



# Strategisk utblick 9

Framtida hot

Jenny Lundén, Anders Melander, Elin Hellquist,  
Björn Ottosson, Anders Strindberg och  
Liselotte Steen (red.)

FOI-R--5103--SE

JANUARI 2021





# Strategisk utblick 9

## Framtida hot

Jenny Lundén, Anders Melander, Elin Hellquist,  
Björn Ottosson, Anders Strindberg och  
Liselotte Steen (red.)

JANUARI 2021

ISSN 1560-1942

Tryckt i Stockholm 2020 av Totalförsvarets forskningsinstitut, FOI

Omslagsbild: Shutterstock

FOI-R--5103--SE

Godkänd av Malek Finn Khan

# Strategisk utblick 9 Framtida hot

## **FÖRORD**

Vart är vi på väg? Frågan ställs om och om igen i miljontals hem årligen via tävlingsprogrammet "På spåret". När vi försöker förstå vilka framtida hot vi kommer att möta så har vi dessvärre ingen allvetande domare som snabbt kan ge oss det rätta svaret. Trots att vi inte har facit eller en domare till hjälp så har vi oaktat försökt att svara på frågan vart vi är på väg. Kommer vi i framtiden att möta super soldater, vilka militära hot är under uppsegling och kommer framtidens algoritmer från sociala medier att i än större skala kunna användas för att påverka vår verklighet? Kan vi idag skönja vad som utgör våra framtida hot, genom att titta bakåt och se oss om i vår samtid? Genom att forskare från amerikanska RAND Corporation medverkar med ett bidrag i den här skriften så tillför vi ytterligare perspektiv på hur hot utvecklas över tid.

En av författarna använder ordet hotkavalkad vilket väl fångar vad vi har att hantera. Även om aktörer och hotbild kommer att förändras över tid så måste totalförsvaret fungera över och mellan olika samhällssektorer. Att kunna möta, hejda och slå en kvalificerad motståndare är en avgörande pusselbit. Dessvärre kommer antagonistiska hot alltid riktas mot områden där vi är som svagast. Genom forskning, utveckling, analys och samarbete så kan vi bidra till ett robustare samhälle. Din uppgift som läsare när du tar språnget in i framtiden med oss är att ställa dig frågan vilka andra hot som vi måste omhänderta?

Stockholm 2021

Jens Mattsson  
Generaldirektör



# Innehåll

Inledning.....	7
1. Perspektiv på framtida militära hot.....	9
RIITTA RÄTY, GÖRAN KINDVALL OCH ANN ÖDLUND	
2. Hoten mot Väst och transatlantiska relationers framtid.....	15
NIKLAS H. ROSSBACH	
3. Demokratisk säkerhet.....	21
ANDERS STRINDBERG OCH ERIK SVENSSON	
4. Robusta beslut för hantering av ett förändrat klimat.....	27
CHRISTOFFER WEDEBRAND, KARIN MOSSBERG SONNEK OCH PER WIKMAN-SVAHN	
5. Framtidens hot – ser vi dem komma?.....	33
VIDAR HEDTJÄRN SWALING OCH JENNY INGEMARSDOTTER	
6. AI och påverkansoperationer i sociala medier.....	37
FREDRIK JOHANSSON, MAGNUS ROSELL OCH DAVID GUSTAFSSON	
7. Svärmande drönare – ett reellt militärt hot i framtiden?.....	43
MARTIN HAGSTRÖM, LARS FORSELL, OCH NICLAS STENSÄCK	
8. Kan laservapen ändra spelplanen i framtida konflikter?.....	49
MATTS BJÖRCK, MARKUS HENRIKSSON OCH LARS SJÖKVIST	
9. Svensk beredskap för att möta krig mot rymden.....	53
SANDRA LINDSTRÖM OCH KRISTOFER HALLGREN	
10. Framtida antagonistiska biologiska och kemiska hot.....	59
ANDERS LARSSON, SUSANNE BÖRJEGREN OCH BIRGITTA LILJEDAHL	
11. En hotkavalkad mot global hälsa kryddat med desinformation.....	63
ANNICA WALEIJ	
12. Supersoldater.....	69
BRITTA LEVIN, SOFIA HEDENSTIERNA, OVE JANSSON OCH MARTIN HAGSTRÖM	
13. Future Threats and Some Considerations for the Next U.S. National Defense Strategy.....	75
GENE GERMANOVICH, GABRIELLE TARINI, AND K. JACK RILEY	
Författarpresentationer.....	81



# Inledning

Att förbereda sig för att möta och hantera hot är ingen lätt uppgift. När det dessutom ligger i framtiden måste man även identifiera vilka hot som är möjliga, troliga eller enbart fantasier. Trots det, eller kanske på grund av det, tycks många av de hot som finns beskrivna inom science fiction ha letat sig in i verkligheten, om än i mindre och mer modesta former.

Men hur ser framtidens hot ut? Media och populärvetenskapen tar flitigt upp ämnet, men ofta begränsat till det som är uppmärksammat idag, exempelvis hybrid- och cyberhot. I Strategisk utblick 9 vill vi vidga vyerna och ta upp hot som kanske förbises. Genom artiklarna har forskare på FOI blickat framåt och beskrivit tänkbara framtida hot. Bilden som målas upp genom deras bidrag är bred då det inte finns någon entydig definition av vare sig hot eller framtid.

I den första artikeln kan man läsa om hur synen på framtida hot har ändrats genom åren. *Perspektiv på framtida militära hot* tar upp det strukturerade arbete som bedrivits under lång tid inom Försvarsmakten med stöd av FOI. Genom studien sätts perspektiv på framtida hot för att skapa koncept och bygga förmågor som syftar till att stödja utvecklingen av vårt försvar inför framtiden. Men kommer framtidens krig att föras i rymden eller är vi redan på väg dit? Vårt moderna samhälle är redan idag beroende av satelliter vilket gör oss sårbara för konflikter i rymden. Denna utveckling lyfts fram i *Rymden en ny arena för krigföring*.

Sett ur ett globalt perspektiv kan även förändringar i den världsordning som vi vant oss vid upplevas som ett hot. Det kan vara förändringar i internationella relationer, försvagade allianser eller nya säkerhetspolitiska samarbeten. Dessa perspektiv tas upp i *Hotet mot Väst och transatlantiska relationers framtid* och i årets gästbidrag som är från RAND Corporation. I deras artikel *Future Threats and Some Considerations for the Next U.S. National Defense Strategy* tar RAND den amerikanska nationella säkerhetsstrategin som utgångspunkt och diskuterar hur den kan utformas i framtiden för att bidra till global säkerhet.

Även själva demokratin hotas, något som belyses i artikeln *Demokratisk säkerhet: Att bemöta de tysta hoten mot samhällets grundprinciper*. Detta är ett svårgripbart hot som består av många olika komponenter. Synsättet som presenteras i artikeln vidgas bortom de gränser som normalt finns inom forskningsområdet. En annan frågeställning handlar om huruvida vårt språk räcker till för att kommunicera när hoten faller utanför ramen för vår egen uppfattning – i gränslandet mellan cyber och den fysiska världen. Det vill säga har vi förmåga att förstå hot på en konceptuell nivå. Dessa utmaningar diskuteras i *Framtidens hot – ser vi dem komma?*

En annan sak är att beslut nästan alltid är förknippade med osäkerheter. Detta gäller i synnerhet om besluten ska fattas för att möta framtida hot, vars omfattning i sig själv är mycket osäkra. Denna utmaning tas upp i artikeln *Robusta beslut för hantering av ett förändrat klimat*.



Precis som klimatet har hälsohot en global dimension. Hotet mot hälsan påverkas både av internationell politik och av desinformation. Dessutom finns en oroande utveckling mot en ökad vilja att använda biologiska och kemiska vapen. Detta diskuteras i artiklarna *En hotkavalkad mot global hälsa kryddat med desinformation* och *Framtida antagonistiska biologiska och kemiska hot*. Inom dessa områden är teknikframstegen ett tveeggat svärd, som både ökar hotet men även möjligheterna att försvara sig mot det.

Teknikutvecklingen utlovar positiva möjligheter till nytta för oss i framtiden. Artificiell Intelligens (AI) har visserligen stor potential att förenkla vår vardag, men vilka risker finns det med tekniken? Några av hoten diskuteras i *AI och påverkansoperationer i sociala medier*. Annan teknik, som enkelt finns tillgänglig för alla, exempelvis de populära hobbydrönarna, kan modifieras för att användas i konflikter och krig. Detta kan man läsa om i *Svärmande drönare – ett reellt militärt hot i framtiden?* Science fiction har kanske gjort det enklare att föreställa sig vilka hot laser kan utgöra som vapen. Hur ett sådant vapen skulle kunna fungera diskuteras i artikeln *Kan laservapen ändra spelplanen i framtida konflikter?* Än mer science fiction är så kallad mänsklig förstärkning, där soldater utrustas med exoskelett, implantat eller ökar sin prestation med hjälp av kemikalier – teknik som nu håller på att hinna ikapp fantasin. Några av dessa framtidsvisioner förs fram i artikeln *Supersoldater*.

För den som vill fördjupa sig inom något av ämnena som tas upp i Strategisk utblick 9, finns det tips för vidare läsning i slutet av de flesta artiklarna.

Redaktionen

# 1. Perspektiv på framtida militära hot

Riitta Rätty, Göran Kindvall och Ann Ödlund

*Det är genuint svårt att uttala sig om framtiden, särskilt när det gäller hot där det finns en målmedveten och resursstark antagonist. När det gäller att bedöma framtida nya hot och vilka som faktiskt kan realiseras behöver man navigera mellan det förväntade och det oväntade. Det finns behov av att identifiera vilka hot som prioriteras just nu, vilka som ignoreras och skälen till dessa val. Det är också viktigt att försöka förstå vilka hot som bara är beta för tillfället, för att sedan mer eller mindre försvinna, vilka nya hot som är under uppsegling och vilka hot som är ungefär desamma som förr. Denna artikel är en reflektion över bedömningar om framtida militära hot och hur Försvarmakten har sett på dessa från kalla kriget och framåt.*

## **PERSPEKTIVSTUDIEN – ATT TITTA 20 ÅR FRAMÅT FÖR ATT GE RÅD IDAG**

Vilka framtida hot Sverige kan komma att möta och hur dessa ska hanteras är viktiga frågor för utvecklingen av totalförsvaret. Bedömningar av vad som kan förväntas i framtiden bidrar till att beslutsfattare redan idag kan göra viktiga vägval för att möta kommande behov. Det handlar ofta om stora investeringar som kommer att påverka inriktningen under lång tid framöver och då är det viktigt att välja så rätt som möjligt redan nu. Försvarmakten har i sin perspektivstudie under årtionden studerat detta ur ett militärt perspektiv för att ge kunskap och sammanhang till de långsiktiga beslut som behöver tas i närtid.

Perspektivstudien genomförs i fleråriga cykler bland annat syftande till att skapa underlag inför de försvarspolitiska inriktningsbeslut (nedan kallade försvarsbeslut) som fattas av riksdagen med cirka fem års mellanrum. Detta görs parallellt med genomförandet av innevarande försvarsbeslut. Perspektivstudien kan sägas bestå av fyra delar: Framtidsinriktad omvärldsanalys, framtagande av försvarskoncept på cirka 25 års sikt, framtagande av alternativa försvarsmaktsstrukturer på cirka 15 års sikt och slutligen konkreta råd inför kommande försvarsbeslut.

Omvärldsanalysen i nuvarande perspektivstudie, det vill säga inför försvarsbeslut 2025, undersöker brett utvecklingen mot 2045 och vad som kan påverka Sveriges säkerhet. Den innefattar analyser av globala trender, säkerhetspolitik, motståndare, samarbetspartners, svensk samhällsutveckling, militärteknik och framtida operationsmiljö. I omvärldsanalysen identifieras framtida drivkrafter, utmaningar och hot och den används för att skapa en uppsättning scenarier som försöker fånga framtidens osäkerhet. Scenarierna används för att åskådliggöra militära problem och bidrar till att skapa idéer för framtida lösningar på dessa, så kallade försvarskoncept. I nästa steg konkretiseras dessa idéer ytterligare i försvarsmaktsstrukturer och hänsyn tas då till dagens försvarsmakt såväl vad avser nuvarande förmåga som långsiktiga bindningar inom personal-, materiel- och infrastrukturförsörjning. Dessa alternativa strukturer är en utgångspunkt

för hur Försvarsmakten skulle kunna se ut med olika framtida inriktningar. Strukturernas förmåga att hantera olika hot värderas sedan genom exempelvis spel. Slutligen analyseras hur den framtida försvarsförmågan kan realiseras och vilka beslut som behöver fattas i närtid.

I den senaste perspektivstudien 2016 – 2018, inför försvarsbeslut 2020 anges att Rysslands geopolitiska intressen och militära aktiviteter fortsatt utgör dominerande utmaningar i Östersjöområdet. Det påtalas dock att det råder viss osäkerhet om Sveriges säkerhetspolitiska position eftersom den globala säkerhetspolitiska miljön är i förändring. Vidare anges att den tekniska utvecklingen medför att Försvarsmakten i hög grad behöver beakta hot från rymden och cyberdomänen samt att så kallad gråzonsproblematik mellan krig och fred ställer nya krav. Det kan dock konstateras att många av dagens hot har diskuterats under lång tid. En tillbakablick på tidigare bedömningar och hur situationen förändrats kan ge perspektiv och lärdomar inför dagens ställningstaganden.

### **TILLBAKABLICK**

Under kalla kriget var den säkerhetspolitiska bedömningen att situationen i Europa karaktäriserades av stabila relationer. Utvecklingen styrdes av stormakternas politiska och militära intressen. I perspektivstudien från 1975 beskrivs hotet som tydligt och stabilt. Det fanns ett klassiskt invasionshot att planera för, däremot var hotnivån inte heller då självklar utan varierades. Kärnvapenhotet var en realitet att förhålla sig till liksom hotet om det överraskande angreppet. Det stora totalförsvaret som byggts upp under och efter andra världskriget ansågs tillräckligt för att hantera ett storskaligt väpnat angrepp där hela samhället skulle drabbas.

Försvarsbeslutet 1987 blev starten för ett antal neddragningar i det militära försvarets organisation, bland annat föranledd av underfinansierade försvarsbeslut men sedan accelererad på grund av Berlinmurens fall och Sovjetunionens upplösning. Efter de första årens turbulens ledde det ändrade säkerhetspolitiska läget till bedömningen att det inte längre fanns något påtagligt militärt hot mot Sverige. Invasionsförsvaret ansågs därmed vara otidsenligt och feldimensionerat för den nya tidens hot och uppgifter. Detta ledde i sin tur till en avveckling av totalförsvaret. I perspektivstudien från 1997, i övergången mellan invasionsförsvaret och det senare insatsförsvaret, talas om en bredare hot- och riskbild. Liksom idag talades det om det som numera ofta kallas hybrida hot: ”... angreppsmetoder som i sig kan spänna från dolda informationsinsatser till olika former av väpnade insatser – ibland hänförliga till militärstatligt ursprung – ibland med mer obestämbart ursprung”. Den bredare hotbilden blev tydlig i perspektivstudien från 2006 där man talar om att hantera hot i hela skalan från krishantering i låga konfliktnivåer till fullt krig mot en högteknologisk motståndare. Det talas om hot mot globala flöden, snabba händelseutvecklingar och att händelser i mer avlägsna delar av världen snabbt kan ge konsekvenser även nationellt.

## **FRAMTIDA HOT GENOM TEKNISK UTVECKLING**

Den tekniska utvecklingen bedöms få stor påverkan både på framväxten av möjliga hot från en motståndare och för utvecklingen av inte bara det militära försvaret utan hela totalförsvaret. Idag diskuteras vilken påverkan artificiell intelligens, automation, bioteknologi, kvantteknologi med flera teknikområden kan få i framtiden, både allmänt i samhället och för militär förmåga. Bland dessa och andra teknikområden spanas det efter så kallade disruptiva teknologier, det vill säga teknik som på något sätt innebär ett revolutionärt genombrott och helt eller delvis skulle kunna förändra förutsättningarna för en väpnad konflikt. En spännande utveckling för vissa, en skräckvision för andra. Kommer den som har den vassaste artificiella intelligensen eller som är först med operativa system som bygger på kvantteknologi bli dominant? Vad händer om människorna i stor utsträckning försvinner från det främre stridsfältet och ersätts med obemannade eller autonoma system? Om en överlägsen artificiell intelligens i realiteten även tar beslut om insats. Om kvantdatorer innebär att dagens krypton knäcks eller om prestationshöjande teknik och medel möjliggör övermänskliga soldater? En del av dessa tillämpningar diskuteras redan idag utifrån legala och etiska perspektiv.

Disruptiva tekniska genombrott är inget nytt. Det finns många sådana i historien. Två exempel med tydlig påverkan på den militära effekten är krut och kärnvapen. Är vi på väg mot nya sådana genombrott nu? Och vad innebär det för synen på det framtida hotet?

Studier pekar på att det egentligen inte är så svårt att uttala sig om vilka teknikområden som är intressanta. Desto svårare är det att veta exakt vilka tillämpningar som kan vara användbara och till vad. Det är också svårt att veta när tekniken är tillgänglig och vilka problem man måste lösa på vägen.

## **UTVECKLING AV HOTBILDEN I ETT FRAMTIDSPERSPEKTIV**

Det väpnade angreppet och motståndarens militära förmåga har traditionellt helt dominerat beskrivningar av den konfliktmiljö som Försvarsmakten ska verka i. Angriparen har här varit känd, tekniskt och numerärt överlägsen och våldsnivån hög. Idag läggs fokus även på angrepp mot Sverige av en okänd avsändare i en gråzon mellan krig och fred. En motståndare kan idag, inte minst på grund av den tekniska utvecklingen, med relativt små medel träffsäkert nå sina mål och därmed undvika en upptrappning som leder till väpnad konflikt. Angreppen kan ske med olika grad av intensitet och utgöras av till exempel sabotage, påverkansoperationer och cyberattacker som riktas främst mot civila mål. En fråga är hur sådana angrepp ska hanteras. En annan fråga är om den nuvarande verktygslådan som finns inom totalförsvaret behöver stärkas. Tydligt är att samverkan och samordning inom ramen för totalförsvaret blir allt viktigare för att identifiera en angripare och att möta ett angrepp som sker i fredstid, utan att beslut om höjd beredskap fattats.

## REFLEKTIONER KRING FRAMTIDA MILITÄRA HOT

Bedömningen av möjliga militära hot har varit central för finansiering och inriktning av försvaret, vilket medfört stora kast mellan utveckling och avveckling och lett till att det nu finns stora brister i totalförsvaret. Försvarsberedningens rapporter visar att det idag finns politisk vilja att satsa på en grundförmåga som behöver finnas över tid oavsett aktuell hotbild.

Vid utveckling av framtida militär förmåga är det viktigt att titta brett på möjliga militära hot och speciellt den palett av medel som en antagonist kan använda sig av. Hot behöver förstås ur flera olika perspektiv. Vad händer exempelvis om antagonisten är tekniskt mer avancerad och bättre övad? Då kan en satsning på stor kvantitet vara otillräckligt. Å andra sidan kan en satsning på kvalitet innebära så få resurser att det blir en svaghet i sig.

Mycket av de resonemang som förs kring hot idag känns igen från tidigare bedömningar. Hot och risker bedöms beröra hela samhällsstrukturen och en motståndare förväntas utnyttja samhällets känslighet genom att slå mot vitala funktioner. Man får inte glömma bort att militära medel kan användas mot civila mål. Militära hot blir därmed relevanta även för andra än Försvarsmakten.

Avslutningsvis är det lätt att i framtidsstudier drunkna i osäkerheter både om framtiden i sig och om möjliga framtida hot. Vissa saker går att förutsäga mer eller mindre bra genom att samla information medan annat är genuint osäkert och innebär att det är nödvändigt att leta efter lösningar som kan hantera uppkomsten av oförutsedda händelser. Det är rimligt att börja analysen i det som är minst osäkert, undersöka förutsättningarna i olika framtida förhållanden och låta det som är osäkert tydligt framgå i slutresultatet. Detta innebär också att man behöver prioritera mellan hoten och börja med dem som bedöms som mest säkra. Detta understryker också vikten av att jobba med flexibla strategier som kan anpassas för att möta olika omvärldsutvecklingar. Sådana analyser är en del i perspektivstudiens roll när det gäller utvecklingen av det militära försvaret.

Att i perspektivstudien studera framtida hot ger möjligheten att värdera dagens lösningar i ljuset av framtida möjliga hot. Sådana studier bör även bedrivas inom det civila försvaret. Att titta på andra hot än de som ligger högst på agendan idag ger förutsättningar för ett robustare totalförsvaret som är relevant över tiden. Historien visar att det är lätt att bygga in sig i en återvändsgränd och den typ av framtidsinriktade arbeten som beskrivits här ger en möjlighet att motverka detta.

## **FÖR VIDARE LÄSNING**

Göran, Kindvall, Lindberg, Anna, 2020, *Militärteknin 2045 – Ett underlag till Försvarsmaktens perspektivstudie*, FOI-R--4985--SE.

Kindvall, Göran, 2019, *Hur kan den framtida operationsmiljön se ut?*  
FOI Memo 6844.

Försvarsmakten, 2018, *Tillväxt för ett starkare försvar*, FM2015:13192:15.



## 2. Hoten mot Väst och transatlantiska relationers framtid

Niklas H. Rossbach

*Bara veckor innan Rysslands angrepp på Ukraina 2014 drog Sveriges dåvarande statsminister slutsatsen att "Samarbetet i EU och Nato gör att det är svårt att tänka sig något avgörande militärt hot mot något av Europas länder." Det är förstås lätt att vara efterklok. Ofta fungerar linjärt tänkande, där morgondagen förväntas vara som idag, men inte alltid. Men att glömma århundranden av konfliktfylld europeisk historia och hävda att krig i Europa i praktiken är en omöjlighet är alltid våghalsigt.*

*En stor risk för Västs säkerhetspolitiska sammanhållning är ifall Väst är oförberett på såväl nya som gamla säkerhetspolitiska hot. Beredskap kräver fantasi att föreställa sig dem. Utan fantasi går det vare sig att förstå omvärldsutvecklingen eller förbereda sig på farorna med revanschistiska stormakter. Fantasibrister riskerar att leda till misslyckad beredskap, vilket skulle kunna drabba utvecklingen av Sveriges totalförsvar. Ett bra avstamp för att förbereda sig på utvecklingen är att uppmärksamma tre scenarion gällande Västs viktigaste relation, nämligen den inom Väst – mellan USA och Europa, de transatlantiska relationerna.*

### **SAMMANHÅLLNINGEN BÖRJAR RÄMNA**

Finanskrisen, som bröt ut 2008, sädde tvivel om Västs sammanhållning. Hos revanschistiska stormakter, som Ryssland, väckte krisen förhoppningar om att kunna utmana den Västledda internationella regelbaserade ordningen. Sedan länge utgörs kärnan i Väst av USA och Europa. Under det kalla kriget – efter två blodiga världskrig och tack vare beskydd av en utomeuropeisk stormakt, USA – började demokratier i Västeuropa främja europeisk integration. Vid kalla krigets slut var fortsatt europeisk integration en självklar del av den internationella regelbaserade ordningen där global handeln främjades, världsfreden säkrades och mindre stater vann inflytande tack vare multilateralt samarbete.

Efter den ekonomiska krisen 2008 – 2011 har de geopolitiska utmaningarna följt slag i slag. Ryssland annekterade oväntat Krim 2014. Storbritannien röstade 2016 för ett utträde ur EU. Sannolikt bidrog den ekonomiska krisen till att landet blev alltmer EU-skeptiskt. Brexit är ett betydande geopolitiskt bakslag för EU eftersom det innebär att unionen förlorar en av två stormakter med förmågan att skicka stora militära styrkor långt bort. Även valet av Trump till USA:s president 2016 förvånade världen. Att han dessutom, liksom sin företrädare, ofta fokuserat på Asien har överraskat många bedömare.

Det ständiga dilemmat för Europas försvarspolitiska utveckling har varit att om Nato-allierade i Europa gör mindre än vad USA önskar se i form av för-



svarssatsningar eller insatser, så försämrar det transatlantiska relationer. Men om Europa istället ökar sin egen militära förmåga inom EU kan även det irritera USA som vill värna sin ledande roll i Väst.

### **ATT HANTERA REVANSCHISTISKA STORMAKTER**

Vare sig annekteringen av Krim eller Rysslands fortsatta aggression mot Ukraina lyckades splittra Väst. Den svenska försvarsberedningen har pekat på risken för att flera konflikter mellan Väst och revanschistiska stormakter kan äga rum samtidigt i framtiden. Det kan handla om kinesiskt agerande i Asien som ger Ryssland möjlighet att ta större risker i Europa utifall att USA tvingas fokusera på Kina. En sådan situation skulle innebära att Europa i större utsträckning behöver försvara sig själv. Trots dagens närvaro av amerikanska stridskrafter i Europa kan USA:s försvarsmakt behöva koncentrera sig på att hjälpa USA:s allierade i Fjärran Östern. Således behöver Europas försvar stärkas, men det i sig är i dagsläget en säkerhetspolitisk utmaning för transatlantiska relationer.

Om Europa i framtiden i större utsträckning än idag behöver vidmakthålla sin egen säkerhet finns tre alternativ: Renovera traditionella transatlantiska relationer, lansera sig som en mer jämbördig partner till USA eller ta sin säkerhet i egna händer. Det som verkar pågå är det förstnämnda alternativet. Nato rustas upp och fokuserar på försvaret av de europeiska medlemmarna i alliansen. Utvecklingen är dock beroende av USA:s militära förmåga och dessutom har Europa sannolikt inte längre samma geopolitiska huvudmotståndare som USA.

Det andra alternativet vore att fördjupa transatlantiska relationer exempelvis genom att återuppliva frihandelsavtalet mellan EU och USA, *the Transatlantic Trade and Investment Partnership* (TTIP). Det skulle göra EU till en mer jämbördig partner till USA. Ett nytt TTIP-initiativ skulle öka USA:s intresse både för Europas ekonomi och dess säkerhet. En annan möjlighet vore att skapa en så kallad europeisk pelare inom Nato, där de europeiska Nato-medlemmarna har en tydligare egen samlad roll. Men ett starkare europeiskt Nato stärker inte EU:s ställning. Oavsett om alternativ två stärker EU eller Nato skulle Europa ändå som helhet behöva säkerställa sin egen försvarsförmåga inför en framtida stormaktskonflikt. Ätminstone för att vinna tid tills dess att hjälp anländer.

Det tredje alternativet handlar i första hand om att EU ska ta ett större ansvar. Detta är ofta förknippat med vaga visioner som kännetecknas av slogans som exempelvis ”strategisk autonomi”. Risken med sådana visioner är att Europa stöter ifrån sig sin närmsta partner, USA, samtidigt som Europa ökar sitt beroende av Ryssland och Kina vars energiexport respektive handel Europa behöver. Sådana visioner kan alltså försvaga Europas försvar innan en egen militär förmåga är på plats. Detta är ett dilemma för visioner som ska motivera europeiskt försvarssamarbete och stärka Europas säkerhet.

## EN NÄTVERKSBASERAD SÄKERHETSPOLITIK – ETT FJÄRDE ALTERNATIV?

De geopolitiska överraskningarna har bidragit till en rad olika försvars- och säkerhetspolitiska initiativ. Tillsammans kan dessa ses som ett fjärde alternativ även om det inte är avsikten med de enskilda initiativen.

Några exempel på initiativ är EU:s utveckling av försvarsförmågor, exempelvis det permanenta strukturerade samarbetet (Pesco). Storbritannien har använt sin nya snabbinsatsstyrka, *the Joint Expeditionary Force* (JEF), som ett eget forum för samarbete genom att knyta till sig länder som är villiga att bidra till styrkans resurspool. Frankrike har lanserat ett annat initiativ, *the European Intervention Initiative* (EI2), som bland annat ska bidra till en gemensam europeisk strategisk kultur, genom exempelvis samverkan kring hotbilder. Sverige deltar i alla dessa multilaterala ansträngningar och är dessutom ett partnerland till Nato. Samtidigt samverkar EU och Nato alltmer, bland annat när det gäller hybridhot, såsom desinformation.

Överlappande internationella organisationer och multilaterala fora skapade under det kalla kriget en europeisk säkerhetsarkitektur som bidrog till stabilitet inom Väst, men även så småningom i hela Europa. Åtminstone fram tills dess att Krim annekterades. Arkitekturens säkerhetspolitiska stabilitet stod länge i kontrast till andra delar av världen vilka saknade motsvarande mängd överlappande institutioner.

Om det vore möjligt att länka samman alla nya initiativ skulle det innebära en moderniserad säkerhetspolitisk arkitektur som kan liknas vid en nätverksbaserad säkerhetspolitik. Hotbilderna av revanschlystna stormakter delas trots allt i större eller mindre utsträckning av alla länder i Väst. Samverkan blir kanske lättare när olika initiativ väl mognat. En etablerad nätverksbaserad säkerhetspolitik förutsätter dock att alla, eller i vart fall många, europeiska västländer deltar i de flesta samarbetena och att de nya initiativen blir ömsesidigt förstärkande, istället för att konkurrera med varandra. Med en sådan övergripande samverkan kan tryggheten för länder i Väst öka. De deltagande länderna skulle alltid ha möjligheten att använda sig av någon del av detta nya säkerhetspolitiska nät.

Ett sådant nätverkstänkande förutsätter möjligen nya sätt att flexibelt och snabbt koordinera Västs utrikes- som försvarspolitik. Nya säkerhetspolitiska rutiner och former för samarbete har skapats förr när hotbilden krävde det. Det skedde exempelvis när Nato bildades för att skydda Europa mot Sovjetunionen. För de länder som både är medlemmar av Nato och EU finns det också erfarenhet att bygga på. I praktiken skulle en gemensam utveckling och samverkan mellan alla initiativ kunna innebära en renovering respektive uppdatering av den gamla europeiska säkerhetsarkitekturen och transatlantiska relationer.

## **OM SAMMANHÅLLNINGEN SPRICKER**

Om Europa inte lyckas stärka sin egen försvarsförmåga riskerar Västs ledande roll i världen på sikt att vara förbi. Utan ett USA och ett Europa som båda är starka och kan stötta varandra blir det svårare att hävda gemensamma intressen, såsom den internationella regelbaserade ordningen. Om framtiden istället innebär en multipolär värld av jämnstarka stormakter kan USA sannolikt lyckas med att bli den främsta av jämligar. Däremot riskerar ett mer självständigt Europa att få svårare att hävda sig när det inte längre räcker med att vara en ekonomisk stormakt för att få inflytande i världen.

Vare sig EU, Nato eller Sveriges totalförsvar kan enbart handla om att damma av och uppgradera planer från kalla kriget. Nästa krig blir aldrig som det förra – inte heller kalla krig. Det gäller att inte glömma bort Clausewitzs påpekande att ”kriget är blott en fortsättning på politiken med andra medel”. Revanschistiska motståndare använder sin fantasi, vilket exempelvis bidragit till försök att rita om gränserna i Europa. Än så länge finns både EU och Nato kvar, men de har inte visat sig hindra Västs motståndare från att använda sin fantasi.

Dessutom står världen på tröskeln till en ny era tack vare cyber, artificiell intelligens med mera, men framförallt eftersom redan pågående tekniktrender förändrar vår kultur samt krigföring. Ryssland och Kina försöker redan att uppnå sina politiska målsättningar med andra medel än rent traditionella militära maktmedel. Exempelvis är påverkansoperationer, såsom manipulation av andra länders demokratiska val, mer konstadseffektiva och mindre riskfyllda än kärnvapenhot och blixtkrig. Beredskapen måste dock fortsatt beakta det hot som ofta ses som osannolikt – ett nytt storkrig.

För över hundra år sedan trodde initierade bedömare att den tekniska utvecklingen gjorde krig omöjliga, alltför många skulle stupa, kriget riskerade bli orörligt och alltför ekonomiskt kostsamt. Trots att respektive förutsägelse stämde, visade första världskriget att krig ändå både kunde bryta ut och fortsätta i årtal. Som den traditionella realpolitiken konstaterat är det inte alltid de ädlaste och bästa idéerna som vinner gehör i internationell politik. Istället får dåliga idéer ofta många anhängare liksom beslut kan få oförutsedda konsekvenser.

## **VÄGEN FRAMÅT**

Idag är den stora risken med länder som Ryssland och Kina att de kan försöka fullfölja dåliga idéer om aggressiv expansion och hävdandet av intressesfärer med mera, med hjälp av ny teknik. De utvecklar nya förmågor som går att använda med eller utan öppen militär krigföring för att underminera Västs säkerhetspolitiska handlingsfrihet. Väst måste därför leda den tekniska utvecklingen.

Teknikutvecklingen kan bidra med förmågor som kan avskräcka nya typer av angrepp eller avvärja attacker på nya arenor. Dessutom kan tekniksamarbete mellan länder i Väst stärka nya säkerhetspolitiska initiativ och eventuellt ett nytt framväxande mellanstatligt säkerhetspolitiskt nätverk i Väst. Teknicsamarbete kan

till och med växlas mot säkerhetspolitisk sammanhållning och motverka Västs sönderfall. Men målet kan inte vara teknikutveckling för teknikens skull. En sådan utveckling kan dock bidra till en teknisk kapprustning och ett politiskt dödläge mellan Väst och dess motståndare.

I strävan efter ökad trygghet behöver Väst även undvika att militariseras till en grad som riskerar att undergräva de värden Väst vill bevara. För Väst kan teknikutveckling vara ett medel för att främja handel och en fortsatt global fred baserad på den internationella regelbaserade ordningen. Ett modernt och effektivt totalförsvar förutsätter därför att relevant teknikutveckling hänger samman med en realistisk säkerhetspolitisk omvärldsanalys som uppmärksammar motståndarens avsikter och agerande. Med andra ord förutsätter såväl ett sammanhållet Väst som ett fungerande totalförsvar, fantasi hos både ingenjörer och analytiker.

#### **FÖR VIDARE LÄSNING**

Roszbach, Niklas H., 2019, *USA:s framtida säkerhetspolitik – på 30 års sikt*. FOI Memo 6784.

Roszbach, Niklas H., 2019, *Whither transatlantic security? Values, interests and the future of US - European relations*, FOI Rapport FOI-R--4869--SE.

Roszbach, Niklas H., 2018, *The Geopolitics of Russian Energy – Gas, oil and the energy security of tomorrow*, FOI Rapport FOI-R--4623--SE.



### 3. Demokratisk säkerhet

#### ATT BEMÖTA HOTEN MOT SAMHÄLLETS GRUNDPRINCIPER

Anders Strindberg och Erik Svensson

*På ett grundläggande plan är medborgarnas demokratiska fri- och rättigheter och myndigheternas förmåga att trygga invånarnas säkerhet och hälsa i sig själv nationella intressen – alltså kärnan av det som ska försvaras mot angrepp. Dessa skyddsvärden har dock gemensamma sårbarheter som kontinuerligt är utsatta för angrepp. Begreppet demokratisk säkerhet, beskriver en i huvudsak samhällsvetenskaplig forskningsansats inom FOI som ser demokrati och demokratihot som sammanhängande storheter i ett system. Syftet är att bättre förstå kopplingarna mellan olika sårbarheter, sambanden mellan olika hot, samt att stimulera kritiskt nytankande kring motåtgärder och dess konsekvenser. Frågan om hur staten och samhället bemöter hot mot grundläggande värden utan att själv skada dem är en angelägen utmaning som kräver ett breddat perspektiv.*

#### **SÅRBARHETER OCH HOT**

Våra demokratiska fri- och rättigheter, myndigheternas förmåga att genomföra sina uppdrag och statens förtroendekapital är intimt sammankopplade, både som skyddsvärden och genom dess sårbarheter. Det står klart att de i tilltagande utsträckning utgör mål för så kallade asymmetriska hot. Det kan handla om främmande makter som under fred eller kris använder olika former av informationskrigföring för att splittra det svenska samhället och försvaga staten, i syfte att skapa bättre förutsättningar för sina egna strategiska målsättningar. Det kan också handla om inhemska aktörer som genom tvång eller våld försöker främja förändringar av samhället i linje med sina egna särintressen. Informationskrigföring, våldsbejakande extremism, hatbrott, grov organiserad brottslighet samt hedersrelaterat våld och förtryck är exempel på det spektrum av verksamheter som utgör konkreta hot, inte bara mot enskilda utan även mot civilsamhällets grundläggande funktioner och principer.

Forskare har pekat på en ökande social och politisk polarisering i västvärlden inklusive Sverige. För individen kan upplevelsen av att inte förstå komplexa samhällsliga utmaningar, som exempelvis migration eller ökad brottslighet skapa känslomässiga reaktioner som frustration, missnöje och ilska. Så även upplevelsen av att man själv eller ens grupp är marginaliserad eller förfördelad genom exempelvis arbetslöshet och utanförskap. Sådana reaktioner kan leda till ett sökande efter enkla förklaringar och lösningar. Möjligheten att kanalisera dessa känslor – mot andra samhällsgrupper, mot staten och myndigheterna, eller mot samhällets grundläggande principer – är elementära verktyg för både främmande makter i färd med påverkansoperationer och våldsbejakande extremister som håller på att bygga sina nätverk.

## **DESINFORMATION**

Andra staters media- och propagandaresurser är en del av den svenska informationsmiljön och samhällsdebatten men när de används i det fördolda och med fientliga syften kan man tala om påverkansoperationer. Med falska nyheter och annan desinformation tar denna verksamhet ofta sikte på samhällsdebattens mest inflammerade delar. Desinformation skräddarsys i så kallade trollfabriker och av främmande makters underrättelsetjänster i syfte att manipulera förståelse och attityder, bidra till ökad social och politisk polarisering samt minskad tillit till myndigheter och staten. När tonläget i det offentliga samtalet blir så uppskruvat att gemensamma utgångspunkter undergrävs och samhällsgrupper ställs mot varandra sliter detta i samhällsväven.

Desinformationen sprids via falska nyhetssajter, sociala media eller genom angriparens egna nyhetskanaler. Det är ofta svårt att avgöra vad som är sant, vinklat eller helt påhittat. Ännu svårare är det att utläsa vem som står bakom ett påstående, en tweet eller en artikel. I det moderna medielandskapets ofiltrerade mångfald är den okritiske läsaren en stor tillgång för en angripare. När falska nyheter konsumeras på sociala media, tas för sanna och delas vidare bidrar detta till att utöka angreppets omfattning och därmed den skada eller förvirring som desinformationen syftar till. Påverkansoperationer behöver inte i första ledet innebära konkreta säkerhetshot, men på längre sikt riskerar de att nöta ner de institutioner, den tillit och den sammanhållning som behövs för att bemöta säkerhetshot.

## **VÅLDSBEJAKANDE EXTREMISM**

Även de extremistiska grupper som frodas i den svenska informationsmiljön drar nytta av individens känslomässiga reaktioner. De sätter individens frustration, ilska eller naggande känsla av att vara förfördelad i ett enkelt och begripligt sammanhang som i sin tur mynnar ut i enkla och begripliga lösningar. Att framföra förenklade eller felaktiga påståenden i samhällsdebatten är naturligtvis allas rättighet. Problemet uppstår när extremistiska miljöer, fysiska och virtuella, i sin tur skapar individer och grupper som ser tvång eller våld, alltifrån förföljelser av enskilda till folkmord, som vägen framåt. Inom de miljöer som ifrågasätter eller förnekar andra människors lika värde och lagstadgade rättigheter – men samtidigt utmålar sig själva som rättfärdiga offer – är steget ofta kort till tvång och våld.

Våldsbejakande extremism förefaller vara på uppgång i Sverige. Detta gäller i synnerhet inom de islamistiska och högerextrema miljöerna och våldstendenserna finns på både individnivå, så kallade ensamagerande gärningspersoner, och på gruppnivå. I detta sammanfaller utvecklingen i Sverige med bredare trender i Europa och globalt.

## **IN- OCH UTRIKES NÄTVERK**

Våldsbejakande grupperingar delar alltså merparten av sitt tankegodts med bredare extremistiska miljöer i Sverige inom vilka man inte förespråkar våld och därmed håller sig inom lagens ramar. Det är värt att nämna att den islamistiska extremistmiljön även delar väsentliga perspektiv på individen och sam-

hället med en annan form av våldsbejakande extremism, hedersrelaterat våld och förtryck. Detta trots att det inte nödvändigtvis har någon direkt koppling till vare sig Islam eller islamistisk extremism. Begreppet hedersrelaterat våld och förtryck, som det beskrivs av regeringen, innefattar företeelser som tvingande särbehandling, misshandel och till och med mord av enskilda i syfte att skydda ett kollektiv. Även könsstympning, oskuldskontroller, tvångsgifte och andra former av könsbaserad särbehandling förekommer och utgör kollektivets sätt att bevara sin heder och särart. Detta sker alltså på bekostnad av individens fri- och rättigheter och utgör en utmaning mot rättsstatens principer.

Den våldsbejakande vänsterextremismen förefaller ha förlorat mycket av sin slagkraft det senaste årtiondet. Dock förblir den aktiv och befinner sig enligt vissa bedömare i en slags aktivistisk växelverkan med högerextremismen: När högerextremismen blir synligare tilltar aktiviteterna inom den våldsbejakande vänstern. En liknande växelverkan finns även mellan de våldsbejakande islamistiska och högerextrema miljöerna. Den våldsbejakande extremvänstern presenterar sig nu som antifascistisk med en bred definition av vad fascism innefattar, men bland fienderna ingår nästan undantagslöst staten, myndigheterna och den nuvarande samhällsordningen. Den har dessutom ett ökat fokus på bland annat djurrättsfrågor och miljöaktivism, vilket förefaller öka våldspotentialen kring dessa frågor.

Våldsbejakande grupperingar återfinns även i komplexa internationella nätverk vars kontakter tack vare teknologiska framsteg har blivit både snabbare och mer svårövervakade. Nätverken syftar till informationsdelning, inspiration och utbyte av idéer, samt samordning av taktiska initiativ och strategiska ansatser. Exempelvis står en del av den våldsbejakande högerextremismen i förbindelse med en framväxande rörelse i USA för vilken accelerationism – tanken att man genom spektakulära våldsdåd kan påskynda det demokratiska samhällets oundvikliga sammanfall – är tongivande. Andra står i förbindelse med bland annat den ultranationalistiska Ryska imperiska rörelsen och dess paramilitära gren Imperiska legionen, vilken har stridit på rysk sida i Donbass i Ukraina, Syrien och Libyen. De två svenskar som låg bakom bombdåden i Göteborg 2016 hade tidigare samma år genomgått ett paramilitärt träningsprogram vid ett av Imperiska legionen drivet träningsläger utanför Sankt Petersburg.

Samtidigt har våldsbejakande islamister i Sverige knutit kontakter med till exempel Islamiska staten och al-Qaida, vilka båda utövar våld i syfte att upprätta ett världsomspännande kalifat. Dessa kontakter har resulterat i våldshandlingar bland annat inom ramarna för kriget i Syrien men även svenska medborgares inblandning i terrordåd i Europa samt planerade och genomförda terrordåd i Sverige. Både den våldsbejakande islamismen och högerextremismen har dessutom kopplingar till olika former av kriminell verksamhet.



## **KOMPLEXA SAMBAND OCH GEMENSAMMA NÄMNARE**

Man skulle kunna göra det lätt för sig genom att säga att det som beskrivits ovan helt enkelt är en överblick av den asymmetriska hotbildens olika komponenter. För var och en av dessa komponenter finns ett hanteringsansvar som ålagts ett visst departement eller myndighet. Varje myndighet har sitt mandat, sina handböcker och handlingsplaner. Vad som gör en sådan ansats ohållbar är att komponenterna egentligen bara kan förstås som en sammanhängande helhet.

Hur departement och myndigheter väljer att hantera varje enskild komponent kan ha systemomfattande återverkningar. En bristande helhetssyn och samordning kan i sig vara en säkerhetshotande faktor. Hur hanterar man till exempel att inhemska våldsbejakande extremister använder falska nyheter tillverkade av utländsk underrättelsetjänst för att skapa opinion i det offentliga rummet? Vad gör man när ett problem som de demokratihotande effekterna av hedersrelaterat våld och förtryck består av så många komponenter att de i praktiken är uppdelade på åtminstone ett halvdussin myndigheter och departement? Hur gör man när två värden – demokrati och säkerhet – ställs mot varandra?

Det finns alltså goda skäl att röra sig mot ett mer holistiskt perspektiv i forskning och analys såväl som hantering av detta problemkomplex. De olika grupperingarna, nätverken och företeelserna samverkar, påverkar och återverkar på varandra i ett sammanhängande system. Analyser av enskilda komponenter kan aldrig fånga helhetens dynamik och punktsatser kan störa en del av systemet men lämnar helheten intakt.

## **VARFÖR ETT NYTT BEGREPP?**

Begreppet demokratisk säkerhet beskriver en i huvudsak samhällsvetenskaplig forskningsansats inom FOI, som ser antagonistiska hot mot de demokratiska fri- och rättigheterna samt mot rättsstatens principer och funktioner som ett sammanhängande problemområde. Denna helhetssyn har lett till två huvudsakliga utgångspunkter: För det första att analysen av hotets komponenter måste förhålla sig till den sammanhängande helheten och för det andra att hanteringen av hotet måste utgå från och bidra till de demokratiska grundvärden som man avser skydda.

Inom säkerhetsstudier har breddningen av säkerhetsbegreppet pågått en längre tid. Traditionellt snäva uppfattningar om att säkerhet enbart betyder upprätthållandet av statens våldsmonopol och vidmakthållandet av militär makt på den internationella arenan har utvidgats. Detta har skett exempelvis genom att beakta strukturer och diskursers inverkan samt belysa sårbara gruppers situation och perspektiv på konflikter.

Striderna om vetenskapliga metoder har dock varit långa och hårda. Den moderna positivismen med sina mätbara fakta och objektiva sanningar har ställts mot den postmoderna konstruktivismens subjektiva och relativistiska perspektiv. I en metaanalys av forskningsteorier har dock sociologen John R. Hall visat att

de vattentäta skott som satts upp mellan fakta- och värdebaserade metoder inom samhällsvetenskapen egentligen är fiktiva. Det finns goda grunder för integrering av till synes motsatta metoder och förklaringsmodeller. Därmed finns det även goda förutsättningar att skapa en bredare och djupare förståelse av utmaningarnas många dimensioner.

En bredare förståelse av säkerhet innefattar inte bara vad som hotas och av vem, utan också hur och varför hotet uppstår. Det omfattar även om man kan bemöta hotet innan det uppstår, och hur andra hot påverkas av de åtgärder som vidtas. Komplexa problem kräver ändamålsenliga verktyg. De som ansvarar för att bemöta hoten måste förses med verktyg som kan hantera både bredd och djup. Vi menar att det krävs mer än ”uppifrån och ner”-lösningar från traditionella säkerhetsaktörer för att hantera det demokratiska samhällets säkerhet på ett sätt som stärker samhällets resiliens.

Försvarsmaktens förståelse och hantering av konfliktodynamik vid utlandsuppdrag i till exempel Mali och Afghanistan har förbättrats genom att medvetet anlägga genderperspektiv i konfliktanalysen, inte istället för, utan som komplement till befintliga analyser och metoder. På ett liknande sätt har Polismyndighetens förmåga att förebygga våldsamma sammandrabbningar stärkts genom att integrera insikter från Social identitetsteori i den befintliga hanteringen. Denna ansats uppkom efter de omfattande problemen vid hanteringen av Göteborgskravallerna 2001 och har lett fram till inrättandet av Dialogpolisen och framarbetandet av konceptet Särskild polistaktik. Detta visar att det är möjligt även för verksamheter med lång erfarenhet, gedigen kunskap och väl inarbetade metoder att utvecklas och bli mer effektiva genom att anta ett bredare angreppssätt och lära sig från nya och kanske tillsynes sällsamma metoder.

Ansaret att skydda demokratin och rättsstaten kräver aktiv samverkan med och transparens gentemot de aktörer som bygger upp och säkerställer en robust demokrati – det vill säga civilsamhällets olika aktörer och ytterst Sveriges befolkning. Exempelvis är utanförskap eller oförmåga till källkritik naturligtvis inte i sig säkerhetshot – men de är icke desto mindre ständigt återkommande faktorer i demokratihotande verksamheter. Denna observation ger en central roll i demokratiskyddet till långt fler aktörer än de övervakningsansvariga och brottsbekämpande myndigheterna. Ambitionen bör vara att förekomma de akuta säkerhetsproblemen. Demokratisk säkerhet som begrepp skapar bredden som krävs för att kunna förstå och förebygga antagonisters säkerhetshotande verksamhet samt förutse och förhindra säkerhetshotande konsekvenser av statens och myndigheternas egen hantering av utmaningen.

## **FÖR VIDARE LÄSNING**

Strindberg, Anders, 2021, *Social Identity Theory and the Study of Terrorism and Violent Extremism*, FOI-R--5062--SE.

MSB, 2014, *Att värna den demokratiska rättsstaten*, MSB706 – maj 2014, ISBN 978-91-7383-455-1.

## 4. Robusta beslut för hantering av ett förändrat klimat

Christoffer Wedebrand, Karin Mossberg Sonnek och Per Wikman-Svahn

*Efter att Klimat- och sårbarhetsutredningen presenterade sin rapport 2007 har arbetet med klimatanpassning satt igång på allvar vid Sveriges kommuner, länsstyrelser och myndigheter. Arbetet är mycket angeläget, inte minst eftersom kostnaderna för att inte anpassa samhället skulle komma att räknas i miljardbelopp. Men samtidigt försvåras arbetet av de stora osäkerheter som är förenade med klimatiförändringen och dess framtida effekter. Nedan visar vi hur dessa osäkerheter försvårar beslut om förebyggande åtgärder. Vi ger också ett förslag på hur man skulle kunna hantera problemen – förslaget är nära besläktat med metoder som utvecklades av FOA:s forskare under det kalla kriget.*

### **KLIMATFÖRÄNDRINGEN LEDER TILL BÅDE SÄKRA OCH OSÄKRA NATURHÄNDELSER**

Tack vare forskningen har vi god kunskap om att utsläppen av växthusgaser förändrar klimatet. Vi har också kunskap om att ett förändrat klimat ökar risken för olika former av naturhändelser, däribland översvämningar och jorderosion som en följd av en stigande havsnivå. Även Sverige är utsatt för dessa risker – just havsnivåhöjningen hotar såväl bostadsområden som viktiga verksamheter och infrastruktur i våra kustnära samhällen. Dessvärre finns det en tröghet i systemet som gör att även om världens länder kraftigt minskar sina utsläpp kommer klimatet ändå att fortsätta förändras. Därför behöver det även vidtas åtgärder för att minska klimatets påverkan på samhället, vilket kallas för klimatanpassning.

Men samtidigt som vi vet att klimatet förändras vet vi mindre om hur snabbt det kommer att ske och hur det kommer att påverka våra samhällen i framtiden. Flera faktorer bidrar till denna osäkerhet. En avgörande faktor är att vi inte vet hur våra samhällen kommer att utvecklas på sikt. Därför vet vi inte heller hur stora utsläppen av växthusgaser kommer att bli. Dessutom är det svårt att avgöra hur klimatet kommer att påverkas av en viss given koncentration av växthusgaser i atmosfären. Inte minst är det svårt att veta vilka effekter som kommer att uppstå på lokal nivå som en följd av ett globalt förändrat klimat. Tillsammans bildar omständigheter som dessa en kaskad av osäkerhet som gör det omöjligt att i detalj förutse framtiden.

Man kan därför säga att klimatiförändringen och dess effekter i form av naturhändelser är både säkra och osäkra: Vi vet att klimatet förändras och att det kommer att påverka oss, men vi vet inte exakt hur och i vilken grad. Därför är det också svårt att avgöra vilka åtgärder som bör vidtas för att hantera effekterna av det förändrade klimatet.

Ett konkret exempel är kunskapsläget om den stigande havsnivån. Vetenskapliga undersökningar har visat att havsnivån stiger och att det sker i en allt snabbare takt. Forskningen har också klargjort de viktigaste orsakerna till detta, nämligen att varmare vatten medför en ökad havsvolym och att smältande isar på land ökar den totala vattenmängden. Men det är betydligt svårare att avgöra hur mycket och hur snabbt haven kommer att stiga.

Olika organisationers förutsägelser av de framtida havsnivåhöjningarna innehåller därför relativt omfattande marginaler. Exempelvis anger FN:s mellanstatliga klimatpanel (IPCC) i sin rapport från 2019 att den genomsnittliga globala havsnivån, jämfört med referensperioden 1986-2005, kan komma att höjas med 0,29–0,59 meter till 2100 för ett lågt utsläppsscenario och med 0,61–1,10 meter för ett högt utsläppsscenario.

IPCC anger dock att det är 17 procents sannolikhet att havet stiger högre än de högsta värden som anges i intervallen i de båda utsläppscenarierna. I en analogi till tärningsspel motsvarar det sannolikheten att slå en sexa på ett tärningskast. Inte särskilt osannolikt alltså.

Andra organisationer har försökt bedöma sannolikhetsfördelningarna för mer extrema havsnivåhöjningar. Bland dessa kan nämnas en uppmärksammas rapport från USA:s nationella klimatanalys 2017. I ett scenario med höga utsläpp av växthusgaser visar man på en möjlig havsnivåhöjning på 2,5 meter fram till 2100. Sannolikheten för att scenariot ska inträffa bedöms visserligen vara mindre än en procent men det anses trots allt vara möjligt att det inträffar. Rapporten anger också scenarier fram till 2200 som tyder på att havet kommer att fortsätta stiga även efter 2100 och att mycket höga nivåer är möjliga.

Enkelt uttryckt kan alltså havsnivåhöjningen förväntas bli såväl ganska liten som synnerligen stor. Denna osäkerhet medför, eller borde åtminstone medföra, stort huvudbry för de som arbetar med att skydda våra samhällen från klimatförändringens negativa effekter. Speciellt eftersom kostnaderna av havsnivåhöjningens konsekvenser för infrastruktur, bostadsområden och kulturvärden i kustnära samhällen på sikt kan komma att räknas i miljardbelopp.

Är det ens meningsfullt att försöka vidta förebyggande åtgärder när vi inte vet om havet stiger med 0,3 eller 2,5 meter fram till 2100? Jo, vi menar att det är meningsfullt!

### **ROBUSTA BESLUTSSTÖDSMETODER FÖR ATT HANTERA FRAMTIDENS OSÄKERHET**

Med de stora osäkerheter som finns i hur snabbt och hur mycket havsnivån kommer att stiga inser man att anpassningsåtgärder som väljs mot bakgrund av endast ett troligt framtida scenario riskerar att leda fel. Det kan samtidigt anses onödigt att, för att vara på den säkra sidan, rusta sig för ett värsta tänkbart scenario eftersom sannolikheten för att det inträffar är väldigt liten. I så fall har vi gjort investeringar i onödan, kanske på bekostnad av andra angelägna områden.

Ett alternativ kan vara att använda så kallade robusta beslutsstödsmetoder. Dessa metoder handlar om att hitta robusta åtgärder, det vill säga åtgärder som fungerar hyfsat bra oavsett hur framtiden blir. Av den anledningen kan dessa komma väl till pass för att hantera klimatförändringens effekter. Det finns flera olika robusta beslutsstödsmetoder men de bygger som regel på samma principer, nämligen:

1. Att omfamna osäkerheterna
2. Att börja med beslutssituationen
3. Att hitta robusta åtgärder

Att omfamna osäkerheterna handlar enkelt uttryckt om att inte blunda för de osäkerheter som råder om framtiden. Tvärtom understryker denna princip vikten av att förhålla sig till de verkliga osäkerheterna. Till exempel genom att inte nöja sig med IPCC:s intervall för havsnivåhöjningen som bara omfattar 67 procent av de möjliga utfallen. Rådande osäkerheter bör även tydligt speglas i de beslutsunderlag som används. Att omfamna osäkerheterna innebär också att ta hänsyn till risken för extrema utfall – även om dessa har låg sannolikhet.

Att börja med beslutssituationen förstås bäst i kontrast till det vanligare tillvägagångssättet att först försöka förutsäga vad som kommer att hända, exempelvis genom att ta fram den mest troliga utvecklingen eller den förmodade värsta händelseutvecklingen. I motsats till detta handlar principen om att först bedöma vilka sårbarheter som finns i samhället, vilka tänkbara åtgärder som står till buds och hur länge åtgärderna är effektiva. Först därefter görs en fördjupad analys av osäkerheterna och då med ett fokus på relevanta områden.

Principen om att hitta robusta åtgärder handlar, slutligen, om att söka efter åtgärder som fungerar bra för en stor mängd osäkra utfall. Hela poängen med de två första principerna kan sägas vara att främja letandet efter sådana robusta åtgärder. De robusta strategierna kan delas in i statiska och flexibla varianter. De statiska strategierna handlar om att bestämma åtgärderna på förhand. I detta fall sätts åtgärderna på plats en gång för alla och är tänkta att fungera bra under många olika tänkbara framtidsscenarier. De flexibla strategierna består inte av på förhand bestämda åtgärder. Istället består strategin av flera alternativ som anpassas beroende på hur framtiden faktiskt utvecklar sig. För att exemplifiera skulle en statisk strategi kunna vara att idag bygga en hög vall runt ett område för att skydda det mot havsnivåhöjningarna, medan en flexibel strategi skulle kunna vara att höja gatunivåerna och golven inuti byggnader allteftersom havet stiger.

Inom ramen för forskningsprogrammet *Robusta beslut för att hantera klimatrisker i Sverige*, finansierat av Myndigheten för samhällsskydd och beredskap (MSB), undersökte forskare vid FOI, KTH och Lunds universitet i vilken utsträckning som de tre principerna för robust beslutsfattande används i offentliga planeringssammanhang i Sverige. Resultaten tyder på att de inte appliceras i

så stor utsträckning och att det vanligaste är att man planerar utifrån en linje ovanför vilken det anses säkert att bygga. Linjen bestäms oftast utifrån ett troligt värsta-scenario för hur högt havet kan tänkas stiga till 2100 och är oberoende av planeringssituationen. Värt att notera är att linjen inte tar höjd för fortsatta havsnivåhöjningar efter sekelskiftet.

Inom forskningsprogrammet undersöktes också möjligheten att använda de tre principerna för robust beslutsfattande i den fysiska planeringen i tre kommuner som ligger vid havet. Resultaten tyder på att det finns mycket att vinna på att införa ett nytt angreppssätt i den fysiska planeringen men också på att det finns många hinder för detta. Bland annat försvårar nuvarande lagstiftning om detaljplanläggning möjligheterna att ställa krav på framtida (flexibla) åtgärder som skulle kunna införas när havsnivån har nått en viss nivå.

### **HANTERINGEN AV OSÄKERHET INOM DET TIDIGARE TOTALFÖRSVARET**

Även om användandet av robusta beslutsstödsmetoder kan ses som ett nytt sätt att hantera osäkerheterna inom dagens arbete med klimatanpassning så är de tre principerna som beskrivits ovan inte nya i hanteringen av osäkerheter inom andra områden. Liknande principer kom till användning vid planering inom det tidigare svenska totalförsvaret. Forskare vid dåvarande Försvarets forskningsanstalt (FOA), en av föregångarna till FOI, föreslog i en rapport från 1994 ett antal vägledande principer ”till de som arbetar med planering under osäkerhet eller bedriver framtidsstudier”. Principerna byggde på forskarnas egen praxis och erfarenhet av planering inom det civila försvaret.

I likhet med de principer som redogörs för ovan menade forskarna vid FOA att framtidens osäkerhet många gånger måste accepteras och att denna osäkerhet bör lyftas fram i ljuset. Men forskarna framhöll även att det inte alltid lönar sig att upplösa, alltså minska, osäkerheterna. Om det är meningsfullt måste enligt forskarna avgöras mot bakgrund av de beslut som ska fattas. Forskarna föreslog även ett arbetssätt som ligger mycket nära principen om att börja med besluts-situationen, vilket de själva benämner som en nedifrånansats. Det vill säga att inte börja med att formulera scenarier utan istället utgå från en bedömning av tillgängliga resurser och stegvisa förändringar av dessa. Intressant nog förespråkade forskarna även användandet av flexibla åtgärder, vilket de själva kallar aktiva åtgärder, som väljs löpande över tid mot bakgrund av hur framtiden utvecklar sig.

Sammantaget kan vi konstatera att även om det specifika hot som man planerar för skiljer sig åt så kan de angreppssätt som FOA-forskarna använde för att hantera osäkerheter i beredskapsplaneringen under kalla kriget vara relevanta även idag. Samma beslutsstödsmetoder verkar kunna användas oavsett om det handlar om anpassningar till följd av klimatförändringar eller andra samhällsutmaningar.

## FÖR VIDARE LÄSNING

Dreborg, K-H, Eriksson, E. A., Jeppsson, U. och Jungmar, M. 1994. *Planera för det okända? – Om hantering av osäkerhet*. Försvarets forskningsanstalt. FOA-R--94-00005-1.2--SE.

Wedebbrand, Christoffer. 2020. *Planering under osäkerhet: Om att planera för det okända inom krisberedskapen, totalförsvaret och andra områden*. FOI-R--4972--SE.

Wikman-Svahn, P. 2016. *Principer för robusta beslut inför osäkra klimatförändringar*. Kungliga tekniska högskolan. ISSN 1402-7615. TRITA-IM 2016:02.





## 5. Framtidens hot – ser vi dem komma?

OM SVERIGES KAPPLÖPNING IN I EN CYBERFRAMTID  
MED SPRÅKLIGA UTMANINGAR

Vidar Hedtjärn Swaling och Jenny Ingemarsdotter

*På den digitala arenan formas framtidens samhälle och nya hotbilder. Men istället för att blicka utåt mot specifika typer av cyberhot, tittar vi inåt och betraktar hur Sveriges iver att bli världs bäst på digitalisering kan skapa säkerhetsrisker genom att sårbarheter undervärderas. I detta sammanhang belyser vi också en typ av utmaning för vår föreställningsförmåga som Sverige delar med resten av (cyber) världen: Hur kan framtidens hot göras begripliga i en värld av alltmer integrerade intelligenta maskiner? Hur länge till håller de enkla metaforer som genomsyrar vårt språkbruk, och hur kan Sverige rusta sig för en framtid där hoten är överallt och inuti allt?*

### **DET DIGITALISERADE SAMHÄLLETS LOCKELSE**

I Sverige välkomnas den digitala transformationen. Sverige vill vara i framkant – ett modernt land med smarta städer, ett land vid frontlinjen. Kombinationen av teknikoptimism och kapploppningsmentalitet har samtidigt skapat brister i kravställningar vid införandet av ny teknik. I visionernas jakt mot framtiden har sådant som låter tungt och marknära, som infrastruktur och säkerhet, svårt att få uppmärksamhet. Digitaliseringen har i många fall blivit ett mål i sig snarare än ett medel.

Utvecklingshastigheten underblåses av mer eller mindre teknikoffensiva kampanjer. Men föreställningen om exempelvis Stockholm som världens smartaste stad åtföljs inte av en idé om hur staden i motsvarande grad blir säker. I de strategier och visioner som betonar digitaliseringens möjligheter varnas istället för att utvecklingen i Sverige går långsammare än i andra länder. Att det slarvas med grunden kan dock få till följd att tjänster motverkar sitt syfte, till exempel genom att de skapar ökade kostnader, ineffektivitet och frustration snarare än nytta, samt genom att sårbarheter och säkerhetsbrister byggs in i de nya systemen.

Därmed finns idag digitaliseringsprojekt som blivit resursslukande svarta hål, som dessutom har skapat en större administrativ börda för både personal och medborgare. Det finns dessvärre inget som säger att detta reder upp sig med tiden. Tvärtom kan man tänka sig att det uppstår inläsningseffekter genom att problemen blir så komplexa att de blir svåra att överblicka och ta sig ur. *Internet of Things* driver på denna utveckling ytterligare, genom att i princip allt vi har omkring oss – från tandborstar och dammsugare till hissar och klaffbroar – kan kopplas upp och ihop.

Till detta kommer hoten. De kan komma i form av automatiserade men intelligenta attacker mot våra samhällsviktiga system eller mot våra demokratiska

processer. Men när man talar om hot och digitalisering finns ytterligare en problemnivå – risken att man inte ens förstår vad som är ett hot, eller hur det ska beskrivas.

### **VAD HÄNDER NÄR SPRÅKET INTE LÄNGRE RÄCKER TILL?**

Hot är till sin natur abstrakta, åtminstone i meningen att de syftar på något som ännu inte har inträffat. För att förstå hot är man därför beroende av språkets förmåga att fånga och förmedla fenomen som antas kunna bli farliga på något sätt, någon gång. Men vad händer när ny teknik och nya vanor springer ifrån våra invanda begrepp och kategorier?

En av den moderna språkfilosofins insikter är att våra begrepp inte är frikopplade från verkligheten utan tvärtom är oupplösligt förbundna med hur de används. Begrepp är inte abstrakta entiteter som används *om* handlingar, *om* metoder, *om* vanor och konventioner, utan de är en del av allt detta. Kopplingen mellan språket och den vardag det förekommer i är alltså inte tillfällig utan *nödvändig*. Betyder det att den skillnad man har sett mellan vision och praxis när det gäller den digitala utvecklingen också skulle kunna leda till ett förvirrande och missledande språkbruk?

Ett exempel på svårförklarad hot härstammar från den pågående sammansmältningen mellan cyber och fysiskt. Maskiner och processer har styrts av datorer i över ett halvt sekel. Till en början handlade det om skraddarsydd system med mycket specifika uppgifter. Men idag kan i princip vad som helst kopplas upp mot vanlig datorutrustning, lokalt eller över internet, för kommunikation, styrning och övervakning. Att ett system är cyberfysiskt innebär att det har blivit otydligt var det ena börjar och det andra slutar, en otydlighet som växer när allt kan kopplas upp och när uppkopplingen flyttas allt längre ut i cyberrymden. Vad är en pryl i framtiden? Närmare bestämt, vad är cyber, och vad är fysiskt när dessa världar börjar förutsätta varandra? Det framväxande *Internet of Things*, eller sakernas internet, handlar inte bara om ökad uppkoppling utan om en transformerad tillvaro med intelligent system som är överallt och inuti allt (eng. *ubiquitous and pervasive*). Vårt språk, och därmed vårt tänkande, är samtidigt präglad av basala rumsliga metaforer.

### **TRE DIGITALA FÖRÄNDRINGSPARADIGM**

Vi har identifierat tre sociotekniska megatrender eller förändringsparadigm som är på god väg att ändra själva grunden för våra metaforer och i förlängningen vårt sätt att förstå världen.

- Cyber/fysiskt – saker kopplas upp
- Data/individ – data driver samhället
- Människa/maskin – datorer blir intelligent

Att saker kopplas upp för att kanske aldrig mer kopplas ned, som i fallet med *Internet of Things*, ändrar vår förståelse av vad en sak är och sakers förhållande till varandra. På motsvarande sätt gör *Big data*, och data som samhällets nya drivmedel, att individens gränser flyttas ut och luckras upp. Framstegen inom artificiell intelligens (AI) utmanar i sin tur uppdelningen mellan mänskliga och maskin. Utgångspunkten är att fenomen som tidigare varit åtskilda alltmer börjat överlappa eller sammansmälta, samt att de tre förändringsparadigmen tillsammans driver och skapar nya digitala hot och sårbarheter. I skärningen mellan dessa paradigmen kan det uppstå en intelligent entitet med oklar representation i den fysiska världen men med stora möjligheter att påverka den.

Samtidigt som många framtida hot kommer att utvecklas inom dessa förändringsparadigmen, och i gränsytan mellan dem, finns stora vinster att hämta för den som förstår hur man kan utnyttja teknikens nya möjligheter. Förhoppningar finns också om att ny smart teknik ska kunna lösa vår tids stora utmaningar – klimatet, energibehoven och välfärden. Inte minst i Sverige har storslagna visioner formulerats om digitaliseringen som lösningen på framtidens utmaningar. Men förstår vi alltid vad vi håller på med?

I ett land som baserat sin självförståelse på framstegstanken, som i grunden innebär att se sig själv som någon som ständigt rör sig framåt, kan säkerhetsarbete och riskanalyser uppfattas som showstoppers. Samtidigt är problemet med framtidens hot att de ligger just framför oss. Men en adekvat hotförståelse är inget vi kan skaffa oss i efterhand. Den byggs upp långsamt som en del av den tekniska utvecklingen, och den pågår nu.

## FÖR VIDARE LÄSNING

Ingemarsdotter, J., Eidenskog, D. och Swaling, V. H., 2020, *Vilse i lasagnen? En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur*. FOI-R--4814--SE. Stockholm: Totalförsvarets forskningsinstitut (FOI).

Stenlund, S., 1990, *Language and Philosophical Problems*. Cornwall: T J Press (Padstow) Ltd.

Lakoff, G. och Johnson, M., 1980, *Metaphores We Live By*. Chicago: The University of Chicago Press.



## 6. AI och påverkansoperationer i sociala medier

Fredrik Johansson, Magnus Rosell och David Gustafsson

*Det senaste årtiondet har påverkansoperationer kommit att spela en allt större roll i sociala medier. Detta innefattar medvetet skapande och spridande av falsk eller vilseledande information avsedd att påverka en ofta stor målgrupp. Påverkansoperationer kan utföras av alltifrån statliga aktörer med politiska motiv till individuella aktörer som handlar utifrån ekonomiska intressen. Inte minst i samband med folkomröstningar har forskare och anställda på sociala medieplattformar kunnat identifiera hur så kallade trollfabriker systematiskt använt stora mängder falska användarkonton i syfte att sprida påhittade användarkommentarer och falska eller vinklade nyheter. Påverkansoperationer i sociala medier förekommer dock mer eller mindre ständigt. Däremot är det svårare att spåra dessa tillbaka till en specifik utförare, vilket gör det till ett populärt verktyg för att med låg risk för upptäckt och represalier försöka påverka en målgrupps beteende eller åsikt i en viss fråga.*

Den snabba utvecklingen av artificiell intelligens (AI) har lett till en dramatisk förbättring av kvalitén hos automatiskt genererade texter, det vill säga texter som skapas utan mänsklig interaktion. Det är i många fall svårt för människor att särskilja genuina och automatiskt genererade texter, till och med då man på förhand känner till att texten potentiellt kan vara genererad. Liknande tekniker kan användas för att generera och manipulera bilder, videor och röster på ett så pass trovärdigt sätt att det blir svårt för den mänskliga hjärnan att särskilja dessa från äkta vara. Detta kan ha en stark inverkan på vårt digitala informations-samhälle då vi inom en snar framtid riskerar att översköjas av stora mängder automatgenererat innehåll vars kostnad att framställa är minimal och vars äkthet vi inte kan verifiera med våra egna sinnen. Detta riskerar att underblåsa en samhällsutveckling där sanning blir något sekundärt och där subjektivt tyckande det primära. För att komma tillrätta med denna samhällsutmaning krävs en rad åtgärder där AI-tekniker för att detektera automatgenererat innehåll är en viktig men inte tillräcklig del. En ökad medvetenhet kring att problematiken existerar är också en del av försvaret mot påverkansoperationer, vilket är en viktig motivation för att skriva denna text.

### **FALSK INFORMATION OCH PÅVERKANSOPERATIONER I SOCIALA MEDIER**

Att falsk information skapas och sprids i sociala medier är på intet sätt bara ett framtida hot utan något som sker redan idag. Recensioner av produkter och tjänster är ett område där det sedan länge funnits ekonomiska incitament att anlita personer för att skriva påhittade recensioner i syfte att framhäva den egna produkten eller smutskasta konkurrenter. Flera studier visar att detta är ett vanligt förekommande fenomen på tjänster som Yelp och Amazon. Samma sak gäller även för falska nyheter. Ett flertal reportage har lyft fram hur ett stort

antal människor i östeuropeiska länder har skapat påhittade nyheter om allt ifrån kändisar och hälsotrender till amerikansk politik. Dessa falska nyheter sprids via uppseendeväckande rubriker på sociala medieplattformar som Facebook och lockar till klick som genererar pengar i form av annonsintäkter.

Detta har en negativ påverkan på tilltron till digital information i sociala medier och på webben. Dessvärre tar det inte slut där. Även politiska påverkanskampanjer i stor skala utspelar sig i digitala miljöer. Detta uppenbarades exempelvis 2017 under den amerikanska debatten rörande nätneutralitet. Miljontals automat-genererade kommentarer som var kritiska till att internetleverantörer inte hade tillåtelse att kontrollera informationsflödet på Internet skapades baserat på enkla mallar. Sannolikt i syfte att påverka beslutsfattare genom att ge en skev eller kraftigt förstärkt bild av den allmänna opinionen. Ett annat exempel är olika statliga aktörers försök att på bred front påverka opinionen eller skapa splittring i andra länder, med den så kallade trollfabriken i Sankt Petersburg som ett välkänt exempel. Siffror från läckta dokument och journalistiska kartläggningar visar att det varje månad läggs stora belopp på att från ryskt håll skapa och sprida fiktivt innehåll avsett att framstå som vanliga användarkommentarer. Ryssland är dock långtifrån ensam om att ägna sig åt denna typ av aktiviteter.

### **HOTET FRÅN AUTOMATISKT GENERERAT TEXTINNEHÅLL**

Att skapa och sprida falsk information har tills nu varit relativt dyrt eftersom det kräver manuella insatser, vilket sannolikt bidragit till att begränsa problemet. Tillämpningar av AI-modeller som tränats på stora mängder textdata och är kapabla att generera nya texter av god kvalitet finns redan. Dessa brukar kallas för förtränade språkmodeller. Uppträning av språkmodeller kan dock kräva avancerade resurser, men när de väl existerar kostar det nästan ingenting att generera nya texter av god kvalitet med hjälp av dessa modeller.

Detta innebär att vi inom kort riskerar att översköjas av datorgenererade falska nyheter och fiktiva kommentarer i sociala medier. De två främsta anledningarna till att detta inte redan har skett är sannolikt att det tidigare har varit svårt att styra modellerna till att generera texter som passar den egna agendan och dessutom "håller tråden" över en länge textmängd. Dessa hinder håller nu på att övervinnas. Vi tror att det bara är en tidsfråga innan förtränade språkmodeller som är lätta att styra finns allmänt tillgängliga, även för mindre språk som svenska.

Texter som genereras av språkmodeller är rent språkligt svåra att särskilja från texter skrivna av en människa. Den skeptiske läsaren invänder kanske att källkritiskt skolade personer lätt inser att det inte går att lita på att information stämmer bara för att en text är välskriven och att den därför inte skulle ha någon inverkan på vederbörande. Påståenden måste faktagranskas och verifieras mot andra oberoende källor. En försvårande omständighet är att tidspressade journalister ibland plockar upp nyheter från sociala medier, skriver artiklar baserade på dessa och gör avkall på faktagranskningen. Att ta det säkra före det osäkra och bara lita på information från nyhetsmedia med hög journalistisk standard och väl-

etablerad faktagranskning är dock inte nödvändigtvis heller en helt säker strategi. Det finns exempel på verifierade konton tillhörande välrenommerade aktörer, däribland Associated Press, som har blivit hackade och använts för att sprida falska nyheter med snabb spridning, vilket gett stora men tillfälliga ekonomiska konsekvenser. Sammantaget gör detta att ingen enskild faktor är fullständigt tillförlitlig för bedömning av trovärdigheten hos en text, vilket gör textens kvalitet till en av flera faktorer som medvetet eller undermedvetet vägs in vid en sådan bedömning.

### **HOTET FRÅN AUTOMATISKT GENERERAT LJUD, BILD OCH VIDEO**

Ytterligare en försiktighetsåtgärd skulle vara att endast lita på information som går att verifiera med de egna sinnen. Vetskapen om att det går att få e-mail att framstå som att de blivit skickade från en annan adress än den de faktiskt kommer från, eller att kontot har blivit kapat kan leda den medvetne till att i den digitala världen endast lita på röst- eller videosamtal där man kan höra eller se sin samtalspartner. Problemet är, återigen, illasinnad tillämpning av moderna AI-tekniker. Det finns redan exempel på hur denna typ av teknologi använts av bedragare för att få anställda i företag att genomföra överföringar till utomstående konton. Framstegen inom så kallad röstkloning är nu så stora att några minuters ljudinspelning av en persons röst är tillräckligt för att man med god kvalitet kan generera nytt tal med valfritt innehåll som låter som om det sagts av personen vars röst klonats.

Även på bild- och videoområdet har det gjorts så pass stora framsteg att det nu är möjligt att generera helt syntetiska högupplösta ansiktsbilder på personer som inte finns eller att manipulera attribut som kön, hårfärg och ålder på ett trovärdigt sätt. Man kan även byta ut ansikten på personer i filmer, så kallade *deep fakes*, eller rent av skapa videoklipp i nära realtid där såväl verkliga personer som syntetiskt genererade avatare kan fås att tala och röra sig på samma sätt som en verklig person. Videoklipp kan än så länge genereras med relativt begränsad upplösning men vi tror att det bara är en tidsfråga innan vem som helst kan åstadkomma högupplösta videosekvenser av god kvalitet som är mycket svåra att särskilja från äkta videofilmer.

En konsekvens av denna utveckling är att det blir allt svårare att med hjälp av våra mänskliga sinnen bedöma om digital information i form av såväl text, ljud, bild eller video är korrekt eller ej. Givet denna beskrivning av våra möjligheter att bedöma digital information är det lätt att bli pessimistisk. Vårt samhälle är trots allt mycket mer digitalt nu och om vi återgick till att bara lita på det vi kan pröva med våra egna sinnen skulle vi förlora många av de fördelar och möjligheter som det uppkopplade informationssamhället faktiskt erbjuder.



## **AI-TEKNIK SOM FÖRSVAR MOT AUTOMATISKT GENERERAT ELLER MANIPULERAT INNEHÅLL?**

Ett försvar mot de hot som vårt öppna och demokratiska uppkopplade informationssamhälle står inför kräver utbildningsinsatser inom en rad områden. Det kan handla om källkritik och kunskap om vad som faktiskt kan åstadkommas i termer av generering eller manipulering med modern AI-teknik för text, ljud, bild och video.

Ökad medvetenhet och kunskap i källkritik är dock inte nog. Utifrån vårt teknologiska perspektiv är teknikutveckling och AI-forskning inte bara anledningen till att hotet existerar utan också möjligheten att finna en lösning på problemet. På FOI bedriver vi forskning kring möjligheterna att med hjälp av maskininläring ta fram metoder som kan stödja människan i att avgöra om ett material är autentiskt eller ej. Till exempel om en text har skrivits av en människa eller en dator, om en bild på en person är tagen i den verkliga världen eller genererats med hjälp av AI, eller om ljud eller bild i en videosekvens manipulerats eller ej. Detta är forskningsområden som på senare tid fått ökat intresse och på kort tid visat stor potential. En utmaning är att få de detektionsmetoder som fungerar bra i välkontrollerade experiment att också fungera på data som avviker från den som metoderna tränats på, samt att vara robusta och skalbara nog att fungera bra i praktiken. Faktorer som att data kan ha andra egenskaper än de som använts vid träning, exempelvis olika grad av komprimering, påverkar också resultaten negativt. Dessutom utvecklas ständigt nya förbättrade metoder för att generera eller manipulera data. AI-baserade detektionsmetoder kan aldrig vara vårt enda försvar mot illasinnade aktörer, däremot är det ett viktigt verktyg. Vi menar att tilltro till denna typ av teknik kräver att detektionsalgoritmerna inte bara har hög träffsäkerhet utan även att de resulterande modellerna också kan göras transparenta så att en mänsklig användare kan förstå vad bedömningen baseras på. Detta gäller inte minst om tekniken ska användas som bevis, till exempel i en polisär förundersökning eller en rättegång.

Sociala medieföretag har också en viktig roll i detta. Utöver att de har tillgång till innehåll har de också information om IP-adresser och spridningsmönster som kan nyttjas för att till exempel identifiera suspekta eller samordnade konton. Facebook gick i början av 2020 ut med ett förbud mot vilseledande manipulerade bilder och videor på sin plattform. Twitter har vid ett flertal tillfällen stängt ned och offentliggjort listor på konton som de bedömt har varit inblandade i olika former av statsaktörsstödda påverkansoperationer. Detta är lovvärda initiativ av privata företag men det finns också behov av en tydligare och uppdaterad lagstiftning på området.

Olika former av autentiseringsmekanismer kan i framtiden hjälpa till att på olika sätt verifiera äkthet eller integritet hos digital media. Till exempel genom användandet av blockkedjeteknologi liknande de som används i digitala kryptovalutor eller olika former av digitala signaturer som förstörs om media på något sätt förvanskas. Någon universallösning existerar sannolikt inte men det finns gott

hopp om att genom tillämpandet av flera tekniska lösningar, utbildning och uppdaterad lagstiftning kunna försvåra genomförandet av digitala påverkansoperationer.

## **FÖR VIDARE LÄSNING**

Johansson, F., Horndahl, A., Stiff, H. och Garcia Lozano, M., 2020, *Data Synthesis using generative models*. FOI-R--5041--SE.

Johansson, F., Horndahl, A., Lilja, H., Garcia Lozano, M., Lundmark, L., Rosell, M. och Stiff, H., 2021, *Detection of fabricated media*. (kommande FOI rapport).



## 7. Svärmande drönare – ett reellt militärt hot i framtiden?

Martin Hagström, Lars Forssell, och Niclas Stensbäck

*Vi har väl alla förmodligen sett någon film där det kommer ett moln av små beväpnade drönare som filmen hjälte slutligen lyckas besegra. Utvecklingen av små drönare går i en rasande takt och på konsumentmarknaden finns det nu civila system som både blir allt billigare och har fler autonoma funktioner som underlättar för piloten. Kommer det på framtidens slagfält finnas svärmar av beväpnade drönare och i så fall finns det några begränsningar?*

En framtid där små beväpnade drönare som använder avancerad bildbehandling och samarbetar för att slå ut en motståndare har länge funnits på film och lyfts regelbundet upp som ett framtida hot som kommer att revolutionera krigföringen. I filmen *Slaughterbots*, producerad av organisationen *Future of Life Institute*, har ett fiktivt företag utvecklat drönare som ett förment militärt vapen men som används för att via sociala medier spåra och döda både politiska motståndare och ungdomar som deltar i protester. Filmen togs fram 2017 för att skapa debatt om användningen av artificiell intelligens (AI) i vapen och fick relativt stor uppmärksamhet. Andra exempel på när en AI löper amok är den klassiska filmen *2001: A Space Odyssey* från 1968 och *Stealth* från 2005.

Men hur realistiska är dessa framtidsvisioner med avancerade målsökande drönare som både kan känna igen sitt mål och verka mot det? Hur ser utvecklingen av beväpnade drönare ut, och kommer framtidens beväpnade svärmar att utgöra ett militärt hot?

Mindre obemannade luftfarkoster, populärt kallade för drönare, kan sedan många år köpas över disk eller byggas av hobbyister med lättillgängliga komponenter. I enklare utformningar har drönare använts sedan flera år som vapen, bland annat av icke-statliga aktörer i konflikterna i Libyen och Syrien samt i ett möjligt mordförsök på president Maduro i Venezuela. De har även använts av bland andra Islamiska staten för att släppa granater på motståndare, dock med varierande precision och framgång. Företag från flera länder marknadsför UAV:er, *Unmanned Aerial Vehicle*, med olika beväpningsalternativ. Det israeliska företaget Uvision har utvecklat en produktfamilj av patrullrobotar. Den minsta väger endast 1.8 kg och innehåller en stridsdel som är byggda för att användas både för spaning och för bekämpning.

Många privatpersoner flyger redan idag drönare eller har sett drönare med funktioner som till exempel förmågan att autonomt följa en person samtidigt som den undviker att kollidera med träd (exempelvis Skydio 2). Trots att graden av

intelligens (autonomi) har utvecklats kontinuerligt under lång tid, så har dock dessa drönare ett antal grundläggande begränsningar som förväntas begränsa det svärmande hotet.

### **FLYGFARKOSTERNAS BEGRÄNSNINGAR**

De grundläggande faktorer som främst begränsar effekten av en svärm små drönare är räckvidd, verkansförmåga, kommunikation, navigering samt förmåga att adaptivt anpassa uppdraget till nya förutsättningar. Lägg därtill att något som ska kunna användas i många situationer måste tåla en tuff miljö och dessutom kunna lösa komplexa uppgifter.

Räckvidden och flygtiden hos mindre drönare är kraftigt begränsad och även om batteriutvecklingen har gått långt det senaste decenniet förväntas räckvidden vara en begränsande faktor även i framtiden. Det innebär att de behöver transporterats till operationsområdet för att ha tillräcklig flygtid kvar för att drönaren ska nå målet. Drönare med funktion som små helikoptrar med flera rotoror är relativt ineffektiva flygfarkoster. Den manöverförmåga som multikoptern har, att kunna lyfta vertikalt och hovra samt flytta sig horisontellt kommer till priset av en avsevärt högre energikonsumtion jämfört med att flyga samma sträcka med ett flygplan med fasta vingar.

För alla flygande farkoster finns en fundamental konflikt mellan räckvidd och bärförmåga. Det gäller i allra högsta grad för en liten drönare, som kan bära en högst begränsad vikt. Då måste ett val göras mellan bränslemängd, ofta i form av batterivikt, och nyttolasten. För en beväpnad drönare är det framför allt vapendelen som utgör nyttolasten. Lång räckvidd begränsar den last som kan tas med, varken tunga sensorer eller någon effektiv sprängladdning är möjligt att bära. Med en större last blir å andra sidan räckvidden ytterligare begränsad.

Miljötolighet är ett begrepp som används för att beskriva hur robust ett system är mot yttre störningar. För en mindre drönare är till exempel vind och regn en starkt begränsande faktor. Blåser det kraftigt kan de helt enkelt inte flyga och om det regnar blir kamerorna på drönaren snabbt oanvändbara, något alla som har glasögon säkert har märkt en regnig höstdag. Även kyla påverkar genom att begränsa den elektriska effekten som det är möjligt att få ur batterier. De små drönarna som säljs på marknaden idag är i princip vackert-väder-system. Att bygga en miljötolig kompakt drönare är inte bara förenat med högre kostnader, det innebär även det avvägningar mellan räckvidd och sensorprestanda.

### **ATT NAVIGERA RÄTT**

För att kunna samverka i svärmar måste drönarna kunna veta var de är, kunna navigera, och kunna kommunicera med varandra. Utrymmet i drönarna kommer att vara begränsad för fysiska komponenter, som riktade antenner för satellitnavigering (GNSS) och kommunikation, i små drönare. I miljöer där det redan idag är svårt att kommunicera, till exempel i städer och kuperad terräng kommer det vara enkelt att störa ut drönarens förmåga att navigera. I en inte

alltför avlägsen framtid kommer navigeringen att kunna baseras på terrängigenkänning och därmed inte vara lika beroende av satellitsignaler. Detta är dock inte problemfritt, dels är sensorerna beroende av goda förutsättningar och dels kommer navigeringstekniker behöva hantera att miljöer förändras, från snöfall och dimma till en förändrad miljö efter vapenverkan.

### **FÖRMÅGA ATT SE OCH VERKA I MÅLET**

För att en drönare ska kunna bekämpa ett mål som inte är fast placerat måste de kunna söka och följa målet. Drönaren behöver alltså en målsökarfunktion, vilket enkelt uttryckt är en sensor som kan söka och hitta det mål som vapnet ska slå mot. Ett område som utvecklas starkt är möjligheten till kvalificerad bildbehandling ombord på drönaren. Utvecklingen går mot både mindre och kraftfullare processorer, som dessutom är specialbyggda för att använda algoritmer för bildbehandling både snabbt och med låg effektförbrukning. En framtid där system med både vanliga kameror och IR-sensorer, känsliga i det infraröda området, har möjlighet att automatiskt detektera och klassificera till exempel motståndarens soldater med en hög konfidens är inte osannolik, men motmedel i form av avancerat kamouflage kommer samtidigt att utvecklas.

I en liten plattform som en drönare finns det begränsad möjlighet att bära beväpning. I filmen *Slaughterbots* använder man därför en effektiv verkansprincip, det som kallas riktad sprängverkan, en sprängladdning där effekten riktas och ett penetrerande material skjuts ut med mycket hög hastighet, högre än kulan i ett vanligt gevär. Det är en välkänd verkansprincip från andra världskriget som i modern tid används mot stridsvagnar och andra väl bepansrade mål. I större storlekar kan en sådan stridsdel slå igenom metertjocka pansarplåtar. När laddningen görs mindre avtar dock effekten i relation till vikten på laddningen. Riktad sprängverkan skalar helt enkelt inte bra och det är svårt att bygga miniaturiserade laddningar lämpliga för små drönare. Dessutom är laddningarna beroende av att vara nära målet när de detonerar och ett enkelt skydd, som inte kanske är så praktiskt i alla tillämpningar, är helt enkelt att sätta upp nät runt det objekt som ska skyddas. Därmed kommer små laddningar inte att vara särskilt effektiva. Ett annat sätt att beväpna en drönare är att montera någon form av ballistiskt vapen, till exempel en del av ett handeldvapen, och använda drönaren som lavett. Det finns många exempel på drönare där detta gjorts, men hur ett drönarburet finkalibervapen kan uppnå nödvändig precision och eldhastighet för att slå ut ett militärt mål på ett kostnadseffektivt sätt är däremot inte uppenbart.

### **ATT UPPTÄDA I SVÄRM**

Ordet svärm är lånat från naturen där insekter, fåglar eller fiskar tillsammans uppvisar ett sammansatt beteende olikt de enskilda individerna. Forskningen kring hur en sammansatt högre eller framväxande förmåga skapas av samverkande enkla individer, som insekter, har ännu inte något tydligt svar. Det finns även andra drivkrafter till samordnade svärmar. Exempelvis finns forskningsprojekt där enskilda operatörer styr en uppsättning farkoster genom att dela ut uppdag och där farkosternas flygbanor genereras automatiskt för att lösa dessa.

Det finns dock fortfarande många obesvarade frågor om hur svärmar kan bygga robusthet genom att vara självorganiserande och själva anpassa sitt beteende för att tillsammans lösa uppgifter.

Ytterligare utmaningar uppstår i och med att en svärms interna maskininlärning, så kallad AI, kan skapa algoritmer som gör det svårt att i förväg observera och förutsäga vilka beslut som svärmen kommer att göra i en given situation. Dessutom ökar forskningen inom *Counter-AI*, hitta sätt agera för att lura ett system som styrs av AI.

En viktig förmåga för att kunna nå högre systemeffekt och verka som en svärm är att det finns någon form av kommunikation mellan drönarna. Tekniker utvecklas för att utnyttja nya frekvensområden eller civila kommunikationsmetoder. Även detta ingår i en kapprustning där en motståndare kan störa med olika motmedel.

Styrningen av svärmar kan ske genom olika principer, centraliserat eller decentraliserat. Vid en centraliserad styrning är det en övergripande nod som samlar in data och beslutar vad varje drönare ska göra. Denna princip ger operatören bra kontroll på vad svärmen gör, men ställer höga krav på kommunikationen och är känslig för yttre och inre störning. Ett exempel på centraliserad styrning är den civila luftfarten där varje enskilt flygplan för sitt agerande bland annat har i förväg godkända instruktioner och flygplaner samt leds från ett flygledningssystem.

En decentraliserad styrning innebär att varje enskild drönare fattar egna beslut baserat på sin egen lokala uppfattning om läget, sina styrprinciper och den övergripande uppgiften. I en fågelflock strävar alla fåglarna efter att flyga i ungefär samma riktning och hastighet, och alla undviker kollisioner när de märker att de kommer för nära varandra. Dessa två regler räcker för att koordinera en stor mängd fåglar. Denna typ av lösningar är mer robust mot störning och kan anpassas till en föränderlig omvärld, men ger en operatör mindre kontroll över svärmens beteende. Vilken princip, centraliserad och decentraliserad styrning av svärmar, som är optimal vid en given situation är en öppen forskningsfråga.

Styrprinciperna kan användas för att bygga intelligenta funktioner som formationsflygande svärmar eller förmågan att till exempel genomföra spaning i komplexa urbana miljöer. Att utveckla algoritmer som möjliggör autonoma beslut, exempelvis att i realtid planera flygbanan för att optimera sensorns förmåga att detektera och klassificera mål är tekniskt sett mycket komplexa problem, som sannolikt kommer vara mycket dyra att utveckla och driftsätta.

Framtidsvisioner om svärmar som skickas ut för att själva söka upp och bekämpa motståndaren saknar också ofta ett viktigt krigföringsperspektiv. Den militära nyttan i ett tekniskt system består bland annat av funktionssäkerhet och kontrollförmåga. Detta innebär att den som är ansvariga för en insats i förväg måste ha en god uppfattning vilken verkan systemet har i tid och rum.

Det är långt ifrån självklart att den militära nyttan av intelligenta svärmar kommer att motivera den kostnad som det innebär att utveckla sådana funktioner.

Det kan konstateras att små, enkla drönare i en överskådlig framtid förväntas ha en fortsatt begränsad räckvidd, uthållighet och ha svårigheter att agera i en miljö där kommunikations- och navigeringsförmåga påverkas av en motståndare. Det är inte heller självklart att små drönare alls har förmåga att utgöra ett klassiskt hot mot kvalificerade mål. För att ge dem bättre räckvidd, större verkan samt göra dem tåligare måste drönarna göras större och mer kvalificerade i sin utformning. Detta medför att kostnaden för de enskilda drönarna ökar markant och att antalet drönare som ingår i en svärm förväntas minska. Drönare används redan idag som terrorvapen och mot civila eller oskyddade mål och kan i de perspektiven fortsatt att utgöra ett hot.

Vår bedömning är att under en överblickbar framtid kommer svärmar av beväpnade drönare, på grund av de begränsningar som systemen har, inte vara ett dimensionerande hot för en kvalificera motståndare med modern utrustning och skydd. Det finns dock en relevans i hoten från en asymmetrisk motståndare eller sabotageförband i freds- eller kristid som är väl värd fortsatt forskning. De svärmar som ska komma att revolutionera kriget på slagfältet är dock fortfarande snarare science fiction och en framtidsbild än ett reellt hot.

## FÖR VIDARE LÄSNING

Merel Ekelhof and Giacomo Persi Paoli, 2020, *Swarm Robotics: Technical and Operational Overview of the Next Generation of Autonomous Systems*, UNIDIR.

Schmuel Schmuel, 2018, *The Coming Swarm Might Be Dead on Arrival*, <https://warontherocks.com/2018/09/the-coming-swarm-might-be-dead-on-arrival/> (hämtad 2021-01-13).

Paul Scharres, 2014, *Robotics on the Battlefield Part II: The Coming Swarm*, Center for a New American Security.





## 8. Kan laservapen ändra spelplanen i framtida konflikter?

Matts Björck, Markus Henriksson och Lars Sjökvist

*När den första lasern demonstrerades av Theodore Maiman 1960 insåg många direkt möjligheterna att använda den som vapen. Laservapen börjar nu bli verklighet och prototyper utvecklas av många länder, vissa har även använts i fält under pågående konflikter. Det är lätt att tro att laservapen kommer att bli lika kraftfulla som de strålvapen som visas i science fiction-film, men kommer det att bli så? Nedan beskrivs hur laservapen kan användas och vad det skulle innebära att möta en fiende som har dessa vapen.*

### **ETT SNABBT PRECISIONSVAPEN MED OÄNDLIGT MAGASIN**

Det finns flera anledningar till att de flesta större militärmakter utvecklar laservapen. För det första är ljushastigheten ungefär en miljon gånger snabbare än en gevärskula. Målet hinner alltså inte flytta sig från det att laserstrålningen lämnar vapnet tills den träffar målet. För det andra kan laserstrålen fokuseras till en yta stor som ett frimärke på flera kilometers avstånd, vilket betyder att man med precision kan välja de mest sårbara delarna av målet. För det tredje, avsaknaden av projektil och sprängämne innebär att risken för sidoskador begränsas. Slutligen, dagens lasrar drivs med el vilket betyder att så länge det finns elektrisk kraft kan vapnet avfyras, något som i militära termer brukar kallas djupa magasin. Ett fulladdat elbilsbatteri innehåller energi nog för att bekämpa flera mål, och för kraftfulla laservapen räcker effektuttaget från några parallellkopplade batterier.

Dagens laservapen använder fiberlasrar som tillhör kategorin fastatillståndslasrar. Fiberlasrar med hög effekt används i tillverkningsindustrin för laserskärning och svetsning. I fiberlasern används den elektriska effekten för att med ett stort antal diodlasrar skapa strålning som absorberas i fiberkärnan. Den absorberade energin används för att skapa en ny laserstråle som kan fokuseras mycket bättre än strålningen från diodlasrarna. Laservapen består inte bara av en laser. Det behövs även kamerateknik för att följa målet samt mekanik och optik för att rikta laserstrålen mot rätt punkt på målet. Dessutom behövs ett elsystem som snabbt kan ge hög effekt när lasern ska användas och ett kylsystem som för bort spillvärme. Laservapen behöver även integreras i ett stridsledningssystem där till exempel invisning mot tänkta mål sker.

När en laserstråle träffar ett objekt kommer en del av strålningen att reflekteras och resten absorberas och bli värme. När ett material värms upp till höga temperaturer påverkas dess bärighet och målet kan brytas sönder av yttre krafter, exempelvis kan en styrfena på en robot brytas av. Om materialet värms upp ytterligare kommer det att börja smälta och lasern bränner därmed hål i materialet. Innehåller objektet sprängmedel eller bränsle kan upphettningen från

laserstrålen antända dessa. Eftersom verkan sker genom att materialet värms upp behöver lasern belysa samma punkt på målet under den tid som krävs för att nå verkan, vilket kan vara upp till några sekunder.

### **LASERVAPEN FÖRR OCH NU**

Under det kalla kriget fanns hotet från kärnvapenbestyckade interkontinentala ballistiska robotar. USA satsade stora resurser på laservapen installerade på flygplan för att bekämpa robotarna under startsekvensen. Då robotarna var stora massiva objekt som befann sig på långt avstånd från laservapnet krävdes mycket höga lasereffekter och komplexa optiska system. Imponerande prototyper demonstrerades, men tekniken var alltför komplicerad och kostnaderna för höga för att tillverka dem i större omfattning.

Under 2000-talet har istället fokus flyttats till att använda precisionen och snabbheten hos laservapen för att skjuta ner små, snabba och lättmanövrerade objekt. Prioriterade måltyper är drönare, raketer och artillerigranater, vilka är svåra att bekämpa med konventionella vapen. Laservapen kan också verka mot mindre båtar och lättare fordon. I dagsläget ses laservapen främst som defensiva.

Det mest kända laservapensystemet just nu är USA:s demonstrator LaWS (eng. *Laser Weapon System*) med en effekt på 30 kilowatt. Systemet monterades 2014 på fartyget USS Ponce för att testas och fick därefter tillåtelse att användas operativt i Persiska viken fram till 2017, då fartyget skrotades. LaWS installerades sedan på ett annat fartyg samt uppgraderades till en högre lasereffekt. Systemet har demonstrerats mot mål som granater, små drönare och mindre båtar.

Kina har på mässor visats upp ett laservapen, kallat *Silent Hunter*, designat främst för att skjuta ner lågt flygande drönare. Ryssland har i officiella uttalanden meddelat att man har laservapen, men detaljer har inte offentliggjorts. Även de stora militärnationerna i Europa, och andra länder som Israel och Turkiet har aktiva program för laservapen. Turkiet har enligt uppgifter lyckats skjuta ner en drönare under kriget i Libyen med sitt egenutvecklade laservapen. Drönaren var kinesiskt tillverkad och ägd av Förenade Arabemiraten.

### **LASERVAPEN HAR ETT ANTAL UTMANINGAR OCH BEGRÄNSNINGAR**

För att laservapen ska vara effektiva mot snabba mål krävs en hög lasereffekt så att målet kan neutraliseras innan det hinner orsaka skada. Den största utmaningen är att ha tillräckligt med tid för att bekämpa inkommande projektiler innan de träffar målet, särskilt om flera kommer samtidigt. Laservapnet måste då hinna växla mål och bekämpa flera hot på mycket kort tid. För större mål som kryssningsrobotar och ballistiska robotar, som kommer med hög hastighet, krävs längre verkansavstånd och högre lasereffekt än vad som demonstrerats hittills.

Absorption och spridning i atmosfären minskar effekten hos lasern när den når målet. Detta gör att prestandan bland annat minskar i dimma eller vid låga moln. Optisk turbulens i atmosfären, det fenomen som exempelvis får luften att dallra

över en varm sommarväg, sprider ut lasereffekten över en större yta på målet och förlänger därför tiden som krävs för att uppnå verkan på längre avstånd, särskilt om laserstrålen går nära marken. Effekten av optisk turbulens kan minskas genom att anpassa laserstrålen till turbulensen vilket kan göras med till exempel adaptiv optik eller avancerade strålstyrningstekniker.

En annan begränsning för ett laservapen är att det måste vara fri sikt från vapnet till målet. Det betyder exempelvis att det inte går att bekämpa mål bortom horisonten. Om en person befinner sig stående vid havsytan är horisonten ungefär fem kilometer bort. Detta kan utgöra en fundamental begränsning för räckvidden, men naturligtvis beror det på hur högt över jordens yta laservapnet och målet är placerade. I komplexa miljöer med byggnader och träd utgör fri sikt en ännu större begränsning.

### **VAD INNEBÄR DET ATT MÖTA EN STYRKA SOM SKYDDAS AV LASERVAPEN?**

En fiende som angriper Sverige skulle kunna använda laservapen som ett luftvärn, monterat både på fartyg och på lastbil, för att skydda landstigningar och brohuvuden. De kraftfullaste laservapen som demonstrerats hittills skulle kunna bekämpa en inkommande artillerigranat på några sekunder, med ett maximalt verkansavstånd på tre till fyra kilometer. Det betyder i princip att en fiende som medför laservapensystem kan förhindra att de brohuvud man tar bekämpas av artilleri och granatkastare. Även inkommande robotar kan stoppas med laservapen. Upptäcktsavståndet kan dock vara kortare i de fallen, och därmed är det inte säkert att laservapnet hinner uppnå verkan mot roboten. Ett undantag är robotar med semiaktiva lasermålsökare, såsom Robot 17, där målsökaren omedelbart skulle förstöras av en högeffektlaser, vilket skulle leda till att roboten tappade styrningen.

Även spaning med drönare och andra flygande plattformar mot en anfallande styrka kommer vara mycket svårt. Kameror kan slås ut på mycket långt håll med laservapen. Drönare kan snabbt skjutas ner om de kommer inom några kilometers avstånd och upptäcks. Hur känsliga våra avancerade plattformar, som JAS 39 Gripen, är mot laservapen är inte känt. Men på nära håll kommer laservapen att kunna skada alla typer av plattformar.

### **HUR KAN VERKAN AV LASERVAPEN MINSKAS?**

Liksom alla militära dueller handlar det om medel och motmedel. Eftersom laservapen behöver några sekunder för att verka är ett uppenbart motmedel att ge dem mindre tid. Detta kan uppnås genom att använda robotar med högre hastighet, att skjuta ur positioner där laservapnet så sent som möjligt får fri sikt till sitt mål eller att helt enkelt skjuta med fler pjäser så att laservapnen inte hinner bekämpa alla projektiler. En annan möjlighet är att förlänga tiden det tar att verka mot en projektil. Detta kan göras genom att förändra ytan så att mer laserstrålning reflekteras, vilket innebär att mindre laserstrålning absorberas och omvandlas till värme. Alternativt kan strukturer som tål mer värme användas, exempelvis genom tjockare hölje i en granat eller genom förbättrade värmeledningsegenskaper.

Idag har troligen de konventionella vapnen ett försprång i striden. Artilleri skulle kunna slå ut laservapen med hjälp av hög eldhastighet. Vid en konflikt skulle laservapen dock inte verka ensamma och objekten som de skyddar skulle hinna verka på andra sätt. Laservapen är också fortfarande en ung teknologi där utvecklingen kan förväntas gå fortare än för konventionella vapen. Därmed behöver plattformar och vapen kontinuerligt vidareutvecklas för att minska verkan av laservapen för att inte bli föråldrade i förtid.

Än så länge bör laservapen ses som ett defensivt vapen för skydd av fartyg eller grupperingsplatser på land, vilket därmed möjliggör operationer i områden där styrkan inte har kontroll på omgivande territorium. Däremot pågår utveckling av flygplansbaserade system som kan angripa känsliga mål, och laservapen kan i framtiden även bli offensiva vapen mot mål på marken.

### **BLIR DET SOM I FILMENS VÄRLD?**

Den bild som framträder är att laservapen inte kommer att vara lika spektakulära som i science fictionfilm. Det är inte vapen som kommer vara överlägsna allt annat. Laservapen kommer ändå starkt påverka effektiviteten hos konventionella vapen genom att vara ett närskyddsluftvärn med hög precision. Detta innebär att mycket större eldkraft kommer att behövas för att bekämpa en fiende som har laservapen, alternativt behövs vapen som är anpassade till laservapens egenskaper.

### **FÖR VIDARE LÄSNING**

Sjöqvist, L., 2017, *Laser för skydd av strategiska objekt t.ex. flygbas*, FOI Memo 6139.

Hecht, J. 2018, *The ray guns are coming*, IEEE Spectr. 55, 24–50.

## 9. Rymden är en ny arena för krigföring

Sandra Lindström och Kristofer Hallgren

*Framtida krig kommer att bedrivas i, genom och mot rymden. Det är en ny verklighet som har växt fram på kort tid och som kommer få konsekvenser för hela samhället inklusive vår försvarsförmåga. Det kommer därför behövas en samordning och samsyn för uppbyggnaden av totalförsvaret inom rymdområdet. För att stödja totalförsvarsplanering kommer det att behövas en god kunskapsnivå hos berörda myndigheter och en medvetenhet hos beslutsfattare om den internationella utvecklingen av rymddomänen.*

*I den här artikeln beskrivs den pågående internationella rymdkapprustningen och hur rymden har utvecklats till att idag betraktas som ännu en arena för krigföring. Detta bör ses utifrån att samhällets säkerhet och militära förmågor är mer eller mindre beroende av satellittjänster samtidigt som andra länder genomför tester av antisatellitförmågor. En framtida konflikt kommer att involvera rymddomänen. Därför föreslår vi att Sverige börjar bygga upp en beredskap för att kunna hantera andra aktörers agerande i rymden samt de eventuella negativa konsekvenser det kan få för svensk säkerhet och svenskt försvar.*

### **DET PÅGÅR EN RYMDKAPPRUSTNING**

Rymdområdet har förändrats dramatiskt under de senaste åren. Inte minst ur ett militärt perspektiv där flera stora aktörer numera beskriver rymden som en egen domän för krigföring. Synen på rymden har därmed skiftat från en understödjande roll till att den har ett strategiskt egenvärde. En följd av denna ändrade syn är en målmedveten upprustning av vapen med syfte att påverka satelliter. Öppenheten kring denna upprustning är relativt ny. De strategiska fördelar antisatellitvapen kan bidra med innebär också att flera aktörer eftersträvar att utveckla en egen förmåga.

Rymden har sedan de första satelliterna sköts upp nyttjats för militära intressen. Efter kalla kriget började fler aktörer använda satellittjänster som en följd av en snabb teknikutveckling och spridning av rymdteknologi. Rymden ansågs vara fredad från konflikter och krigföring. Idag talar dock flera länder om krig i rymden som en verklighet att förhålla sig till. Det har bland annat inneburit att doktriner och försvarsstrukturer utvecklats med fokus på rymden. Man pratar om rymdkrig ur ett brett perspektiv, allt ifrån att störa och hindra motståndaren från att använda satellittjänster till att fysiskt förstöra satelliter. Gränserna mellan vad som anses vara krigshandling och accepterat beteende är dock oklara. Det förekommer exempelvis regelbundet medvetna störningar och cyberkrigföring mot satelliter. Satelliter som kan användas i både civila och militära syften, exempelvis manövrerande satelliter, skapar ytterligare osäkerhet och försämrat säkerhetspolitiskt klimat. Detta då satelliter med förmåga till precisionsmanövrar

kan närma sig andra satelliter. Ett sådant närmande kan misstas för militärt hot, framförallt vid avsaknad av transparens och öppenhet kring avsikterna med närmandet.

Liksom under kalla kriget pågår det idag en rymdkapprustning, vilket inte ska misstas för en kapprustning i rymden. Den kapprustning som sker handlar i huvudsak om olika typer av markbaserade vapen riktade mot rymden och i mindre grad av vapen avsedda att placeras i rymden. Nya vapen som kan användas mot satelliter och tjänsterna som de tillhandahåller offentliggörs allt oftare. Tester av antisatellitvapen är däremot inte något nytt och genomfördes regelbundet av USA och Sovjetunionen fram till slutet av kalla kriget. Efter decennier av teststopp har det dock återigen börjat genomföras tester. Den stora skillnaden idag är att det är betydligt fler aktörer och fler satelliter i bana runt jorden som kan ta skada som en följd av testerna. Det finns till och med de som talar om att det sker en sakta förskjutning mot normalisering av antisatellitvapen och tester av dessa. Det senaste destruktiva antisatellittestet genomfördes 2019 då Indien sköt sönder en egen satellit i låg bana. Testet resulterade i relativt lite rymdskrot varav det mesta redan återinträtt i jordatmosfären. Reaktionerna på testet var inte så starka som man kunde förvänta sig, men diskussionerna kring ett förbud mot destruktiva tester har återigen hamnat i fokus. Det är dock värt att notera att huvuddelen av de kända vapen som utvecklas idag syftar till att störa eller förhindra användandet av satellittjänster och inte att fysiskt förstöra satelliterna.

En konflikt i rymden skulle snabbt kunna sprida sig och eskalera till en konflikt på marken, och vice versa. Vissa stater anser att ett angrepp på deras satelliter är att likställa med ett angrepp på staten i sig och man hänvisar till FN-stadgar om rätten till självförsvar. Detta grundar sig i bedömningen att samhället och den nationella säkerheten är kritiskt beroende av satelliter. På samma sätt kan en konflikt på marken snabbt komma att innebära direkta aktioner mot satelliter. Det är därför högst sannolikt att framtida konflikter kommer att involvera och ha en negativ påverkan på satelliter och satellittjänster på ett mer direkt sätt än vad vi sett hittills.

### **SVERIGE ÄR BEROENDE AV RYMDEN**

Vårt samhälle är beroende av att tjänster från satelliter levereras till rätt plats och i rätt tid. Regeringen anser även att en förutsättning för genomförandet av svensk rymdverksamhet är att samhällsnyttan ska stå i centrum. Satelliter är idag nödvändiga för att ge en överblick över klimat- och miljöförändringar på jorden. De är också oumbärliga för att hantera och begränsa konsekvenser av naturkatastrofer. Satellitinformation bidrar till global transparens och därmed också till en ökad säkerhetspolitisk stabilitet genom att olika aktörer blir varse om aktiviteter som pågår på jorden över hela världen. All transport blir säkrare genom att den styrs och övervakas med hjälp av satelliter. De är även en ovärderlig resurs i exempelvis polisens och räddningstjänstens arbete. Vårt elnät skulle inte fungera utan tidsreferens från satelliter. För börser, banker samt tradingbolag är den exakta

tidsangivelsen från satelliter nödvändig för att verksamheten ska kunna bedrivas. Detta utgör bara några exempel på hur samhället dagligen nyttjar satellittjänster.

Användningen av satellittjänster är idag självklar men samtidigt inte alltid uppenbar för en slutanvändare då satellitinformationen förädlas i flera steg. Detta gör att det ibland är svårt att veta om en samhällsfunktion är beroende av information som levereras från satelliter eller inte. Det finns sannolikt både medvetna och omedvetna beroenden av satellittjänster, vilket försvårar identifikationen av sårbarheter i kritisk infrastruktur och i viktiga samhällsfunktioner. Olika sårbarheter kan troligtvis dessutom accepteras i varierande grad beroende på om de uppstår i fred, under kris eller i krigstid. Det förutsätter dock att sårbarheterna är kända och att det gjorts ett medvetet risktagande.

Satelliter och tjänsterna de levererar kan påverkas, störas ut eller periodvis helt försvinna på grund av naturfenomen eller illasinnade aktörer, med både direkta och indirekta konsekvenser för samhället som följd. En indirekt konsekvens är till exempel när satelliter har ägarförhållanden med intressen som avviker från svenska samhällets. När vi köper satellittjänster från en kommersiell aktör kan vi aldrig vara helt säkra på att dessa tjänster kommer att fortsätta levereras om det uppstår en kris eller en konflikt i fredstid och framförallt inte i krigstid. Vi ser också att vårt beroende av kommersiella aktörer ökar, både för att de blir fler och för att de erbjuder fler attraktiva tjänster som baseras på satellitinformation.

Satellittjänster ger liknande fördelar militärt och civilt, skillnaden ligger framförallt i hur informationen används. Satelliter bidrar med allt ifrån under rättelser, precisionsnavigering och långräckviddig kommunikation vilket både ökar och stärker den militära förmågan. Även om det i militära sammanhang inte accepteras en hög grad av sårbarhet så finns det idag kritiska beroenden av satellittjänster även för militära förmågor. Många länder är idag så beroende av satellitbaserade tjänster att det skulle kunna nyttjas av en motståndare. Utan rymdbaserade tjänster tvingas moderna försvarsmakter och vapensystem att anpassa sig och sitt agerande med försämrad effekt som följd. I en konflikt kan därför nyttjande, eller hot om nyttjande, av antisatellitvapen tvinga motparten att förändra sitt agerande. Genom att förneka en högteknologisk aktör de satellitbaserade tjänsterna kan fördelarna denne har i termer av teknologi begränsas eller neutraliseras. Detta tydliggör de asymmetriska fördelarna en mindre aktör får genom anskaffning av antisatellitförmåga. Flera länder har på senare tid visat sig ha kapacitet att störa eller förstöra satelliter och dess tjänster. Detta driver på den rymdkapprustning som nu sker. Internationellt används detta som ett motiv till att bygga upp såväl skydds- som försvarsmekanismer samt offensiva förmågor både på marken och i rymden.

### **BYGGA SVENSK BEREDSKAP FÖR ATT MÖTA KRIGET MOT RYMDEN**

Det är svårt att överblicka hur omfattande beroendet av satellittjänster är i Sverige. Det är en utmaning att identifiera och förstå komplexa beroenden i syfte att minimera negativa konsekvenser för både det civila och militära försvaret.



Medvetenheten om denna problematik är relativt låg och det finns idag ingen tydlighet kring hur eller vem som ska hantera detta i totalförvarsplaneringen. Sverige behöver förhålla sig till att det redan nu pågår konflikter i rymden och att det kan uppstå svårösta kriser eller att krig kan starta i rymden. I förlängningen kommer en sådan konflikt påverka Sverige.

Det skulle innebära en fördel om vi hade en beredskap för att hantera andra aktörers agerande i rymden. Ett första steg i detta vore att ha en svensk försvars- och totalförvarsplanering som tar höjd för ett säkerhetsläge där rymden utgör ännu en domän med en unik hotbild.

Beredskapen skulle innefatta höjd medvetenhet och kunskap kring rymddomänens inverkan på, och betydelse för, framtida konflikter hos den försvarspolitiska ledningen och berörda totalförvarsmyndigheter. Det skulle underlätta vid strategiska beslut relaterat till försvars- och säkerhetspolitiska aspekter kring rymdverksamhet. Det skulle även bidra till förståelsen för hur den internationella säkerhetspolitiska utvecklingen inom rymddområdet kan komma att påverka Sverige och vårt totalförvar.

En beredskap skulle på ett naturligt sätt skapa samordning och samsyn för försvars- och säkerhetsrelaterade rymdfrågor inom totalförsvaret, både avseende praktiskt nyttjande av satellittjänster, men även vilken forskning, teknikutveckling och expertstöd som behövs för att fortsatt kunna hantera den internationella utvecklingen av rymddomänen. Detta skulle leda till att alla berörda organisationer blir tilldelade en tydlig roll och ett tydligt ansvar.

För att kunna stödja försvars- och totalförvarsplanering i dessa frågor behövs konkreta kunskapshöjande insatser. Exempel på områden där insatser behövs är krigföring på rymdarenan, konsekvenser av detta och eventuella skyddsåtgärder. Andra delar innefattar rymdmaktsteori som handlar om den existerande hotbilden, olika aktörers perspektiv och vilken typ av agerande som kan leda till ökade spänningar i rymden. Det behövs även kunskap om de mest kritiska och utsatta systemen i termer av beroenden och sårbarheter. Frågeställningar som bör studeras rör vilka risker och hot som finns mot svenska intressen som är beroende av rymden och konsekvenserna om satellittjänster slås ut. Prioriteringen nationellt, inklusive att tydliggöra vilka skillnader som finns mellan samhällets behov och Försvarsmaktens behov, måste också fastställas.

## **FÖR VIDARE LÄSNING**

Regeringens skrivelse 2017/18:259 *En strategi för svensk rymdverksamhet*, 2018-05-09, Skr. 2017/18:259, [https://www.riksdagen.se/sv/dokument-lagar/dokument/skrivelse/en-strategi-for-svensk-rymdverksamhet\\_H503259](https://www.riksdagen.se/sv/dokument-lagar/dokument/skrivelse/en-strategi-for-svensk-rymdverksamhet_H503259) (uppslagsdatum 2020-05-28).

Faria, D., Hallgren, K. och Lindström, S., 2019, *Förändringar inom rymdområdet och dess påverkan på svensk utrikes- och säkerhetspolitik*, FOI Memo 6993.

Lindström, S. (red.), 2020, *Omvärldsanalys Rymd 2020 - Fokus på försvar och säkerhet*. (kommande FOI rapport).



# 10. Framtida antagonistiska biologiska och kemiska hot

Anders Larsson, Susanne Börjegen och Birgitta Liljedahl

*Att Sverige skulle drabbas av en attack med biologiska eller kemiska vapen, så kallade BC-ämnen, kan idag verka osannolikt. Tänk dig följande scenario: 2025 upptäcks ett antal fall av en ovanligt smittsam och svårbehandlad variant av multiresistent TBC på några av landets asylboenden. Flera dödsfall inträffar och även personal smittas. Oro uppstår för en allmän smittspridning i samhället och kraven hårdnar på stoppad asylinvandring. Analyser indikerar att bakterien har likheter med en tidigare känd stam som härjade i ryska fångelser på 1990-talet, men misstänks vara manipulerad för att ge ett snabbare sjukdomsförlopp. Polisens utredning visar att smittan tycks ha spridits medvetet på flera asylboenden. Av vem är ännu okänt.*

*Även om Sverige hittills inte drabbats av några antagonistiska angrepp med kemiska eller biologiska ämnen visar händelser i omvärlden samt den snabba teknikutveckling som sker inom främst det biologiska området att ovanstående scenario inte kan uteslutas och det är viktigt att ha en beredskap för att kunna hantera det.*

## **ÖKAD ANVÄNDNING AV KEMISKA ÄMNEN SOM VAPEN**

Mordförsöken på den ryske politiske oppositionsledaren Aleksej Navalnyj 2020 och på den före detta spionen Sergej Skripal och hans dotter i Salisbury 2018 samt mordet på den nordkoreanske ledarens bror i Malaysia 2017 är tre aktuella exempel där nervgifter använts i syfte att undanröja oönskade individer. Den syriska regimens användning av sarin och klorgas mellan 2013 och 2019 samt det faktum att terrororganisationen Daesh producerat och använt senapsgas i Irak och Syrien innebär att tröskeln för användning av kemiska stridsmedel har sänkts.

Arbetet inom Organisationen för förbud mot kemiska vapen, OPCW, den organisation som arbetar med att säkerställa att kemvapenkonventionen efterlevs, försvåras av den starka politisering som uppstått. Variationen av ämnen som är möjliga att använda som kemiska stridsmedel är i det närmaste oändlig, vilket också försvårar möjligheterna att förutse och skapa nödvändiga regelverk för framtidens hot.

## **TEKNIKSPRÅNG INOM UTVECKLINGEN AV BC-ÄMNEN**

Redan i dag finns tillräckligt potenta kemiska och biologiska vapen samt möjliga metoder för att sprida dessa. Drivkraften för att utveckla nya ämnen består därför troligtvis inte i att kunna åstadkomma större skada utan snarare att göra en framtida attack svårare att förutse, upptäcka, spåra och hantera, exempelvis inom ramen för kemvapenkonventionen.

Bioteknologi är det område där utvecklingen går allra snabbast. Upptäckten av gensaxen CRISPR/Cas9, som gör det möjligt att med stor noggrannhet redigera i levande organismers DNA, har skapat förutsättningar för att mer eller mindre skraddarsy biologiska organismer och deras egenskaper. Med syntetisk biologi är det möjligt att både skapa nya farliga mikroorganismer och att återskapa de som är utrotade. Läkemedelsutvecklingen leder till nya sätt att skydda mot eller lindra effekterna av till exempel bakterier och virus, men kunskapen från forskningen kan också missbrukas till att göra dessa mer skadliga eller smittsamma.

Möjligheten att ta fram ny kunskap inom det biotekniska forskningsområdet har ökat under de senaste åren, vilket illustreras med den relativt nya företeelsen *Do-it-yourself biology*. Detta är en informell rörelse som samlar människor med olika bakgrund för att diskutera, experimentera och dela erfarenheter inom områdena biologi och bioteknik utanför de traditionella forskningsmiljöerna.

Coronapandemin förutspås leda till större fokus på forskning och utveckling inom det medicinska området. Den globala karaktären och komplexiteten på krisen medför att forskare världen över delar information och gör data och resultat publika i större utsträckning än tidigare. Jakten på kunskap och motmedel riskerar att leda till att granskningen av forskningsresultat inte blir lika noggrann som under normala omständigheter. En viktig aspekt av granskningsprocessen är den etiska, till exempel om de publicerade resultaten kan användas i ett illasinnat syfte. Pandemin har också påvisat vilka oerhörda konsekvenser en naturlig förekommande sjukdom kan ha för samhället och världen. Ett biologiskt stridsmedel, som förmodligen skulle vara dödligare än det virus som nu sprids, skulle därmed få ännu allvarigare konsekvenser.

### **TRENDER SOM PÅVERKAR BC-HOTET**

Teknikutvecklingen påverkar vilka förutsättningar som finns för att utnyttja, skapa och sprida farliga ämnen. Digitaliseringen har inneburit och kommer även i framtiden innebära att även avancerad kunskap inom området giftiga och smittsamma ämnen är publikt tillgänglig och därmed också möjlig att missbruka.

Den snabba utvecklingen av digitala sociala plattformar skapar möjligheter att dela information, åsikter, desinformation och rykten i en hastighet som kvalitetskontrollerade medier och myndigheters informationsplattformar idag saknar förmåga att hålla jämna steg med. En viktig del i användningen av BC-ämnen är den psykologiska effekt den har på människor, där ryktesspridning och desinformation kan öka människors rädsla och oro. En fortsatt trend med en snabb utveckling av informella sociala informationskanaler passar därför utmärkt för den som vill använda sig av dessa ämnen i syfte att skada och skrämja.

Den framtida utvecklingen av antagonistiska BC-hot är svår att förutsäga. Den snabbt ökande användningen av kemiska vapen vid militära konflikter av både statliga och icke-statliga aktörer i Irak och Syrien kom som en överraskning för

de flesta. Det går inte att utesluta att vissa stater även framöver skulle kunna använda kemiska eller biologiska vapen i en militär konflikt och då även på svenskt territorium om detta ger taktiska eller strategiska fördelar.

Användning av nervgifter vid mord och mordförsök på politiska motståndare är en oroväckande trend och de konsekvenser som samhället kan drabbas av illustrerades tydligt vid händelserna i Salisbury. Två personer utan anknytning till den ursprungliga händelsen drabbades fyra månader senare i det närliggande Amesbury när de av misstag kom i kontakt med den parfymflaska som använts för att förgifta Skripals. En av dessa personer avled. Det visar att det finns stater som inte drar sig för att använda nervgifter i fredstid utan hänsynstagande till om och i vilken utsträckning oskyldiga civila drabbas. Att en liknande händelse skulle kunna inträffa i Sverige går inte att utesluta.

### **KLARAR SVERIGE UTMANINGEN?**

I Sverige har vi hittills fokuserat på att höja förmågan att hantera olyckor med farliga ämnen. Det är viktigt att samhället även förbereder sig för en avsiktlig, antagonistisk användning av BC-ämnen, genom bland annat utbildning, övning och beredskapshöjande åtgärder. En sådan händelse kan inkludera ämnen som aldrig kommer i fråga vid olyckor. Hanteringen av situationen blir också annorlunda då den kommer med krav på noggrann forensisk analys och då den medför en psykologisk dimension att ta hänsyn till.

För att utveckla Sveriges förmåga att hantera händelser med kemiska- biologiska- och radioaktiva ämnen, samt kärnvapen och explosivämnen formulerades 2017 den aktörsgemensamma CBRNE-strategin. Då enades MSB med flera myndigheter kring fyra målområden (samverkan, hot och risker, förmåga och styrande instrument) samt nio prioriterade områden inom vilka den svenska förmågan behöver öka. Under 2020 utvärderades arbetet med avseende på hur väl dessa mål uppfyllts och hur arbetet inom de prioriterade områdena fortlöpt. Utvärderingen är tänkt att resultera i en rekommendation om vad i strategin som behöver revideras. Mycket återstår att göra men de framsteg som gjorts senaste åren, till exempel inom viss samverkan mellan nationell och regional nivå, utgör viktiga grundpelare för fortsatt förmågehöjande arbete. Under hanteringen av Coronapandemin finns flera exempel där vikten av samverkan och i förväg fastställda roll- och ansvarsfördelningar blivit tydlig. Något som också återstår att hantera är förekomsten av mål och riktlinjer för vad civilsamhället förväntas kunna hantera vilket förutsätter tydliga direktiv från beslutsfattare på politisk nivå.

Coronapandemin har synliggjort samhällets sårbarheter vid en allvarlig smittspridning och på ett påtagligt sätt belyst konsekvenserna av exempelvis kraftigt reducerade beredskapslager. Coronapandemin, det fortsatta arbetet med totalförsvarsplaneringen, och det faktum att kemiska stridsmedel på senare tid använts vid ett flertal tillfällen har lett till en ökad medvetenhet hos många

aktörer. Denna medvetenhet behöver också omsättas i arbete som på ett strukturerat sätt höjer civilsamhällets förmåga att hantera händelser med biologiska och kemiska stridsmedel.

Nya tvära kast i antagonisters användning av farliga ämnen måste också fångas upp och framtida förändringar av tillvägagångssätt i möjligaste mån förutsägas. Området behöver kontinuerligt följas upp och analyseras ur ett totalförsvarsperspektiv. Förmågehöjande insatser kommer att behöva prioriteras, baserat på en bedömning av det framtida hotet. Det är inte tillräckligt att förbereda sig för det som redan har inträffat.

### **FÖR VIDARE LÄSNING**

Normark, M., Lindblad, A., Sandström, B., Tunemalm, A.K., Wikteliuss, D., Wikström, P. och Vesterlund, A., 2020, *CBRN-hot från ickestatliga aktörer - Årsrapport 2019*, FOI-R--4953--SE.

Börjegren, S., Holmgren Rondahl, S., Larsson, A., Liljedahl, B., Normark, M., Tunemalm, A.K., Sandström, B., Waleij, A. och Wikström, P. 2019, *Totalförsvarsplanering med fokus på CBRN - Framtida antagonistiska CBRN-hot*, FOI-R--4765--SE.

Waleij, A., Liljedahl, B., Börjegren, S. och Lindahl, D., 2019, *Vidare kontext för en CBRN-relaterad hotbild*, FOI-R--4781--SE.

# 11. En hotkavalkad mot global hälsa kryddat med desinformation

Annica Waleij

*Av de främsta globala hälsoboten som Världshälsoorganisationen (WHO) uppmärksammat återfinns svåra smittsamma sjukdomar. På både global och nationell nivå präglades 2020 av Coronapandemin, som i början av december har smittat fler än 63 miljoner människor över världen och skördat fler än 1,4 miljoner människors liv. I pandemins spår har även världsekonomin drabbats hårt och enorma mängder av desinformation florerat. Pandemin har dock inte gjort att andra hälsobot försvunnit. Att det globala hälsobotet inte är ett enskilt bot, utan en väv av sammankopplade bot som ofta förstärker varandra, har kanske aldrig varit tydligare. Detta innebär både att grundorsakerna till ohälsa måste förstås i ett större sammanhang än sina enskilda ingående komponenter och att lösningarna till ohälsa är flerfaldiga och måste samverka såväl i tid som i rum.*

Hälsa sägs vara något man inte tänker så mycket på förrän man saknar den. Å andra sidan tänker man desto mer på den då, när den fattas. Enligt WHO är hälsa ”ett tillstånd av fullständig fysiskt, psykiskt och socialt välbefinnande och ej blott frånvaro från sjukdom och handikapp”. Det räcker alltså inte med att vara fri från sjukdom – man ska också må bra. Att mäta människors hälsa är svårt eftersom det ofta handlar om individuella upplevelser. Global hälsa mäts därför på olika sätt och omfattar många olika aspekter av utvecklingen i världens länder.

## **HÄLSA ÄR POLITIK!**

Hälsa är en grundläggande mänsklig rättighet, vilket medför att hälsoaspekter lätt blir politiska. Hälsa är inte en vara eller tjänst som är tillgänglig i lika stor omfattning för alla, överallt. Vissa individer och grupper har generellt bättre hälsa än andra. Så kallade sociala bestämningsfaktorer för hälsa, det vill säga de rådande omständigheter där människor föds, växer upp, lever, arbetar och åldras, ser olika ut mellan länder men också inom länder.

Internationellt är hälsodiplomati ett verktyg som används i politiska syften som en form av mjukt maktmedel (eng. *soft power*) för att främja folkhälsa och stärka svaga hälsosystem, eller för att gjuta olja på vägorna vid frostiga diplomatiska förbindelser mellan länder. Hälsa kan också användas för att få fördelar i andra politiska frågor eller som ett politiskt påtryckningsmedel.

Ytterst är begränsandet av tillgången till hälsa ett konkret och effektivt vapen. I inbördeskrigets Syrien försöker Assad-regimen kontrollera delar av befolkningen genom att förneka den tillgång till sjukvård. Vårdpersonal och vårdinrättningar utgör ofta direkta mål för krigshandlingar. En trend från krigszoner rent generellt är att Genèvekonventionens skydd och krigets lagar respekteras allt



mindre. Övergrepp begås av olika sidor i konflikter, utan synbara konsekvenser för förövarna. Exempelvis skedde det under våren 2020 en politiskt motiverad attack mot en förlossningsklinik i Kabul, Afghanistan.

Kopplingen mellan nationell säkerhet och sjukdomsövervakning samt bio-terrorer blev tydligt i och med de så kallade anthraxbrevet som cirkulerade i såväl Sverige som USA början av 2000-talet. Händelserna i USA politiserades även genom konspirationsteorier om genetiskt manipulerade mjältbrands-sporer (anthrax) och antydningar om främmande makts inblandning. För svensk del har hälsohoten ett eget avsnitt i den svenska nationella säkerhetsstrategin, vilket faller sig naturligt då ett av målen för det svenska samhällets säkerhet är att värna befolkningens liv och hälsa. Det konstateras bland annat att hälsohoten har en gränsöverskridande dimensionen samt att hotens natur till stora delar är oförutsägbara då den mikrobiologiska världen är i ständig förändring.

Coronapandemin har påvisat många exempel på politisering. Några sådana exempel är President Trumps beslut om att USA ska sluta finansiera och senare helt lämna Världshälsoorganisationen, samt Kinas motdrag om att erbjuda kompensation för det ekonomiska bortfallet. Nedmonteringen av demokratiska processer, där auktoritära stater med hänvisning till Coronaviruset drivit igenom tveksamma undantagslagar eller installerat olika typer av övervakningssystem är andra exempel. Även om åtgärderna har bidragit till smittbekämpningen så finns det också antidemokratiska baksidor, som till exempel att vissa statschefer utnyttjat situationen för att öka sin makt.

### **EN VÄV AV SAMMANKOPPLADE HOT**

WHO har listat tio av de största hoten mot global hälsa. Där återfinns förutom smittsamma sjukdomar som blödarfebern ebola, denguefeber, AIDS och influensa andra typer av hälsohot som svaga hälsosystem, fragila och konfliktdrabbade stater, ökad antibiotikaresistens, luftföroreningar och klimatförändringen samt icke smittsamma sjukdomar, välfärdssjukdomar och vaccinationsmotstånd. Några ytterligare angränsande hot och risker som identifierats av Världsekonomiskt forum (WEF) är den eskalerande utarmningen av biologisk mångfald, ökande klyftor mellan rika och fattiga, mental ohälsa, extrema väderhändelser, cyberhot samt CBRN-hot, det vill säga händelser involverande farliga smittsamma biologiska, giftiga kemiska, eller radiologiska ämnen.

Det globala hälsohotet är namnet till trots, inte ett enskilt hot, utan en väv av sammankopplade hot. I vissa fall förstärker hoten varandra men det kan även finnas motverkande krafter. Behovet av ett holistiskt angreppssätt har därför identifierats i olika globala initiativ, till exempel FN:s agenda för hållbar utveckling Agenda 2030, bestående av 17 mätbara mål. Ett annat exempel är *One Health Approach* som berör det faktum att människan, mikroorganismer, djur och miljö är nära sammankopplade i ett kretslopp där tydliga gränser saknas och att en förändring i ett led påverkar andra led.

I Coronapandemins spår har det blivit tydligt hur sårbara våra samhällen är och hur nära sammanlänkade många hälsohot är. Svaga hälsosystem gör länder sämre rustade att stå emot utmaningar som när olika hot sammanfaller, till exempel extrema väderhändelser och hot mot hälsan. Det är sårbarheter som man normalt förknippar med utvecklingsländer och konfliktområden. Coronapandemin har dock visat att det finns omfattande sårbarheter även i mer utvecklade länder. Effekter på folkhälsan kan ses då viktiga vaccinationsprogram inte kan genomföras som planerat eller att människor av rädsla inte uppsöker nödvändig sjukvård för andra åkommor med ökad fattigdom och ökad förekomst av förebyggbara sjukdomar som följd. Det är dock inte bara Coronaviruset i sig, utan även responsen mot den, som orsakar konsekvenser för samhället. Stängda gränser, nedstängda länder och strandsatta migranter ökar riskerna för förlorade skördar, osäker matförsörjning och stort mänskligt lidande.

En åldrande befolkning och välfärdssjukdomar utgör andra problem, även i utvecklingsländer. En paradox är att fetma ökar samtidigt som stora delar av befolkningen kan lida av undernäring och att båda problemen ibland kan ses hos en och samma person. Läkemedel är en viktig del i såväl sjukdomsbekämpning av akut eller kronisk natur som lindrandet av effekter av naturligt åldrande. Läkemedelsförsörjningen globalt är emellertid sårbar eftersom råvarutillverkningen i huvudsak är koncentrerad till ett mindre antal företag med tillverkning i Asien. Beroendena till Kina för ingående substanser och Indien för tillverkning av läkemedel är starka. En annan sårbarhet är den tydliga kopplingen till naturmiljön och den eskalerande utarmningen av biologisk mångfald. Nästan 50 procent av dagens läkemedel har sina ursprungliga nyckelsubstanser i naturen och framtida innovation kommer fortsatt att behöva inspireras av lärdomar från naturen. Att bevara naturmiljön och de ekosystemtjänster naturen tillhandahåller är centralt för såväl läkemedelsinnovation som livsmedelsproduktion. Färre pollinerande bin riskerar till exempel att bidra till ökad matosäkerhet, vilket i sin tur kan leda till ökad undernäring och ökad dödlighet, något som blir särskilt allvarligt i sköra områden med svaga hälsosystem. Det är inte sällsynt med lokala uppror som en följd av akut brist på mat och vatten.

### **VEM KAN MAN LITA PÅ?**

Utveckling av vaccin är ett av mänsklighetens största hälsofrämjande vetenskapliga genombrott. Smittkoppor har utrotats och polio, som i början av 1900-talet var en mycket vanlig sjukdom, förekommer nu naturligt i endast två länder. Den väldigt smittsamma mässlingen har tack vare en världsomspännande vaccinations-täckning i princip kunnat kontrolleras. Ett vaccin mot ebola finns framtaget.

Samtidigt finns exempel på motgångar, till exempel återfinns idag flera välutvecklade länder bland de som inte längre räknas som fria från mässling. Polio har återfått fäste i konflikttrubbade stater som östra Ukraina och det senaste ebolautbrottet i Demokratiska Republiken Kongo (DRK) drabbar de mest konfliktfyllda platserna värst. Trenderna spås på av ökat motstånd mot vaccinationer, inte sällan orsakat av en kombination av okunskap och desinformation, men vaccin-

motstånd är emellertid inget nytt. Att människor avstår från att vaccinera sig och sina barn kan bero på bristande förtroende för vacciners säkerhet eller på religiösa motiv. Människor kan både vägra att vaccinera sig eller ta mediciner och samtidigt testa överksamma eller direkt farliga ämnen i hopp om resultat. Detta drabbar den enskilde individen, men bidrar även till att försämra flockimmuniteten vilket påverkar hela samhället. Polariseringen mellan de som är för och de som är emot vacciner ökar och riskerar att skapa splittring i samhällen.

I Coronapandemins spår har såväl felaktig information som desinformationskampanjer florerat. WHO klassade tidigt Coronapandemin som en så kallad infodemi, det vill säga en pandemi av desinformation, med internet som spelplan. En portal på WHO:s hemsida har skapats för att bemöta de vanligast förekommande myterna. Även Folkhälsomyndigheten, Myndigheten för samhällsskydd och beredskap (MSB) och EU har tagit initiativ för att motverka felaktig information och rykten. En allmänt accepterad teori om Coronavirusets ursprung är att det härrör från en fiskmarknad i Wuhan där även vilda djur fanns till försäljning. Det finns även mer konspiratoriska narrativ, allt från att viruset ska ha spridits av en amerikansk deltagare under militär-OS i Wuhan hösten 2019 till teorier som att viruset sluppit ut från ett högsäkerhetslaboratorium eller att det skulle vara framtaget som ett biologiskt vapen.

Konspirationsteorier om sjukdomar och pandemier är inget nytt. Den vanligaste konspirationsteorin runt HIV är till exempel att viruset skapades genom experiment med biologiska vapen i USA och att smittan sedan spreds av den amerikanska underrättelsetjänsten CIA. Teorin, som i själva verket var iscensatt av sovjetisk underrättelsetjänsten KGB, fick global spridning i mitten av 1980-talet.

Mindre uppmärksammade händelser är den falska information som starkt bidragit till omfattningen av ett mässlingsutbrott i ö-nationen Samoa i slutet av 2019. I Samoa var vaccinationstäckningen låg till att börja med och mässlingsutbrottet förvärrades ytterligare av desinformation. Sociala medier, inklusive regeringens Facebook-sida, översvämmades av antivaccinationspropaganda från konton som föreföll finnas i USA. Ett annat exempel är det senaste ebolautbrottet i DRK, där rykten spreds om att Ebolavaccinet orsakar sterilitet och att viruset fabricerats av den kongolesiska regeringen. Dessa två felaktiga påståenden har försvårat insatsen i DRK mot viruset och även lett till våld mot sjukvårdspersonal i landet.

Konspirationsteorier får konsekvenser genom att seriös forskning undergrävs och det blir svårare att nå ut med korrekt information. Det finns också många exempel där hälso- och sjukvårdspersonal stigmatiseras, utsätts för näthat, hot och även fysiskt, ibland dödligt, våld.

### **TVÅL. EN GANSKA SCHYST UPPFINNING!**

I Coronapandemins spår kan en tillfällig nedgång i länders utvecklingskurva mot Agenda 2030 och millenniemålen förväntas. Kortsiktigt kan det bli värre innan det blir bättre. Hälso- och sjukvårdssystemen kommer att uppleva långvariga kon-

sekvenser i såväl personella som finansiella resurser. Påverkan på psykisk ohälsa är svårt att dra slutsatser om, men säkert är att det kommer att vara märkbara dominoeffekter för folkhälsan.

Jaha, men då är det kört alltså? Kanske tvärtom? En titt i det visuella statistikverktyget *Gapminder* som Hans Rosling, den svenske optimisten, läkaren och professorn i internationell hälsa, var med om att grunda, visar bland annat att medellivslängden i världen ökar och att spädbarnsdödligheten – ett mått på välbefinnande – minskar. Fler flickor går i skolan och allt fler människor lyfts ur absolut fattigdom, fler människor får bättre levnadsvillkor och en framtidstro.

Det finns flera exempel på tekniksprång och avancerad teknikutveckling av betydelse för att minska konsekvenserna av WHO listade hälsohoten. Några exempel innefattar genteknik, artificiell intelligens (AI) och artificiell pollinering av grödor med mekaniska bin. Teknikutvecklingen kan i många fall rent av bidra till att minska hälsohoten.

Ibland är det lätt att glömma bort att det inte alltid är de nyaste och mest avancerade uppfinningarna som är bästa lösningen. Det första kända receptet för tillverkning av tvål antas härstamma från Babylonien kring år 2 200 före Kristus. Som Coronapandemin har visat är tvål och vatten, rätt använt, en av de viktigaste uppfinningarna för att förhindra spridning av viruset. Att upprätthålla basal personlig hygien och att hålla avstånd förebygger även andra infektionssjukdomar som vinterkräksjuka, diarrésjukdomar och säsongsinfluensa.

Trots alla negativa effekter Coronapandemin fört med sig finns det också positiva förändringar, som ändrade levnadsmönster. Några kommer dessutom mest troligt att bestå över tid, mer distansarbete och ändrade resvanor är exempel på sådana som inte behöver vara av ondo.

Hälsohoten påverkas av globaliseringen och ett holistiskt samlat förhållningssätt som utgår från ett brett perspektiv på hoten, lösningar och förmågor behövs. Utöver det måste varje land också bryta ner hoten till en nationell nivå. Enligt den svenska nationella säkerhetsstrategin krävs en nationell förmåga för att förebygga, upptäcka och hantera hälsohoten samt att säkra en god svensk beredskap mot dessa. Vidare krävs väl fungerande interdisciplinära samarbeten på både nationell, europeisk och global nivå. Här har Sverige, som en pionjär inom många internationella hälsofrämjande initiativ, en roll att spela.

## **FÖR VIDARE LÄSNING**

Wikström, P., 2020, *Kommer coronaviruset från ett laboratorium eller ej?*  
FOI Memo 7239.

Rosling, H., Rosling, O. och Rosling Rönnlund, A., 2018, *Factfulness: tio knep som hjälper dig förstå världen.* Natur & kultur. ISBN 978912714995.

Bucht, G., Waleij, A., Frithz, E., 2016, *Ebola – Vetenskap, samhälle, säkerhet.*  
FOI-R-4355--SE.

## 12. Supersoldater

Britta Levin, Sofia Hedenstierna, Ove Jansson och Martin Hagström

*Människan har länge eftersträvat att förstärka sina fysiska och kognitiva förmågor med hjälp av såväl tekniska hjälpmedel som genom fysiska ingrepp i kroppen eller genom mental påverkan. Teknikutvecklingen är nu på väg att förändra spelplanen för vilka förstärkningar av mänsklig förmåga som är möjliga och vilka förmågeförhöjningar dessa kan leda till. Framtidens arméer kan komma att fyllas med supersoldater som hämtade ur science fiction-litteraturen.*

*Supersoldater har potential att förändra militära styrkeförhållanden mellan aktörer som förstärker och de som inte gör det. Vad förstärkningar innebär i form av militära tillämpningar och dess potentiella etiska dilemman behöver studeras utförligt. Vilka aktörer kommer vara benägna att modifiera sina soldater till supersoldater och vad innebär det att avstå?*

### **MÄNSKLIIG FÖRSTÄRKNING – ETT HETT UTVECKLINGSOMRÅDE**

Principen med mänsklig förstärkning är inte ny – under väpnade konflikter har det experimenterats i stor skala med både medicinska preparat och mekanisk förstärkning. I många fall har individer själva valt att använda preparat men det har också förekommit ett organiserat bruk. Under andra världskriget användes exempelvis metamfetamin för att ge ökad energi, vakenhet, uppmärksamhet och mod. Bieffekter i form av övermod, aggressivitet och utmattning uppstod emellertid i stor omfattning, samt en omdömeslöshet som ledde till att soldaterna kom att engageras i strider som omöjligt gick att vinna. Nutida ansatser till förstärkning av soldaters förmåga inriktas mot andra metoder och tekniska lösningar.

Utveckling i gränsytan mellan medicin och teknik har lett fram till nya möjligheter att behandla sjukdomar och ersätta skadade kroppsdelar. En del av dessa tekniker och metoder kan även nyttjas för att öka prestationsförmågan hos friska individer utöver det som är biologiskt normalt. Intresset för området är stort och utvecklingen sker till stor del inom den civila sektorn. Länder som USA, Kina och Ryssland lägger dock stora forskningsinsatser på att utforska framtida tekniker för militära tillämpningar. Exempel på områden där utvecklingstakten är hög och avgörande för hur människan kan förstärkas är bland annat bioteknik, miniaturisering av elektronik, artificiell intelligens, materialteknik och energiförsörjning.

### **FÖRSTÄRKNING IDAG OCH I MORGON**

Forskningen banar väg för nya framsteg både inom redan existerande tekniker och inom nya områden som ännu är i sin linda men som har potential att på ett fundamentalt sätt förändra människans funktion eller biologi. Förstärkningen förväntas bidra med verktyg för att hantera fysisk såväl som mental påfrestning

och därmed öka soldatens förmåga att lösa sina uppgifter. Eftersom området är brett handlar det om allt från ökad uppmärksamhet och längre uthållighet till förmågor som vi inte ens kan föreställa oss idag.

Exoskelett, en term lånad från biologin, betecknar ett styvt skal som placeras utanpå kroppen. Ett exoskelett kan användas för att ge människan stadga, fysiskt skydd och generera övermännisklig styrka. Idag finns exoskelett för militär personal i form av stöttande skenor eller fjädrar som avlastar vid bärande av tung utrustning och därmed förebygger belastningsskador. Nästa generationers soldatsystem utvecklas mot att inkludera aktiva exoskelett där energi tillförs från inbyggda motorer vilka kan generera stora krafter som exempelvis förstärker förmågan att lyfta eller hoppa. Dagens aktiva exoskelett är stora och kräver stor energitillförsel men utvecklingen går mot smidigare och mindre energikrävande system. Med hjälp av artificiell intelligens kan ett exoskelett tränas till att agera tillsammans med individen så att de rör sig som en enhet med övermännisklig styrka och smidighet.

Bioniska kroppsdelar är implantat eller robotdelar som med hjälp av nervimplantat kopplas ihop och styrs av det mänskliga nervsystemet. Detta finns idag i enklare former för att ersätta förlorade kroppsdelar såsom viljestyrda konstgjorda armar med händer som kan greppa och flytta objekt. Med utvecklad teknik kommer dessa kunna förbättras med ökad nervkontroll och större rörlighet och styrka. En möjlig framtida utveckling är en kombination av exoskelett och nervimplantat där exoskelettet styrs av hjärnan och leder till både övermännisklig styrka och snabbhet.

Nervimplantat som ersätter kroppens sinnen finns redan idag i form av exempelvis Cochlea-implantat som skickar signaler från mikrofoner direkt till hörselnerven. System med kameraförsedda glasögon som skickar signaler till synnerven är under utveckling. Dessa tekniker kan användas även för sensorer som utökar de mänskliga sinnen med exempelvis syn i det infraröda våglängdsområdet eller förmåga att höra ultraljud. En ny typ av biokompatibel lins som kirurgiskt implanteras i ögat närmar sig kliniska försök. Linsen uppges vara första steget mot både ökad synskärpa och möjlighet att projicera information och interagera med omgivningen. Denna utveckling ligger sannolikt längre in i framtiden och är beroende av fortsatt miniaturisering av elektronik och sensorer samt förbättrad energiförsörjning.

Genteknikens framsteg förväntas revolutionera möjligheten att förändra och skraddarsy organismers egenskaper, och detta inom en snar framtid. Gener kan förändras eller ersättas med skraddarsyddes gener som har konstruerats för att producera en önskad förbättring. Den nya genredigeringsmetoden, den så kallade gensaxen, CRISPR/Cas9 har visat sig effektiv för att skapa riktade förändringar i arvsmassan. Myostatin är ett protein som reglerar uppbyggnaden av muskelmassa. Vid ett försök på en hund av rasen beagle vid Guangzhou Institute of Biomedicine and Health stängdes den gen av som tillverkar myostatin, varvid hundens muskler växte till den dubbla normalstorleken.

Tillämpningar sker både i en aktiv forskningsvärld och genom en gör-det-självkultur som omfattar olika ansatser att förstärka sig själv i syfte att bli friskare, starkare och smartare. Området inkluderar allt från intag av vitaminer till illegala substanser och experiment med genmodifikation. Träningskulturen ligger långt framme i sin strävan efter optimal prestation och nyttjar bland annat avancerade smartphone-applikationer för att skapa rekommenderade träningsrutiner anpassade till individens utvecklingskurva.

### **MILITÄRA TILLÄMPNINGAR – ETT HOT**

Framtida tekniker öppnar för möjligheter att skapa människor som är fysiskt och kognitivt överlägsna de som lever idag. I militära tillämpningar kan styrkeförhållanden dramatiskt förändras om stater eller ickestatliga grupperingar väljer att skapa supersoldater utifrån de nya teknikerna. Många förstärkningstekniker är och kommer att förbli kostsamma och förbehållna ekonomiskt starka aktörer i begränsad omfattning, medan andra tekniker som idag används som självmedicinering kan vara förhållandevis billiga men osäkrare både när det gäller effekt och kvalitet och därmed mer riskabla. För en aktör som vill öka sina militära styrkors prestationsförmåga genom mänsklig förstärkning kan utvecklingen nyttjas på olika sätt; antingen genom att höja grundnivån hos flertalet soldater eller att ett fåtal utvalda individer specialiseras för en unik uppgift.

Konkret skulle en supersoldat kunna förflytta sig snabbare och längre samt agera med större styrka, uthållighet och beslutsamhet jämfört med en vanlig människa. Soldater med övermänsklig muskelstyrka, till exempel med hjälp av exoskelett, kan belastas med kraftigare skyddsutrustning och tyngre vapen vilket medför både ökad verkansförmåga och lägre sårbarhet. Utöver ökade fysiska förmågor skulle en supersoldat kunna erhålla skarpere eller utökade sinnen till exempel genom att kunna se infrarött eller höra ultraljud samt högre kognitiv förmåga att hantera stora mängder information och dra slutsatser även under hård mental belastning.

Moderna krig visar hur den väpnade striden till stor del utövas i urbana miljöer. Stora mekaniska stridsplattformar, såsom stridsvagnar, är otympliga att framföra i bebyggelse. En supersoldat rör sig däremot med lätthet i stadsmiljön, är smidig nog att verka på korta avstånd och samtidigt stark nog att bära vapen som ger hög verkans effekt även på längre avstånd. På så sätt kan en supersoldat verkansmässigt sägas motsvara ett flertal konventionella soldater eller ett fordon, men tar sig fram lättare utan att upptäckas. Vidare har högspecialiserade soldater med förstärkta sinnen och förbättrad kognitiv förmåga bättre förutsättningar att genomföra avancerade operationer, exempelvis mot utvalda högprioriterade mål.

Den psykologiska aspekten av supersoldater är viktig. Hotet att möta en både fysiskt och mentalt överlägsen soldat på framtidens stridsfält riskerar att påverka stridsmoralen negativt. Om styrkeförhållandet på individnivå är mycket skevt till motståndarens fördel, eller om en motståndare antas vara omänsklig i sitt psyke,



påverkar det synen på möjligheten att vinna striden. Detta kan i sin tur påverka den psykologiska motståndsviljan hos den som möter dessa styrkor, både bland stridande enheter och i civilsamhället.

## **HUR KAN VI MÖTA HOTET**

Mänsklig förstärkning förekommer redan privat i Sverige och det är inte otänkbart att Försvarsmakten kan införa ett antal mindre kontroversiella tekniker på bred front. I likhet med annan militär teknikutveckling är dock risken stor att en eventuell motståndare går längre och skaffar fördelar genom mer extrem förstärkning på bekostnad av individen.

Ett hot i form av supersoldater måste inte nödvändigtvis mötas med egna supersoldater. Träning och traditionella metoder för att nå högsta möjliga förmåga hos soldater i kombination med spetsteknologier som intelligenta sikten som hittar sårbara punkter och obemannade system som ersätter soldaten i frontlinjen kan skapa fördelar som kompenserar gentemot motståndarens förmågor. Att möta en motståndare med supersoldater som är överlägsna i både verkans- och skydds-förmåga kräver utveckling av stridsteknik med nya kombinationer av vapen och metoder för hur dessa används. Om stridsavstånden sträcks ut så att våra vapen inte når verkan måste vi planera striden för att komma närmare hotet eller agera i större enheter med mer utvecklade vapenplattformar.

## **ETISKA UTGÅNGSPUNKTER OCH VÄGVAL**

Utveckling av teknik för att genomföra förstärkningar av människokroppen medför flera etiska dilemman. Lika positiv och avgörande som tekniken kan vara för att bota sjukdomar och förbättra livskvaliteten för många människor – lika negativ och farlig kan den bli om den används på ett okontrollerat eller destruktivt sätt. Förändringar av kroppen kan medföra risker för individen i form av biverkningar, skador till följd av felfunktion eller modifieringar som är så extrema att dessa inverkar negativt på livskvaliteten i stort. Genteknikens användning är inte okontroversiell på vare sig individnivå eller samhället i stort – det är en sak att förändra en enskild individ och en annan sak att modifiera genuppsättningen så att förändringen kvarstår till kommande generationer.

I fallet med supersoldater står risken för individen mot förmodade fördelar och nytta för försvaret av landets suveränitet. Vissa risker kan vara acceptabla om de eventuella vinsterna är tillräckligt stora, men frågan är i vilken utsträckning en militär förmågehöjning kan motivera en risk för individen. En annan aspekt är vad som gäller när soldaten slutat att vara i aktiv tjänst – vem ansvarar då för ett eventuellt livslångt behov av medicinering och uppgraderingar eller återanpassning till samhället?

Medicinska risker och etiska överväganden påverkar möjligheterna att implementera de nya teknikerna. Kunskapen inom området måste utvecklas för att kunna värdera teknikernas möjligheter och utforma riktlinjer för forskningen. Flera olika regelverk kommer ifråga när det handlar om mänsklig förstärkning

för militära tillämpningar, allt ifrån de arbeten som baseras på FN:s deklaration om de mänskliga rättigheterna (1948), Nürnbergkonventionen (1947) om experiment på människor och Genevedeklarationen av läkaretiken (1948). Internationella överenskommelsers omsättning till nationell lagstiftning varierar dock mellan länder.

I Sverige finns hårda restriktioner för att genomföra forskning och utveckling kring tekniker som kan påverka människan och dess integritet. En motståndare med andra värderingar och regelverk skulle kunna få ett försprång i utvecklingen genom att genomföra mer riskabla experiment och implementering av teknik som i våra ögon är oetiskt. Liknande frågeställningar finns inom andra teknikområden, exempelvis nyttjande av autonoma system för militära tillämpningar.

### **FIKTION BLIR TILL VERKLIGHET**

Tekniken för mänsklig förstärkning är under utveckling och närmar sig det som idag ses som fiktion. I nuläget är det för tidigt att veta hur tekniken kommer att användas av olika aktörer i militära tillämpningar, men det går inte att utesluta att den kan komma att utgöra ett militärt hot. Det är därför hög tid att inleda en diskussion om hur tekniken kan komma att påverka framtidens strid i form av val av arena, materiel och metoder. En del i detta är att utreda värdet av potentiella förstärkningstekniker och metoder. Teknikförståelse behövs för att kunna bedöma såväl hot som möjlig användning. Det är därför viktigt att fortsätta utveckla området genom kontrollerad och transparent forskning.

Mänsklig förstärkning på det militära området innebär att spelplanen kommer att förändras. Fungerande kontrollmekanismer behövs för att på bästa sätt tillvarata den nya tekniken. Idag finns internationellt skiftande regelverk om forskning i medicinska tillämpningar men tydliga internationella överenskommelser om militära tillämpningar saknas och måste skapas i en kontext av internationell rätt. För att kunna bedriva forskning och utveckling utan att generera säkerhetspolitiska spänningar behövs en internationell diskussion gällande forskningens inriktning. I slutändan kommer olika stater behöva bedöma vilken väg de ska välja för att bemöta hotet. Antingen genom egna supersoldater, genom val av annan materiel och stridsteknik eller en kombination av de båda.

### **FÖR VIDARE LÄSNING**

Levin, B., Hedenstierna, S., Hagström, M., Svensson, J. och Hermelin, J., 2018, *Förstärkning av mänsklig förmåga – en framtidsvy*, FOI-R--4716--SE.

Matthews, M. D. och Schnyer, D. M. (Red.), 2018, *Human Performance Optimization: The Science and Ethics of Enhancing Human Capabilities*. Oxford University Press.

Mehlman, M., Lin, P. och Abney, K., 2013, *Enhanced warfighters: Risk, ethics, and policy*. Case Legal Studies Research Paper, 2013-2.



# 13. Future Threats and Some Considerations for the Next U.S. National Defense Strategy

Gene Germanovich, Gabrielle Tarini, and K. Jack Riley

*Even prior to the COVID-19 pandemic, the security and defense environment the United States faced was characterized by a range of sophisticated, evolving state and non-state threats and transnational challenges. The U.S. Department of Defense's 2018 National Defense Strategy (NDS) articulates goals for U.S. military planning, and identifies capabilities required to support the approach set forth in the broader National Security Strategy. The RAND Corporation, a non-profit, non-partisan research organization, supported the framing, shaping, and implementation of the NDS, which represented a noteworthy shift in focus for the Pentagon. In this article we offer a U.S. perspective on the evolution of threats from the recent past, and posit several considerations for the next NDS, expected sometime within the next year.*

## **EVOLUTION OF U.S. THREAT PERCEPTIONS**

In the wake of the September 11, 2001 attacks, U.S. national security policy reoriented toward a global counterterrorism campaign and counterinsurgency operations in Southwest Asia and the Middle East. The United States sought a global coalition against terrorism, which included China and Russia, and most elements of strategic competition were deemphasized. As early as 2011, uncertain about a rising China's intentions and recognizing that U.S. economic and security interests were increasingly linked to the Asia-Pacific, the United States endeavored to adopt a more balanced security posture. Then-Secretary of State Hillary Clinton summarized the logic of the nation's so-called rebalance to the Pacific: "The future of politics will be decided in Asia, not Afghanistan or Iraq, and the United States will be right at the center of the action." The Pentagon codified this rebalance in its 2012 Defense Strategic Guidance. This shift reflected a growing skepticism toward previously held U.S. and Western assumptions about how China's integration into the global economy would result in a benign presence on the global stage and harmonious Sino-American relations.

But despite U.S. intentions to shift its strategic focus to Asia, the Arab Spring, military intervention in Libya, failure to stabilize Afghanistan, and rise of ISIS made it difficult to follow through. Russia's aggression in Ukraine, hostile actions against NATO and Europe, and military modernization – not to mention the development of North Korean and Iranian nuclear and missile programs – continued to test Washington's strategic calculus and stretch its resources. Technological advancements and adversarial pursuit and, in some cases, aggressive use of space and cyberspace capabilities also contributed to the growing list of security concerns.

The 2018 NDS represented an unambiguous prioritization of this array of threats. The United States intends to orient its military on China, Russia, and then everything else, in that order. The strategy, promulgated by Secretary of Defense Jim Mattis, emphasized: “Long term strategic competitions with China and Russia are the principal priorities for the Department and require both increased and sustained investment, because of the magnitude of the threats they pose to U.S. security and prosperity today, and the potential for those threats to increase in the future.” Current Secretary of Defense Mark Esper has clarified which of the two competing powers would be the foremost driver of U.S. defense choices by repeatedly denoting the Indo-Pacific region as America’s “priority theater.”

### **RECENT ORIENTATION AND CURRENT OUTLOOK**

Competition with China will be ongoing and open-ended, and likely represents a generation or longer endeavor. The Department of Defense has indeed stepped up its focus on the Indo-Pacific, and dedicated new resources—money, forces, and senior leader attention—to engage in the evolving strategic competition with China. The military is adopting a deterrent posture with augmented deployments and preparations for a future conflict in Asia. Ongoing changes within the U.S. Marine Corps represent one prominent example of the importance of the Pacific in U.S. defense strategy. After two decades of land warfare in Afghanistan and Iraq, the Commandant of the U.S. Marine Corps initiated an overhaul of the 186,000-strong branch of the armed forces. As part of his strategy, the Marines’ force design, procurement, training, and posture will be tailored to competing and, if needed, warfighting with China.

Yet no strategy can have an entirely singular focus. Other actors called out in the 2018 NDS—Russia, North Korea, Iran, and global terrorist organizations—threaten the United States and its allies. Although it is difficult to anticipate the future security environment, most American experts broadly agree that each of these actors will continue to pursue objectives that are incompatible with U.S. interests. None of these threats will materially diminish in the coming decade, but given the strategic emphasis on China, U.S. policymakers are increasingly willing to accept greater risk and economize efforts in these areas. The strategy also highlights the threat of weapons of mass destruction proliferation and hybrid challenges such as disinformation campaigns and economic coercion. Such “irregular warfare” tactics require the U.S. military to maintain capabilities relevant for strategically competing below the threshold of armed conflict. These will remain issues of concern, albeit with the understanding that the Department of Defense will generally play a supporting role to other agencies.

Some common threads tie together each of the threat actors identified by the NDS. State adversaries and sophisticated non-state actors increasingly possess capabilities that make U.S. power projection less tenable. Long-range precision strike weapons deployed on increasing numbers of smaller, mobile platforms and enabled by persistent surveillance and targeting networks challenge key tenants of U.S. military advantage. Such capabilities will make it increasingly difficult

if not prohibitive for U.S. forces to enter theaters of operations during a crisis. China and Russia's extensive investments in these systems have the potential to create large "no go" zones for U.S. and friendly conventional ground, air, and naval forces. Even smaller states and non-state actors can acquire and employ these weapons for significant effect, as several Houthi rebel missile attacks on U.S. and Saudi warships in the Gulf of Yemen have vividly demonstrated. While the U.S. defense establishment has begun to tackle these dilemmas, maintaining interoperability with NATO and other key allies remains a prime challenge in need of constant attention through joint development of technologies, operational concepts, and training plans.

Looking ahead, COVID-19 will have a significant near- and far-term impacts on U.S. defense strategy. In addition to negatively affecting U.S. military readiness, the current pandemic and future waves of the disease will place renewed demands on the military to support civilian authorities for disaster response, an issue not emphasized in the current NDS. More broadly, the pandemic could accelerate worrisome global trends such as populism, the deterioration of U.S.-China relations, the slowing of European integration and defense cooperation, and the incidence of weak or failing states—all of which contribute to a more dangerous and complex threat landscape for United States, NATO, and other allies and partners. Further, a prolonged crisis could ignite calls for governments to focus inwards, despite the fact that now more than ever, domestic well-being is affected by the rest of the world. COVID-19 and its geopolitical fallout cannot be solved with military tools alone, but the Department of Defense has and will need to continue to play an important supporting role. Tasks may include contingency planning, global transportation, medical assistance, construction, and, potentially, stabilization missions abroad.

From an economic and budgetary perspective, the pandemic will likely intensify existing domestic pressure to overhaul the U.S. healthcare system, expand the social safety net, and prepare for future pandemics. Continuing to spend half of the nation's discretionary budget on defense may become politically and financially unsustainable. Even if Americans continue to support current levels of defense spending, the U.S. government may be unable to afford it due to a ballooning national debt. This fiscal reality poses significant risks for executing the NDS. American decisionmakers will need to make hard choices about which of the strategy's priorities will need to be reexamined. Additionally, the defense policy establishment, including the research community, will need to focus on designing innovative concepts and identifying creative methods that address multiple threats as efficiently as possible.

### **CONSIDERATIONS FOR THE NEXT NDS**

The architects of national security policy and authors of the next NDS will face a herculean task, potentially while still in the midst of a pandemic and likely a prolonged economic recession. The next National Security Strategy and initial NDS deliberations will need to focus on setting a level of ambition within the projected

available resources. One plausible outcome of these reviews might be that some of the goals outlined in the 2018 NDS need to be scaled back. Additionally, some defense funding could be repurposed to support civilian agencies with national and international health security tasks, as well as to account for COVID-related challenges internal to the military.

Three considerations, or guiding principles, may help. While these suggestions do not substitute for fundamental decisions about the extent to which U.S. objectives vis-a-vis the range of military and non-military threats outlined above will need to change, they will help make the most of the resources available for achieving the nation's defense goals as informed by the forthcoming National Security Strategy.

First, the next NDS should strive for concepts, systems, and organizations capable of addressing a spectrum of conflicts and adversaries. China's economic and military clout make it the most dangerous threat facing the United States, but a war with China is not necessarily the most likely scenario to materialize. Rather than attempting to optimize every weapons system, posture decision, and training regimen for a potential China conflict, the U.S. could take a more flexible approach to address a broader range of threat actors while still prioritizing the Pacific. Developing operational concepts that apply to multiple theaters, tailored by region and to specific threat actors, will be a more sustainable long-term approach that leaves fiscal and intellectual space to address pressing needs in other parts of the world. For example, the U.S. Army's development of its Multi Domain Operations concept involves standing up experimental Task Forces in both the Pacific and Europe. Each Task Force will be tailored to deter China and Russia, respectively, but both aim to undermine similar technologies and adversarial concepts intended to deny U.S. forces operational access during a crisis.

Second, affordability will be a greater concern than in the recent past, and not just for the United States, but for its allies as well. In the United States, defense expenditures will be judged against their contributions to difficult-to-measure concepts such as lethality, readiness, and, increasingly, resilience. Allies' ability to support and enable these concepts will depend to considerable extent on their own budget situations and interpretation of regional and other threats. Harmonizing allied support for the NDS will continue to require considerable attention through bilateral consultations and, in the case of NATO, collective defense planning processes.

Third, the strategy will need to emphasize international cooperation. Washington and its allies do not always see threats from shared adversaries in the same way. But faced with a rising China and dangerous Russia—each of whom have few allies of their own—the United States will need to reinforce and recommit to its partnerships. Fulfilling U.S. strategic ambitions in the Pacific will require dedicated maintenance and cultivation of a network of bilateral security partner-

ships and multinational groupings. NATO remains the lynchpin for deterring Russia, and many allies increasingly view China as a threat, not just a challenge, to European and transatlantic prosperity and security. Finally, international cooperation will need to go beyond traditional military threats. The pandemic underscores global interdependencies and demonstrates the perils of a stunted international response to borderless threats like disease outbreaks and climate change. The next NDS should acknowledge hard geopolitical realities while reinforcing the central role for global institutions and coalitions rooted in shared values and interests in coping with a wide range of challenges where the military will likely be engaged.

The trifocal lens suggested here—flexibility, affordability, and international cooperation—offers a framework the NDS could incorporate to assist in addressing the range of traditional and new security challenges. At the level of research institutions, collaboration across the Atlantic and beyond can serve as a useful mechanism to generate the kind of independent, evidence-based insights that the United States and its defense partners will require to advance common objectives in a flexible, affordable, and cooperative manner.

#### **FURTHER READING**

Cohen, R. S., Chandler, N., Efron, S., Frederick, B., Han, E., Klein, K Morgan, F. E., Rhoades, A. L., Shatz, H. J. and Shokh, Y., 2020, *The Future of Warfare in 2030 Project Overview and Conclusions*, RAND Corporation, DOI: <https://doi.org/10.7249/RR2849>.

Dobbins, J., Tarini, G. and Wyne, A., 2020, *The Lost Generation in American Foreign Policy How American Influence Has Declined, and What Can Be Done About It*, RAND Corporation, DOI: <https://doi.org/10.7249/PEA232-1>.

RAND Corporation, 2020, *Supporting the National Defense Strategy*, DOI: <https://doi.org/CPA174-1>.





## Författarpresentationer

**MATTS BJÖRCK** är teknologie doktor i fysik från Uppsala Universitet och forskare vid enheten Elektrooptiska system. Hans nuvarande forskning handlar om laservapen, speciellt verkan och effektskalning med hjälp av koherent strålkombinering. Han har tidigare forskat inom tunnfilmfysik samt arbetat med forskning och utveckling av friktionsomrörningssvetsning vid SKB AB.



**SUSANNE BÖRJEJEGREN** är kemist och forskare vid enheten för Kemiska hot och effekter. Hon arbetar inom flera områden med koppling till kemiska stridsmedel. Bland annat ger hon tekniskt stöd åt Utrikesdepartementet i arbetet med nedrustning av kemiska vapen inom ramen för OPCW, och är också på flera sätt engagerad i hur skydd mot kemiska stridsmedel bör integreras i totalförsvarsplaneringen.



**LARS FORSELL** är forskare vid FOI:s enhet Systemteknik. Han har en examen från Kungliga Tekniska Högskolan i Flygteknik. Han lett såväl nationella som internationella forskningsprojekt inom flygteknik och automation samt arbetat med värdering och analys av Försvarsmaktens vapen och skyddssystem.



**GENE GERMANOVICH** is an international defense researcher at the RAND Corporation. His research areas of interest include European security, the NATO alliance, maritime and amphibious forces, and security cooperation. Prior to joining RAND, he spent eleven years at a national security consulting firm where he conducted policy analysis, strategic planning, and wargaming for the Office of the Secretary of Defense, Marine Corps, and other U.S. government clients. He earned a B.S. in international affairs from Georgia Tech and an M.A. in security studies from Georgetown University.





**DAVID GUSTAFSSON** är förste forskare och projektledare vid FOI:s enhet Sensorinformatik. Han 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 doktorexamen i datalogi med inriktning mot bildanalys från Köpenhamns universitet.



**MARTIN HAGSTRÖM** är forskningsledare vid FOI:s enhet Systemteknik. Han är programansvarig för forskningen inom vapen och skydd samt obemannade autonoma farkoster med en bakgrund inom systemteori. Hans arbete har under senare år bl.a. omfattat etiska och legala aspekter av automatisering av vapen och människans ansvarsroll i bekämpningssystem. Martin har en examen i flygteknik samt matematisk systemteori från Kungliga Tekniska Högskolan och arbetar med systemanalys inom alla arenor.



**KRISTOFER HALLGREN** är förste forskare vid FOI:s enhet Flyg- och rymdsystem. Han har en doktorexamen från Max Planckinstitutet för Sol-systemsforskning i Göttingen och en civilingenjörsexamen från Luleå tekniska universitet. Kristofers fokusområde är omvärldsanalys med fokus på rymden samt rymdlägesbild. Han har bland annat ansvarat för utvecklingsprojekt inom rymdlägesbild och stöttat Försvarens strategiska arbete inom rymdfrågor.



**SOFIA HEDENSTIERNA** är forskningsledare vid FOI:s enhet Systemteknik. Hon har en doktorexamen i biomekanik vid Kungliga Tekniska Högskolan. Hennes expertområden inkluderar människans sårbarhet, verkans- och sårbarhetsvärdering samt kroppsskydd och burna vapensystem. Hon har arbetat i integrerade projekt (IPT) grupper med Försvarens FMV gällande målsättningar för soldatutrustning. Hon har även jobbat internationellt inom t.ex. EU-projekt och internationella arbetsgrupper.



**VIDAR HEDTJÄRN SWALING** är forskningsledare vid FOI:s enhet Samhällets säkerhet. Han har en bakgrund inom teknisk riskanalys och arbetar med metodutveckling inom det svenska krisberedskapssystemet, ofta med fokus på risk- och sårbarhetsanalyser och kritisk infrastruktur. Han är aktiv inom återuppbyggnaden av det nya totalförsvaret.



**ELIN HELLQUIST** är analytiker med fokus på internationella militära insatser vid FOI:s enhet Operationer och insatser. Hon är med i redaktionen för Strategisk utblick 9. Hon är disputerad statsvetare från Europeiska universitetsinstitutet (EUI) i Florens och har lång erfarenhet av säkerhetspolitisk forskning.

**MARKUS HENRIKSSON** är förste forskare vid FOI:s enhet Elektrooptiska system. Han har en doktorexamen i lasarfysik från Kungliga Tekniska Högskolan. Han forskar bland annat om laserbaserade motmedel, lidarsensorer och laserutbredning i atmosfären.



**JENNY INGEMARSDOTTER** är forskare vid FOI:s enhet Samhällets säkerhet med fokus på krisberedskap, civilt försvar och totalförsvar. Hon har en civilingenjörsexamen och en doktorexamen i Idé- och lärdomshistoria, båda från Uppsala universitet. För närvarande är hon engagerad i ett forskningsprojekt om civilt försvar i gråzon. Jennys forskningsintressen är breda och täcker in såväl totalförsvarets historia som etiska perspektiv på artificiell intelligens.



**OVE JANSSON** är en kognitionsvetare och bedriver forskning vid enheten Människa, Teknik, Organisation. Han arbetar med frågor som rör människans tänkande och beteende på olika nivåer – från gränssnitts-utveckling av personliga system till metodutveckling för att genomföra verksamhetsanalyser. Förutom att arbeta med människoförstärkande utrustning har han även arbetat med frågor inom autonoma farkoster, simuleringsmiljöer, spelsystem samt urval och rekrytering.



**FREDRIK JOHANSSON** är förste forskare vid FOI:s enhet Beslutsstödssystem. Han har en teknologie doktorexamen i datavetenskap från Örebro Universitet och forskar om tillämpningar av artificiell intelligens inom försvar och säkerhet med fokus på verktyg för underrättelseanalys. Utöver mångårig forskarerfarenhet från FOI har Fredrik också arbetat operativt med analys av stora datamängder och metodutveckling på Säkerhetspolisen.



**GÖRAN KINDVALL** är förste analytiker vid FOI:s enhet Strategi och policy. Han har en civilingenjörsexamen i Teknisk Fysik och en Teknisk Licentiat i atom- och molekylfysik. Hans huvudsakliga arbetsuppgifter är långsiktig planering, teknikvärdering och utforskning av nya koncept. Under de senaste åren har han mest arbetat med försvarskonsekvenser av den pågående och framtida teknikutvecklingen.



**ANDERS LARSSON** är forskningsingenjör på enheten Skydd där han bland annat jobbar med indikeringsmetoder för kemiska och biologiska ämnen samt CBRN-relaterade frågor inom krisberedskap och hot.





**BRITTA LEVIN** är förste forskare vid enheten Människa, Teknik, Organisation. Hon arbetar med frågor som rör interaktionen mellan människa och system ur ett brett perspektiv. Hennes expertområden inkluderar mätning och värdering av mänsklig prestation, metodutveckling och simulering. Britta har en examen i flygteknik från Kungliga Tekniska Högskolan men verkar både inom luft- och markarenan, något som de senaste året inriktats mot soldatsystem i en nationell såväl som internationell kontext.



**BIRGITTA LJLJEDAHL** är förste forskare på enheten CBRN skydd och säkerhet. Hon arbetar med frågor som rör CBRN-, hälso- och miljöfrågor i kris och konflikt. För närvarande med fokus på framtagande av robusta verktyg och scenarieutveckling, delvis med VR moduler, för komplexa CBR händelser i hybridkontext, där oklarhet råder om en incident är en olycka, eller antagonistisk.



**SANDRA LINDSTRÖM** är förste forskare vid FOI:s enhet Flyg- och rymd-system. Hon leder och koordinerar arbetet med fokus på rymd för försvar och säkerhet. Hennes expertis är omvärldsanalys inom rymdområdet, vilket innefattar global rymdutveckling inom både teknik- och policyområdet samt vilka risker, hot och möjligheter det för med sig för svenskt försvar och svensk säkerhet. Sandra har en civilingenjörsexamen i rymdteknik från Luleå tekniska universitet.



**JENNY LUNDÉN** är projektledare och redaktör för Strategisk utblick 9. Hon är analytiker vid FOI:s enhet Strategi och policy, med fokus på totalförsvar. Hon har en magisterexamen i fysik från Lunds universitet och en doktors-examen i meteorologi med fokus på Arktis från Stockholms universitet.



**ANDERS MELANDER** är biträdande projektledare och redaktör för Strategisk utblick 9. Han har bl.a. en magisterexamen i mikrobiologi från Uppsala Universitet. Han är analytiker vid FOI:s enhet Strategi och policy, med fokus på civilt försvar och totalförsvar.



**KARIN MOSSBERG SONNEK** är Teknologie Doktor och forskningsledare vid enheten Samhällets säkerhet. Hon har forskat inom klimatanpassning med fokus på kommunalt beslutfattande. Hon har därutöver studerat effekter av klimatförändringarna på samhällsviktiga verksamheter på uppdrag av MSB, Livsmedelsverket och Sida.

**BJÖRN OTTOSSON** är forskare vid FOI:s enhet Säkerhetspolitik, med USA som expertområde. Han är med i redaktionen för Strategisk utblick 9. Till hans primära analys- och studieområden hör amerikansk utrikes-, säkerhets- och försvarspolitik, samt transatlantiska relationer. Björn har doktorerat i statsvetenskap vid Stockholms Universitet och har tidigare arbetat vid Stockholms Universitet, Södertörns Högskola och Försvarshögskolan.



**MAGNUS ROSELL** är forskare vid FOI:s enhet Beslutsstödsystem. Han arbetar med metoder inom maskininlärning och artificiell intelligens med fokus på verktyg för underrättelseanalys och leder projekt med den inriktningen. Magnus har en doktorsexamen från Kungliga Tekniska Högskolan i datalogi. Hans avhandling handlar om automatisk textanalys och han har även utvecklat metoder för automatisk omvärldsbevakning hos cybersäkerhetsföretaget Recorded Future.



**NIKLAS H. ROSSBACH** är förste forskare vid FOI:s enhet Säkerhetspolitik och analyserar bland annat amerikansk och europeisk säkerhetspolitik, energi och geopolitik samt försvarsvilja. Dessutom är han projektledare för långsiktig omvärldsanalys. Han har doktorerat i historia vid Europeiska universitetsinstitutet (EUI) i Florens på transatlantiska relationer och forskat om psykologiskt försvar vid universitet i Oxford.



**RIITTA RÄTY** är forskningsledare vid FOI:s enhet Strategi och policy. Hon är disputerad fysiker och arbetar med Försvarsmaktens förmågeutveckling, framtidsforskning inklusive Perspektivstudien samt studier av hot och risker mot samhället åt olika myndigheter. Hennes intressen inkluderar operationsanalys, facilitering och workshops, framtidsstudier och osäkerheter.



**K. JACK RILEY** is vice president and director of the National Security Research Division at the RAND Corporation. He leads a team of professionals who collectively conduct over 300 projects and produce hundreds of publicly available reports each year for top leadership in the national security community. As a researcher at RAND, he has led and co-led numerous projects on national and homeland security topics. Prior to joining RAND, Riley worked as a senior civil servant at the U.S. Department of Justice. Riley has a Ph.D. in public policy analysis from Pardee RAND Graduate School, an M.S. in foreign service from Georgetown University, and a B.A. in economics and Russian from the University of Michigan.





**LARS SJÖKVIST** är forskningschef i laserteknologier vid enheten Elektrooptiska system vid FOI. Han är även docent i kemisk fysik vid Linköpings Universitet och har tidigare arbetat med magnetiska resonansmetoder. Nuvarande forskning är inriktad mot militära- och säkerhetstillämpningar där olika typer av lasersensorer och lasersystem används.



**LISELOTTE STEEN** arbetar vid FOI:s enhet Förmågeutveckling. Hon är med i redaktionen för Strategisk utblick 9. Hon är operationsanalytiker placerad vid Marinstaben och hennes främsta uppgift är att stötta studier av marina system. Hon har en lång bakgrund på FOI och tidigare FMV. Hon har en examen som gymnasielärare i naturvetenskapliga ämnen.



**NICLAS STENSBÄCK** är datavetare verksam som forskare vid FOI:s enhet Systemteknik. Han är projektledare inom vapensystemvärdering och generell systemanalys. Han har arbetat inom ett flertal forskningsprojekt rörande autonoma system, både som utvecklare av beteendemodeller och för bedömning av framtida tekniska förmågor.



**ANDERS STRINDBERG** är förste forskare vid enheten Asymmetriska hot. Han är även med i redaktionen för Strategisk utblick 9. Han arbetar främst med frågor som rör terrorism och våldsbejakande extremism. Han har en doktorexamen i internationella relationer från universitet i St Andrews, Skottland samt examina i filosofi och teologi. Han undervisar även i asymmetriska hot inom Mastersprogrammet vid Center for Homeland Defense and Security, U.S. Naval Postgraduate School, i Monterey, Kalifornien.



**ERIK SVENSSON** är analytiker vid FOI:s enhet Asymmetriska hot. Erik har en bakgrund inom freds- och konfliktvetenskap samt statsvetenskap med inriktning mot krishantering. Han har i huvudsak jobbat med frågor om cybersäkerhet, framtidsteknologiers inverkan på militär ledning, och som analysstöd åt Försvarsmakten och dess studieverksamhet.



**GABRIELLE TARINI** is a policy analyst at the RAND Corporation. Her research areas of interest include security cooperation, the NATO alliance, European security, and humanitarian and civilian security issues. Previously, she was a fellow in the Office of the Secretary of Defense for Policy and a research associate at the James Martin Center for Nonproliferation Studies. She has a M.P.P from the Kennedy School of Government at Harvard University and a B.A in international studies from Boston College.

**ANNICA WALEIJ** är förste analytiker vid FOIs enhet Skydd. Hennes forskning har främst fokuserat på hälso- och miljörisker i internationella insatser. Internationell erfarenhet inkluderar arbete för FN:s fredsfrämjande insatser och en sekondering till FN:s kontor för humanitära frågor i Genève. Hon har gjort fältresor till Afrika, där hon bl.a. utfört miljö- och hälsoutredningar och utbildat FN- och ECOWAS-personal.



**CHRISTOFFER WEDEBRAND** har en kandidatexamen inom teologi med fokus på etik samt en masterexamen inom freds- och konfliktvetenskap. Han arbetar som analytiker vid FOI:s enhet Samhällets säkerhet med studier om framförallt den fredstida krisberedskapen och den civila delen av totalförsvaret.



**PER WIKMAN-SVAHN** arbetar som forskare vid Avdelningen för filosofi vid Kungliga Tekniska Högskolan i Stockholm där han forskar om filosofiska aspekter på risk och osäkerhet och undervisar i bland annat Riskfilosofi, Forskningsetik och Teknik, och etik. Per har också tidigare arbetat på avdelningen Förvarsanalys på FOI.



**ANN ÖDLUND** är förste forskare vid FOI:s enhet Strategi och policy. Hon har en utbildningsbakgrund inom beteendevetenskap och organisationspsykologi. Hon genomför studier främst inom totalförsvaret, både ur ett militärt och civilt perspektiv och har publicerat flera rapporter i ämnet.







ISSN 1650-1942

[www.foi.se](http://www.foi.se)