parallellt har den demokratiska utvecklingen under det senaste decenniet försvagats i en del hänseenden, bland annat med minskad respekt för medborgerliga rättigheter och för rättsstatens principer. Denna trend är tydlig i stort sett i alla världens regioner, inklusive i Europa, med ökade säkerhetspolitiska risker som följd. En källa till oro är att flera av världens största länder, såsom Ryssland och Kina, utvecklas i en än mer auktoritär riktning. I flera länder utmanas demokratierna av populistiska krafter som är kritiska till globalisering och multilaterala organisationer. Trots att den internationella handeln alltjämt är mycket omfattande, finns en tydlig trend i riktning mot isolationism och mot att återföra kontrollen över politiska och ekonomiska beslut till nationell nivå.

Som ett litet och exportberoende land gynnas Sverige av internationell handel, en demokratisk omvärld, starka multilaterala institutioner och en regelbaserad ordning. Dessa värden hotas av ekonomisk isolationism, auktoritära regimer, starka staters underminering av internationell rätt och en ytterligare försvagning av den nuvarande världsordningen.

Förändringarna i omvärlden, i synnerhet i Sveriges närområde, ställer högre krav på totalförsvaret. Sverige är i hög grad beroende av välfungerande, öppna och fria marknader för sin import av livsmedel och strategiska råvaror. Utmaningarna mot den internationella handeln gör att totalförsvaret behöver höja sin beredskap för att kunna hantera situationer där Sveriges energi- och livsmedelsförsörjning hotas.

Konflikternas natur förändras

Påverkan i gråzonen mellan fred och krig genom så kallad hybridkrigföring utgör en växande utmaning. Detta innebär att stater använder sig av såväl militära som icke-militära maktmedel. Det senare inbegriper informationskrig, cyberangrepp och ekonomisk påtryckning, i syfte att påverka andra länders politik och samhällen. Öppna militära konflikter kan komma att kompletteras med exempelvis angrepp som riktas mot civil infrastruktur och beslutsfattare, eller genom spridning av desinformation. Cyberrymden är en allt viktigare arena för konflikter. Detta innebär att exempelvis påverkansoperationer kan bedrivas på allt längre geografiskt avstånd, samtidigt som det är svårt att identifiera angriparen, vilket försvårar avskräckning och motåtgärder.

Den tekniska utvecklingen och digitaliseringen innebär många fördelar men har samtidigt medfört nya sårbarheter. Statliga och

icke-statliga aktörer har fått nya redskap för att påverka samhällen utan att behöva använda traditionella militära maktmedel. Beredskap hos samtliga myndigheter och ett stärkt totalförsvar blir därför allt viktigare.

Kärnvapnens mer framträdande roll

Rysslands retorik och moderniseringen av dess kärnvapenarsenal bidrar till större osäkerhet i Sveriges närområde. Risken för att kärnvapen används i närområdet har ökat. Totalförsvaret behöver därmed förhålla sig till en värld där kärnvapnens betydelse blir mer framträdande.

De västliga stormakterna har påbörjat en modernisering av sina kärnvapen. Huruvida Ryssland och USA kommer att bli överens om och förnya befintliga avtal för rustningskontroll är osäkert. Även Kina, Indien och Pakistan fortsätter att utveckla och utöka sina kärnvapenarsenaler. Konflikterna kring Irans och Nordkoreas kärntekniska program är fortsatt olösta. Det finns även en risk att kärnvapenteknologi och andra typer av massförstörelsevapen sprids till fler stater, men också till icke-statliga aktörer.

Klimatförändringarna får allt större påverkan på säkerhetspolitiken

Konsekvenser av en stigande global medeltemperatur är höjda havsnivåer, extremväder, påverkan på jordbruket, bränder, vattenbrist, översvämningar och migration. Klimatförändringar i kombination med bristande institutionell kapacitet hos utsatta stater riskerar att leda till instabilitet och konflikt om resurser.

De säkerhetspolitiska effekterna av klimatförändringarna kommer att vara stora, framför allt i Mellanöstern, Afrika och Sydasien. Klimatförändringarna påverkar även Sveriges närområde. Isavsmältningen i Arktis öppnar nya transportleder till havs och möjliggör för ny energi- och mineralutvinning. Utvecklingen förstärker dock intressekonflikter och rivaliteter exempelvis mellan aktörer i och utanför Arktis där Kina, USA och Ryssland är de viktigaste staterna. Klimatförändringarna kan även påverka Sverige direkt, exempelvis i form av bränder, vilket ställer krav på krisberedskapen.

Den snabba teknikutvecklingen får stora konsekvenser

Inom teknikområden som informationsteknologi, artificiell intelligens och robotik, sker en snabb utveckling som kan få stora ekonomiska och militära konsekvenser och leda till en förändrad maktbalans globalt. Förbättrad tillgänglighet och spridning av ny teknik medför att stater och icke-statliga aktörer kan få tillgång till civil och militär teknologi som tidigare har varit förbehållen väst.

Exempelvis har Kina en långsiktig plan för att bli världsledande vad gäller artificiell intelligens.

Den nya tekniken ger fler möjligheter för stater att agera i gråzonen mellan krig och fred, utan att tröskeln för väpnat angrepp behöver överträdas. Mot bakgrund av detta är det viktigt att Sverige noga följer teknikutvecklingen och säkerställer att totalförsvaret kontinuerligt uppdateras för att kunna hantera nya hot och utmaningar.

Militärutgifter i världen ökar

De globala militärutgifterna är i dag de högsta sedan kalla krigets slut. Detta beror framför allt på kraftigt växande militärutgifter i Kina, Ryssland, Indien och Saudiarabien under det senaste decenniet. Under samma period har demokratiska och västerländska staters andel av de globala militärutgifterna minskat; detta gäller främst de västeuropeiska staterna. Tillväxtländer som Kina och Indien kommer troligen fortsätta att öka sina andelar av världens totala militärutgifter. I dag motsvarar USA:s militärutgifter en dryg tredjedel av världens samlade utgifter.

Mot bakgrund av Rysslands agerande har militärutgifterna i Europa återigen börjat växa. Även om USA har ökat sin militära närvaro på den europeiska kontinenten finns i dag en större medvetenhet i Europas länder om behovet av att ta ett större eget ansvar för Europas försvar och säkerhet.

Sedan kalla krigets slut har Sveriges militärutgifter i relation till BNP sjunkit och motsvarar cirka en procent av BNP. För att uppnå målen i försvarsbeslutet från 2015 finns idag behov av en förstärkning av både det civila och det militära försvaret.

Sverige står inför viktiga säkerhetspolitiska vägval

Det försämrade säkerhetsläget i omvärlden gör att återuppbyggnaden av Sveriges totalförsvar har fått förnyad aktualitet. Planeringen av ett nytt totalförsvar påverkas av hur Sveriges relationer med EU och NATO utvecklas och av hur dessa organisationer anpassar sig till det nya läget i världen. Utformningen av totalförsvaret påverkas även av hur Sveriges samarbete utformas inom Norden och med Baltikum och av samarbetet med strategiskt viktiga länder som USA och Storbritannien.

Medan det gamla totalförsvaret främst var utformat för att möta och hantera ett militärt väpnat angrepp, måste ett modernt totalförsvar förbereda sig för en betydligt bredare hotbild där angriparen inte alltid går att identifiera. För att kunna möta de utmaningar som teknikutvecklingen och det förändrade

säkerhetspolitiska läget för med sig behöver totalförsvaret ha ökad motståndskraft, anpassningsförmåga och kapacitet.

Sammanfattningsvis måste Sverige som en globaliserad stat förbereda sig för en mer osäker omvärld samt utveckla sin förmåga att försvara svenskt territorium, värna samhällets säkerhet och skydda demokratin från extern fientlig påverkan. Utmaningarna ställer höga krav på Sveriges totalförsvar.

För vidare läsning

Jerker Hellström, *Asien - ett nytt maktcentrum*, 2018, FOI Memo 6327.

Krister Pallin (red.), *Västlig militär förmåga. En analys av Nordeuropa 2017*, 2018, FOI-R--4563--SE.

Niklas H. Rossbach, *The Geopolitics of Russian Energy*, 2018, FOI-R--4623--SE.

2. Totalförsvarets förutsättningar då och nu

Maria Lignell Jakobsson

Totalförsvarsplaneringen har återupptagits med start 2015. Senast det bedrevs ett aktivt arbete var under 1990-talet. Sedan dess har Sverige blivit EU-medlem, Försvarsmakten har minskat i omfattning, teknikutvecklingen har accelererat och Sverige har öppnats mot en alltmer föränderlig omvärld. Samtidigt har vi nu samma behov som då av grundläggande försörjning och säkerhet. Ett nytt totalförsvarskoncept behöver dra lärdom av tidigare erfarenheter, men framförallt bygga ny förmåga och kunskap utifrån aktuella förutsättningar. Denna text lyfter fram några exempel på skillnader och likheter avseende förutsättningar mellan vår tid och slutet av den period då en aktiv totalförsvarsplanering förekom, det vill säga 1990-talet.

De stora nedläggningarnas tid

Under 1990-talet genomfördes en omställning av totalförsvaret från det kalla krigets kärnvapenhot och invasionsförsvar till ett försvar med strategiskt överfall som planeringsgrund. Den nya inriktningen handlade om ett militärt angrepp med endast kort förvarning, med begränsade styrkor av hög kvalitet, som riktades mot vitala funktioner inom landets ledningssystem och totalförsvar. En övergång inleddes, från ett totalförsvar som omfattade en stor del av befolkningen, med bland annat värnplikt, civilförsvar, frivilligrörelser, hemvärn och så kallade krigsviktiga företag. Det inbegrep även omfattande lager av bland annat drivmedel och livsmedel. Utvecklingen av ett mindre men vassare totalförsvar hade startat.

Arbetsmetoderna förändrades stegvis från ett fokus på planering där pengar, prylar och pärmar stod i centrum till utveckling av operativ förmåga. Det fanns genomgripande förändringsbehov och arbete bedrevs på stor bredd för att börja hantera dessa, bland annat handlade det om att öka kvaliteten på bekostnad av kvantiteten. Under mitten av 1990-talet bildades Försvarsmakten efter en sammanslagning av ett stort antal myndigheter. Förutom denna omstöpning av verksamheten påbörjades en nedskärning av kostnaderna för totalförsvaret. Sammantaget resulterade det bland annat i en omfattande nedläggning av förband och civila beredskapsresurser.

Begreppet gråzon användes redan på 1990-talet och då för att markera otydligheten i vilka förutsättningar som rådde, men var då liksom nu inte tydligt definierat. Några parametrar var

beredskapsläge i hela hotskalan fred-kris-krig, *totalförsvarsaktörer*, både civila och militära, men även offentliga och privata samt *antagonister*, det vill säga fiender som kunde vara en nation, organisation eller individ. Beroenden mellan Försvarsmaktens delar och olika civila funktioner belystes och ett behov av bättre samordning började därmed tydliggöras.

Det fanns då en lång tradition och mycket samlad erfarenhet inom totalförsvarssektorn, eftersom så många hade haft och fortfarande hade en roll i systemet. Många personer med militär bakgrund arbetade dessutom inom den civila delen av totalförsvaret. Förutom en bred kunskap fanns nätverk och strukturer för ledning och styrning, även på högre regional nivå. En indelning i funktioner med utsedda funktionsansvariga myndigheter bidrog då till att tydliggöra totalförsvarets ansvarsfördelning.

I och med EU-inträdet 1995 började Sverige öppna sig för samverkan inom många områden, inte minst försvarssektorn, och avvecklade en livsmedelspolitik baserad på en hög grad av självförsörjning. EU-inträdet i kombination med globaliseringen förändrade de grundläggande förutsättningarna för såväl säkerhetspolitiken som totalförsvaret.

Andra betydande trender under denna period var dels marknadsliberaliseringen och de internationaliserade handelsflödena, dels en reducering av statens roll i samhället. Detta medförde bland annat en övergång från offentligt till privat ägande inom många samhällssektorer. Idag ställer detta nya krav på tydlighet och precisering av eventuella beredskapskrav vid upphandling – ofta med underleverantörer i flera led.

Under perioden från millennieskiftet till 2015 ställdes fokus om från totalförsvar till internationella operationer på militär sida och till krisberedskap på civil sida. Nedläggningen av förband och totalförsvarsresurser fortsatte. Ansvaret för totalförsvaret delades upp mellan två departement och det finns idag inte längre någon särskild organisation eller några särskilda resurser för höjd beredskap och krig. Kunskap om hur man planerar för krig föll i glömska.

Förändrade och nya förutsättningar

Från slutet av 1990-talet har inte bara omvärlden förändrats utan även Sverige och svenskt försvar. En viktig detalj i sammanhanget är att avsevärt färre personer har kontakt med totalförsvarsrelaterad verksamhet idag. Värnplikten lades vilande under ett antal år och färre personer engagerar sig idag i de frivilliga försvarsorganisationerna. Medborgarna är inte delaktiga i samma utsträckning som förr och därmed blir kunskapen också lägre i stora delar av befolkningen. Ett generationsskifte har skett

på många myndigheter och få av deras medarbetare har idag en egen erfarenhet av totalförsvarsplanering.

Efterfrågan på utveckling och kunskap om totalförsvaret har växt med behovet av att kunna hantera förändrade eller nya förutsättningar. Ett exempel är teknikskiftet med det moderna informations- och medieflödet som ställer helt andra krav på bland annat informationssäkerhet och säkerhetsskyddsverksamhet. En tydlig struktur behöver dessutom utvecklas för styrning och ledning av totalförsvaret med såväl geografisk som funktionell indelning, det vill säga vilken uppgift myndigheter och andra aktörer har. Arenorna för krigföring har blivit fler, vilket kräver såväl kunskap som planering. Mark, sjö och luft har kompletterats med cyber och rymd. Det finns även ett behov av att klargöra begrepp utifrån de nya förutsättningarna för att skapa en tydlig grund för inriktningen av totalförsvaret. Att arenorna blivit fler, och det faktum att en motståndare kan använda andra medel än de traditionellt militära, ställer nya krav på förmågeutveckling inom det civila försvaret.

Internationell samverkan sker på många områden och på ett helt annat sätt idag, framförallt inom EU och Norden, och stöd ges och tas emot på olika sätt. Ett exempel är de av Sverige inlånade flygresurserna för brandbekämpning under de omfattande skogsbränderna somrarna 2014 och 2018. Inom EU pågår nu även utvecklingen av det mellanstatliga samarbetet inom försvarsområdet genom det permanenta strukturerade samarbetet (PESCO) som Sverige deltar i.

Tidlösa behov och förutsättningar

Även om dåtidens och dagens förutsättningar i olika avseenden skiljer sig åt så finns det också gemensamma nämnare. Våra behov av fungerande samhällstjänster och grundläggande säkerhet kvarstår. Fokus nu liksom då är att höja den operativa försvarsförmågan, individens förmåga till överlevnad samt robustheten hos viktiga samhällsfunktioner. Det kan ses som grundläggande utgångspunkter för totalförsvarskoncept oavsett vilken tid vi lever i. Det finns ett antal generiska förmågor som behöver utvecklas och som alltid kommer att behövas utifrån dessa grundläggande behov, exempelvis energi- och livsmedelsförsörjning, sjukvård, kommunikation och transporter.

Hotbilden kännetecknas nu liksom då av stor osäkerhet och vikten av att kunna hantera ett gråzonsläge med tydliga inslag av överraskning. Idag används ibland begreppen hybridkrigföring och icke-linjär krigföring för att beskriva dessa förutsättningar.

Gemensamt för 1990-talet och nutiden är även behovet av en gemensam övergripande prioritering avseende såväl resurs-

uppbyggnad som nyttjande av dessa resurser för att stärka totalförsvarets samlade förmåga. Behovet av att tydliggöra beroenden mellan olika samhällsfunktioner kvarstår, liksom behovet av att planera, utbilda och öva för att kunna ge ett adekvat ömsesidigt stöd.

Vägen mot ett nytt totalförsvar

Med försvarsbeslutet 2015 inleddes ett trendbrott då det väpnade angreppet åter lyftes fram, nya medel tillfördes och bland annat försvaret av Gotland betonades. Det pågår en mängd aktiviteter hos många av totalförsvarets aktörer. Till exempel har totalförsvarsplaneringen återstartats, värnplikten har återinförts, resursuppbyggnad har påbörjats, det militära försvaret har omorganiserats och utredningar har tillsatts.

Det finns framförallt ett stort behov av att åter bygga upp ny kunskap om totalförsvaret, men även att söka kunskap från förr, exempelvis genom att konsultera pensionerade nyckelpersoner med relevant erfarenhet som kan ge stöd i förståelsen av systemet. Såväl Krigsarkivet som FOI:s arkiv har blivit källor för återtagande av kunskap. Det är viktigt att dra lärdomar från det arbete som genomfördes med att modernisera totalförsvaret på 1990-talet och samtidigt anpassa förmågeuppbyggnaden efter nuvarande och framtida förutsättningar. En svårighet är att stärka förmågan inom vitala delar av totalförsvaret utan att först ha utrett förutsättningarna ordentligt och då riskera utveckling av gamla lösningar, det vill säga sådana som inte behöver återskapas eller som är föråldrade. En annan risk är suboptimering om inte olika behov vägs mot varandra i en samhällsövergripande avvägning.

Den stora utmaningen inledningsvis är dock att kunna ge enkla och begripliga svar till myndigheter och andra aktörer som kan användas för styrning och planering av totalförsvaret, ett område där komplexiteten är omfattande och en hög grad av osäkerhet råder. Eftersom det civila försvaret består av alla berörda myndigheter, organisationer och företag så är verksamheten inte lätt att styra, inrikta och följa upp. Det gör det också svårt att formulera tydliga krav. Det finns därför ett utvecklingsbehov avseende styrning, finansiering och uppföljning för att hantera aktörsbredden på den civila sidan.

Ett nytt totalförsvarskoncept behöver ges utrymme att växa fram, vilket kräver kunskap inom många och delvis nya områden, analyskapacitet, samverkan och inte minst tid att tänka.

För vidare läsning

Maria Lignell och Lennart Uller, *Hotstruktur för totalförsvarsgemensam planering – med exempel på scenarier*, 1997, FOA-R--97-00503-240--SE.

Maria Lignell, Kerstin Castenfors, Mikael Lindén, Magnus Norell, Paula Stenström, Lennart Uller, Gunnar Wieslander och Kent Zetterberg, *Hotbeskrivningar för totalförsvarets nya uppgifter*, 1998, FOA-R--98-00901-240--SE.

Maria Lignell, Henrik Andersson, Maria Arblom, Björn Backström, Staffan Molin, Gabriella Nilsson och Örjan Sundblad, *Att värdera operativ förmåga – definitioner och förslag*, 1998, FOA-R--98-00806-170--SE.

3. Det finns inget snabbspår till ett civilt försvar

Carl Denward

Nätverket av civila aktörer som bär upp svensk krisberedskap och civilt försvar kan i enkla ordalag kallas för det svenska beredskapssystemet. Det står vid startpunkten på en lång utveckling mot ett nytt civilt försvar som utgör en av två delar av totalförsvaret. Arbetet med totalförsvaret ska axlas i samarbete med Försvarsmakten. Det finns dock tecken på att utvecklingen riskerar att präglas av svårigheter.

Avstamp i krisberedskapen

Det nya civila försvaret tar avstamp i den befintliga krisberedskapen, som i sin tur skapades i samband med den så kallade Sårbarhets- och säkerhetsutredningen från 2001. Denna utredning markerade slutet på det tidigare civila försvaret, som präglades av det kalla kriget, och introducerade en renodlad fredstida krisberedskap. Det nya civila försvaret behöver inte enbart förhålla sig till krisberedskapen och det tidigare civila försvaret under kalla kriget, utan även ett antal nygamla förutsättningar. Bland exemplen återfinns:

Aktörspluralism. Vi har nu till skillnad från förr ett annorlunda myndighetslandskap med fler och mer specialiserade myndigheter. Vidare drivs många traditionellt offentliga verksamheter idag i privat regi. Det privata ägandet är i sin tur mer komplext, då vissa företag som driver samhällsviktig verksamhet har utländska ägare och styrs utifrån principer som inte nödvändigtvis bejakar det svenska beredskapsintresset.

Teknisk utveckling och framväxten av sårbarheter. Vårt moderna samhälle förlitar sig idag i större utsträckning än tidigare på ett antal kritiska tekniska och sociotekniska system, som innebär ett beroende av både teknik och människor. Detta är under fredstid gynnsamt, men utgör samtidigt en potentiell sårbarhet om samhället skulle sättas under hård press. Det går dessutom att argumentera för att dessa sårbarheter är större för den del av befolkningen som bor i städer, till skillnad från de som bor på landsbygden och överlag är något mindre beroende av (eller inte har tillgång till) all den service som samhället sammantaget erbjuder.

Gråzon och hybridkrigföring. Med så kallad hybridkrigföring finns nya sätt att påverka Sverige. Det gör gråzons-problematiken mer aktuell än någonsin. Det handlar om angrepp som ligger på en nivå under öppen väpnad konflikt,

i ett läge där det råder varken fred eller ofred. Oavsett vilket representerar denna problematik ett antal nygamla aspekter som ett totalförsvar behöver ta höjd för när det kommer till behovet av nya förmågor vid sidan av det mer traditionella väpnade angreppet.

Vikten av att styra upp styrningen

Aktörspluralismen gör styrning, utveckling av konkreta förmågor, finansiering och uppföljning till svårbemästrade frågor. Det betyder att anpassade modeller för styrning behöver tas fram för att det civila försvaret ska få ut en effekt av beredskapssystemets olika aktörskategorier, såsom kommuner, länsstyrelser, landsting, näringsliv, och centrala myndigheter. Efterfrågan på genomtänkta styrningsinsatser från staten är stor, och förenad med viss komplexitet eftersom beredskapen är tvärsektoriell – beredskapsfrågan berör flera delar av samhället men är sällan en kärnfråga.

I styrningssammanhanget går det att argumentera för att det idag råder en otillräcklighet i de ingångsvärden som behövs för att planera det civila försvaret. Inriktningen för vilken eller vilka hotbilder inom väpnat angrepp och gråzon som aktörer ska ta höjd för är i bästa fall översiktlig och i värsta fall otydlig. Det är svårt för en enskild person inom beredskapssystemet, exempelvis en säkerhetschef på en kommun eller en handläggare vid en bevakningsansvarig myndighet, att utifrån befintlig styrning bedöma och prioritera vilka förmågor som den egna organisationen ska bidra med, och hur dessa sedan ska samspela med resten av systemet.

Försvarspolitisk inriktning 2016-2020, Myndigheten för samhällsskydd och beredskaps (MSB) och Försvarsmaktens så kallade grundsynsarbete och Försvarsberedningens rapport Motståndskraft från 2017 ger vissa indikationer på vilka förmågor som möjligtvis ska ingå i ett civilt försvar. Det saknas dock en systematisk och uttömmande ansats om vilka aktörer som förväntas göra vad och hur saker och ting konkret ska hänga ihop. Det finns heller ingen tydlig ”nedbrytning” av det civila försvarets tre huvudsakliga målsättningar; att värna civilbefolkningen, säkra samhällsfunktionaliteten och stödja Försvarsmakten. Dessa översiktligt formulerade målsättningar skulle kunna brytas ner i form av ett antal önskade förmågor som i nästa led axlas av beredskapssystemets aktörer i form av konkreta verksamheter. Denna nedbrytning gjordes, till en viss grad, inom det tidigare civila försvaret.

Att undvika krisberedskapens analysfällor och suboptimala ansvarsstrukturer

Några svårigheter återfinns i arvet från 2000-talets krisberedskap. För det första präglas krisberedskapen i viss utsträckning av otydliga ansvarsstrukturer och roller. Det är ett fenomen som manifesteras i de så kallade samverkansområdena och deras relation till det så kallade sektorsansvaret. Samverkansområdena representerar tvärsektoriella samverkansfora för myndigheter, exempelvis på områdena farliga ämnen, transporter eller teknisk infrastruktur. Fokus på samverkan inom samverkansområdena har blivit ett självändamål snarare än att fokusera på planering och samordning som tar sikte på konkreta förmågor.

Till detta börjar nu insikten infinna sig om att krisberedskapens sektorsansvar, det vill säga den ansvarsstruktur som förväntas garantera de centrala myndigheternas deltagande i beredskapen, i många avseenden är alltför vag för att ge någon verklig effekt. Ett sektorsansvar behöver sannolikt förtydligas för att samverkansområdena ska vara meningsfulla. Viss ljusning finns inom sektorer som energi och transporter, men vägen till ett fungerande sektorsansvar är lång. I sammanhanget kan tilläggas att sektorsansvaret är ett medel, snarare än ett mål – varför beredskapsmålsättningar till att börja med behöver formuleras sektorsvis. Vidare kommer sektorsansvaret se annorlunda ut beroende på vilken sektor som avses, då varje enskilt område kännetecknas av sina egna särskilda aktörer, verksamheter och förutsättningar.

För det andra anlägger svensk krisberedskap ett oproportionerligt stort fokus på riskanalysarbete, vilket innefattar analys av i många fall redan klarlagda risker och sårbarheter, medan analys av lösningar och åtgärder nedprioriteras. En del aktörer har helt eller delvis fastnat i denna analysfälla, varför det i framtiden blir viktigt att från statligt håll efterfråga smarta lösningar och åtgärder snarare än uppdaterade risk- och sårbarhetsunderlag.

Regeringen anger att det civila försvaret ska baseras på krisberedskapen, vilket är en god ansats för att hushålla med samhällets resurser. Samtidigt är det viktigt att utvecklingen av ett civilt försvar undviker att reproducera krisberedskapens tillkortakommanden. Ett framväxande civilt försvar kan dessutom hjälpa krisberedskapen att bli bättre.

Några frågor att beakta i det civila försvarets framväxt

Svårigheterna ovan medför en risk för att ett nytt civilt försvar växer fram på ett organiskt, kaotiskt och godtyckligt sätt. En sådan utveckling kan medföra att aktörer planerar på varsitt håll,

vilket ger dåliga utsikter för systemet som helhet att arbeta mot ett gemensamt mål. Det försvårar också möjligheterna för aktörerna att verka tillsammans på ett koordinerat sätt, såsom att skapa så kallad interoperabilitet mellan förmågor. En utveckling av detta slag medför också en risk för att resurser förslösas eller läggs på fel saker och att utvecklingsinsatser genomförs i fel ordning, vilket kan innebära onödiga påfrestningar på beredskapspersonalens motivation och drivkraft.

Med dagslägets vaga styrning är det för aktörer, såsom statliga myndigheter och kommuner, svårt att räkna ut vilka roller deras kärnverksamheter ska spela i beredskapen – under vilka förhållanden ska de kunna verka, tillsammans med vilka andra, och vad är viktigast? Därför finns en tendens att aktörerna fokuserar på att utveckla andra förmågor, som visserligen behövs i beredskapen, men som inte är deras kärnverksamhet, vilken faktiskt är den som kommer behövas i kris och krig. Ett exempel på detta är ett överdrivet fokus på ”stödförmågor”, till exempel övningar, ledning och säkerhetsskydd, istället för vad som skulle kunna benämnas som ”kärnförmågor” som ligger närmare aktörernas respektive verksamhetsidé (till exempel livsmedelsförsörjning eller sjukvård). Med undantag för säkerhetsskydd, som behövs för att aktörer ens ska kunna börja planera, kan en väg framåt vara att i större utsträckning än nu anlägga ett nedifrån och upp-perspektiv som fokuserar på att arbeta med aktörernas kärnförmågor – vad är det egentligen som respektive aktör ska bidra med till det civila försvaret? Med grund i fastställandet av kärnförmågorna och dess tillväxt kan stödförmågor utvecklas – exempelvis i form av en övnings- och ledningsstruktur.

Förslagen nedan utgör en grund för en fortsatt diskussion om vad som leder till framväxten av ett ändamålsenligt civilt försvar.

Gör saker i rätt ordning. MSB har i dagsläget ett uppdrag att ta fram så kallade dimensionerande utgångspunkter för aktörernas planering. Dessa bör i sin tur kunna ligga till grund för formuleringen av målsättningar för förmågor avseende både väpnat angrepp och gråzonsproblematik. Detta målformuleringsarbete bör genomföras i samråd med beredskapssystemets aktörer, inte minst de så kallade sektorsansvariga myndigheterna. Därefter är det lämpligt att bestämma vilka aktörer som ska bidra med vilken förmåga och hur dessa förmågor ska omsättas i konkreta verksamheter. Detta behöver följas upp med exempelvis styrning, finansiering, eventuella förändringar i lagstiftning samt övrigt stöd.

För samman hotbildsexperter och verksamhetsexperter. FOI:s föregångare Försvarets forskningsanstalt (FOA) konstaterade redan på 1990-talet att de personer som arbetar med att skapa

förmåga i verksamheter och de personer som arbetar med att förstå hotet, vanligtvis på någon myndighet, behöver mötas för att underlätta förmågeskapande. Skälet är att kunskap om både hotbilder och verksamheter sällan återfinns i en och samma person.

Förmågebalans. Verka för en genomtänkt framväxt av ett civilt försvar som syftar till att skapa en balans mellan olika förmågor, en förmågebalans, inom det civila försvaret, men också mellan det civila försvaret och det militära försvaret. Ett starkt civilt försvar behöver resurser för att bygga en motståndskraftig samhällsviktig verksamhet, i syfte att förneka en motståndare möjligheten att exploatera samhällssårbarheter i civila verksamheter genom insatser i gråzonen. En balans inom det civila försvaret förutsätter en duglig beredskap inom samtliga områden som medverkar till samhällets grundläggande funktionalitet. Avseende balans inom totalförsvaret är en stark militär tröskelförmåga högst åtråvärd, samtidigt som denna behöver vägas mot en ”civil tröskelförmåga”, för att inte ge en motståndare alternativet att istället agera mot sårbarheter i civilt driven samhällsviktig verksamhet.

Låt utvecklingen ta tid. Ett civilt försvar värt namnet är ett omfattande samhällsprojekt som kommer att ta tid att genomföra. Upprätta en långsiktig utvecklingsplan och tilldela resurser först när det finns en bedömning om vad som ska åstadkommas och hur saker och ting bör hänga ihop.

Glöm inte krisberedskapen. Det bör övervägas hur de förmågor som tas fram i samband med civilt försvar kan gagna samhällets möjligheter att hantera fredstida kriser. Detta kan påverka hur vissa förmågor och verksamheter utformas för det civila försvaret, i syfte att göra dessa kompatibla med krisberedskapen. Vidare bör lärdomar dras utifrån vårt snart tjugoåriga krisberedskapssystem rörande vad som har fungerat bra respektive dåligt. Till sist är det viktigt att prata om den ibland förekommande missuppfattningen att vi måste välja mellan krisberedskap eller civilt försvar: den fredstida krisberedskapen tjänar på satsningar inom det civila försvaret. Draghjälp kommer sannolikt att erhållas på en rad områden där krisberedskapen underpresterar.

Studera gränsytorna mellan sektorsansvar och geografiskt områdesansvar. Svensk krisberedskap lider av en otydlighet i ansvarsfördelning och sammankoppling mellan geografiskt områdesansvariga aktörer (exempelvis kommuner, länsstyrelser) och sektorsansvariga myndigheter (exempelvis med ansvar för el, livsmedel eller finansiella system). I detta sammanhang fyllde civilbefälhavarna, som tidigare fanns

inom det gamla civila försvaret, en roll. De fungerade som kontaktyta mellan det civila och det militära, men också mellan de geografiska områdena såsom kommuner och länsstyrelser och de centrala funktions- eller sektorsmyndigheterna. Är en motsvarande kontaktyta önskvärd, och bör den återupprättas?

Till syvende och sist beror mycket på hur den rikspolitiska nivån, Regeringskansliet och MSB väljer att ta ett samlat grepp om området. Var vill vi vara om fem år, vilket civilt försvar ser vi framför oss? När den målbilden finns, är det hög tid att sätta samman ett strategiskt styrpaket för att de som är längst ut i systemet, som ska skapa den riktiga förmågan, ska kunna börja arbeta på allvar. I detta arbete är de aviserade och påbörjade utredningarna på området instrumentella, inte minst utredningen om Ansvar, ledning och samordning inom civilt försvar.

För vidare läsning

Per Larsson, Christoffer Wedebrand och Carl Denward, *Personal för ett nytt civilt försvar – förutsättningar, problem och möjligheter*, 2018, FOI-R--4675--SE.

Carl Denward, Per Larsson och Ann-Sofie Stenerus, *Sektorsansvar – ansvarssystem eller semantik?*, 2017, FOI-R--4542--SE.

Bengt Johansson, Kristoffer Darin Mattsson, Eva Mittermaier och Niklas H. Rossbach, *Det civila försvarets utgångspunkt i krisberedskapen. En övergripande analys av förutsättningar och utmaningar*, 2017, FOI-R--4431--SE.

4. Att skapa engagemang och förmåga för totalförsvaret

Bengt Johansson

För att bygga ett motståndskraftigt totalförsvar krävs både vilja och förmåga. Det är viktigt både med hotbilder som uppfattas som relevanta och en tillit till samhällets institutioner för att kunna skapa en tillräcklig drivkraft att agera. Den information och de uppmaningar som kommer från det offentliga behöver uppfattas som rimliga. Att betona betydelsen av en allmän robusthet i samhället och nyttan med detta i såväl fred, gråzon som krig kan öka motivationen hos individer, myndigheter och företag att bidra till totalförsvarsarbetet.

Totalförsvaret kräver nya prioriteringar

Att stärka totalförsvaret kräver nya prioriteringar. Ökade insatser inom området kan innebära att annat måste avstås. Företag förväntas delta i planeringsarbetet, vilket normalt inte ligger i deras kärnverksamhet. Medborgarna förväntas klara sig under en relativt lång tid under svåra förhållanden med endast begränsat samhällsstöd. Slutligen står en prioritering av robusta system inte sällan i konflikt med de effektivitetssträvanden som karaktäriserar det moderna samhället.

För att skapa ett engagemang hos organisationer och enskilda för att de ska avsätta tid och resurser för förberedelser, behöver de hotbilder som används uppfattas som tillräckligt relevanta. Att hotbilderna är viktiga och användbara är emellertid inte ett tillräckligt villkor för att skapa en vilja att agera. Det kräver också en tilltro till att försvar är meningsfullt och att det som ska skyddas är värt att försvara.

Som exempelvis sociologen Ulrich Beck påpekar är hotbilder något som skapas. Hotbilderna kan komma att ifrågasättas både i fråga om deras faktiska innehåll, hur de ska tolkas, vilken relevans de har och vems intressen de avspeglar. Den hotbild som Försvarsberedningen beskriver kan ur det perspektivet ses som en gemensamt skapad bild, förankrad i de demokratiska institutionerna. Det hindrar inte att bilden på olika sätt kan diskuteras och problematiseras ute i samhället. En sådan problematisering är en del av ett demokratiskt samhälle, men diskussioner och ifrågasättanden kan försvåra styrningen av totalförsvaret.

Att varsebli hotbilder

Efter det kalla krigets slut uppkom en förväntan om fredlig samvaro i närområdet. Bilden av ett krig i Sverige eller i närområdet uppfattades inte längre som realistisk. Samhället vande sig vid lugna och fredliga förhållanden och samhällsviktiga system dimensionerades därefter.

En viktig utmaning för planeringen av den civila delen av totalförsvaret (det civila försvaret) är därmed att beskriva vad krig, krigsliknande förhållanden och gråzonshot innebär och att sprida dessa berättelser, så kallade narrativ, till olika samhällsaktörer och allmänheten. Exempel på sådana narrativ är de fem typfall som FOI har tagit fram på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB). Typfallen är scenarier som är tänkta att användas av samhällets aktörer, till exempel statliga myndigheter, vid planeringen av det civila försvaret. Ett annat exempel är Försvarsberedningens beskrivning av det säkerhetspolitiska läget och dess betydelse. Medvetenheten om riskerna för psykologisk krigföring, störningar av valprocesser och en uppfattat ökad risk för väpnade konflikter i närområdet har också ökat genom myndigheters och medias rapportering.

Att tolka hotbilder

De hotbilder som presenteras kan tolkas på olika sätt. De kan ifrågasättas avseende relevans eller vägas mot andra hot. Som nämnts ovan är hot något som konstrueras, och det är i ett demokratiskt samhälle legitimt att hävda en annan tolkning än de som myndigheter och andra aktörer sprider.

En särskild komplikation är att det finns en risk att även fientliga aktörer kommer att ifrågasätta hotbilders riktighet och relevans. Kritik mot hotbilden kan föras fram direkt eller indirekt via organisationer, enskilda eller fiktiva konton på sociala medier. I sammanhanget blir det därför viktigt för det offentliga att det finns en tillit till samhället och dess institutioner för att med trovärdighet kunna hävda legitimiteten i just den hotbild myndigheterna själva vill presentera.

Att agera efter hotbilder - att vilja och att kunna

Även om det finns en medvetenhet om en hotbild och den tolkas som relevant, kan den leda till olika typer av beteenden. För att agera efter en hotbild, på det sätt staten och myndigheterna önskar, krävs en faktisk vilja att agera, ofta kallad försvarsvilja, men också kompetens och resurser att verkligen kunna agera.

Försvarsvilja är inte ett entydigt begrepp och kan förstås på många olika sätt. I totalförsvarets framtida planering kan det handla om att det anses rimligt att prioritera försvaret istället för att lägga

sin kraft på att uppnå andra politiska mål som inte rör försvaret. Under en pågående konflikt kan det handla om viljan att inte ge upp, att personligen kämpa mot en pågående aggression, med mera. Genom att använda begreppet motståndsvilja vid en konflikt är det möjligt att skilja på försvarsvilja före och under en konflikt, se figur.

	Före	**Under**
Aktivitet	Planering	Hantering
Verklighet att förhålla sig till	Hotbild Vad kan hända?	Lägesbild Vad händer?
Försvars- och motståndsvilja	Försvarsvilja • Acceptans för prioritering av beredskapsåtgärder • Acceptans för plikt- och annan beredskapslagstiftning • Deltagande i frivilligorganisation • Byggande av egenberedskap	Motståndsvilja • Stöd för att inte ge upp • Vilja att personligen kämpa mot pågående agression • Vilja att delta frivilligt i räddnings- och reparationsarbete

Figur 1. Begreppsbild för att förstå likheter och skillnader mellan totalförsvaret före och under ett angrepp. Bilden är en principskiss och det finns inte alltid en skarp gräns mellan ”före” och ”under”, vilken är en av utmaningarna med angrepp i gråzonen.

För individen kan försvarsvilja handla om acceptans för att göra egna uppoffringar i form av tid, pengar och bekvämlighet för att bygga en försvarsberedskap. Det kan också handla om att medborgare accepterar inskränkningar i den egna friheten i form av till exempel plikttjänstgöring. För samhället som helhet kan det handla om huruvida mer resurser ska avsättas till totalförsvaret, eventuellt på bekostnad av att exempelvis lösa andra samhällsproblem, utveckla annan samhällsinfrastruktur eller att sänka skatter.

Olika aktörers prioriteringar påverkar viljan att agera

Offentliga aktörer, såsom statliga myndigheter, landsting och kommuner arbetar mot ett stort antal samhällsmål inom sina respektive politikområden, där många frågor är lika viktiga. De regelverk som styr verksamheten är i många fall vaga och målen tolkningsbara. Detta innebär att de olika aktörerna i stor grad själva har att väga hur resurserna ska prioriteras.

Det betyder att prioriteringar mellan samhällsmål kan komma att skilja sig åt mellan olika myndigheter, kommuner och regioner

beroende på vilka områden och vilka hot som anses vara de viktigaste. Det är begripligt eftersom förutsättningarna att agera skiljer sig kraftigt åt. Även synen på hotbildens relevans kan skilja sig åt beroende på enskildas eller grupper av tjänstemäns och andra aktörers förståelse av omvärlden.

Ett sätt att hantera detta från regeringens och riksdagens sida vore att tydligare prioritera mellan olika samhällsmål. Detta har hittills inte skett i någon större utsträckning och är kanske inte heller möjligt. Det gäller i synnerhet när det handlar om övergripande mål som ofta inte är tillräckligt väldefinierade för att det ska gå att tydligt fastställa om och när de har uppnåtts. En hård prioritering av ett sådant mål skulle i teorin kunna leda till att det inte genomförs några insatser för att uppnå andra mål, vilket så småningom med största säkerhet kommer att uppfattas som orimligt. Därför kommer det vara nödvändigt med kompromisser mellan olika mål.

Staten kan också styra genom riktat finansiellt stöd, något som varit vanligt inom krisberedskapen, men dessa stöd är i allmänhet otillräckliga för att täcka alla behov. Så frågan om prioritering mellan olika samhällsmål kommer sannolikt till stor del att ligga på enskilda aktörer även i framtiden. Hur viktigt totalförsvaret bedöms vara i jämförelse med annan verksamhet i samhället och vad inom totalförsvaret som bör prioriteras kommer med stor sannolikhet skilja sig mellan dessa olika aktörer.

Näringslivet är en viktig aktör i det civila försvaret men företagens huvuduppgift är att producera varor och tjänster samt generera vinster till ägarna. Att bidra till det allmänna samhällsintresset är inte en huvudprioritering för företagen. Företagen kan trots det ha ett egenintresse att bidra till det civila försvaret exempelvis eftersom det kan stärka varumärket och därmed indirekt bidra positivt till det ekonomiska resultatet. Företagen består dessutom av individer som kan driva på för att verksamheten ska ta större hänsyn till totalförsvarets intressen.

Även om det finns en vilja i samhället att agera behövs resurser och kompetens för detta. Ekonomiska resurser och personal kommer att behöva avsättas. Anställda som behövs inom totalförsvaret kommer att behöva utbildning och det kommer att ta tid. Prioriteringar kommer att behöva göras och dessa kommer inte att kunna göras enbart på central nivå.

Är en gemensam förståelse av hotbild möjlig?

Det behövs hotbilder att förhålla sig till för att motivera aktörer att avsätta tid och resurser för planering och åtgärder. En samlad lägesbild lyfts av många källor fram som central för en effektiv hantering av en pågående händelse. Det finns även stora fördelar

med en ökad gemensam samsyn i sektorsövergripande planering mellan olika sektorer, såsom energi och transport. Frågan är dock vilken grad av samsyn som kan nås mellan den breda uppsättningen aktörer med deras olika intressen och prioriteringar. Att ha tillgång till samma hotbilder kan vara värdefullt men det innebär inte nödvändigtvis att aktörerna har samma förståelse av hotbilden.

Även om det går att skapa narrativ i form av till exempel FOI:s typfall behöver dessa tolkas från aktörernas olika sammanhang. Det är till exempel inte självklart samma scenario som uppfattas vara bäst för planering i alla sektorer; i vissa fall kan scenariot om krig ses som mest relevant, i andra gråzonen.

Som nämnts ovan har de olika sektorerna fullt upp med att bidra till olika typer av samhällsmål och det är i förhållande till detta som deras prioriteringar av totalförsvaret måste förstås. Sannolikt blir det svårt att verkligen enas om en gemensam hotbild i hela samhället. Det behöver dock inte innebära att arbetet med att bygga ett civilt försvar behöver stå stilla.

Ett robust samhälle för en bred hotskala

Ett sätt att inte bli så beroende av en allmän acceptans av en viss hotbild, och även motivera arbete också när acceptansen är låg, är att i högre grad fokusera på att bygga ett robust samhälle som kan vara stryktåligt utefter en bred hotskala. Det kan handla om en livsmedelsförsörjning som är motståndskraftig mot störningar oavsett vad orsaken till störningen är. Det kan också handla om en förmåga att hantera desinformation eller cyberangrepp oavsett om den som ligger bakom är en statlig aktör eller en grupp av aktivister. Allra viktigast blir kanske att arbeta för att bibehålla förtroendet för de demokratiska institutionerna. Dessa utgör grunden för att alla de åtgärder som staten förväntar sig av individer, organisationer, företag och myndigheter ska uppfattas som legitima.

Ett sådant perspektiv i planeringen för civilt försvar kan sannolikt underlätta för olika aktörer att enas om värdet av aktiviteter som gör samhället mer robust utan att därför behöva omfamna samma specifika hotbild. På så sätt torde det också finnas större möjligheter att bygga koalitioner av intressenter för att genomföra åtgärder. Ett konkret fokus på robusthet kan också vara fördelaktigt utifrån gråzonshotets otydlighet där det kan vara oklart om händelser är resultat av fientliga attacker och, om så är fallet, vilka intentioner dessa antagonister kan ha.

Detta innebär inte att alla aspekter av det civila försvaret kan hanteras på detta sätt. Det finns flera delar av det civila försvaret

som inte är direkt kopplade till byggande av en generell robusthet. Det gäller till exempel samhällets stöd till Försvarsmakten.

Grundförutsättningar för framgång i totalförsvaret

Både relevanta hotbilder och tydlig statlig styrning behövs för att bygga ett civilt försvar. Det är dock viktigt att vara medveten om att mål och hotbilder är värdeladdade och att motivationen samt viljan att arbeta utifrån dem inte är given. Att förändra perspektiven hos medborgare, näringsliv, myndigheter och andra aktörer, så att totalförsvaret prioriteras i högre grad i deras dagliga verksamhet är inte gjort i en handvändning. Om det går att finna synergier mellan totalförsvarets behov och olika aktörers andra intressen kan det stärka viljan att ta hänsyn till totalförsvaret i verksamheten. För att dessa försök ska bära frukt behövs ett förtroende för samhällets institutioner. Därför måste den information och de uppmaningar som presenteras uppfattas som rimliga av befolkningen.

För vidare läsning

Daniel K. Jonsson, Jenny Ingemarsdotter, Bengt Johansson, Niklas H. Rossbach, Camilla Eriksson, Christoffer Wedebrand. *Civilt försvar i gråzon*, 2019, FOI-R--4769--SE.

Bengt Johansson, Kristoffer Darin Mattsson, Eva Mittermaier och Niklas H. Rossbach, *Det civila försvarets utgångspunkt i krisberedskapen. En övergripande analys av förutsättningar och utmaningar*, 2017, FOI-R--4431--SE.

5. Totalförsvar, informationsdelning och nya gränsytor

Ann Ödlund och Matilda Olsson

Allvarliga brister i informationsdelning mellan totalförsvarets aktörer kan leda till att det istället för en sammanhängande planering och samordning skapas "öar" inom olika delar av totalförsvaret och Sveriges geografiska områden. Om informationsdelningen inte fungerarar blir det svårt att ur ett nationellt perspektiv svara på frågor som; Vad har vi? Vad kan vi? och Hur prioriterar vi? - oavsett om det gäller planering eller hantering i skarpt läge. En fungerande informationsdelning inom och mellan totalförsvarets aktörer är en förutsättning för totalförsvarsplanering och civil-militär samordning.

Informationsdelning är kittet i totalförsvaret

För att kunna planera och fatta underbyggda beslut är beslutsfattare på olika nivåer beroende av både specifik information och samlade lägesbilder som ger överblick över till exempel ett visst område, en situation eller ett händelseförlopp. Lägesbilder används inom krisberedskapen och det militära försvaret och bygger på informationsinhämtning, analys av information, sammanställningar och delgivning. Lägesbilder tas i grunden fram specifikt av myndigheter och andra aktörer för intern överblick. Detta för att delge andra myndigheter efterfrågad information eller i syfte att utgöra underlag för samlade lägesbilder på högre nivåer. Lägesbilder är kontextberoende. Sjölägesbild är ett sådant exempel.

Framför allt myndigheter med uppgifter inom beredskapen har en skyldighet att dela information och lägesbilder med varandra. Skyldigheterna leder i sin tur till att det bildas ett nätverk där information ska kunna delas mellan aktörer och administrativa eller hierarkiska nivåer i fred så väl som i krig. När det gäller information till regeringen i fredstid ska varje myndighet efter förfrågan från Regeringskansliet eller Myndigheten för samhällsskydd och beredskap (MSB) lämna den information som behövs för samlade lägesbilder. Under höjd beredskap ska de bevakningsansvariga myndigheterna hålla regeringen informerad om det aktuella tillståndet och händelseutvecklingen inom respektive ansvarsområde, samt om vidtagna och planerade åtgärder. Försvarsmakten ska även få de underlag som myndigheten behöver från de bevakningsansvariga myndigheterna, till exempel Socialstyrelsen och Energimyndigheten, samt från övriga försvarsmyndigheter,

till exempel Försvarets materielverk och Försvarets radioanstalt, för att kunna fullgöra sin informationsskyldighet till regeringen vid höjd beredskap.

Informationsdelning och lägesbildshantering kan vara problematiskt redan i fredstida sammanhang, vilket har konstaterats bland annat under stormarna Gudrun 2005 och Per 2007, skogsbranden i Västmanland 2014, terrordådet på Drottninggatan 7 april 2017 och skogsbränderna sommaren 2018. Problemen har varit tekniska eller berott på bristande rutiner och oklarheter i hur information ska delas inom organisationer och mellan aktörer.

Perspektiven gråzon och höjd beredskap ställer ytterligare krav på aktörerna. När det gäller gråzon finns en betydande osäkerhet om huruvida störningar eller andra händelser orsakas av främmande makt, terrorism, sabotage eller olyckor. Denna osäkerhet medför att de som är ansvariga för informationsdelning samt för att sammanställa och tolka lägesbilder ställs inför situationer som är svåra att bedöma, där felbedömningar riskerar att ge en eventuell motståndare en fördel. Även vid höjd beredskap där det finns en känd motståndare i form av främmande makt kommer osäkerhet att finnas kvar för beslutsfattare. Här tillkommer dessutom krig eller krigsfara som bedömningsgrund vilket gör att fokus på åtgärder och prioriteringar skiftar från fredstida krisberedskap till ett aktiverat totalförsvar. Både informationsdelning i gråzon och höjd beredskap, liksom vid en övergång från fred till krig behöver planeras och övas.

Vad är normalt, vad är annorlunda - och för vem?

När det gäller den framtida konfliktmiljön framförs i Försvarsmaktens perspektivstudie 2016-2018 bedömningen att denna miljö år 2035 kommer att omfatta ett brett spektrum av hot. Dessa fientliga aktiviteter kommer att ha betydande element av icke-linjär krigföring, där gränsen mellan fred och krig suddas ut och där cyber- och påverkansoperationer kan ingå. I den gråzonen behöver angrepp upptäckas tidigt, vilket i sin tur kräver överblick över incidenter såväl i ett civilt som i ett militärt sammanhang. Frågan är dels vilka aktörer som ska samla in sådan information och sammanställa den, dels hur den ska delges. I gråzonen handlar det kanske främst om möjligheten till tidig förvarning och att upptäcka dolda angrepp. Studiet av anomalier, det vill säga signifikanta förändringar i normalläget, är här grundläggande. Underrättelser och kunskap om normalbilden inom olika områden är därför central för att kunna bedöma olika händelser, skapa korrekta beslutsunderlag och ytterst vidta lämpliga åtgärder. En ytterligare fråga blir vem som idag har kompetens och resurser att bedöma och förmedla vad som är normalt inom olika områden.

Mycket har förändrats på senare år när det kommer till vilka som äger eller driver samhällsviktig verksamhet. Kompetens har flyttats från det offentliga till det privata och det finns många nya aktörer. Ett tydligt exempel där en sådan förflyttning har skett är inom området telekommunikationer. Denna samhällsutveckling innebär att det behövs en grundläggande analys avseende vilka områden och aktörer som är relevanta för totalförsvaret i dagens kontext. Det finns med andra ord ett behov av att inventera vilka aktörer som har kunskap och därmed möjlighet att förmedla information om vad som är normalt och vad som är avvikande ur ett totalförsvarsperspektiv.

Utöver gråzonens karakteristika finns två försvårande faktorer. En är privata ägandeförhållanden inom samhällsviktig verksamhet, vilket kan medföra att det till exempel finns affärsmässiga hinder för att dela viss information. En annan har att göra med behovet av att vid distribution av information upprätthålla sekretess. Informationsdelning och samordning sker i gränsytorna inom och mellan myndigheter och aktörer. Forskning har visat att det finns begränsningar i nationella förutsättningar för delning av sekretessbelagd information, till exempel mellan underrättelse- och säkerhetstjänsterna och den breda kretsen av krisberedskapsmyndigheter. Här finns brister i tekniska system för informationsöverföring, kulturskillnader, begränsade resurser, avgränsade mandat samt en tydlig gräns mellan underrättelsesystemet och övriga myndigheter. Vissa av problemen utgör exempel på barriärer och bristande tillit mellan myndigheter eller i detta fall sektorer.

Att bygga nytt och förändra gammalt

En adekvat funktion för informationsdelning och lägesbildshantering är viktig för beslutsfattande i fred, gråzon och krig och bör därför säkerställas i utformningen av totalförsvaret. Gränsytan civil-militärt är central i allt från exempelvis planering, stöd till mobilisering, förnödenhetsförsörjning av livsmedel, drivmedel och el till utveckling av sjukvård och transporter. Hur civil-militär samordning ska inriktas strategiskt, verkställas mellan centrala och regionala nivåer samt realiseras mellan Försvarsmakten och olika civila aktörer behöver utredas. Det behövs en organisering av totalförsvaret som kan ge förutsättningar för detta.

Sett till behoven av fungerande strukturer för totalförsvaret är det positivt att regeringen i syfte att skapa tydligare ansvars- och ledningsförhållanden 2018 har gett direktiv till en utredning om ansvar, ledning och samordning inom civilt försvar. Denna ska analysera och föreslå en struktur för civilt försvar på central, regional och lokal nivå. Enligt direktivet ska förslagen utgå från Försvarsberedningens rapport Motståndskraft från 2017,

som bland annat föreslår en indelning av statliga myndigheter i samhällssektorer med en sektorsansvarig myndighet. Denna och andra kommande utredningar leder sannolikt till nya ansvarsförhållanden och gränssnitt mellan aktörer, både civil-civilt och civil-militärt. Att bygga nytt innebär en chans att utforma strukturerna och ansvarsfördelningen efter de behov som finns inom totalförsvaret. Sammantaget ges nu totalförsvaret möjligheter att stärkas och förbättras, vilket inte minst omfattar en grundläggande förmåga till informationsdelning.

Fungerande informationsdelning är i allas intresse

Lägesbilder handlar om sammanställning av information utifrån ett visst syfte i en viss kontext och utgör planerings- eller beslutsunderlag både för långsiktiga avvägningar och vid operativa beslut. Om aktörerna saknar organisatoriska strukturer, teknik, utbildning samt förståelse för syftet och sin egen roll, riskerar informationsdelning att nedprioriteras. Detta kan i sin tur resultera i att viktig information inte tas med i planering eller beslutsunderlag. Om skyldighet att dela information för att tillgodose behovet är den ena sidan av myntet kan rättighet att ta del av information representera den andra sidan. Den ena sidan av myntet kan inte fungera utan den andra. Rätten till information diskuteras mer sällan än skyldigheten att dela den. Förmåga att hantera sekretess, skillnader i kultur och bristande förståelse för olika behov kan utgöra barriärer.

Det torde ligga i allas intresse att skapa bästa möjliga förutsättningar för beslutsfattare både i planering och i skarpt läge. Att ta ansvar för sin del i en fungerande kedja av informationsdelning kan ytterst vara avgörande för vilka beslut som fattas. I skarpt läge där tiden är knapp och pressen stor behöver beslutsfattare snabbt få tillgång till relevant information. För att informationsdelning ska fungera effektivt i kris och krig måste fungerande strukturer för både fredstida kriser och för höjd beredskap vara på plats. Utformningen av strukturerna behöver föregås av analyser och planering kring likheter och skillnader utifrån fredstida respektive krigstida behov. Ytterst är detta en balansgång mellan användningen av kända fredstida rutiner och strukturer och en övergång till en organisation anpassad till totalförsvarets krav.

Under de senaste åren har totalförsvaret gått från att vara en i huvudsak illa sedd gäst, både inom krisberedskapen och på den försvarspolitiska arenan, till att bli en alltmer central verksamhet vars närvaro inte kan negligeras. Det finns idag både intresse och engagemang för totalförsvarsfrågor; politiskt lika väl som bland myndigheter och andra aktörer. Detta kan innebära förnyelse och förbättring av totalförsvaret, där möjligheten till

informationsdelning mellan myndigheter och privata aktörer torde ligga högt upp på agendan.

För vidare läsning

Malin Severin, T*idig förvarning och icke-militära angreppssätt – Utmaningar för underrättelsetjänsten*, 2018, FOI-R--4577--SE.

Magnus Normark, Per Thunholm och Runar Viksten, *Kartläggning av förutsättningar för delgivning av hemlig information*, 2017, FOI-R--4418--SE.

6. Delad sensordata förbättrar hantering av kriser, terrorism och höjd beredskap

Maria Andersson, David Lindgren, Peter Nilsson, Åsa Berglund och Ola Svenonius[1]

Förutom följder av den säkerhetspolitiska utvecklingen riskerar Sverige att drabbas av terroristattacker och ökad grov brottslighet. Totalförsvarsförmågan och krisberedskapen behöver stärkas. Samverkan mellan berörda myndigheter, samt räddningstjänsten och Försvarsmakten, gällande tekniska sensorer och sensordata kan bidra till en stärkt totalförsvarsförmåga och krisberedskap. Men för att detta ska ske krävs en förändring i myndigheternas arbetssätt.

Totalförsvaret kan stärkas genom samverkan

Terrorattacken på Drottninggatan våren 2017 och skogsbränderna sommaren 2018 är exempel på allvarliga händelser där samverkan mellan myndigheter får stor betydelse för krishanteringsförmågan. Samverkan ger till exempel möjlighet att skapa en samlad lägesbild, det vill säga en sammanställning av kritisk information från flera olika myndigheter. En samlad lägesbild skapar ökade möjligheter för att förstå omfattningen av en kris.

Sensorer, och de data sensorerna ger, är viktiga bidrag till den samlade lägesbilden. Kameran är en vanlig sensor hos myndigheterna. Exempel på sensordata är kamerabilder och så kallade detektioner av objekt, såsom fordon eller specifikt ett fordons registreringsskylt. Kameror finns bland annat på torg och tunnelbanestationer samt längs med vägar och järnvägar. Vid en allvarlig kris kan räddningstjänsten, Trafikverket och Polisen samverka avseende kamerabilder för att snabbare få information om omfattningen av det akuta krisläget. Utan en på förhand bestämd procedur för samverkan finns en risk att det tar mycket lång tid att få informationen, vilket kan leda till att krisen blir allvarligare.

Att utveckla en på förhand bestämd procedur för samverkan mellan myndigheter avseende sensorer och sensordata är ett viktigt steg mot att höja totalförsvarsförmågan. Sensorsamverkan kan vara avgörande under pågående kris eller samhällsstörning där en aktuell, korrekt och kontinuerligt uppdaterad samlad lägesbild är nödvändig för att avvärja en pågående kris.

[1] Artikeln baseras på forskning i samarbete med Polisen.

I dag sker ingen formaliserad samverkan avseende sensorer eller sensordata; snarare sker detta ad hoc när akuta situationer uppkommer. När sådan samverkan sker är det ofta baserat på personliga kontakter mellan enskilda tjänstemän inom olika myndigheter. Risken är stor att viktiga personliga kontakter saknas och att systemet blir känsligt för personalförändringar. Konsekvensen av detta ad hoc-system är ett ineffektivt nyttjande av samhällets tillgångar, och bristande tid och resurser för att hantera de eventuella juridiska eller organisatoriska spörsmål som kan uppstå vid sådan samverkan. För en effektivare totalförsvarsförmåga krävs etablerade rutiner för utbyte av sensordata samt en beredskap att både dela och ta emot andra myndigheters sensorresurser. Samverkan och samarbete måste fungera i vardagen för att fungera vid en kris.

Bevakningsansvariga myndigheter är myndigheter som har vissa särskilda uppgifter vid kris och höjd beredskap. Dessa har ett ansvar att planera för sitt eget kris- och säkerhetsarbete. Om en myndighet saknar egna sensorer, eller endast har ett fåtal, så blir myndigheten särskilt beroende av samverkan för att tillfredsställa behovet av sensordata vid en akut kris.

För att sensorsamverkan ska fungera är det av stor vikt att ge bevakningsansvariga myndigheter, samt räddningstjänsten och Försvarsmakten, bättre kunskap om varandras sensorer, hur de används och vilken typ av information de tillhandahåller. Det är även av stor vikt att ge bättre kunskap om de möjligheter som finns att med sensordata få en förbättrad samlad lägesbild. Sådana möjligheter kan exempelvis vara olika typer av databearbetningstjänster som kan underlätta vid analys av stora datamängder, eller ge en tydligare bild av ett område. Här kan obemannade flygande farkoster användas, vilka kallas *Unmanned Aerial Vehicle* (UAV) eller *Unmanned Aerial System* (UAS).

Behovet av sensorsamverkan är stort bland annat när det gäller bilder från områden där en akut kris pågår. Med en kamera monterad på en obemannad flygande farkost eller en helikopter ges information om områden som annars kan vara omöjliga att nå eller riskabla att vistas i. Det finns vidare goda möjligheter att från luften få en snabb överblick vilket ofta är avgörande i en krissituation.

Vid en svår samhällskris sprids ofta effekter långt efter att krisen uppstått, och geografiskt långt utanför den plats där krisen äger rum. Terrordådet i Stockholm är ett exempel på det. Därför är även kameror på järnvägs- och tunnelbanestationer samt längs med vägar, järnväg- och tunnelbanespår efterfrågade vid samverkan. Sådana kameror ger information om hur flödet av människor och fordon påverkas under en kris.

En annan typ av samarbete som kan vara av intresse för myndigheterna är samverkan vid statliga inköp av nya sensorer. Gemensamma inköp kan gynna en standardisering, vilket i sin tur kan underlätta för sensorernas drift och i hanteringen av sensordata hos olika myndigheter. Gemensamma inköp bör dessutom kunna leda till bättre avtal genom att myndigheterna bland annat kan dra nytta av varandras kompetenser vid kravställning av sensorerna.

Juridiska utmaningar

Det svenska krisberedskapssystemet bygger till stor del på samverkan mellan myndigheter och andra aktörer på lokal, regional och central nivå och mellan olika sektorer. Det regelverk som gäller till vardags ska tillämpas även i krissituationer. Utgångspunkten i svensk förvaltning är att myndigheter har definierade uppgifter och är självständiga i förhållande till regeringen och varandra. Krav på att myndigheter ska samarbeta och samverka framgår av olika bestämmelser i lagstiftningen men det framgår inte hur de ska göra detta. Det innebär att det kan uppstå situationer när rättsregler som gäller i myndighetens ordinarie verksamhet passar sämre i samverkanssituationer vilket hindrar en effektiv samverkan.

En annan aspekt när det gäller myndigheters självständighet i förhållande till varandra är att sekretess som huvudregel gäller mellan olika myndigheter. Sekretessen, som bland annat utgör ett skydd för myndighetens egna informationstillgångar och för enskilda som förekommer i myndigheternas verksamhet, ser olika ut för olika myndigheter och förs över till andra myndigheter i olika utsträckning. Det kan också vara så att det faktum att en myndighet har tillgång till en viss typ av sensor eller sensordata är känsligt ur ett sekretessperspektiv eftersom det avslöjar myndighetens och därmed rikets förmågor. Detta innebär sammantaget att bestämmelser om sekretess har en begränsande inverkan på möjligheterna att fritt samverka mellan myndigheter.

Vidare kan dataskyddsförordningen (GDPR), som utgör ett integritetsskydd för enskilda personers personuppgifter, komplicera myndighetssamverkan. Sensorer registrerar ofta personuppgifter och dessa får enligt dataskyddsförordningen endast registreras för ett särskilt ändamål som bestäms av den myndighet som sätter upp kameran. Om myndigheten i fråga delar med sig av personuppgifterna behandlas personuppgifterna plötsligt för ett annat ändamål än det ursprungliga, vilket alltså kan vara otillåtet. Dataskyddförordningen ligger även till grund för den nya kamerabevakningslagen som medför att myndigheter, med några undantag, måste söka tillstånd för att få sätta upp sensorer.

Sammanfattningsvis blir samverkan mellan myndigheter när det gäller sensorer juridiskt komplicerad men inte omöjlig. Det är följaktligen viktigt att jurister tillåts komma in tidigt i utvecklingen av metoder och tekniker för sensorsamverkan, det vill säga redan under planeringsstadiet på myndigheterna. I det tidiga skedet kan tekniken och metoderna fortfarande anpassas till vad som gäller enligt juridiken så att samverkan kan ske på ett både framgångsrikt och rättsligt korrekt sätt. Planering för samverkan mellan myndigheterna när det gäller sensorer bör ske på förhand, det vill säga innan det operativa behovet uppstår.

Organisatoriska utmaningar

Att samverka med sensorer och sensordata är komplext eftersom det är flera perspektiv som måste beaktas, till exempel teknisk kompabilitet, lagstiftning, informationssäkerhet och inte minst metoder och verksamhetsprocesser. Alla myndigheter måste inte göra likadant, men hur man interagerar och genomför gemensamma aktiviteter bör vara likartat.

Eftersom sensorsamverkan i grunden handlar om tekniskt utbyte så är det dessutom svårt att improvisera. Teknisk samverkan kräver förberedelser. Men att förbereda sensorsamverkan är svårt eftersom det inte finns någon enskild del av staten som har det övergripande ansvaret även om alla myndigheter har till uppgift att stödja varandra.

Samverkan förutsätter att man kan kommunicera med varandra och att man har förståelse för varandras verksamheter. Detta i sin tur innebär att man behöver ha gemensamma begreppsapparater och kontinuerligt genomför gemensamma aktiviteter. Hur man beskriver sensorer och sensordata varierar mellan myndigheterna, vilket är naturligt eftersom man bedriver olika verksamheter och har olika syften med sina sensorer. Ett exempel är att det, som av Polisen och andra civila myndigheter kallas för bevakningssystem, inom Försvarsmakten benämns underrättelsesystem. Ett annat exempel är obemannade flygande farkoster, såsom UAS eller UAV under myndighetsutövning, som även kallas *Remotely Piloted Aircraft System* (RPAS) eller allmänt drönare. De olika benämningarna kan användas både mellan och inom myndigheterna. Semantiska skillnader leder lätt till förvirring och missförstånd.

En central utmaning är att veta vad man kan få stöd med och av vem. Många myndigheter är av olika skäl inte öppna med vilka sensorer de har, och inte heller sensorernas prestanda. Det är därför inte praktiskt att göra en sammanställning med information om sensorerna. Men genom att föra en kontinuerlig dialog och öva tillsammans kommer kunskapen om varandras förmågor

att gradvis byggas upp. Dessutom kommer förtroendet mellan myndigheterna att öka, vilket stärker samverkansmöjligheterna. Dock kommer det sannolikt alltid att finnas särskilda bevakningsresurser som är för känsliga för att dela.

Ett sätt att överbrygga skillnaderna mellan myndigheterna och reducera risken för missförstånd är att utforma en gemensam vägledning. En sådan bör förslagsvis inkludera ett klassificeringssystem (taxonomi) för olika typer av sensorer, tillämpliga standarder och en övergripande sensorsamverkansmetod som beskriver vilka frågeställningar som behöver adresseras och vilken hänsyn som behöver tas vid samverkan. Att diskutera principiella sensortyper är inte lika känsligt som konkreta tekniska sensorer eftersom prestanda och eventuella svagheter inte behöver avslöjas.

Tekniska utmaningar

Sensorer genererar ofta stora mängder sensordata. Att analysera sensordata manuellt, och hitta kritisk information i den stora datamängden, är komplicerat. Det är dessutom svårt för en mänsklig operatör att uppehålla en koncentration i en sådan uppgift under en längre tid. Olika databearbetningstjänster kan därför vara till hjälp för att stödja operatören genom att automatiskt urskilja viss kritisk information.

Dagens sensorer blir alltmer avancerade och kräver ofta särskilt utbildade operatörer för att dels hantera sensorn på rätt sätt, dels tolka sensordata. Det kommer antagligen att bli än mer problematiskt allteftersom nya och mer avancerade sensorer anskaffas. Sannolikt kommer det framöver inte vara meningsfullt att endast tillhandahålla sensorn. Det kommer även behövas specialutbildad personal. Sensorsamverkan innebär således att man delar på både tekniska och mänskliga resurser.

Vägen framåt

För att sensorsamverkan ska fungera krävs en förändring i myndigheternas arbetssätt. Överlag kräver samverkan mellan myndigheter även en samverkan mellan olika funktioner inom och mellan de olika myndigheterna, och på olika nivåer inom myndigheterna. Detta gäller såväl utbyte av information som när nya metoder och verktyg för samverkan utvecklas. Förutom att juridiken måste involveras tidigt i planeringen av hur delning ska ske rent tekniskt finns det också en nära koppling till säkerhetsfunktioner hos myndigheterna.

Den snabba tekniska utvecklingen kommer på sikt att ge myndigheterna nya förmågor men också nya utmaningar, gällande tekniska system och juridiska spörsmål, vilket leder till frågor som: hur ska myndigheterna hantera mängden sensordata? Hur

ska sensordata användas och av vem? Vem äger informationen? När och hur ska den visualiseras?

För att sensorsamverkan ska kunna fungera under press bör samverkansformer utvecklas under ordnade förhållanden, före en eventuell krissituation. Myndigheter som rimligen kan förväntas stå som avsändare och mottagare av sensordata behöver få en möjlighet att öva. Alla olika steg av sensorsamverkan som är tänkta att ske i kris måste också fungera väl i vardagen.

För att komma vidare är det nödvändigt att myndigheter prioriterar utvecklingen av nya samverkansformer och engagerar sig i Myndigheten för samhällsskydd och beredskaps aktiviteter för att stärka krisberedskapen. Det är också nödvändigt att myndigheterna utvecklar en fördjupad samverkanskultur där utbyte av sensordata och därtill kopplade resurser ses som något självklart och berikande för det egna ansvarsområdet. För att detta ska vara möjligt är det viktigt att operativa enheter inom myndigheterna får tillräckligt stöd för att redan idag utveckla formerna för sensorsamverkan så att det under en pågående kris finns etablerade rutiner att falla tillbaka på. Om Sverige säkerställer detta kommer totalförsvarsförmågan och krisberedskapen att stärkas avsevärt – utan stora investeringar.

För vidare läsning

David Lindgren, Maria Andersson, Åsa Berglund, Peter Nilsson, Mikael Krona, Ola Svenonius, Niclas Wadströmer, Mats Persson och Jiri Trnka, *BEViS 2018*, 2018, FOI Memo 6613.

Stefan Nilsson, Maria Andersson, Thord Andersson, Erika Bilock, Andersson, Maria, Viktor Deleskog, Louise Funke, Fredrik Hemström, David Lindgren, Sara Molin, Jonas Nordlöf, Fredrik Näsström och Joakim Rydell, *Multisensorsystem för övervakning – Slutrapport*, 2017, FOI-R--4486--SE.

7. Långsiktiga utmaningar för Sveriges militära materielförsörjning

Per Olsson

Sveriges militära materielförsörjning står inför omfattande utmaningar. Försvarsmakten möter ett försämrat säkerhetsläge i vårt närområde samtidigt som mycket av dess befintliga försvarsmateriel kommer att nå slutet av sin livslängd och behöver ersättas. Idag råder politisk enighet kring behovet av att höja försvarsanslagen i syfte att öka Sveriges militära förmåga, men neddragningar efter det kalla kriget har skapat avsevärda materielbehov. Ökade kostnader för allt mer avancerad materiel kommer också att ställa omfattande krav på effektivitet samt prioriteringar vid upphandling och användning, såväl för regeringen och riksdagen som för Försvarsmakten. Detta i syfte att få ut största möjliga förmåga från de satsningar som nu genomförs.

Ett försämrat säkerhetsläge efter historiska neddragningar

Sveriges största säkerhetspolitiska utmaning utgörs av Rysslands ökade militära förmåga och den ryska ledningens ökade beredvillighet att använda denna förmåga för att uppnå sina politiska mål. Samtidigt har historiskt stagnerande och minskade försvarsbudgetar i Västeuropa, efter det kalla krigets slut, gjort att ett teknologiskt övertag gentemot Ryssland inte längre kan tas för givet.

De problem som har orsakats av historiska neddragningar av västeuropeiska försvarsbudgetar har inte bara inneburit säkerhetspolitiska konsekvenser, utan även försvarsindustriella. Ur detta perspektiv utgör även vänligt sinnade stater konkurrenter. Bland annat har relativt små försvarssatsningar i Europa inneburit att USA har kunnat befästa sitt teknologiska försprång inom allt fler områden på försvarsmaterielmarknaden. Samtidigt har nya försvarsindustriella aktörer börjat ta andelar av den internationella marknaden. Exempelvis har Sydkorea nyligen sålt artilleri, i form av bandgående haubitsar, till Norge, Finland och Estland. Allt fler av Västeuropas traditionella exportkunder, såsom Indien och Gulfstaterna, satsar dessutom stora resurser på att bygga egen försvarsindustriell kapacitet.

Rysslands illegala annektering av Krim 2014 och pågående militära intervention i östra Ukraina är starkt bidragande orsaker till att flera västeuropeiska länder de senaste åren åter har börjat öka sina

försvarsutgifter inklusive materielanslag. För europeiska NATO-medlemmar är påtryckningar från Trump-administrationen också en viktig faktor och flera utfästelser har gjorts om att möta alliansens målsättning om att satsa minst två procent av BNP på försvar. Även i Sverige har försvarsanslagen ökat och det tycks finnas ett brett politiskt stöd för ytterligare satsningar. De senaste åren har Sverige fattat beslut om eller genomfört ett antal betydande materielanskaffningar. Försvarsmakten har bland annat tillförts självgående artilleripjäser av typen Archer och beslut har fattats om att anskaffa den senaste varianten av stridsflygplan JAS 39 Gripen, version E, ubåtar av en ny klass, A26, samt det amerikanska luftvärnssystemet Patriot. Utöver detta har beslut redan fattats om att ett stort antal stridsvagnar och stridsfordon ska renoveras samt att ubåtar ur Gotlandsklassen ska byggas om.

Nya behov av materiel

Satsningar på att stärka landets försvarsförmåga kompliceras av att flera av Försvarsmaktens nuvarande materielsystem anskaffades under 1990-talet och kommer att behöva ersättas eller uppgraderas inom de närmaste tio till tjugo åren. Under 2000-talet anskaffades materiel som var inriktat mot internationella insatser, men det försämrade säkerhetsläget i Sveriges närområde har skapat förnyat fokus på nationellt försvar. Detta har lett till ett omfattande behov av nygamla förmågor, som exempelvis ett starkare luftvärn samt moderniserade ledningssystem och förbättrad logistik. Den snabba teknologiutvecklingen har även skapat helt nya behov av satsningar på exempelvis cyberförmågor. Om dessa system och förmågor inte ersätts eller tillförs kommer Sveriges sammantagna militära förmåga i relation till omvärldens att minska snarare än öka. Dessa utmaningar är inte unikt svenska, utan utgör problem för flertalet västeuropeiska länder. Detta är knappast en tröst då europeiska länder förlitar sig på varandra för sin säkerhet, antingen genom bilaterala avtal, inom NATO, partnerskap med NATO eller genom medlemskap i EU.

Trots satsningarna som nu görs kommer materielbehoven under de kommande tio till tjugo åren att bli omfattande. Enligt Materielbehovsutredningen kan upp till 168 miljarder kronor komma att behöva tillföras mellan 2021 och 2030 ifall krigsförbandens operativa förmåga ska kunna höjas för att möta det försämrade omvärldsläget. Detta innefattar att höja den så kallade ”basplattan”, det vill säga rena nödvändigheter som uniformer och reservdelar. Det innefattar också uppgradering av marinens korvetter, men även en förbättring av ledningssystem och skydd av baser. Utredningen föreslår endast blygsamma ökningar av förbandsvolymer, däremot förslår Försvarsmaktens

egen Perspektivstudie från 2018 avsevärt ökade volymer av antalet vapensystem och förband. Ifall Perspektivstudiens ambitioner skulle förverkligas skulle det innebära ett närmast fördubblat försvarsanslag jämfört med idag.

Höjda krav skapar ökade kostnader

Fördubblade anslag innebär dock inte per automatik en fördubblad försvarsmakt. Det beror på att kostnaden för försvarsmateriel erfarenhetsmässigt ökar exponentiellt över tid. Exempelvis har kostnaden för varje enskilt stridsflygplan historiskt ökat med i genomsnitt sju procent årligen, vilket motsvarar en fördubblad kostnad vart tionde år. Motsvarande siffra för ubåtar är fyra procent och sju procent för marinens fartyg. Denna utveckling är en konsekvens av att militär materiel blir alltmer avancerad. Förutom högre krav på ökad eldkraft, skyddsnivå och rörlighet kräver moderna vapensystem även alltmer avancerade sensorer, såsom radar och robusta nätverk för en ökad förmåga till strid tillsammans med övriga delar av Försvarsmakten.

Incitamenten att hänga med i den teknologiska utvecklingen är starka. Länder som släpar efter riskerar att utkämpa framtidens krig med föråldrad materiel. Det finns även en risk att ett alltför stort fokus på högre kvalitet tvingar länder att dra ner på antalet vapensystem och förband, vilket är vad som har hänt i Sverige. Trenden är inte unikt svensk. Flera västeuropeiska länder har under de senaste decennierna valt att byta kvantitet mot kvalitet. Konsekvensen har blivit att små länder som Sverige, Norge och Danmark numera kan räkna flera förbandstyper i fåtal eller ental.

Behov av effektivitet

Försöken att bromsa kostnadsutvecklingen av militär materiel har varit många. I flera västländer förordades exempelvis under 1990-talet inköp av materiel som redan fanns på marknaden. Skälet var att befintliga system skulle kunna införas snabbare och billigare än om man utvecklade ny materiel på egen hand. Internationella materielsamarbeten eftersträvades också då det antogs kunna leda till skalfördelar där utvecklingskostnader och andra fasta kostnader fördelades på ett större antal enheter.

Sveriges nuvarande principer för materielförsörjning är formulerade utifrån insikterna ovan, med syftet att motverka kostnadsökningar och minska tiden till dess att vapensystemet kan tas i bruk. I regeringens nuvarande principer för materielförsörjning från 2009 liksom i Försvarsmaktens och Försvarets materielverks Materielförsörjningsstrategi från 2007 framgår att kostnadseffektivitet och snabba leveranser bör prioriteras. I första hand ska Försvarsmaktens befintliga materielsystem vidmakthållas. Därefter ska anskaffning ske av materiel som redan finns på marknaden. Endast i sista

hand bör ny materiel utvecklas. I samtliga fall ska internationella samarbeten övervägas för att uppnå skalfördelar. Krigsförbandens operativa förmåga är dock överordnad alla andra prioriteringar. Kostnadseffektivitet är trots allt inte detsamma som låg kostnad, utan handlar om största möjliga effekt för pengarna.

Att vidmakthålla vissa materielsystem under längre tid är ett sätt att bibehålla större förbandsvolymer till en relativt låg kostnad. Ett närliggande exempel är den finska armén som inte sällan anskaffar begagnad materiel och även behåller äldre materiel längre jämfört med övriga nordiska länder. Detta tillvägagångssätt skulle även för svensk del kunna avhjälpa de minskande förbandsvolymerna, men medför samtidigt mindre önskvärda konsekvenser. Vissa förband skulle behöva nöja sig med föråldrad materiel vilket begränsar hur de kan användas operativt. Dessutom kan gammal materiel ställa till problem ur ett försörjningsperspektiv då reservdelar till äldre system ofta upphör att tillverkas efter ett antal decennier.

Hur ser det då ut för Sverige? De ekonomiskt stora materielsystem som har anskaffats och inplanerats den senaste tiden gör det tydligt att de flesta system är nyutvecklade. Artillerisystemet Archer och stridsflygplan JAS 39 Gripen E, Helikopter 14 och ubåtar av klass A26 är några exempel. Anskaffningar av på marknaden befintlig materiel är relativt få. Helikopter 16 och Pansarterrängbil 360 brukar dock nämnas som exempel. Det är lätt att dra slutsatsen att principerna för materielförsörjning inte har efterlevts, men då vet man ju inte hur mycket befintlig materiel som hade anskaffats utan principerna. Dessutom är försvarets operativa förmåga överordnad alla andra prioriteringar. Detta kriterium är extremt svårbedömt och kan mycket väl motivera en hög andel nyutvecklade system.

Dessutom har regering och riksdag själva gjort betydande avsteg från principerna för materielförsörjning genom utpekandet av tre väsentliga säkerhetsintressen. Idag utgörs dessa av stridsflygförmågan, undervattensförmågan och de så kallade integritetskritiska delarna av ledningssystemområdet. Genom att peka ut väsentliga säkerhetsintressen möjliggörs en riktad upphandling av stridsflyg, ubåtar och ledningssystem, vilket understryker det fortsatt nära förhållandet mellan Sveriges försvar och försvarsindustri.

Det finns med andra ord inga tecken på att anskaffningen av avancerad och nyutvecklad materiel har minskat eller skulle minska inom någon nära framtid. Därmed finns risken att trenden med ökade materielkostnader fortsätter även framöver.

Behov av prioriteringar

Frågan om avancerade men dyra kontra flera men billigare materielsystem är dock endast en av de avvägningar politiska och militära beslutsfattare behöver ta ställning till. För regering och riksdag är första steget resursfrågan, där försvarets behov ställs mot andra resursbehov i samhället. Detta gäller även de övriga delarna av totalförsvaret.

Det mesta tyder på att försvaret kommer att få ökade resurser framöver, men tillförseln måste vara tillräcklig och samtidigt ske i en takt så att Försvarsmakten kan absorbera ökningen. Försvarsmakten måste i sin tur definiera en tydlig prioriteringsordning kring vilka åtgärder som behöver göras först. Hur man än gör behöver satsningar på materiel ske med den militära personalförsörjningen och Försvarsmaktens övriga strategier och doktriner i åtanke. Hur väl överensstämmer materielförsörjningsstrategin med övriga militärstrategiska styrdokument? Hur ser vi till att materielförsörjningen fungerar tillsammans med den återinförda värnplikten? Detta är bara några exempel på prioriteringsfrågor som beslutsfattare står inför idag och framöver.

En långsiktig planering för materielförsörjningen bör även innefatta en strategi för de väsentliga säkerhetsintressena. Idag saknas såväl en tydlig strategi för de väsentliga säkerhetsintressena som en enhetlig och tydlig definition av vad dessa innefattar. Enligt EU-lagstiftning har varje medlemsstat rätt att undanta försvarsmateriel som utgör väsentliga nationella säkerhetsintressen från unionens gängse konkurrensregler. Men att Sverige har identifierat hela förmågor, som stridsflygförmågan och undervattenförmågan, som väsentliga säkerhetsintressen skapar ett behov av tydliga definitioner av vad dessa förmågor innefattar. Den nationella säkerhetsstrategin från 2017 pekar på att väsentliga säkerhetsintressen och därmed förknippade industriell och teknisk kompetens ska bibehållas och utvecklas, om det är militärt och ekonomiskt rationellt. Men vilka konsekvenser får detta för statens förhållande till industrin och vilka förpliktelser, om några, har staten åtagit sig? Detta är frågor som behöver hanteras i framtiden.

Det förekommer många åsikter i debatten kring nyttan och kostnaderna förknippade med en omfattande svensk försvarsindustri, men oavsett ställningstagande i denna fråga så krävs långsiktiga satsningar ifall landets försvarsindustri effektivt ska kunna bidra till landets försvarsförmåga framöver. Då handlar det inte enbart om satsningar på anskaffning och vidmakthållande av materiel för att hålla industrin igång, utan även om satsningar

på forskning och utveckling som möjliggör nya koncept och ny spetsteknologi för att möta framtidens behov och utmaningar.

För vidare läsning

Per Olsson, Peter Bäckström, Mattias Johansson, Jens Lehman, Jens Lusua, Maria Ädel och Josefin Öhrn-Lundin, *Strukturella utmaningar inom det militära försvarets materiel- och personalförsörjning*, 2018, FOI-R--4593--SE.

Per Olsson och Peter Nordlund, *Effektiv materielförsörjning – Nordiska länders strategi, organisation och försvarsindustri*, 2017, FOI-R--4452--SE.

Peter Nordlund, Per Olsson, Ulf Jonsson och Peter Bäckström, *Effektiv materielförsörjning – Utveckla, anpassa eller köpa från hyllan?*, 2016, FOI-R--4265--SE.

8. Vem levererar om kriget kommer? – Om näringslivet, försörjningsberedskapen och framtidens totalförsvar

Jenny Ingemarsdotter och Jenny Lundén

Näringslivets medverkan är central för totalförsvarets utveckling och för en god försörjningsberedskap, det vill säga planering för tillgång och fördelning av exempelvis livsmedel, läkemedel och bränsle. Detta var tidigare huvuduppgiften för det så kallade ekonomiska försvaret, vilket var en central del av det gamla totalförsvaret. Ambitionen var att vid en avspärrning av landet klara försörjningen av befolkningen under flera år. Idag diskuteras återigen kvantitativa mål för den svenska försörjningsberedskapen. Centralt för uppbyggnaden av en sådan försörjningsberedskap är att på ett tidigt stadium involvera näringslivet. Men vilka är förutsättningarna för detta?

Näringslivet och försörjningsberedskapen

Mål och ambitionsnivå för en återuppbyggd försörjningsberedskap är ytterst en politisk fråga, som till stor del handlar om att väga kostnaderna för att trygga försörjningen mot risken att hoten blir verklighet. Till skillnad från krisberedskapssystemet, som fokuserar på relativt kortvariga kriser, så talas det nu om att totalförsvaret måste byggas för att klara utdragna störningar, gråzonslägen mellan fred och krig, och ytterst väpnat angrepp. Dessa hotbilder aktualiserar behovet av en nationell försörjningsberedskap.

Näringslivet spelar en betydande roll i totalförsvaret eftersom samhällsviktig verksamhet, som till exempel telekommunikationer och elförsörjning, vilka tidigare i högre grad drevs i offentlig regi, idag i stor utsträckning utförs av privata företag. Inom ramen för den återupptagna totalförsvarsplaneringen har detta förhållande genererat en mängd analyser och utredningsdirektiv. Kort sagt, många pratar om näringslivet – men vad är det som sägs egentligen?

Utmaningen gäller hur näringslivet i praktiken ska delta i utvecklingen av totalförsvaret. Det kan handla om en återkomst av så kallade krigsviktiga företag, eller K-företag, beredskapskontrakt, och kanske ett centralt näringslivsråd. Med fokus på försörjningsberedskapen tar kapitlet upp några av de vanligaste frågorna och förslagen gällande näringslivets framtida roll i totalförsvaret, samtidigt som kapitlet lyfter fram näringslivets egna perspektiv och intresse av att delta i totalförsvarsutvecklingen.

En historisk återblick

Begrepp som K-företag, beredskapsplanering och försörjningsberedskap härstammar från det totalförsvar som fanns i Sverige under det kalla kriget. Dessa historiska erfarenheter är viktiga att ha med sig när ett nytt totalförsvarskoncept ska utvecklas för dagens samhälle, för att förstå skillnader men också likheter i de förutsättningar som fanns då och de som finns nu.

Utifrån erfarenheter från första världskriget, då Sverige drabbades av livsmedelsbrist och handelsstörningar, drog staten slutsatsen att hela samhällsekonomin inklusive näringslivet måste engageras för att säkerställa tillgång till strategiskt viktiga varor, som exempelvis bränsle och livsmedel. För att strukturera detta arbete bildades år 1928 Rikskommissionen för ekonomisk försvarsberedskap. Under de följande decennierna pågick en målmedveten uppbyggnad av Sveriges försörjningsberedskap. Under andra världskriget drogs slutsatsen att det moderna kriget skulle drabba hela samhället och civilbefolkningen. Detta krävde ett ”totalt försvar” som skulle bygga materiell uthållighet och mental beredskap hos befolkningen. I detta totalförsvar skulle det ekonomiska försvaret fortsatt spela en central roll.

Från och med 1960-talet ansvarade Överstyrelsen för ekonomiskt försvar (ÖEF) för den statliga beredskapslagringen av varor som inte producerades inom landet och som skulle komplettera näringslivets egna lager. Dessutom skulle ÖEF samordna en detaljerad planläggning som skulle tillgodose företagens behov av arbetskraft, råvaror, energi och transporter i händelse av krig. Kontaktytor mellan näringslivet och staten fanns också genom Kommerskollegiet som genom planering och övning hade i uppdrag att säkerställa att utrikeshandeln fungerade under säkerhetspolitiska kriser och krig.

Som en del av det ekonomiska försvaret engagerades delar av näringslivet genom att avtal upprättades med utvalda företag. Dessa K-företag skulle fortsätta sin verksamhet vid kris eller krig, ibland med ändrad inriktning. Fördelar för de utvalda företagen kunde vara att personalen skyddades från annan tjänstgöring inom totalförsvaret, att företagen fick förtur till reparationer av telekommunikation samt att de undantogs från ransonering av till exempel bränsle och transporter. K-företagens uppgifter kunde handla om att ta fram ersättningsvaror eller beredskapslagra strategiska råvaror. Bakgrunden till dessa åtgärder var oron under det kalla kriget för avspärrning, det vill säga situationer då Sverige i princip skulle vara avskuret från omvärlden.

Beredskapsplaneringen och K-företagssystemet fasades i praktiken ut under slutet av 1990-talet. Med anledning av det kalla krigets slut bedömdes det inte längre nödvändigt att ständigt ha en hög

försörjningsberedskap som var förhållandevis dyr. Detta innebar mer konkret att beredskapslagren såldes ut eller avvecklades och att beredskapsavtalen med företag avslutades.

Moroten och piskan

Lite hårddraget kan sägas att det som lämnades intakt i samband med totalförsvarets avveckling var den lagstiftning som reglerade statens befogenheter. Staten har fortfarande rätt att styra över näringslivets resurser under vissa omständigheter, exempelvis kan fastigheter, industrianläggningar, fartyg och fordon tas i anspråk för statens räkning under höjd beredskap. Denna lagstiftning utvecklades i ett historiskt sammanhang då det antogs att resurser fanns att tillgå inom landet och att företag hade viss egen lagerhållning. Kontrasten är därmed stor till dagens förhållanden med *just-in-time*-leveranser och minimerad lagerhållning. I en värld av globaliserade flödeskedjor kan den svenska staten helt enkelt inte räkna med att resurser finns tillgängliga när de behövs som mest – såvida man inte har planerat för sådana situationer.

Arbetet med att bygga upp en ny försörjningsberedskap kan visserligen ta sin utgångspunkt i existerande lagstiftning och regelverk men anpassningar kan behöva göras till dagens förhållanden. Exempelvis skulle, som Försvarsberedningen har föreslagit i Motståndskraft, krav kunna ställas på företag att lagra vissa strategiskt viktiga varor. Andra typer av krav kan handla om att öka samhällsviktiga funktioners robusthet och skydd, inklusive åtgärder för stärkt informationssäkerhet. Företag har förvisso ett egenintresse av att utveckla sin förmåga att motstå incidenter såsom störningar och intrång, och på så sätt upprätthålla produktion och verksamhet. I ett totalförsvarsperspektiv behövs emellertid också ett samlat grepp där privata och offentliga aktörer tillsammans arbetar utifrån en gemensam ambitionsnivå, förståelse av en gemensam hotbild och överväganden om vad som är skyddsvärt.

En morot för att engagera näringslivet i detta arbete kan vara att få tillgång till fördjupade nätverk. Som jämförelse har man i Finland under lång tid genomfört olika typer av övningar och totalförsvarskurser tillsammans med näringslivet, vilket anses skapa värdefulla nätverk inom och mellan olika sektorer och branscher. Finska företag som bedriver samhällsviktig verksamhet baserar sina beredskapsåtgärder på affärsmässiga grunder, exempelvis genom riskhantering och i avtal. Samordningen av de finska beredskapsåtgärderna, både i samhället och inom näringslivet, sker genom landets Försörjningsberedskapscentral.

Oavsett hur näringslivet engageras i totalförsvaret kommer en gemensam offentlig-privat förståelse av vad som behöver göras

att vara en nyckelfaktor för den fortsatta utvecklingen av ett nytt totalförsvar. En fördjupad offentlig-privat samverkan kommer dock att få begränsad effekt om inte ekonomiska resurser tillförs. Även om näringslivet kan ha ett intresse av att delta i totalförsvarsutvecklingen kan inte enskilda företag förväntas bära stora kostnader som inte är affärsmässigt motiverade. Därför har Myndigheten för samhällsskydd och beredskap och Försvarsberedningen påpekat att en övergripande finansieringsmodell behöver tas fram.

Försörjningsberedskap 2.0

Mot bakgrund av de samhällsförändringar som har skett sedan totalförsvarsplaneringen avvecklades i slutet av 1990-talet kommer en rad överväganden att behöva göras inför en återuppbyggnad av försörjningsberedskapen, till exempel:

- Vilka varor och tjänster ska ses som strategiska eller samhällsviktiga?
- Är lagerhållning vägen framåt, och i så fall, hur ska rollerna gällande bland annat omsättning och distribution fördelas mellan privata och offentliga aktörer?
- I vilken grad bör andra metoder än lagerhållning övervägas, som till exempel produktionsomställning eller nya typer av avtal eller beredskapskontrakt?

Även om svaren på dessa frågor kommer att se olika ut i olika sektorer står det klart att näringslivets aktörer kommer att spela en viktig roll vad gäller vägval inom olika områden. Försvarsberedningen 2017 har föreslagit att ett näringslivsråd bör inrättas. Detta ska vara ett komplement till befintliga forum inom branschorganisationer och syfta till ömsesidigt informationsutbyte. Ett näringslivsråd skulle gemensamt ta fram inriktningar, planer och villkor för samverkan mellan offentliga och privata aktörer.

Försvarsberedningen har 2017 även föreslagit återinförandet av någon slags version av K-företag. Oavsett vilka former som kan bli aktuella för detta kan man konstatera att trender som effektivisering, globalisering och digitalisering har förändrat spelplanen avsevärt i jämförelse med det tidigare totalförsvarets modell med produktionsinriktade K-företag. Förutom varor måste även ett stort antal tjänster idag ses som strategiska, till exempel digitala system för att möjliggöra distribution av läkemedel och livsmedel, men även personal som kan hantera dessa system. En viktig utmaning är att identifiera vilka aktörer, varor och tjänster som ska definieras som krigsviktiga i dagens samhälle. Även om K-företag återinförs kommer dessa inte kunna utgöra

den enda modellen för näringslivets medverkan i totalförsvaret. Beredskapsperspektiv kan rimligen tas om hand i avtal och upphandlingar utan att begreppet K-företag används.

Flera näringslivsrepresentanter har ställt sig generellt positiva till Försvarsberedningens förslag, givet att formerna blir rimliga, såsom att konkurrensneutralitet och finansiering beaktas. Samtidigt anser många företag att det är viktigt med tydlig ansvarsfördelning och en långsiktighet när det gäller totalförsvarsplaneringen som helhet.

Tre framgångsfaktorer

Begrepp som K-företag och näringslivsråd är på ett sätt enkla och konkreta att använda i debatter om näringslivets roll i framtidens totalförsvar. Samtidigt finns vissa grundläggande förutsättningar som är viktiga att fastställa innan fokus hamnar på former för samverkan. Dessa kan sammanfattas i mål, ansvar och kommunikation.

Vad gäller frågan om mål har näringsliv såväl som myndigheter länge efterfrågat en större tydlighet vad gäller totalförsvarets ambitionsnivå. Här finns ett brett spann mellan en ambition om att förse allmänheten med ”livets nödtorft” till att trygga tillgången till internet dygnet runt. Utan konkreta mål är det svårt för enskilda myndigheter, kommuner och landsting att ställa rimliga beredskapskrav, exempelvis inom ramen för offentliga upphandlingar.

Företag har också efterfrågat ett klargörande av vilken ansvarsfördelning som gäller mellan olika offentliga aktörer inom försörjningsberedskapen. En större tydlighet i vem som ”äger frågan” inom och mellan olika sektorer, såsom energi, livsmedel, transporter, med flera förs ofta fram.

Slutligen är det viktigt att kommunicera totalförsvarets mål, ambitioner och uppgifter till berörda aktörer. Oavsett utformningen av styrningen för att engagera näringslivet i totalförsvaret – från lagar och regelverk, K-företag, avtal, beredskapskontrakt, kurser och övningar – kommer en gemensam offentlig-privat förståelse av vad som hotar och vad som behöver göras att vara en framgångsfaktor för den fortsatta utvecklingen av ett nytt totalförsvar.

För vidare läsning

Ann-Sofie Stenérus Dover, Anders Odell, Per Larsson och Johan Lindgren, B*eredskapslagring: En kunskapsöversikt om beredskapslagring som ett verktyg för ökad försörjningsberedskap i Sverige*, 2019, FOI-R--4644--SE.

Jenny Ingemarsdotter, Anna Sparf, Linda Karlsson och Jenny Lundén, *Näringslivets roll i totalförsvaret – centrala frågor och vägar framåt*, 2018, FOI-R--4649--SE.

Matilda Olsson, Charlotte Ryghammar och Jenny Lundén, *Näringslivets syn på roller och ansvar i totalförsvaret*, 2017, FOI-R--4551--SE.

9. Syntetisk biologi – möjligheter och utmaningar för totalförsvaret

Fredrik Ekström, Jonas Näslund och Per Stenberg

Tänk dig ett totalförsvar där växter ändrar färg och varnar för giftiga gaser, där civila och militära insatsfordon drivs av bränslen framställda av mikroorganismer, där grödor designats för att klara ett förändrat klimat. Med skyddande ämnen cirkulerande i kroppen bryts kemiska stridsmedel ned innan de hinner göra skada. Dessa koncept är inte science fiction utan har redan i dagsläget demonstrerats i laboratorier. Syntetisk biologi handlar om att artificiellt modifiera organismer. Teknikutvecklingen har på detta område den senaste tiden varit väldigt snabb. Utvecklingen har potential att på ett omvälvande sätt påverka totalförsvarets förmågor. Men utvecklingen leder också till nya risker eftersom fienden kan använda syntetisk biologi för sina syften, för angrepp mot jordbruk, genetiska lönnmord med mera.

Betydelsen av syntetisk biologi för Totalförsvaret

Utveckling och tillämpning inom syntetisk biologi påverkar redan i dagsläget viktiga delar av det civila samhället och potentialen för framtidens totalförsvar är avsevärd. Produktion av viktiga läkemedel liksom avancerade motmedel mot kemiska stridsmedel är redan en realitet. Grödor designade med en inneboende klimat- och patogenresistens, det vill säga resistens mot bland annat skadliga virus och bakterier, kan bidra till Sveriges livsmedelsförsörjning och skogsbruk vid ett varmare klimat. Organismer kan designas för att indikera utsläpp av toxiska ämnen och för att rena dricksvatten, jord och mark från gifter och miljöföroreningar. Genetiskt modifierade alger och cyanobakterier används redan idag för att i provrör producera biodiesel och andra drivmedel från lokalt tillgängliga råvaror, såsom restprodukter från skogsbruk. På längre sikt kommer utvecklingen ge nya material med helt nya egenskaper. En mer spekulativ utveckling på lång sikt är att utvecklingen kan komma att inkludera soldater som har genetiskt modifierats för att tåla kemiska och biologiska stridsmedel eller för att förbättra fysisk styrka och uthållighet.

Ett inneboende problem med utvecklingen är att samma tekniker som används för att göra gott även kan användas i fientligt syfte. Även om möjligheterna för missbruk till viss del begränsas av internationella regimer genom lagstiftning och kontrollorgan

är metoder och kunskap för att exempelvis modifiera eller flytta gener mellan arter universella, oavsett vilka egenskaper som tillförs. Designade, väldigt smittsamma, mikroorganismer som undgår upptäckt och medicinsk behandling är ett uppenbart hot. Ett fientligt angrepp med en designad mikroorganism kommer sannolikt att kräva en snabb respons, till exempel i form av ett avancerat motmedel. Det finns en berättigad oro för genetiska lönnmord och riktade genetiska vapen designade för att slå ut specifika delar av arvsmassan. Det är dock viktigt att notera att antagonistiska tillämpningar av syntetisk biologi inte nödvändigtvis behöver riktas mot Sveriges befolkning, även jordbruk och skogsbruk är tänkbara mål för ett angrepp. Det krävs en hög vetenskaplig nivå hos berörda svenska myndigheter för att förstå hotets natur men också en infrastruktur, inklusive laboratorier och specialistkompetens, som är dimensionerad för att snabbt använda kunskapen om hotet och genomföra effektiva motåtgärder.

Exempel på aktuell användning av syntetisk biologi

Med stor sannolikhet kommer syntetisk biologi på ett genomgripande sätt att påverka nästan hela vårt samhälle. Tillämpningarna återfinns inom många områden, något som gör det svårt att ge en heltäckande bild. För att illustrera potentialen, beskrivs nedan några områden där syntetisk biologi redan i dagsläget har gjort ett stort avtryck.

Läkemedelsförsörjning. Enzymer är ämnen av biologiskt ursprung som ökar kemiska reaktioners hastighet. Enzymer är inblandade i nästan alla processer som sker i levande organismer och är därför en förutsättning för allt liv. Enzymer omvandlar socker till energi, gör så att växter kan tillgodogöra sig koldioxid från atmosfären och ger bakterier resistens mot antibiotika. Att överföra den arvsmassa som kodar för ett enzym mellan olika organismer är idag rutin. Redan för ett decennium sedan överfördes arvsmassa från sommarmalört till bagerijäst. Den nya arvsmassan gav jästcellerna förmåga att producera en substans som enkelt kan modifieras till Artemisin, ett läkemedel som rekommenderas av WHO för behandling av malaria. På senare tid har på liknande sätt kemiska processer konstruerats genom att kombinera arvsmassa från vitt skilda organismer. Ett slående exempel är jästceller som har modifierats med över 20 fragment av arvsmassa från däggdjur, växter och bakterier för att producera opioider, läkemedel som används för smärtstillande behandling och palliativ vård.

Av relevans för Sveriges skydd mot kemiska stridsmedel är de enzymer som utvecklas bland annat i USA och Israel och som har förmåga att bryta ner kemiska stridsmedel. Utvecklingen

av dessa enzymer har till stor del skett med en kontrollerad evolution i laboratoriemiljö. Det modifierade enzymet bryter ner vissa nervgaser mer än 17000 gånger snabbare än den naturliga förlagan och experiment visar att djur som har behandlats med det modifierade enzymet har en avsevärt förbättrad tolerans mot nervgas. Laborativ evolution är idag en vanligt förekommande teknik som används inom vitt skilda frågeställningar, något som uppmärksammats av 2018 års nobelpris i kemi.

Levande sensorer. Sensorer som upptäcker kemikalier är viktiga i många sammanhang, allt från att upptäcka utsläpp från industrier till att förhindra införsel av olagliga substanser. Att använda växter som levande sensorer är attraktivt eftersom de kan leva i ett stort antal miljöer om de förses med solljus och vatten. En forskargrupp lyckades nyligen utnyttja växten backtrav för att skapa en mycket känslig biosensor för detektion av fentanyl. Fentanyl är ett mycket kraftigt smärtstillande preparat som också produceras illegalt och har orsakat flera dödsfall bland missbrukare.

Att upptäcka fentanyl kompliceras av att molekylen förekommer i ett stort antal olika tredimensionella strukturer. Med hjälp av datormodellering designade forskarna först ett antal proteiner som teoretiskt borde binda till de vanligaste formerna av fentalyl. Detta kan liknas vid att man konstruerar lås som passar specifika nycklar. Generna för dessa proteiner syntetiserades och introducerades sedan i växter tillsammans med ett signalsystem som gjorde växten självlysande när den kom i kontakt med fentanyl, i form av en lösning. Det pågår många andra projekt där man försöker utnyttja växter och andra organismer som sensorer för detektion av allt från utsläpp av kemikalier i miljön till tidig detektion av sjukdomar hos människor. Ett exempel på det senare är projekt där forskare försöker skapa bakterier som kan upptäcka till exempel cancer eller infektioner i tarmen. Vid behov ska bakterien även på egen hand kunna frisätta läkemedel som den själv bär med sig.

*Livsmedelsförsörjnin*g. Att med begränsade jordbruksresurser försörja befolkningen med livsmedel under en utdragen krissituation är en betydande utmaning, speciellt om Sverige samtidigt utsätts för en påverkanskampanj mot jordbruket eller om importförbindelser har drabbats. Den kanske mest uppenbara användningen av syntetisk biologi är att modifiera befintliga grödor så att de får förbättrad motståndskraft mot växtskadegörare eller kan odlas trots förändrat klimat. Det är också möjligt att modifiera grödor så att näringsvärdet eller produktiviteten förbättras. Det pågår även utveckling

för att använda celler som fabriker för att producera speciella näringsämnen eller helt nya födoämnen. Kanske kommer man på sikt att kunna utveckla mikroorganismer som tillverkar födoämnen som har sitt naturliga ursprung i växt- eller djurriket.

Mänsklig modifiering. Med dagens teknik är det inte bara möjligt att förändra specifika delar av arvsmassan, man kan också avlägsna eller tillföra hela gener. Exempelvis finns det läkemedel som används för att behandla olika sorters blodcancer som bygger på att en patients egna immunförsvarsceller modifieras genetiskt så att de siktar in sig på, och dödar cancercellerna. Modifieringen sker med hjälp av ett virus som levererar nytt genetiskt material till immunförsvarscellerna.

Satstningar inom syntetisk biologi

Globalt satsas stora pengar inom syntetisk biologi och utvecklingen kan leda till en ny industriell revolution. Inflytelserika nationer som Storbritannien och USA investerar dessutom en betydande del av försvarsforskningsbudgeten på syntetisk biologi. Ett konkret exempel är amerikanska *Defence Advanced Projects Agency* (DARPA) som mellan 2010 och 2014 ökade sin satsning på syntetisk biologi med 100 miljoner dollar. Sverige är en nation som satsar en betydande del av sin BNP på forskning men jämfört med andra länder ligger Sverige inte lika bra till vad gäller bioteknik vilket är det område under vilket satsningar på syntetisk biologi sorterar.

I Sverige saknas satsningar för att exploatera syntetisk biologi och nyttja dess potential i syfte att höja den svenska totalförsvarsförmågan. Konsekvenserna är potentiellt allvarliga, och begränsar dessutom Sveriges beredskap att möta en antagonistisk användning av syntetisk biologi. Globala skillnader finns inte bara inom finansieringen. Även lagstiftningen varierar avsevärt. Kina har till exempel en mer tillåtande lagstiftning på detta område, något som bland annat har möjliggjort genetiska modifieringar av mänskliga embryon. Även USA har en betydligt mer tillåtande lagstiftning än EU.

Vägen framåt

Idag fokuserar man i stor utsträckning på att modifiera sådant som redan existerar i naturen. Man kan exempelvis förändra ett existerande enzym så att det tål en högre temperatur, vilket krävs i vissa industriella processer. Att designa ett helt nytt enzym med helt nya egenskaper är mycket svårare. För att göra det krävs ofta väldigt många så kallade ”*design-build-test*”-cykler, vilket blir mycket resurskrävande. För att den syntetiska biologin ska mogna och uppfylla sin fulla potential krävs en ökad kunskap om komplexa

biologiska och kemiska system. Den obundna akademiska forskningen är därför viktig för den framtida utvecklingen av syntetisk biologi. Dessutom måste myndigheter och andra aktörer med verksamhet som berörs av utvecklingen höja sin kompetens gällande syntetisk biologi för att Sverige ska kunna ta tillvara på möjligheterna inom området. En grundläggande förutsättning för att uppfylla potentialen också från ett totalförsvarsperspektiv är ett effektivt samspel mellan akademi och totalförsvarsmyndigheter. Steget från en grundläggande förståelse av syntetisk biologi till en användning med relevans för totalförsvaret är stort. En utmaning är exempelvis att anpassa koncept som fungerar i laboratorieskala för industriell produktion, något som kräver ett tätt samarbete med industriella partners.

Det som idag bör prioriteras är en överbryggande forskning som knyter samman framstegen inom grundforskningen med totalförsvarets behov. Inom den försvarsanknutna forskningen bör fokus ligga på att utveckla metoder, kunskap och infrastruktur inom syntetisk biologi. Först när dessa förutsättningar finns på plats kan produkter och lösningar direkt riktade mot svenska totalförsvarsbehov utvecklas. Välavvägda satsningar med tydliga mål ger möjligheter att skräddarsy forskningen efter svenska behov och gör dessutom Sverige till en attraktiv samarbetspartner på den internationella arenan.

För vidare läsning

Karin Hjalmarsson, *CRISPR - Verktyg för redigering av gener Pandoras Ask*, 2018, FOI Memo 6435.

Elisabet Frithz, Anders Allgardsson och Per Stenberg, *Genomics in perspective science - science-society-security*, 2016, FOI-R--4217--SE.

Anders Allgardsson, Christine Akfur, Elisabet Artursson, Fredrik Ekström och Nina Forsgren, *Kemiska hot och medicinskt skydd: Mekanism och molekylära interaktioner*, 2016, FOI Memo 5929.

10. Cyberförsvar – färdighet kräver övning

Tommy Gustafsson och David Lindahl

Sedan millennieskiftet har cyberincidenter och förmodade cyberoperationer haft en omfattande påverkan på många länder och organisationer. Sverige har en hög grad av digitalisering av samhällsviktiga system och de personer som dagligen hanterar dessa system har en central roll inom vårt totalförsvar. Därför är det viktigt att regelbundet öva dessa personer i att hantera cyberincidenter. I dagens läge sker för få övningar och det är dessutom svårt att genomföra dem realistiskt och pedagogiskt. För att säkerställa den nationella totalförsvarsförmågan behövs relevanta övningsmiljöer, ökad övningsvolym och forskning kring övningsmetodik.

Cyberoperationer

Cyberrymden är en arena där det under de senaste decennierna har skett en betydande utveckling av både förmåga och doktrin. Det är en arena där militära och civila aktörers intressen möts och hotet från cyberangrepp ställer nya krav på Sveriges totalförsvar. En konventionell konflikt begränsas av geografi. För att en fiende ska kunna slå mot Sverige måste de först passera rikets gräns och det skydd som Försvarsmaktens förband utgör. En cyberoperation, det vill säga aktiviteter i cyberrymden utförda av en stat för att nå militära eller politiska mål, gör det möjligt för en angripare att slå mot alla de datorer som är nåbara för kommunikation utan att det konventionella försvaret kan göra något.

Det innebär att enskilda systemadministratörer i civila organisationer riskerar att hamna i konfliktens frontlinje. De behöver därför ha den kompetens som krävs, både för att se till att systemen har en bra säkerhetsnivå och för att kunna hantera angrepp.

Cyberoperationer används idag regelbundet för underrättelseinhämtning, industrispionage och sabotage. Internationella konflikter har förekommit som helt eller delvis har utspelat sig i cyberrymden. Det finns exempel på cyberoperationer där nationer har anfallit civila mål både direkt och indirekt med hjälp av proxyorganisationer såsom hackergrupper. Under kriget mellan Ryssland och Georgien 2008 störtdes en dryg tredjedel av Georgiens internet allvarligt, myndigheters kommunikation stoppades och riksbanken tvingades stänga ner alla datortjänster i elva dygn.

En annan betydande verksamhet är olika typer av påverkansoperationer. De flesta påverkansoperationer verkar vara fokuserade på att manipulera opinionen i en viss fråga, men det finns exempel som indikerar att cyberoperationer också har använts för att påverka suveräna nationers strategiska beslut. Ett sådant är cyberangreppen 2009 mot Kirgizistan i samband med att landet förhandlade om att husera en NATO-bas på sitt territorium.

Det är svårt att begränsa verkan av cybervapen, som exempelvis skadlig kod, och cyberangrepp. År 2010 tog sig cybervapnet Stuxnet långt utanför sina avsedda mål i Iran och sju år senare slog angreppet NotPetya inte bara mot tio procent av Ukrainas datorer, utan spred sig utanför landet och blev världens hittills mest kostsamma cyberangrepp. Sammantaget visar utvecklingen inom cyberarenan att det finns ett hot mot Sveriges samhällsviktiga system även om Sverige i sig inte är målet för ett visst angrepp.

Cyberförsvarets förmågebehov

Många ramverk och vägledningar inom cybersäkerhet lyfter fram behovet av kunskap om hot och skyddsåtgärder. Denna kunskap behövs bland annat för att göra rätt saker med de resurser som finns till hands, exempelvis att prioritera tekniska och administrativa skyddsåtgärder. Proaktiva åtgärder är viktiga och det är ofta enskilda systemadministratörers kunskap och agerande som avgör om en incident inträffar och om dess konsekvenser i så fall blir allvarliga eller inte. Ett bra sätt att bygga upp denna kunskap är att öva. Övning ger en erfarenhetsbaserad inlärning utan att behöva hantera skarpa incidenter. Genom att öva blir systemadministratörer skickligare och systemen säkrare.

Cyberövningar används internationellt för att öka försvarsförmågan, till exempel *Locked Shields* och *Crossed Swords* som arrangeras i Estland samt *Cyber Czech* i Tjeckien. Att öva är också i linje med Sveriges nationella strategi för cybersäkerhet från 2017, som bland annat konstaterar att ”[r]egelbundna nationella och internationella övningar är en förutsättning för att utveckla och utvärdera strukturer för hantering av allvarliga IT-incidenter…”.

Förutom kunskapsnivån hos enskilda systemadministratörer har det visat sig att samverkan också är en viktig framgångsfaktor för att snabbt och effektivt kunna hantera avancerade storskaliga cyberincidenter. När Estland år 2007 utsattes för angrepp drog de stor fördel av en sedan flera år etablerad nationell samverkan mellan systemadministratörer från olika organisationer inom samhällsviktig verksamhet. Övningar är ett sätt att etablera denna typ av samverkan.

En nationell förmågeuppbyggnad

För att åstadkomma en nationell förmågeuppbyggnad inom cyberområdet finns det tre betydande övningsrelaterade utmaningar som behöver adresseras: för det första krävs tillgång till relevanta övningsmiljöer och scenarier, för det andra en ökad övningsvolym, och för det tredje behövs forskning som säkerställer att rätt kompetens lärs ut på rätt sätt.

För att skapa relevanta övningsmiljöer och scenarier behövs dels betydande kunskap om IT och om hur aktuella cyberangrepp går till, dels ett pedagogiskt handlag för att utveckla övningar som förmedlar de komplexa detaljerna hos cyberincidenter. Idealt skulle övningar bedrivas direkt i övningsdeltagarnas normala IT-miljöer men det är sällan möjligt eftersom det skulle medföra betydande driftstörningar i just den IT-miljö man vill skydda.

Ett alternativ är då att skapa en replik av den egna IT-miljön men de flesta organisationer har inte tillräckliga resurser för att prioritera att sätta upp parallella IT-miljöer. Även om man kopierar de tekniska systemen är det mycket svårt att simulera användarnas aktiviteter vilket därmed begränsar scenarionas relevans. Ett ”tyst” nät där bara angriparna och de övade är aktiva skiljer sig mycket från verkligheten.

Ytterligare problem är att det ofta krävs flera iterationer av en övning innan de pedagogiska momenten fungerar optimalt och förändringstakten inom området medför också att övningsmiljöer snabbt skulle blir föråldrade. De flesta organisationer är för små för att ha egen personal som kontinuerligt vidareutvecklar övningsmiljöer och scenarier.

Det finns vissa kommersiella initiativ inom området, men dessa har hittills saknat relevanta övningsmiljöer för totalförsvaret. Resurser för att utveckla själva övningen måste därför fortfarande avsättas av den organisation som vill öva, vilket aktualiserar de svårigheter som beskrivs ovan. I de fall där de kommersiella initiativen är utländska, medför detta ett säkerhetsproblem ur ett totalförsvarsperspektiv. Sammantaget medför svårigheterna med att utveckla och underhålla övningsmiljöer och scenarier, samt avsaknaden av relevanta kommersiella alternativ, att det behövs en nationell totalförsvarssatsning inom detta område.

Liknande satsningar sker redan i flera länder, med framträdande exempel i Estland och Norge. Dessa satsningar syftar till att stärka den nationella cyberförsvarsförmågan i respektive land och inkluderar ofta aktörer från försvarsmakt, civila myndigheter, aktörer inom samhällsviktig verksamhet och högre lärosäten. Denna blandning av aktörer säkerställer att de övningar som utvecklas bygger på relevant teknik, och relevanta scenarier

och att de får en tillräcklig spridning för att få en positiv och långvarig effekt på den nationella cyberförsvarsförmågan. En central komponent i dessa satsningar är upprättandet av en nationell cyberanläggning (på engelska *cyber range*) där övningar kan utvecklas och genomföras.

I samarbete med Myndigheten för samhällsskydd och beredskap och Försvarsmakten driver FOI anläggningen *Cyber Range And Training Environment* (CRATE) som används såväl inom forskningsprojekt som inom övnings- och kursverksamhet. Det är idag en avancerad cyberanläggning och inkluderar en omfattande IT-infrastruktur samt en mängd specialutvecklade verktyg för att ta fram och genomföra övningar. CRATE skulle kunna utgöra en bra grund för en svensk nationell cyberanläggning.

Utmaningen att öka övningsvolymen kräver både en större medvetenhet och en bättre tillgång till relevanta cybersäkerhetsövningar. Många organisationer som bedriver samhällsviktig verksamhet är inte medvetna om sin roll för Sveriges totalförsvarsförmåga och därmed är de inte heller medvetna om hur viktig deras cybersäkerhetsförmåga är. De dimensionerar i första hand sitt säkerhetsarbete för att hantera driftstörningar och skulle därför troligen inte prioritera cybersäkerhetsövningar även om dessa fanns tillgängliga. Att enbart förbättra övningsmöjligheterna utan att höja medvetenheten skulle därför inte leda till ökad övningsvolym.

För att adressera utmaningen med att säkerställa att rätt kompetens lärs ut på rätt sätt krävs forskning inom pedagogik relaterat till cybersäkerhet. Trots att Sverige i likhet med flera andra länder har genomfört övnings- och utbildningsinsatser under mer än ett decennium har det endast skett begränsad forskning inom detta område. Att arrangera övningar med fokus på totalförsvarets behov förefaller som en fungerande metod, inte minst med tanke på de effekter detta får för framtida samverkan, men ytterligare forskning som styrker detta är nödvändig.

Andra viktiga forskningsfrågor inom området är teknik- och metodutveckling i cyberanläggningar, metoder för att öka övningsvolymen samt hur övningar kan användas för att ta fram nya data. Internationella exempel visar också att en nationell cyberanläggning kan användas för att bidra till kompetensförsörjningen på längre sikt genom att låta högre lärosäten nyttja den i forskning och utbildning.

Genom att adressera utmaningarna med att tillhandahålla övningsmiljöer, skapa en ökad övningsvolym och en kunskapsuppbyggnad kring dessa genom forskning kan Sveriges cyberförsvarsförmåga,

och därmed vår totalförsvarsförmåga, utvecklas för att möta framtidens behov.

För vidare läsning

Mikael Wedlin och Erik Westring, Internet som militär arena, *Strategisk utblick 7*, 2017, FOI-R--4454--SE.

Ann-Sofie Stenérus Dover och Camilla Trané, *NCS3-studie: Påverkan på organisationers säkerhetsarbete av kursverksamhet inom området säkerhet i industriella informations- och styrsystem*, 2016, FOI Memo 5920.

11. Antagonistiska elektromagnetiska hot mot det civila försvaret

Sten E Nyholm, Tomas Hurtig, Kia Wiklundh och Sara Linder

Flera samhällsviktiga verksamheter förlitar sig idag på elektroniska styrsystem och trådlösa kommunikationssystem, som GPS, mobiltelefoni och WiFi. Många talar idag om cyberhot mot mjukvaran i datoriserade system, men man får inte glömma bort hårdvaran eftersom trådlösa kommunikationssystem och oskyddad elektronik även kan vara känsliga för elektromagnetiska (EM) hot, såsom störsändare och mikrovågsvapen. Avsiktliga EM-störningar utgör ett hot mot det civila försvarets förmåga att stödja det militära försvaret. Det är därför viktigt att EM-hot beaktas i de risk- och sårbarhetsanalyser som görs av bland annat myndigheter, kommuner och privata aktörer med uppgifter inom det civila försvaret, speciellt avseende operativ förmåga vid höjd beredskap.

Ett EM-hotscenario

Föreställ dig följande: De senaste månaderna har kännetecknats av en tilltagande internationell spänning och ett ökande antal konfrontationer mellan militära fartyg och flyg i Östersjöområdet. Många servrar vid myndigheter, nyhetsbyråer och företag utsätts för avancerade cyberattacker, och falsk information sprids dagligen i sociala medier. Regeringen överväger att mobilisera totalförsvaret för att hantera situationen.

I detta läge utsätts ett större antal viktiga apparater, som datorservrar och trådlös kommunikation, i olika samhällssystem för EM-störningar och några upphör helt att fungera. Blåljusmyndigheternas kommunikationscentraler tappar kontakten med enheter ute på fältet. Passage- och larmsystem vid flera kraftverk och myndighetsbyggnader fungerar inte. Störningar i eldistributionen gör att reservkraftanläggningar vid sjukhus och larmcentraler startar. Det blir trafikkaos i storstäderna när trafikljusen i flera korsningar slocknar. Tåg blir stående på linjerna när signalsystem eller elförsörjning faller bort. Fasta telefoner och mobiltelefoner fungerar bara sporadiskt. Vattenförsörjningen i storstäderna fallerar eftersom pumparna inte har elkraft. Invånarna kan inte handla mat eller tanka bilar eftersom elektroniska betaltjänster upphört att fungera. Allmänheten kan inte ta emot några radio- eller TV-sändningar för att få veta vad som hänt eller vad man ska göra. Transporter av sådant som livsmedel och bränsle med mera

försvåras kraftigt vilket leder till att matbrist uppstår och fordon blir stående.

Vad har hänt? Det visar sig så småningom att det finns ett stort antal störsändare utplacerade i bland annat bilar, väskor och barnvagnar i närheten av kommunikationscentraler, myndighetsbyggnader och kopplingsstationer för el- och telenäten. Störsändare på obemannade flygande farkoster som cirkulerar över större städer och flygplatser slår ut all trådlös kommunikation. Dessutom har elektroniska komponenter inuti viktiga apparater bränts sönder i radio- och TV-sändare, i styrutrustningen till ställverk och i vissa myndighetsbyggnader.

Hur sker en elektromagnetisk attack?

En elektromagnetisk attack åstadkoms med utrustningar som sänder ut elektromagnetisk strålning på radiofrekvenser, vilka i sin enklaste form kan exempelvis vara en vanlig radiosändare eller en mobiltelefon. Attacken kan ske med smalbandig radiostrålning av endast en eller ett fåtal frekvenser, eller med bredbandig strålning som täcker alla frekvenser inom ett brett frekvensintervall.

En enkel metod är att använda störsändare som sänder ut ohörbart EM-brus. Det gör att datakommunikation, så kallade nyttosignaler, drunknar i bruset och den trådlösa kommunikationen på en eller flera frekvenser slutar att fungera eller försämras. Den kraftfullare strålningen från mikrovågsvapen kan störa funktionen i enskilda elektroniska komponenter, som transistorer eller mikroprocessorer, antingen så att de temporärt förlorar sin funktion eller fungerar på fel sätt, eller så att komponenter bränns sönder av en inducerad strömrusning i kretsarna. En skillnad mellan dessa verkansformer är att störsändare främst påverkar trådlös kommunikation, medan mikrovågsvapen kan påverka all elektronik, även icke-kommunicerande sådan. Gemensamt för dem är att de verkar lokalt inom sin räckvidd, vilken kan variera från några få meter till flera kilometer.

EM-attacker slår direkt mot hårdvaran i elektroniska system, och skiljer sig därigenom från cyberhot, som slår mot mjukvara i kommunicerande digitala system. Vissa tekniska system kan vara beroende av ett system som slås ut av en EM-attack, vilket kan vara mycket allvarligt och leda till kaskadeffekter som sprider sig i samhället. Till exempel slås vattenförsörjning och trafiksignaler ut om elförsörjningen upphör. Därför bör man vara särskilt uppmärksam på eventuella beroenden mellan olika samhällsviktiga system.

Bland potentiella antagonister som kan tänkas använda EM-hot finns främmande makt, terrorister och kriminella. Vid en militär konflikt är ett civilsamhälle som för sina viktigaste

funktioner enbart förlitar sig på trådlös kommunikation och satellitbaserade navigeringssystem, som exempelvis GPS och den europeiska motsvarigheten Galileo, mycket sårbart för moderna telekrigsattacker. Med införandet av *Internet of Things* (IoT), det vill säga att fler saker kopplas upp mot internet, kommer denna sårbarhet sannolikt att öka ytterligare.

Samhällets ökande beroende av elektronik och kommunikation

Scenariot ovan skulle kunna inträffa eftersom alla samhällssektorer de senaste decennierna har genomgått en snabb utbyggnad av elektronisk utrustning för styrning av olika funktioner, databearbetning och kommunikation. Parallellt med detta har det tagits fram avancerade, kommersiellt tillgängliga, störsändare med kapacitet att störa flera olika frekvensband samtidigt (även om dessa är olagliga att inneha). I flera länder utvecklas militära mikrovågsvapen som kan störa eller fysiskt förstöra elektronik. Under det kalla kriget var dessa hot mot det civila försvaret inte lika påtagliga som idag.

Militära system har oftast försetts med skydd mot dessa verkansformer, medan civil elektronik vanligen är oskyddad. Under 1900-talet växte området telekrig fram som ett medel att skaffa sig informationsöverläge under militära konflikter. Detta består av elektronisk spaning (att man avlyssnar motståndarens signaler, såväl kommunikation som oavsiktliga signaler från utrustning), elektronisk attack (att man genom att sända ut elektromagnetisk energi stör eller förvillar motståndarens elektroniska apparatur) samt elektroniskt skydd (att man vidtar åtgärder för att minska effekterna av motståndarens telekrigföringsoperationer). Det militära försvaret har sedan decennier utvecklat metoder och teknik för att hantera telekrig, inte minst för att skydda egna viktiga elektroniska system och stödfunktioner.

Den snabba elektronikutvecklingen de senaste decennierna, med en enorm ökning av datorstyrning och trådlös kommunikation såväl mellan människor som mellan maskiner, har inneburit att många samhällsfunktioner kommit att basera sin funktion på denna teknologi. Exempel är styrning av industriella processer eller samhällsinfrastruktur via trådlösa nätverk, kontroll av behörighet vid inpassering till viktiga anläggningar, utfärdande av varningar via radio och sms, betalsystem, med mera. Digitaliseringen av samhället fortgår inom alla sektorer, även samhällsviktiga tjänster. Det innebär att samhället blir allt mer beroende av att elektroniken fungerar samtidigt som man hittills inte har haft några incitament att införa skydd mot antagonistiska EM-störningar. Kanske saknas medvetenhet om sådana hot mot de egna systemen, eller så har man inte bedömt dem som särskilt

allvarliga eller sannolika, och därför valt de kortsiktigt mest ekonomiska lösningarna vid anskaffning och installation. All kommersiell elektronik ska uppfylla svenska och internationella standarder vad gäller tålighet mot oavsiktliga störningar, som kan vara naturliga eller orsakade av andra apparater i närheten. Men dessa störnivåer ligger långt under vad som är möjligt att åstadkomma med avsiktliga EM-hot. För militära system ställs hårdare krav på tålighet mot störningar vilket ger ett betydligt bättre skydd men till en ökad kostnad.

Det händer ibland att elektronisk utrustning störs ut av naturliga fenomen, som åska och solstormar, eller oavsiktligt av andra elektroniska apparater i närheten. Men även kunniga privatpersoner kan störa samhällsfunktioner; exempelvis utsattes polisens radiokommunikation för störningar och falska meddelanden vid Göteborgskravallerna 2001. Sådana störformer är blygsamma jämfört med militär telekrigförmåga i en konfliktsituation. Det har även förekommit uppgifter om att mobiltelefoni och GPS har störts som en del av den ryska informationskrigföringen vid konflikterna i Ukraina och Syrien.

Totalförsvarstanken är idag central för att förbereda det svenska samhället inför många olika typer av hot. Ett sammanhållet totalförsvar innebär att civila aktörer måste överväga samma skyddsnivåer som Försvarsmakten. Idag finns begränsad medvetenhet och sparsamt med EM-skydd inom den civila sektorn medan Försvarsmakten sedan länge har tagit höjd för detta. Det är angeläget att inom civila samhällssektorer öka medvetenheten om bland annat antagonistiska EM-hot, så att man kan skydda de samhällsviktiga system som kommer att behövas vid höjd beredskap.

Hur kan man reducera sårbarheter för elektromagnetiska hot?

Uppbyggnaden av det nya totalförsvaret innebär att många myndigheter kan möta skärpta krav på robusthet mot fler typer av avsiktliga och oavsiktliga störningar, däribland antagonistiska EM-hot. Samtidigt skapar den pågående digitaliseringen av samhället nya risker för olika typer av elektromagnetisk påverkan. Om totalförsvaret inte har detta i åtanke finns risken att man inte upptäcker eller åtgärdar sårbarheter. Vid eventuell nyanskaffning av utrustning är det ofta enklare och billigare att vidta skyddsåtgärder vid installationen i stället för att göra detta i efterhand.

Ansvariga för samhällsviktiga civila verksamheter har vanligen inte samma kännedom om EM-hot och skyddsåtgärder som finns inom den militära sektorn. Medvetenheten om de EM-hot som

finns idag behöver öka för att kunna ta itu med dessa i risk- och sårbarhetsanalyser och för att kunna åtgärda identifierade kritiska svagheter.

Trådlös kommunikation är mycket svårare att skydda än ledningsbunden, som går i metalledningar eller optiska fibrer. Därför bör trådlösa kommunikationslösningar för samhällsviktiga funktioner göras tåliga mot störningar eller ha redundans. Detta kan realiseras på olika sätt. Exempelvis kan det ske med kommunikationssystem som byter frekvens antingen regelbundet eller vid störning. Tåligheten ökar med flera antenner placerade på olika platser, flera kommunikationssystem som använder olika frekvensområden eller genom att trådlösa kommunikationssystem kompletteras med fiberlösningar där så är möjligt.

Det är inte en trivial uppgift att utforma ett fullgott skydd mot oönskad elektromagnetisk strålning. Det finns ett flertal strategier för att skydda elektronisk utrustning mot EM-hot. Beroende på hur kritisk utrustningen är och vilken skyddsnivå man väljer kan skyddet konstrueras på olika sätt. När det gäller antagonistiska EM-hot mot verksamhetskritiska system finns dock några generella råd som kan ges:

- Sprid inte information i onödan om kritiska system och hur de fungerar, var utrustning finns och vilka frekvenser som används. Fienden kan utnyttja det vid ett angrepp
- Använd helst inte trådlös kommunikation mellan kritiska system utan hellre ledningsbunden kommunikation som är avsevärt mindre störningskänslig. Alternativt bör man använda utrustning med skydd mot telekrig eller ha redundanta system.
- Se till att det inte går att komma nära inpå kritiska system eftersom effekten avtar med avståndet mellan strålkälla och mål. Det lönar sig att flytta ut avspärrningar för att förhindra obehöriga med störutrustning att komma nära en kritisk anläggning.

Att säkra tillgången på reservdelar och se till att man har tillgång till snabb service eller reparation om systemet har blivit utsatt för en EM-attack är också en god strategi för att minimera störningar i elektroniska samhällsfunktioner. Man kan även behöva bygga in verksamhetskritisk utrustning i skyddande skal och montera skyddskomponenter eller olika typer av filter på ledningar.

Det är dock viktigt att inse att det inte går att skydda all kommunikation och elektronisk utrustning mot EM-hot. Man bör prioritera de system som har en kritisk funktion, det vill säga vilkas bortfall skulle leda till stora störningar i viktiga funktioner.

För att åstadkomma detta bör man regelbundet genomföra risk- och sårbarhetsanalyser där man inkluderar de risker som EM-hot kan medföra för verksamheten. Det är alltid en avvägningsfråga vilka sårbarheter som ska åtgärdas och vilken skyddsnivå som krävs för att erhålla den robusthet som behövs för att en verksamhet ska kunna fungera om den utsätts för EM-angrepp i en allvarlig krissituation.

Ett första steg när det gäller att skydda kommunikationslösningar och elektronisk utrustning är att skaffa sig kunskap om vilka EM-hot som finns och hur man tar med dessa i en risk- och sårbarhetsanalys bland alla andra typer av hot som man har identifierat. Nästa steg är att bestämma om man har tillräcklig kunskap inom verksamheten för att genomföra en risk- och sårbarhetsanalys och åtgärda identifierade brister eller om man behöver anlita extern expertis. Slutligen gäller det att genomföra analysen, vidta lämpliga skyddsåtgärder, verifiera att dessa har gett önskad effekt, och därefter regelbundet tillse att skyddet bibehålls. Glöm inte bort hårdvaran!

För vidare läsning

Tomas Hurtig, Sara Linder, Kia Wiklundh, Karina Fors och Sten E. Nyholm, I*ntroduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur*, FOI-S--5835--SE, MSB1180 - februari 2018.

Kia Wiklundh, Sara Linder, Karina Fors, Tomas Hurtig, och Sten E. Nyholm, *Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur*, FOI-S--5840--SE, MSB1178 - februari 2018.

Sten E. Nyholm, Tomas Hurtig, Sara Linder, Kia Wiklundh och Karina Fors, *Genomförande av huvudstudie rörande antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur*, FOI-S--5842--SE, MSB1179 – februari 2018.

12. Artificiell intelligens – möjligheter och utmaningar för Sveriges nationella säkerhet

Christer Andersson, Tove Gustavi och Maja Karasalo

Artificiell intelligens (AI) antas av många få en betydande påverkan på samhällsutvecklingen under de kommande åren. AI kommer att tillämpas i många olika tekniska system vilket innebär att AI också kommer att påverka vitala delar av den svenska försvarsförmågan och den nationella säkerheten i bred bemärkelse. Frågan är om svenska myndigheter, och samhället i stort, är förberett för att nyttja de möjligheter som tekniken erbjuder och – inte minst – möta de utmaningar och hot som ett nytt säkerhetspolitiskt landskap med AI medför?

Artificiell intelligens - ett omtvistat begrepp

En del menar att Artificiell Intelligens (AI) handlar om att få datorer att imitera mänskligt beteende. Andra anser att det istället handlar om att skapa datorsystem som, till skillnad från människan, resonerar och beter sig ”rationellt” i alla situationer. Det finns ingen allmänt vedertagen definition av AI, men generellt refererar begreppet till förmågan hos ett datorsystem att i något rimligt avseende resonera eller agera korrekt utifrån tillgänglig information och tidigare erfarenheter.

Rent tekniskt skapas AI genom att information hanteras med matematiska metoder och logik. AI baseras alltså inte på en specifik teknik utan det kan handla om olika typer av maskininlärning, men även exempelvis statistiska metoder. Maskininlärning kan beskrivas som metoder som använder tillgänglig information för att träna och förbättra matematiska modeller av omvärlden. Modellerna används för att tolka och analysera omvärlden. Ju mer information som finns tillgänglig för träning, desto mer exakta modeller och bättre analysresultat kan förväntas.

Den uppmärksamhet som AI har fått de senaste åren följer av att vissa centrala tekniker har nått en sådan mognadsgrad och tillförlitlighet att de kan byggas in i produkter och användas i samhället. För maskininlärning i synnerhet hänger teknik-mognaden till stor del ihop med utvecklingen av kraftfulla datorer, samt med digitaliseringen av samhället vilket har gjort att stora mängder data har blivit allmänt tillgängliga. Dessa förutsättningar har bidragit till en utveckling av algoritmer och metoder som inte tidigare har varit möjlig.

AI är ett område som inte har några tydliga gränser mellan civila och militära tillämpningar. Ett tekniskt system som har tagits fram för att identifiera cancerceller i mikroskop kan i princip också läras att hitta bombmål i satellitbilder. Mycket av den framtagna tekniken finns fritt tillgänglig, vilket innebär att det är svårt att överblicka vilka aktörer som använder sig av den och för vilka syften. Tillgängligheten och de dubbla användningsområdena medför både för- och nackdelar ur ett nationellt säkerhetsperspektiv.

Möjligheter och utmaningar med AI i totalförsvaret

Rapporteringen om den praktiska militära användningen av AI kännetecknas av teknikoptimism, där olika tillämpningar av AI-metoder beskrivs med lyckade resultat, men också av oro för vad utvecklingen mot mer självständiga tekniska system kan innebära.

För Sveriges totalförsvar kan AI-metoder medföra förbättringar ur flera aspekter. För Försvarsmakten kan AI-system bidra till militära operativa och taktiska fördelar. För den administrativa verksamheten i både civila och militära delar av totalförsvaret kan till exempel effektiviseringar åstadkommas genom automatisering av olika arbetsuppgifter.

Tillämpningar av AI

I dagens väpnade konflikter har konventionell militär krigföring ofta inslag av hybridkrigföring, såsom IT-attacker eller propagandakampanjer på sociala media. Analys av stora mängder data från olika domäner blir därmed nödvändig för att upprätthålla en korrekt lägesbild. Användning av AI kan mot bakgrund av detta ge avsevärda fördelar. Bearbetning av sensordata och analys av underrättelser är två områden där AI-tekniken tack vare sin förmåga att snabbt klassificera och hitta mönster i stora mängder data lämpar sig väl.

I militära sensorsystem gör AI det möjligt att samtidigt och på ett integrerat sätt analysera olika typer av sensordata, till exempel radarsignaler och sonardata, och att med hög hastighet dra slutsatser. Resultaten av databehandlingen kan sedan antingen bidra till ett självständigt agerande hos AI-systemet, eller användas för att skapa beslutsunderlag och rekommendationer för mänskliga beslutsfattare. Vid strid med system i samverkan, där ett stort antal sensorer samverkar med flera olika vapensystem, kan AI-system exempelvis bidra till att leverera en uppdaterad helhetsbild av snabba skeenden. I dagens stridssituationer, där kraven på snabba beslut hela tiden ökar, kan förmågan till snabba analyser av stora datamängder vara en avgörande överlevnadsfaktor.

För underrättelsetillämpningen erbjuder AI en möjlighet att hitta det oväntade – den så kallade ”svarta svanen” – genom analys av stora mängder traditionella underrättelsedata i kombination med öppen webbdata. Den totala mängden data som produceras i dag är inte möjlig att analysera med traditionella metoder. Bearbetningen begränsas därför ofta både till mängden data och till ett känt sammanhang. Detta minskar möjligheterna till upptäckt av oförutsedda händelser. Historien har gett oss flera exempel där underrättelsearbetet inte i tid har förutsett kommande händelser, däribland Pearl Harbor och 11 september-attackerna. AI har potential att förbättra säkerhetspolitiska analyser genom att underlätta upptäckten av såväl snabba som utdragna händelseförlopp. Med AI kan mindre uppenbar eller till och med vid första påseendet irrelevant information tas med i en analys.

AI kan bli ett kraftfullt verktyg för att förbättra och utveckla förmågan hos en rad olika funktioner inom totalförsvaret. För Försvarsmakten kan AI erbjuda kvalitets- och effektivitets-förbättringar gällande både analys av sensordata och hanteringen av komplexa lednings- och underrättelseoperationer. I andra delar av totalförsvaret kan AI användas till exempel för att upptäcka avvikelser i nätverkstrafik vilka kan tyda på attacker mot kritisk infrastruktur såsom el- och vattenförsörjning. Bredden i tänkbara tillämpningar tillsammans med förbättringspotentialen gör AI-tekniken attraktiv även av ekonomiska skäl. Det krävs dock kunskap och personella resurser för att realisera möjligheterna.

Nya sårbarheter att hantera

I takt med att utvecklingen inom AI-området går framåt växer en oro i samhället för vad teknikutvecklingen medför i termer av minskad insyn i och kontroll över självstyrande och intelligenta system.

Det finns gott om exempel på hur så kallade ”intelligenta system” som vanligen ger goda resultat i vissa fall kan göra anmärkningsvärda misstag. Ett exempel är ett automatiskt system från Amazon som har utvecklats för att värdera sökande till utlysta tjänster. Systemet hade tränats i att analysera ansökningar, men efter en tids användning upptäcktes att det diskriminerade kvinnliga sökande. Anledningen till detta var helt enkelt att det fanns så få resuméer från kvinnor i de data som systemet hade tränats på, att systemet under träningen uppnådde större precision om dessa ansökningar förkastades. Det oönskade utfallet belyser en aspekt av maskininlärning som är viktig att beakta: systemets beteende kommer att styras av de data det har tränats på. Om träningsdata inte speglar den verkliga problemställningen, så kommer AI-baserade system emellanåt att göra oväntade och

ibland synnerligen olämpliga ”fel”, som i säkerhetskänsliga sammanhang kan få allvarliga konsekvenser.

Utöver denna typ av oavsiktliga misstag finns även exempel på hur AI-system kan manipuleras av fientligt sinnade aktörer. Studier har visat att med kunskap om hur en viss AI-metod fungerar kan man manipulera den så att modellen ger felaktiga svar. Exempelvis kan en, för en mänsklig betraktare, omärkbar förändring av en bild på pixelnivå få AI-systemet att tolka bildinnehåll helt fel. Det har även demonstrerats att bildigenkänningssystem avsedda att identifiera olika typer av trafikskyltar kan manipuleras att ge fel svar om en skylt har försetts med ett klistermärke på ett visst ställe. En viktig aspekt vad gäller sårbarheter är att mycket av AI-tekniken är öppet tillgänglig, vilket innebär att även terrororganisationer och kriminella grupperingar kan ha tillgång till de senaste metoderna för att utnyttja svagheter i AI-system.

Mot bakgrund av exempel som ovan pågår en debatt om de etiska aspekterna av AI-användning, som bland annat handlar om möjligheten att utkräva ansvar för beslut och handlingar utförda av AI-baserade system. En i sammanhanget central fråga är hur man ska kunna säkerställa att AI-system fungerar tillförlitligt och begripligt. Säkerhet kopplat till AI är ett växande forskningsområde som studerar frågor som exempelvis:

- Transparens – hur kan man designa intelligenta system som samtidigt är transparenta och går att förstå för en människa?
- Väldefinierade mål – hur kan man säkerställa att det mål som sätts för ett intelligent system verkligen leder till önskat resultat utan allvarliga bieffekter?
- Robusthet och stabilitet vid ändrade förutsättningar – hur kan man säkerställa att oväntade förändringar i systemets förutsättningar (strömavbrott, kommunikationsproblem med mera) inte leder till allvarliga negativa effekter?
- Hantering av sårbarheter – hur kan man skapa och träna system för att minimera risken för felbedömningar på grund av avsiktlig manipulation?

För verksamheter kopplade till försvar och säkerhet är det rimligen mer kritiskt än för andra verksamheter att de AI-system som används fungerar robust och utan negativa bieffekter. I många militära tillämpningar är det också avgörande att systemen är transparenta för att det ska vara möjligt att spåra och motivera de beslut som fattas. Då fördelarna med AI är så stora får man utgå ifrån att tekniken ändå kommer att användas både i militära system och i samhällskritiska verksamheter såsom

elkraftsdistribution, hälso- och sjukvård, och finanshandel. Det är därmed nödvändigt att det inom Sveriges totalförsvar finns kunskap om teknikens sårbarheter och en beredskap för möjliga incidenter.

Sveriges förutsättningar i en föränderlig värld

2017 genomförde Vinnova en utredning om AI:s utveckling och potential i svenskt näringsliv och samhälle. I utredningen konstateras att svensk AI-forskning i nuläget har ”begränsad internationell konkurrenskraft”. Man pekar på otillräckliga AI-investeringar i både större och mindre företag, brist på statlig styrning och på att AI-kompetens lämnar landet. Utredningen lyfter emellertid fram att Sverige har en teknikvänlig befolkning, hög teknikkompetens, ett utvecklat innovationssystem och att landet ligger långt framme med IT och digitalisering. Det finns alltså goda grundförutsättningar för Sverige att bli en större aktör inom AI.

En oroväckande slutsats i rapporten är att ”Omvärlden satsar mer och snabbare än Sverige”. På sikt kan en sådan utveckling få stora konsekvenser för den svenska industrins konkurrenskraft, men även för den nationella säkerheten. Länder som ligger i framkant på AI-området kommer bland annat att kunna skaffa sig ett informationsöverläge vilket kan förändra det säkerhetspolitiska landskapet. På den internationella arenan utmärker sig Kina med stora satsningar inom AI. Även länder som kan sägas vara mer jämförbara med Sverige satsar aktivt på AI-utveckling. Exempel på detta är Frankrike som 2018 lanserade en AI-satsning på över 15 miljarder kronor fram till 2022, och Finland som 2017 blev första land i EU att ta fram en nationell AI-strategi. I Sverige utgörs den enskilt största AI-satsningen av forskningsprogrammet *Wallenberg AI, Autonomous Systems and Software Program* (WASP), där en miljard är särskilt reserverad för AI-forskning. WASP är dock ett privat initiativ, finansierat av Knut och Alice Wallenbergs Stiftelse. Programmets inriktning kan inte förväntas täcka svenska statens intressen, utan WASP bör ses som ett komplement till statliga satsningar.

Vinnovas slutsatser bör innebära att även den svenska försvars-sektorn – myndigheter såväl som försvarsindustrin – har goda grundförutsättningar att kunna introducera mer AI-baserade system. Värt att notera i sammanhanget är att AI i kombination med annan teknik skulle kunna ha en stor påverkan på det som länge har varit en av Försvarsmaktens stora utmaningar att hantera, nämligen bevakningen av ett utsträckt och bitvis mycket glesbefolkat territorium. Inte minst den långa kustlinjen har ur försvarssynpunkt varit en utmaning. Autonoma över- och

undervattensfarkoster i kombination med intelligenta sensorsystem skulle kunna ge bättre förutsättningar för gränsbevakning.

För att totalförsvarets verksamheter ska kunna ta till sig och utnyttja AI-tekniken behövs personal med specialistkompetens, samtidigt som kunskaperna om AI generellt behöver lyftas inom organisationerna. Personer med utbildning inom området är eftertraktade på den civila marknaden och därmed svåra att rekrytera till statlig och annan offentlig verksamhet. Lyckas man inte lösa kompetensförsörjningen riskerar överföringen av AI-teknik till försvarsmyndigheter att försvåras, och kunskapsgapet mellan offentlig och civil verksamhet att öka ännu mer.

Konkurrensen om AI-kompetens pågår inte bara mellan privat och offentlig sektor utan även mellan länder. Såväl svenska företag som myndigheter konkurrerar på en global marknad, där stora löneskillnader mellan olika nationer kan leda till kunskapsflykt från de nationer som inte kan erbjuda konkurrensmässiga löner eller arbetsvillkor. För att inte Sveriges nationella säkerhet ska bli helt beroende av utländsk expertis är det viktigt att agera för att bygga upp och behålla en inhemsk kompetens inom avancerad databehandling.

AI-kompetens central för Sveriges nationella säkerhet

För att totalförsvaret ska kunna nyttja de möjligheter som AI-tekniken erbjuder och möta de utmaningar som följer med utvecklingen, är det angeläget att kunskapen om AI ökar inom berörda organisationer. Att säkerställa kompetensförsörjningen inom ett område som utvecklas snabbt, och som i hög grad är utsatt för internationell konkurrens, är en stor men viktig utmaning för Sverige. En annan stor utmaning för totalförsvaret och samhället i stort är att lära sig hantera de nya sårbarheter som AI medför. Sverige har goda grundförutsättningar att ta sig an dessa utmaningar, men att i för stor utsträckning förlita sig på att industrin och privata forskningsinitiativ ska ta ansvar för frågor av nationellt intresse är riskabelt.

För vidare läsning

Tove Gustavi, Jörgen Karlholm, Daniel Oskarsson, Tam Beran, Oscar Björnham, Erik Gudmundson, Hugo Heden, Henrik Karlzén, Johannes Lindblom, Jonas Nordlöf, Ioana Rodhe, Theodor Sommestad, Peter Svenmarck och Markus Svensson, *Försvarsnära tillämpningar av Artificiell Intelligens*, 2019, FOI-R--4707--SE.

Joel Brynielsson, Martin Nilsson, Johan Schubert, Peter Svenmarck, *Artificiell intelligens för beslutsstöd i ledningssystem*, 2018, FOI-R--4678--SE.

Johan Schubert, *Artificiell Intelligens för Militärt Beslutsstöd*, 2017, FOI-R--4552--SE.

13. Fejkade nyhetsbilder och verklig motståndskraft

Niclas Wadströmer, David Gustafsson och Patrik Thunholm

Främmande makt kan idag skapa och sprida virtuella bilder och filmsekvenser som belägg för fejkade nyheter, bilder som är svåra att skilja från foton av verkligheten. Framstegen inom artificiell intelligens har gjort att nära på vem som helst med en persondator kan skapa skenbart verkliga filmsekvenser. Dessutom har den digitala informationsmiljön förändrat medielandskapet och förutsättningarna för att kunna sprida information. Detta är en ny utmaning för totalförsvaret i arbetet med att motarbeta främmande makts möjligheter att bedriva informationspåverkan. Samtidigt ska totalförsvaret värna den fria åsiktsbildningen som är grunden för det demokratiska samhället.

Informationspåverkan

Föreställ dig att det dyker upp ett videoklipp i ditt flöde på sociala medier från en presskonferens med en makthavare som redogör för en allvarlig händelse. Klippet har redan delats tusentals gånger innan det når ett mediehus som börjar undersöka dess sanningshalt. En nyhetsreporter får kontakt med makthavaren som med bestämdhet förnekar att presskonferensen ens har ägt rum. Reportern menar att bild och ljud i videoklippet är bevis för att presskonferensen har ägt rum och undrar varför makthavaren förnekar framträdandet. Makthavaren får också frågor om hur det kommer sig att klippet har delats i hens sociala medier och att budskapet dessutom har spridits med dennes officiella e-postadress. Förvirringen är total. Efter en tid står det klart att det viralt spridda nyhetsklippet är fejkat och att makthavarens digitala kommunikationsvägar har utnyttjats för att förstärka vilseledningen. Ändå fortsätter spekulationerna i sociala medier om videoklippets sanningshalt. Går det grävande mediehuset verkligen att lita på? Långt senare avslöjas att den som producerat den fejkade videon och hackat kontona har velat minska den allmänna tilltron till nyhetsförmedling genom att grumla bilden av vad som är verkligt och vad som är fejkat.

Ovanstående scenario illustrerar hur Sverige skulle kunna påverkas och manipuleras eller utsättas för kognitiva påfrestningar, av en enskild aktör men också av en främmande makt, utan att landet befinner sig i krig.

På Youtube publiceras dagligen runt hundratusen videoklipp. Bland dessa finns många exempel på att man både kan manipulera verkliga foton och filmer, och kan skapa foton och filmer som ser

verkliga ut men som är helt datorgenererade. Bland dessa finns ett videoklipp med en datorgenererad nyhetsuppläsare som knappt går att skilja från en verklig person. Ett annat exempel är en video med vad som förefaller vara den förre amerikanske presidenten Barack Obama som gör ett oväntat uttalande. I det fallet har någon läst in en text, gjort om ljudet så att det låter som Barack Obama och ändrat ansiktsrörelserna i en redan existerande film med den före detta presidenten så att de stämmer med det inlästa talet.

Forskare på företaget Nvidia har samlat in många tusentals porträttbilder från internet och använt maskininlärning för att skapa ett program som kan generera högupplösta porträttbilder som ser ut att vara foton av verkliga personer men där ingen av personerna finns i verkligheten. Dessa videoklipp är resultatet av de senaste årens framsteg inom artificiell intelligens (AI), vilka har gjort det möjligt att producera rörlig media där valfritt budskap kan framföras av valfri person på valfri plats.

Manipulerade bilder

Det finns många historiska exempel på manipulerade bilder av verkligheten. Man har länge kunnat retuschera fotografier även om det har krävts skickliga konstnärer för att kunna göra retuscheringen trovärdig.

Filmbranschen har länge kunnat göra tecknade animerade filmer och med datorns intåg har dessa blivit allt mer verklighetstrogna. Nu finns exempel på spelfilmer där man har skapat virtuella bilder av personer som inte vill eller kan vara med vid inspelningen.

Virtuella bilder är bilder som ger sken av att vara fotografiska avbildningar av verkligheten men som helt eller delvis är skapade i en dator. Bilden ser ut att visa något som finns i verkligheten men är en chimär skapad i en dator och det är svårt att skilja dessa skapade virtuella bilder från fotografiska bilder av verkligheten.

Det krävs fortfarande stor kompetens och stora resurser för att göra spelfilmer med datorgenererade personer. Men teknik för att skapa och manipulera bilder med ansikten blir samtidigt allt mer lättillgänglig. Nu kan man enkelt ladda ner en applikation som kan byta ut ett ansikte mot ett annat. Det räcker med en vanlig persondator och kräver inte särskilt djupa kunskaper för att med överraskande god kvalitet lyckas.

Förändrat medielandskap

Den digitala informationsmiljön har blivit en viktig arena för krigföring. Gamla föreställningar om att krig utspelas mellan arméer på ett slagfält har minskat i relevans och en viktig uppgift för det psykologiska försvaret är att kunna identifiera, analysera

och möta påverkanskampanjer från främmande makt. För att lyckas med detta uppdrag krävs bland annat kunskap om vad som är möjligt att göra med modern teknik.

En majoritet av svenskarna är dagligen uppkopplade och med stöd av mobilteknik som smarta telefoner har medievanorna genomgått stora förändringar. Vi kan numera röra oss mellan en traditionell roll som tittare, lyssnare och läsare, till en mer aktiv roll där vi själva producerar och distribuerar innehåll. Denna utveckling har samtidigt gjort det enklare för främmande makt att använda nya psykologiska tekniker för att påverka våra uppfattningar, inställningar och uppträdande i syfte att nå specifika målsättningar. Målsättningarna skulle kunna handla om att påverka den allmänna opinionen och det demokratiska beslutsfattandet genom att underminera beslutsförmåga eller manipulera uppfattningar.

I de fall en främmande makt vill förstärka sin egen position och samtidigt försvaga Sverige och svenska intressen kan denna tänkas sprida information av varierande sanningshalt i informationsmiljön. Det kan handla om händelser som aldrig har inträffat, till exempel övergrepp och misshandel i kända miljöer eller polisbrutalitet mot minoriteter – allt i syfte att göda polarisering och splittra ett land inifrån. Gemensamt för dessa hot är dels att de riktas mot eller utnyttjar värden som är sårbara till sin natur, såsom demokrati och yttrandefrihet, dels att antagonisterna ofta använder ny teknik.

Den nya tekniken gör det möjligt att enkelt producera fejkade nyhetsbilder som sedan kan vara svåra eller omöjliga att spåra tillbaka till den som har skapat dem. Det kan till exempel handla om anonym spridning över internet eller att spridningen sker med hjälp av en kapad digital identitet. Sammantaget är möjligheten till förnekbarhet hög. Den senaste tidens utveckling av maskininlärning har bidragit till att rörliga bilder nu måste betraktas med skepsis. I framtiden kommer uttrycket ”att lägga orden i någons mun” att få en mer bokstavlig mening.

Maskininlärning

Maskininlärning, ett delområde inom artificiell intelligens, har tagit rejäla kliv framåt med artificiella neurala nätverk (ANN). ANN är en struktur för datorprogram som har inspirerats av biologiska hjärnor. ANN lär sig från många exempel av in- och utdata istället för att programmeras med explicita regler för hur utdata fås från indata. *Deep learning* är ANN som har förmåga att representera information i hierarkiska nivåer. Google, Amazon, Facebook och andra aktörer med tillgång till mycket stora mängder bilder med vidhängande bildtexter kan lära sina datorer att inte

bara förstå bilders innehåll utan också att redigera och skapa virtuella bilder. Det går att automatiskt ändra en landskapsbild från vinter till sommar. Man kan göra om en ritad skiss till en bild som ser ut att vara en fotografisk bild av ett verkligt landskap. Det går att byta ut ett ansikte, lägga till och ta bort en person. Man kan skapa syntetisk film där en person framträder som är mycket svår att skilja från en autentisk film.

Maskininlärning innebär att man låter en maskin lära sig från exempel. Säg att man vill skapa ett program som skapar porträttbilder. Man ger då datorn ett stort antal exempel på porträttbilder och låter maskinen hitta särdrag som är typiska för porträttbilder och sedan kan maskinen skapa slumpmässiga bilder med dessa särdrag. Innan det fanns maskininlärning hade en ingenjör fått ta reda på särdrag som är typiska för porträttbilder och skriva ett program som skapar slumpmässiga bilder med de givna särdragen. Med moderna maskininlärningsalgoritmer är datorn i många fall bättre än ingenjören på att hitta relevanta särdrag.

Generativa metoder ger verkligare bilder

Generativa metoder kan skapa syntetiska bilder, text och ljud, det vill säga saker som är helt och hållet skapade i datorn, utan en verklig förlaga. År 2014 introducerades *Generative adverserial networks* (GAN), en ny generativ metod, som medförde ett genombrott inom generering av verklighetstrogna bilder. GAN är en vidareutveckling av *Deep learning* som har fått en mycket stor spridning inom AI. GAN tränas genom motvalls träning. Två olika nätverk tävlar mot varandra – ett generativt nätverk genererar bilder av en bestämd sort och ett klassificeringsnätverk lär sig att särskilja riktiga bilder från genererade bilder. Det generativa nätverket förbättras genom att beakta egenskaper i de genererade bilderna som klassificeringsnätverket använder för att särskilja de genererade bilderna från verkliga bilder. Klassificeringsnätverket fungerar som sparringpartner till det generativa nätverket och genom en iterativ process blir de båda allt bättre. Resultatet är att det genereras bilder som blir allt svårare att separera från de verkliga bilderna. I många fall lyckas GAN-nätverket skapa bilder som en lekman inte kan särskilja från riktiga fotografiska bilder och som kan vara svåra för expertis att särskilja.

Den här förmågan blir allt mer tillgänglig och lättanvänd. Man kan hämta programkod på internet och det behövs inte någon avancerad kunskap för att använda den. I många fall finns det program och färdigtränade modeller för generering av olika typer av bilder eller filmer fritt tillgängliga för nerladdning från internet. Där det tidigare krävdes mycket stora resurser, som bara stater har, för att skapa material av det här slaget till

påverkanskampanjer räcker det idag med en liten grupp personer. Det är också värt att notera att det är privata företag som har publicerat de bästa forskningsresultaten. Här saknas det insyn i vilken förmåga företagen har och vad de väljer att hålla hemligt och för vilka syften de använder tekniken.

Totalförsvaret

I denna nya tekniska och digitala miljö återstartar Sverige totalförsvaret. Liksom under det kalla kriget är ett psykologiskt försvar och motståndskraft mot samhällshotande informationspåverkan en förutsättning för att totalförsvaret ska fungera. Utan samhällelig motivation fungerar ingen del av totalförsvaret – inte heller Försvarsmakten. Betydelsen av psykologiska försvarsåtgärder har ökat i jämförelse med det kalla kriget. Detta eftersom en fientlig statlig aktör nu kan uppnå mål som förr krävde en militär operation, genom att bland mycket annat använda sig av påverkan inom den digitala informationsmiljön. Mot denna bakgrund är det viktigt att totalförsvarets psykologiska delar följer teknikutvecklingen och tar fram metoder som ger verklig motståndskraft mot den som vill skada oss med falska bilder.

En motståndare som ägnar sig åt informationspåverkan ser till att identifiera och utnyttja sårbarheter systematiskt. Sårbarheter finns inom flera olika områden. Det moderna mediesystemet har flera sårbarheter i förhållande till bland annat ny teknik, nya journalistiska affärsmodeller och en tilltagande mängd nyhetskällor på nätet. Även opinionsbildningen har blivit mer sårbar i takt med den digitala informationsmiljöns framväxt. Med internets tillkomst är det lättare än någonsin att fabricera sociala bevis och att väcka ilska, provocera eller uppröra. Kognitiva sårbarheter kan uppstå till följd av att den mänskliga hjärnan tenderar att ta genvägar och inte är konstruerad för att hantera all den mängd information den ibland utsätts för. Här kan informationspåverkan utnyttja tankemönster och information om oss för att påverka uppfattningar, beteende och beslutsfattande.

Verklig motståndskraft

Totalförsvaret ska skydda grundläggande värden som vår demokrati och vårt självbestämmande mot angrepp från främmande makt som vill skada oss. Sveriges motståndskraft mot dessa hot är avhängig av hur digitalt kompetent, tekniskt kunnigt och snabbfotat det psykologiska försvaret är. Detta kommer att ställa krav inte bara på myndigheter, utan också på medborgare, politiker och teknikleverantörer.

Verklig motståndskraft får vi ytterst genom att var och en har ett kritiskt förhållningssätt till bilder och det som bilden säger. Det

behövs dessutom en allmänt ökad kunskap om vilka möjligheter som finns att manipulera och förfalska bilder. Utöver detta krävs forskning om forensiska metoder för att avslöja fejkade bilder och system för att ursprungsmärka bilder så att den som tar del av en bild kan veta vem som är avsändare och upphovsman.

För vidare läsning

Niklas H. Rossbach, Psykologiskt försvar - avgörande för svensk försvarsförmåga, *Strategisk utblick 7*, 2017, FOI-R--4454--SE.

Tove Gustavi, Jörgen Karlholm, Daniel Oskarsson, Tam Beran, Oscar Björnham, Erik Gudmundson, Hugo Heden, Henrik Karlzén, Johannes Lindblom, Jonas Nordlöf, Ioana Rodhe, Teodor Sommestad, Peter Svenmarck och Markus Svensson, *Försvarsnära tillämpningar av Artificiell Intelligens*, 2019, FOI-R--4707--SE.

14. Så kan vi skydda Sveriges säkerhetskänsliga it-tjänster

Anders Elfving och Anton Dahlmark, Fortifikationsverket

En väsentlig del av uppbyggnaden av den svenska totalförsvarsförmågan handlar om skydd av samhällsviktig verksamhet. Det finns därför anledning att se över myndigheternas samlade behov av fysiskt skyddade datacenter för säkerhetskänslig it-verksamhet. Höga krav på exempelvis fysiskt skydd mot vapenverkan och tillgänglighet för it-miljöns försörjningssystem leder dock till ökade kostnader och längre produktionstid. Ombyggnation av befintliga anläggningar måste även vägas mot att bygga nytt. Det förändrade omvärldsläget och insikten kring sårbarheten hos vårt digitaliserade samhälle gör att en nationell satsning inom området är en för samhället och totalförsvaret betydande men nödvändig investering.

Digitaliseringens framfart för med sig sårbarheter

Det har knappast undgått någon hur digitaliseringen av vår vardag har förenklat våra liv och förändrat vårt beteende. De stora mängderna data som genereras processas ofta i molntjänster och lagras över tid i serverhallar. Man tar i regel för givet att dessa tjänster fungerar utan avbrott dygnet runt. Debatten om vår ökade sårbarhet genom den digitala revolutionen pågår med ökad insikt om hur stora konsekvenserna blir vid eventuella störningar, som attacker eller elavbrott.

Medan it-säkerhet numera står högt på agendan hos svenska myndigheter har även det fysiska skyddet av statliga it-tjänster pekats ut som ett mycket viktigt område att se över för att stärka totalförsvaret. 2017 fick Post- och telestyrelsen i uppdrag av regeringen att utarbeta ett förslag till en nationell förvaltningsmodell för skyddade it-utrymmen, vilket i branschen kallas för datacenter. Det är långt ifrån all data som kräver ett förstärkt fysiskt skydd, men delar av den är säkerhetskänslig och behöver skyddas mot både intrång och militära angrepp.

Datacenter i befintliga eller nya anläggningar?

Ett skyddat it-utrymme kan ligga i en skyddad anläggning i berg eller i en säker byggnad ovan mark. En anläggning i berg har de fysiska barriärer som skyddar mot effekterna av vapen men även skydd av datacentrets funktioner och försörjningssystem, ett så kallat fortifikatoriskt skydd. En säker byggnad ovan mark utformas med säkerhetshöjande åtgärder för att förhindra eller försvåra skadeverkan på dess funktioner men har inte samma fortifikatoriska skydd som en berganläggning. Den period vi har

bakom oss med ett stabilt omvärldsläge och besparingar inom försvaret har lett till att skyddade objekt som till exempel bergrum har frigjorts. Därför har myndigheter på senare år ställt frågan om dessa skulle kunna användas för skyddade it-utrymmen eller om det är mer lämpligt att bygga nya anläggningar.

En vanlig uppfattning är att etablering av skyddade it-utrymmen i bergrum är enkla att genomföra. Argumenten brukar handla om:

- att det finns ett stort antal tomma bergrum som efter smärre ombyggnader och till låg kostnad borde kunna användas som it-utrymmen
- att bergrum per automatik innebär ett skydd mot alla förekommande effekter och nivåer av vapenverkan
- att ett bergrum, med bibehållet fortifikatoriskt skydd, enkelt kan anpassas för it-utrymmen på tio megawatt (MW) effekt eller mer, vilket motsvarar elproduktionen från ungefär sex vindkraftverk eller effektåtgången för över 4000 villor
- att bergrum finns inom ett avstånd av 15 till 20 km från nuvarande verksamhets geografiska placering
- att etablering i bergrum går snabbt att genomföra.

Förutom ovan nämnda förväntningar finns också ofta en önskan om höga tillgänglighetsnivåer, det vill säga hur stor del av tiden som något är i drift och levererar avsedd förmåga. Redundanta system ger generellt högre tillgänglighet, men det medför ofta högre kostnader än förväntat.

Verkligheten är emellertid en annan. Det finns få tillgängliga bergrum som är lämpliga för it-utrymmen och de som finns ligger sällan nära städer. Ofta krävs ett stort saneringsbehov och omfattande investeringar innan anläggningen kan tas i bruk. Det är en stor utmaning att med bibehållet fortifikatoriskt skydd skapa en lösning för den nödvändiga kylningen av it-miljön. Trots att berget till stor del är urgrävt, tar anpassningsarbeten längre tid än man räknar med. Anskaffningstiden vid ombyggnad av en tomställd berganläggning är dock väsentligt kortare än vid nyproduktion.

Fördelen med att bygga nytt är att anpassning till it-utrymmen görs redan från början. När det gäller samordning av fysiskt skydd, byggkostnader och kostnader för driftverksamhet finns ekonomiska fördelar med att samlokalisera så att flera samhällsaktörer delar på samma fysiskt skyddade anläggning. Det finns dock även negativa konsekvenser vid samlokalisering. Om det innebär att endast ett fåtal anläggningar etableras riskerar de att

ur en angripares perspektiv ses som mer högvärdiga mål jämfört med ett stort antal utspridda angreppsmål. Konsekvenserna vid ett angrepp mot ett högvärdigt mål riskerar därför att blir större.

Strömförsörjning utan avbrott

En annan aspekt att ta hänsyn till är behovet av robust energiförsörjning. Lagring och hantering av data av väsentlig samhällsbetydelse måste ske utan avbrott i strömförsörjningen. Samtidigt är it-tjänster energiintensiva och behöver en effektiv infrastruktur för kylning. Utan kylning överhettas it-utrustning, ofta så snabbt som inom loppet av minuter, med följden att anläggningens funktioner slås ut. De stora mängderna energi som behöver forslas bort från ett it-utrymme gör att vattenkylning anses vara klart mest effektivt jämfört med luftkylning eller bergkyla. När det gäller datacenter som kräver hög energiförbrukning och är inrymda i bergrum är fysisk placering intill stora vattenreservoarer eller vattendrag därför lämpligt, vilket naturligtvis begränsar antalet möjliga platser för etablering.

Just nu ställer samhället om till fossilfri energianvändning. Samtidigt slår Svenska kraftnät fast att behovet av reservkraft ökar. Driftsäker och tillförlitlig reservkraft är helt nödvändig inom en rad samhällssektorer som är viktiga för att upprätthålla ett fungerande totalförsvar, till exempel landsting, kommuner och frivilligorganisationer. Nuvarande reservkraftförsörjning består i de flesta fall av dieselelverk som har flera begränsningar som (i) stor miljöpåverkan, (ii) svårigheter med distributionen av bränsle i en krissituation (iii) importberoende från andra länder, (iv) hög värmesignatur vid förbränning, vilket gör en anläggning lättare att upptäcka, och (v) buller.

Sammantaget finns det därför behov av att testa nya alternativa energilösningar för driftsäker reservkraft i samhällsviktiga objekt, som exempelvis framtida datacenter. Batteri- och bränslecellsteknologi är exempel på områden där det just nu sker stora framsteg som är intressanta ur ett robust samhällsperspektiv. För skyddade datacenter är det särskilt viktigt att framtidens reservkraft inte bara är robust – den ska även vara lätt att underhålla och billig i drift. Dessutom måste intagen för el- och kylförsörjning skyddas mot tryckvågen från bombangrepp, elmiljöhot (exempelvis elektromagnetisk puls och mikrovågor, *high power microwaves*), och andra hot vilket kan vara en utmaning då de ofta måste dimensioneras med en stor area.

Krav på tillgänglighet och säkerhet varierar

Samhällets grundläggande funktionalitet är sällan beroende av endast en aktörs förmåga att leverera en tjänst under svåra förhållanden. Elkraft, data- och telekommunikation, finansiella

tjänster, transporter, drivmedelsdistribution, livsmedelsförsörjning – allt hänger ihop i olika och invecklade beroenden. Om en samhällsaktörs funktion sviktar, som när en it-tjänst slås ut, kan det få konsekvenser för alla som i sin tur är beroende av att tjänsten fungerar. Samhället skulle vinna på att ha en helhetssyn på enskilda delfunktioners skyddsvärde, valda skyddsnivåer och tillgänglighet.

Hög kravställning på skydds- och tillgänglighetsnivåer är starkt kostnadsdrivande. Kostnaden för ett it-utrymme ökar snabbt med graden av tillgänglighet och kan därför leda till en mycket kostsam etablering. En rimlig utgångspunkt är att huvuddelen av den samhällsviktiga it-verksamheten har varierande krav på tillgänglighet och säkerhet och att de kan variera i fredstid såväl i kris som under krig. En djupare analys är förstås nödvändig, men ett troligt scenario är att antalet it-tjänster med höga tillgänglighetskrav är stort i fredstid och betydligt mindre under krigstid då endast de mest väsentliga funktionerna förväntas vara i drift. I fredstid är antalet it-tjänster som kräver en säker byggnad ovan jord sannolikt betydligt större än de it-tjänster som kräver en skyddad berganläggning. En förenklad beskrivning av förhållandet kan se ut som i Tabell 1.

Tabell 1. Antaget behov av antal och krav på olika it-tjänster under olika skeden.

	Fred	**Kris**	**Krig**
Hög tillgänglighet	Högre behov	Medelstort behov	Lägre behov
Säker byggnad	Högre behov	Högre behov	Medelstort behov
Skyddad anläggning	Lägre behov	Lägre behov	Lägre behov

Enligt krisberedskapens ansvarsprincip har den enskilda aktören, såsom en myndighet, samma ansvar i krig som i fred och tar själv beslut om sitt skydds- och tillgänglighetsbehov. Frågor om vilka aktörers verksamhet som ska utgöra skyddsobjekt alternativt riksintressen, vilka fysiska hotnivåer som ska mötas och vilka tillgänglighetsnivåer varje enskild delfunktion måste uppnå borde vinna på att hanteras på en övergripande samhällsnivå. Post- och telestyrelsens förslag till en aktörsmodell avseende skyddade it-utrymmen kan vara en bra utgångpunkt. Den föreslår följande aktörer:

- **Prioriteringsfunktion**. En funktion inom staten med uppdrag att ur ett övergripande samhällsperspektiv

klassificera och prioritera behov av skydd för säkerhetskänsliga verksamheters it-tjänster.

- **Utrymmesförvaltare**. En organisation som utifrån den föreslagna förvaltningsmodellen förvaltar beståndet av skyddade it-utrymmen.
- **Anläggningsägare**. En anläggningsägande och förvaltande organisation som äger och förvaltar de anläggningar där skyddade it-utrymmen placeras.
- **Nyttjare**. Aktörer som har säkerhetskänslig verksamhet och som har behov av att placera hela eller delar av sina it-miljöer i skyddade it-utrymmen.

Hur kan ett statligt datacenterkoncept se ut?

En skyddad anläggning med hög nyttoeffekt, det vill säga effekt som kommer till nytta för anläggningens funktioner, är dyr och tar lång tid att bygga. Skyddade anläggningar med hög fortifikatorisk kapacitet är dock nödvändiga ur ett totalförsvarsperspektiv. Ett möjligt sätt att balansera förhållandet mellan nytta, risk och kostnad för en skyddad anläggning vore att sänka kraven på hög nyttoeffekt. Detta skulle resultera i ett mindre komplext utförande till en lägre kostnad. Det skulle även skynda på anskaffningsprocessen. Det kan dessutom vara enklare att närma sig miljömålen samt få bättre avsättning för överskottsvärmen.

En säker byggnad bör i de flesta avseenden uppföras så likt moderna kommersiella datacenter som möjligt. För att vinna synergier i takt med en framtida utbyggnad av ett nationellt datacenterkoncept bör principer och erfarenheter återvinnas och utvecklas, men till stor del kan de repeteras till utformning och kapacitet på nya platser. En avgörande skillnad från de kommersiella referensobjekten är dock att fysiska säkerhetsaspekter kommer kosta mer eftersom det är angeläget att skydda it-utrymmet mot de hotscenarier som finns under fredstid. Det kan till exempel handla om inbrott, sabotage, angrepp med skjutvapen, personburna bomber, fordonsburna bomber och forcerande fordon.

Det är sannolikt att det stora flertalet it-tjänster som kan komma i fråga för ett statligt datacenterkoncept har höga krav på fysisk säkerhet, men inte på nivån som en skyddad berganläggning erbjuder. En säker byggnad som planeras, placeras och utformas för ändamålet kan å ena sidan troligen erbjuda en fullt tillfredsställande fysisk säkerhetsnivå för de allra flesta samhällsviktiga it-tjänster. Å andra sidan finns det en hel del it-tjänster som även måste klara krigets krav genom de fortifikatoriska förutsättningar en skyddad anläggning erbjuder.

Ytterligare ett sätt att dra nytta av en skyddad anläggning är att använda den till lagring och backup som på det hela taget är mindre energiintensivt. Energiintensiva servertjänster med högre krav på tillgänglighet kan huvudsakligen hanteras i säkra byggnader. På så sätt ges samhällsviktiga it-tjänster hög kapacitet när det gäller tillgänglighet och god säkerhet i daglig drift medan den samlade datamängden regelbundet säkerhetskopieras till en skyddad anläggning. I detta koncept kommer vid oönskade händelser visserligen säkerhetskopierad data i en skyddad anläggning å ena sidan vara otillgänglig under den tid det tar att återläsa till en annan säker byggnad i drift, men å andra sidan ha god riktighet i bemärkelsen att data inte går förlorad och därmed är möjlig att återställa.

Skyddad anläggning och säker byggnad - en fördelaktig kombination

Dimensionerande nyttoeffekt och behovet av antalet skyddade anläggningar bör utredas djupare ur ett strategiskt perspektiv. Men som ett avslutande exempel nedan kan ett samlat nationellt effektbehov om strax över 20 MW (effektåtgång för ungefär 9000 villor) uppnås genom en fördelning på 15 stycken byggnader samt skyddade anläggningar (nyetablering respektive ombyggda bergrum) fördelade i hela landet:

En konceptuell etablering av ett regionalt datacenterkluster skulle kunna fördelas som:

- två säkra byggnader om två MW effekt vardera (nyetablering)
- en skyddad anläggning om en halv MW effekt (ombyggnad av befintlig berganläggning som inte är i drift).

Fem sådana regionala datacenterkluster fördelade över landet skulle då innebära totalt:

- tio säkra byggnader om två MW vardera (nyetablering)
- fem skyddade anläggningar om en halv MW vardera (ombyggnad av befintliga berganläggningar som inte är i drift).

Det är som tidigare nämnt värt att notera den relativt långa anskaffningstiden för ett datacenterkoncept. Tidskritiska parametrar som påverkar produktionstiden för en ny säker byggnad är bland annat markanskaffning, miljöprövning och säkerhetsskyddad upphandling av entreprenörer.

Anskaffningstiden för en säker byggnad uppskattas vara omkring två år. En ombyggnad av ett fortifikatoriskt skyddat bergrum bedöms ligga på fyra till fem år. Uppförandet av flera regionala

datacenterkluster kan utföras efter hand eller samtidigt. Det är dock rimligt att anta att behovet av den fulla kapaciteten inte inträffar i det korta perspektivet och att det därmed inte finns behov av att utföra hela konceptet parallellt. Det finns även en logik i att ta tillvara erfarenheter från initiala uppföranden innan för stora steg tas. Det är därför skäligt att anta att en total anskaffningstid kan ta cirka tio år.

Sammantaget kan ett tänkbart datacenterkoncept som beskrivs i exemplet ovan erbjuda hög tillgänglighet och redundans till en rimligare kostnad än om alla it-utrymmen består av nyproducerande fortifikatoriskt utformade berganläggingar. Även om tillgängligheten påverkas för samhällsviktiga och säkerhetskritiska it-tjänster i datacenterkonceptet, ger det en god säkerhet både när det gäller fysiska perspektiv och riktighet i bemärkelsen att data inte går förlorat även under stora påfrestningar. Den uppskattade anskaffningstiden på cirka tio år förutsätter dock att nödvändiga strategiska delar är avklarade som kravställning, finansiering och organisation. Det gör att beslutsfattare bör höja medvetenheten kring behov och utmaningar förenade med nationell samordning av skyddade it-tjänster, så att processen kan påbörjas. För Sveriges totalförsvar är det en viktig och nödvändig investering för framtiden.

För vidare läsning

Fortifikationsverket, *Förstudie av skyddade it-utrymmen för offentliga aktörer inom samhällsviktig verksamhet – Delrapport*, 2018, Dnr 727/2017-22.

Fortifikationsverket, F*örstudie av skyddade it-utrymmen för offentliga aktörer inom samhällsviktig verksamhet – Ett statligt datacenterkoncept*, 2018, Dnr 727/2017-29.

Fortifikationsverket, *Handbok Skydd av byggnader*, 2017, Utgåva 4.

15. FOI och totalförsvarets behov

Eva Mittermaier

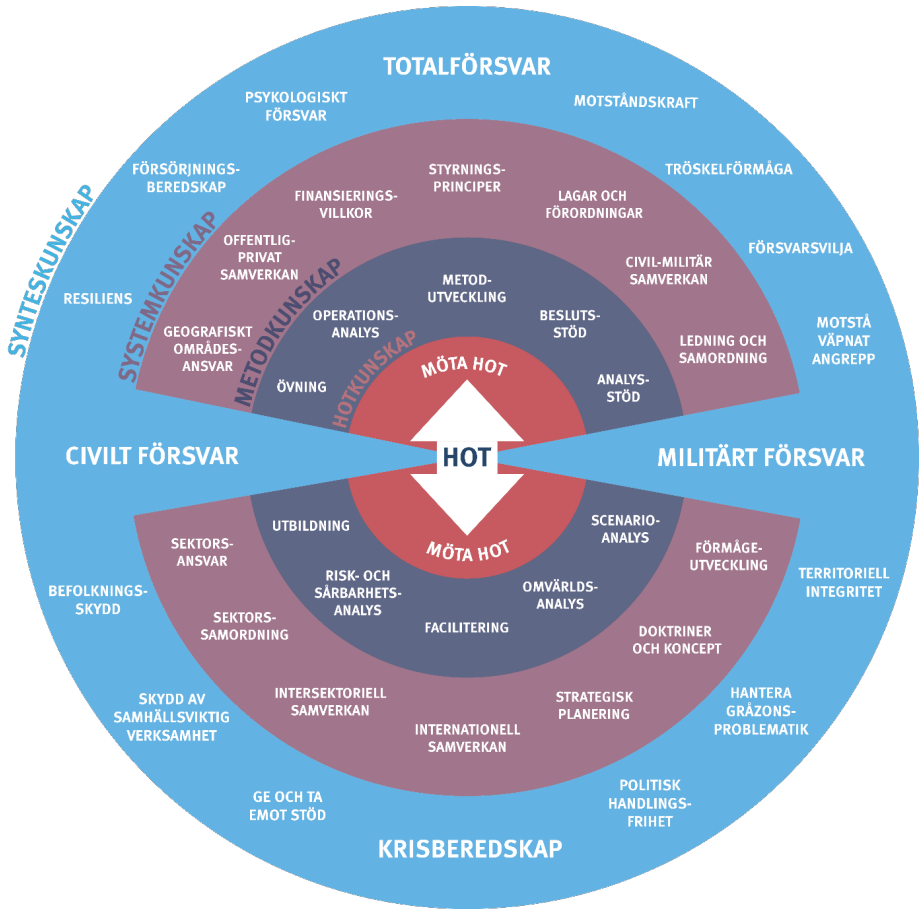
Strategisk utblick 8 belyser viktiga perspektiv inom omvärlds- och teknikutveckling, och därmed sammanhängande utmaningar. För att kunna möta dessa förändringar inklusive de nya hoten har det svenska totalförsvaret ett stort behov av kontinuerlig och sammanhängande kunskapsutveckling. Till hjälp för dialogen mellan olika myndigheter och andra aktörer inom totalförsvaret har forskare på FOI tagit fram en modell för hur man kan se på kunskapsutveckling för totalförsvarets behov.

KUNSKAPSMODELL FÖR TOTALFÖRSVARETS BEHOV

Kunskapsbehoven för det nya totalförsvaret är stora och berör många olika områden. För såväl krisberedskapen som totalförsvaret är en grundläggande utgångspunkt kunskap om olika säkerhetshot och sätten att hantera dem. Denna kunskap är ofta mycket specifik och kräver såväl grundforskning som specialiserad tillämpning inom en rad områden av olika karaktär, exempelvis spridning av virussjukdomar, extremistisk propaganda i sociala medier och tolkning av kärnvapendoktriner.

För att utvecklingen av kunskap om hot ska få önskvärd effekt i uppbyggnaden av totalförsvaret behöver den tillgängliggöras i de samhällsviktiga verksamheter, till exempel sjukvård, betalningssystem och energiförsörjning, där kunskapen ska tillämpas. Detta är långt ifrån en enkel uppgift, eftersom den involverar många olika aktörer, exempelvis myndigheter, kommuner och privat näringsliv, från en rad olika sektorer med olika förutsättningar, behov och roller.

Figuren nedan är en modell som omfattar kunskapsområden för totalförsvarets behov. Modellen är ursprungligen framtagen för att utgöra en plattform för FOI:s fortsatta arbete med totalförsvaret, där FOI i dialog med uppdragsgivare kan tydliggöra specifika områden där FOI skulle kunna bidra – men modellen kan givetvis också användas som ett mer allmängiltigt diskussionsunderlag avseende totalförsvarets kunskapsbehov. Modellen åskådliggör fyra olika kunskapsskikt.



Figur 2. En kunskapsmodell för totalförsvar.

Hotkunskap - det första kunskapsskiktet

Att identifiera, förstå, analysera och möta antagonistiska hot, avser grundläggande sakkunskap och spetskompetens om hoten och hur man kan hantera dem. Hotkunskap handlar exempelvis om informationssäkerhet och cyberfrågor, men också om militära hot, skydd mot konventionella vapen och farliga ämnen (kemiska, biologiska, radioaktiva och nukleära). Bland hoten ingår även potentiella sårbarheter som teknikutvecklingen medför.

När även så kallad gråzonsproblematik inkluderas i totalförsvarsperspektivet utgörs hoten även av exempelvis påverkansoperationer, terrorism, sabotageverksamhet och organiserad kriminalitet. Det handlar om att hitta sätt att skydda människor, samhällsfunktioner, soldater, militära system, civil infrastruktur, egendom, samhällssystem, värderingar osv. I hotkunskapen ingår även sätt att analysera enskilda hot och hur dessa kan mötas, till exempel genom modellering, simulering, och mätteknisk metodik.

Metodkunskap - det andra kunskapsskiktet

Metodkunskap handlar om att på olika sätt stödja analys- och beslutsprocesser och därigenom stärka de berörda totalförsvarsaktörernas förmåga att identifiera och möta hot. Det är kunskap om stöd för att kunna bygga upp och nyttiggöra kunskap hos eller tillsammans med andra aktörer, det vill säga övergripande metodkunskap.

Denna kunskap krävs till exempel inom scenariometodik och spel där scenarier utnyttjas för att beskriva hotbilden och för att utveckla nyttiggörandet av sakkunskapen via exempelvis beredskapsplanering inom samhällets olika sektorer och funktioner. Sårbarheter kan identifieras och hanteras genom att man undersöker dessa och försöker hitta åtgärder. Det kan handla om risk- och sårbarhetsanalyser, scenarioövningar där deltagarna kan identifiera och diskutera sårbarheter, vilka aktörer som behöver samverka för att möta hoten, eller vilka ledningssystem som krävs för att berörda aktörer ska kunna arbeta koordinerat. Det kan också handla om hur aktörerna tillsammans kan utnyttja information från befintliga tekniska sensorer och annat underlag för att åstadkomma förbättrade operativa lägesbilder och kommunicera med varandra på ett robust sätt.

Systemkunskap - det tredje kunskapsskiktet

Systemkunskap omfattar övergripande förståelse för det system där hotkunskap och metoder ska användas, exempelvis inom policyutveckling och strategisk planering, doktrin- och konceptutveckling samt förmågeutveckling. Systemkunskapen omfattar också de förutsättningar som råder i dessa sammanhang,

till exempel ansvarsförhållanden, finansieringsvillkor samt olika former av samordning och samverkan.

Synteskunskap - det fjärde kunskapsskiktet

Ett sammanhängande totalförsvar kräver en sammanhängande kunskapsutveckling. Synteskunskap omfattar bland annat kunskap om totalförsvarets olika delar, vilket berör såväl krisberedskapens och det civila försvarets som det militära försvarets förutsättningar, mål och centrala uppgifter. Här krävs också kunskap om hur viktiga samhällssektorer faktiskt fungerar i praktiken.

Detta kunskapsskikt omfattar också förståelse för hur säkerhets- och försvarspolitiken påverkar totalförsvaret liksom förmåga att identifiera specifika behov för totalförsvaret som i sin tur kan komma att kräva ny forskning samt långsiktig teknik- och konceptutveckling.

Kunskapsutveckling för ett sammanhängande totalförsvar

Avslutningsvis behöver de fyra olika kunskapsskikten kunna integreras för att säkerställa utvecklingen av ett ändamålsenligt och sammanhängande totalförsvar – oavsett var kunskapsutvecklingen sker. För att specialiserad hotkunskap ska kunna nyttiggöras i totalförsvarets olika verksamheter och utvecklingsprocesser krävs såväl metod- som systemkunskap. FOI har ambitionen och uppgiften att fortsätta stödja samhällets olika delar med expertkunnande, analyser, beslutsstöd och strategiska beslutsunderlag – vilket omfattar samtliga kunskapsskikt.

För vidare läsning

Jenny Ingemarsdotter och Daniel Jonsson, *Kunskapsbehov för ett totalförsvar i förändring*, 2019, FOI-R--4770--SE.

Författare

Christer Andersson, är Tekn. Lic., forskare och analytiker vid FOI:s enhet för Undervattensteknik. Han arbetar med olika utvecklingsprojekt för Försvarsmakten avseende tekniska hotbilder för att stärka svensk militär förmåga och kapacitet. Han har en bred internationell erfarenhet från både civil och militär verksamhet med fokus på bildinformationsinhämtning och som expert åt olika organisationer.

Maria Andersson är förste forskare vid FOI:s enhet för Sensorinformatik. Hon är också adjungerad universitetslektor och docent i energisystem vid Linköpings universitet. Hennes expertområden är metoder för automatisk detektion av kritisk information i stora datamängder samt systemanalys med fokus på samverkan mellan aktörer.

Samuel Bergenwall är förste analytiker vid FOI. Han arbetar vid enheten för Säkerhetspolitik där han för närvarande leder ett projekt för långsiktig omvärldsanalys. Under sin tid vid FOI har Samuel framför allt arbetat med frågor som rör säkerhet i Asien och Mellanöstern.

Åsa Berglund är verksam som jurist vid FOI där hon företrädesvis arbetar med stöd och utbildning i myndighetsjuridik. Hennes expertområden är offentlighet och sekretess samt personuppgiftsfrågor. Sedan 2018 är hon FOI:s dataskyddsombud. Åsa kommer närmast från Försvarsmaktens juridiska stab.

Anton Dahlmark är utvecklingsdirektör och avdelningschef för Fortifikationsverkets utvecklingsavdelning. Han har arbetat inom området skydds- och anläggningsteknik för skyddade anläggningar sedan 2010. Antons bakgrund dessförinnan är från Försvarsmakten och han har även arbetat med krisberedskap.

Carl Denward är samhällsvetare och förste analytiker vid enheten Samhällets säkerhet. Hans expertområde är den civila sidan av svensk beredskap, i form av civilt försvar och krisberedskap med fokus på strategi-, policy- och styrningsfrågor. Carl har en bakgrund i kommunal beredskap.

Fredrik Ekström är biokemist och arbetar som forskningschef på enheten för Organisk kemi och biovetenskap på FOI. Tillsammans med akademiska forskningsgrupper forskar Fredrik om nervgaser och deras medicinska motmedel.

Anders Elfving är forsknings- och utvecklingssamordnare på Fortifikationsverket. Han har tidigare arbetat på FOI:s enhet för Värdering och risk där han varit projektledare med inriktning mot detektion av explosivämnen och arbetat med harmonisering av certifieringsprocesser för skyddsprodukter. Anders har disputerat inom materiefysik vid Linköpings universitet och har en bakgrund inom utveckling av halvledarbaserade mikrosensorer.

Carina Gunnarson, är förste forskare vid FOI och verksam vid enheten för Säkerhetspolitik. Hennes forskningsområden är bland annat europeisk politik, Afrika samt organiserad brottslighet. Hon är docent i statskunskap vid Uppsala universitet.

David Gustafsson är förste forskare och projektledare vid FOI:s enhet för Sensorinformatik. David arbetar huvudsakligen med maskininlärningsmetoder, så som *deep learning*, för att analysera bilder av olika modalitet. Han har en magisterexamen i datalogi från Lunds universitet och en doktorsexamen i datalogi med inriktning mot bildanalys från Köpenhamns universitet.

Jakob Gustafsson är analytiker vid FOI:s enhet för Strategi och policy och en av redaktörerna för Strategisk utblick 8. Han arbetar främst med transatlantisk och nordeuropeisk försvars- och säkerhetspolitik och även med tillväxt inom försvaret. Jakob har en utbildningsbakgrund inom statsvetenskap.

Tommy Gustafsson är forskningsingenjör vid FOI:s enhet för Informationssäkerhet och IT-arkitektur. Hans expertområden är nätverkssäkerhet och informationssäkerhet inom samhällsviktig verksamhet. Han är aktiv inom ramen för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NSC3), ett kompetenscentrum som FOI driver i samarbete med Myndigheten för samhällsskydd och beredskap (MSB).

Tove Gustavi är förste forskare vid FOI:s enhet för Beslutsstödsystem. Hon har doktorerat i matematisk systemteori med tillämpningar inom robotik och har arbetat på FOI sedan 2010, bland annat med utveckling av tekniskt stöd för underrättelseanalys och med automatiserad dataanalys inom civil transportsäkerhet. Hon har tidigare varit projektledare för ett FOI-projekt som studerat försvarsnära tillämpningar av artificiell intelligens och var under flera år gästforskare på Kungliga tekniska högskolan.

Tomas Hurtig är teknologie doktor i plasmafysik och laborator vid FOI:s enhet för Växelverkan, Vapen och Skydd. Hans forskning rör tillämpningar av elektro- och plasmafysik, främst för militära ändamål. Han är projektledare för försvarsmaktsprojektet HPM sårbarhetsanalys samt kompetensområdesledare för området Skydd mot elektromagnetisk verkan. Tomas är en av FOI:s representanter i Centrala beredningsgruppen för elektromagnetiska hot.

Jenny Ingemarsdotter är forskare vid FOI:s enhet för Samhällets säkerhet med fokus på krisberedskap, civilt försvar och totalförsvar. Hon har en civilingenjörsexamen och en doktorsexamen i Idé- och lärdomshistoria, båda från Uppsala universitet. Jenny har tjänstgjort i många roller vid FOI, bland annat som operationsanalytiker vid Försvarsmakten och analysstöd till civila myndigheter. För närvarande forskar hon om civilt försvar i gråzon.

Bengt Johansson är forskare vid FOI på enheten för Samhällets säkerhet 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.

Daniel K. Jonsson är en av redaktörerna för Strategisk utblick 8. Han är forskningsledare vid FOI:s enhet för Samhällets säkerhet. Han har en bakgrund inom energi- och miljöforskning, disputerade inom området infrastruktur och samhällsplanering och är docent i energianalys. Daniel leder ett forskningsprojekt om civilt försvar i gråzon och är sammanhållande för FOI:s stöd till Energimyndighetens totalförsvarsplanering.

Maja Karasalo är forskare vid FOI:s enhet för Beslutsstödsystem. Hon arbetar med metoder för automatisk textanalys och forskar inom området artificiell intelligens och maskininlärning. Maja är civilingenjör i Teknisk Fysik och har en teknologie doktorsexamen i Optimeringslära och Systemteori, båda från Kungliga Tekniska Högskolan. Hon har tidigare även arbetat som forskare och systemutvecklare i SAAB:s datafusionsgrupp.

Maria Lignell Jakobsson är planeringsdirektör vid GD ledningsstöd på FOI. Hon ansvarar för samordning av verksamhetsstyrning och andra myndighetsgemensamma processer, omvärldsbevakning och analys samt myndighetens kontakter med Regeringskansliet. Maria har tjänstgjort inom många roller vid FOI. Fram till slutet av 90-talet arbetade hon med studier inom totalförsvar, beroenden och operativ förmåga. Därefter låg fokus främst på strategi- och marknadsfrågor. Hon har även varit avdelningschef för Försvarsanalys.

David Lindahl är forskningsingenjör vid FOIs enhet för Informationssäkerhet och IT-arkitektur. Han arbetar med skydd av samhällets kritiska infrastruktur mot cyberangrepp samt forskning kring användning av cyberangrepp vid konflikter. En stor del av hans arbete de senaste tio åren har varit att ta fram och hålla utbildningar i att möta cyberhot för totalförsvarets aktörer (Försvarsmakten, civila myndigheter och företag).

Sara Linder är förste forskare vid FOI:s enhet för Robust telekommunikation. Hon har arbetat på FOI sedan 1998 med forskning kring robusta radiosystem. Hennes expertområde är konsekvenser i kommunikationssystem av oavsiktliga störningar, ofta kallade telekonflikter. Hon forskar även kring tekniker för att öka robustheten mot såväl avsiktliga som oavsiktliga störningar.

David Lindgren är förste forskare vid FOI:s enhet för Sensorinformatik. Han har en doktorsexamen från Reglerteknik, Linköpings universitet. Hans expertområden omfattar estimeringsteori, sensorfusion och sensornätverk. Han har varit ledare för både nationella och internationella projekt med fokus på övervakningstillämpningar.

Jenny Lundén är analytiker vid FOI:s enhet för Strategi och Policy. Hennes fokusområde är totalförsvar där hon arbetar med analyser inom både civilt och militärt försvar. Som operationsanalytiker ger Jenny direktstöd hos Försvarsmaktens Totalförsvarsavdelning. Hon har tidigare varit teknisk analytiker i näringslivet och gjort utredningar och analyser inom förnybar energi. Jenny har en magisterexamen i fysik från Lunds universitet och en doktorsexamen i meteorologi med fokus på Arktis från Stockholms universitet.

Eva Mittermaier är forskningsledare vid FOI:s enhet för Samhällets säkerhet. Eva har tjänstgjort inom många roller vid FOI och främst arbetat med frågor rörande krisberedskap, samhällssäkerhet och civilt försvar. Eva har under de senaste åren deltagit i ett myndighetsinternt arbete rörande FOI:s möjliga bidrag till uppbyggnaden av det civila försvaret och av totalförsvaret samt därav följande kunskapsbehov.

Peter Nilsson är systemvetare och forskare vid enheten för Människa, Teknik, Organisation. Han arbetar med frågor som rör metoder för behovsanalys, kravställning och metodik för systemutveckling, främst genom modellbaserade metoder och olika arkitekturramverk. Peter arbetar ofta nära andra myndigheter och har deltagit i flera utvecklingsprojekt, framför allt tillsammans med Försvarsmakten, men även med Polismyndigheten.

Sten E Nyholm är forskningsledare vid FOI:s enhet för Växelverkan, Vapen och Skydd. Han har arbetat vid FOI sedan 1996, främst med forskning kring mikrovågsvapen. Därutöver har hans arbete berört mikrovågsvapenteknik, explosivämneskunskap, lågkänslig ammunition samt olika militära tillämpningar av pulsad elektrisk energi. Han var projektledare för den huvudstudie av risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig infrastruktur som genomförts på uppdrag av Myndigheten för Samhällsskydd och Beredskap (MSB).

Jonas Näslund har disputerat i ämnet virologi vid Umeå universitet och arbetar som forskare vid enheten för Biologiska ämnen på Totalförsvarets forskningsinstitut. Jonas expertområde är virus med en specialinriktning mot virala zoonoser och deras vektorer, såsom myggor och gnagare.

Matilda Olsson är analytiker vid FOI:s enhet för Strategi och policy, med fokus på civilt försvar och totalförsvar. De senaste åren har hon bland annat genomfört studier om näringslivet respektive länsstyrelsernas roll i totalförsvaret samt tjänstgjort som operationsanalytiker vid Försvarsmaktens högkvarter. Matilda har en utbildningsbakgrund inom statsvetenskap och hållbar utveckling vid Uppsala universitet.

Per Olsson är forskare vid FOI:s enhet för Försvarsekonomi. Hans expertisområden är försvarsutgifter och militär materielförsörjning. Han arbetar för närvarande med en rapport om Sveriges militära materielförsörjning på uppdrag av Expertgruppen för Studier i Offentlig ekonomi (ESO). Per har en magisterexamen från Lunds universitet.

Sofia Olsson är en av redaktörerna för Strategisk utblick 8. Hon är analytiker vid FOI:s enhet för Asymmetriska hot. Sofia arbetar med cybersäkerhetsfrågor och som analysstöd åt Försvarsmakten. Sofia har en utbildningsbakgrund inom globala utvecklingsstudier och krigsvetenskap.

Niklas H. Rossbach är projektledare och huvudredaktör för Strategisk utblick 8 sedan februari 2019. Han är förste forskare vid FOI:s enhet för Säkerhetspolitik med huvudsaklig inriktning på amerikansk och europeisk säkerhetspolitik. Han forskar även om energi och säkerhetspolitik. Han har doktorerat i historia vid Europeiska universitetsinstitutet och forskat om psykologiskt försvar vid universitet i Oxford med stöd av Axel och Margaret Ax:son Johnsons Stiftelse.

Per Stenberg är förste forskare på enheten för Biologiska ämnen på FOI. Per är genetiker och jobbar halvtid som forskare på FOI och halvtid som forskningsledare på Umeå universitet. Per forskar på hur gener regleras och hur arvsmassan är strukturerad, med hjälp av olika typer av DNA-sekvenseringstekniker i kombination med storskalig dataanalys.

Anna Sundberg är en av redaktörerna för Strategisk utblick 8. Hon är forskningsledare vid FOI:s enhet för Säkerhetspolitik där hon fokuserar på europeiska staters säkerhets- och försvarspolitik. Anna tjänstgör för närvarande som analysstöd på Justitiedepartementet.

Ola Svenonius, fil.dr. i statsvetenskap, är forskare på enheten för Asymmetriska hot på FOI med fokus på totalförsvar och informationspåverkan. Han leder bland annat ett forskningsprojekt med finansiering från MSB och deltar i samverkansprojektet BEViS som leds av Polisens utvecklingscentrum Bergslagen. Under sin tid som forskare vid Stockholms universitet fokuserade Ola på frågor om övervakning, brottsbekämpning och politik i Central- och Östeuropa.

Patrik Thunholm, fil.mag. i informationsvetenskap och fil. mag. i rättsvetenskap, är analytiker vid FOI:s enhet för Asymmetriska hot. Han är reservofficer i Försvarsmakten med fokus på psykologiska operationer. Han är för närvarande tjänstledig från FOI för att arbeta vid EU:s insats i Mali.

Camilla Trané är en av redaktörerna för Strategisk utblick 8. Hon är förste analytiker vid FOI:s enhet för Operationer och insatser. Camilla har i huvudsak arbetat med att tillämpa metoder i praktiken, främst övning, utvärdering och erfarenhetshantering. I sin roll som analytiker har hon mångårig erfarenhet som direktstöd inom dessa metodområden, både från den civila och den militära sidan.

Niclas Wadströmer är förste forskare vid FOI:s enhet för Sensorinformatik. Niclas arbetar huvudsakligen med bild- och signalanalys bland annat med maskininlärningsmetoder som *deep learning*, för signaler av olika modalitet. Niclas är civilingenjör i Datateknik och teknologie doktor i bildkodning från Linköpings universitet.

Kia Wiklundh, tekn.dr., har tidigare arbetat som laborator vid FOI. Hennes expertområde är robusta trådlösa kommunikationssystem. Fokus har främst varit kring militära radiosystem men hon har även arbetat med att undersöka sårbarheter i civila system och har ansvarat för FOI:s telekonfliktsverksamhet.

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.

Josefin Öhrn-Lundin är projektledare och huvudredaktör för Strategisk utblick 8. Hon arbetar som analytiker vid FOI:s enhet för försvarsekonomi, med fokus på materielförsörjning och logistik. Josefin har en MSc i innovations- och tillväxtekonomi från Kungliga Tekniska Högskolan.

FOI är ett av Europas ledande forskningsinstitut för tillämpad forskning inom försvar och säkerhet. FOI är en statlig myndighet under Försvarsdepartementet, och har som sin största kund Försvarsmakten. FOI har även många uppdrag för andra statliga myndigheter, kommuner och företag.

FOI publicerade Strategisk utblick för första gången 2009. Det är en återkommande framåtblickande studie som uppmärksammar säkerhetspolitiska och försvarsteknologiska trender samt deras möjliga konsekvenser inom en rad geografiska och tematiska områden.

Fokus för årets Strategisk utblick är totalförsvarets tillväxt.

Strategisk utblick finns att ladda ner från www.foi.se.

FOI

ISSN 1650-1942

www.foi.se