Tidig förvarning och icke-militära angreppssätt

Utmaningar för underrättelsetjänsten

Malin Severin

FOI-R--4577--SE

Mars 2018

FOI

Malin Severin

Tidig förvarning och icke-militära angreppssätt

Utmaningar för underrättelsetjänsten

Bild/Cover: Scanpix, Shellhawker

Titel	Tidig förvarning och icke-militära angreppssätt – Utmaningar för underrättelsetjänsten
Title	Early warning and non-linear warfare – challenges for intelligence services
Rapportnr/Report no	FOI-R--4577--SE
Månad/Month	Mars
Utgivningsår/Year	2018
Antal sidor/Pages	49
ISSN	1650-1942
Kund/Customer	Försvarsdepartementet
Forskningsområde	6. Metod- och utredningsstöd
FoT-område	Ej FoT
Projektnr/Project no	A18106
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Kombinationen av kraftfull teknik och nya samhälleliga sårbarheter innebär att icke-militära maktmedel har fått en allt mer framträdande roll i mellanstatliga konflikter. Antagonistiska aktörer har i dag goda möjligheter att utöva påverkan mot andra länder utan att korsa tröskeln för väpnat angrepp.

Syftet med rapporten är att belysa olika aspekter av hur det koordinerade användandet av icke-militära maktmedel påverkar svensk underrättelse- och säkerhetstjänst i deras uppdrag att upptäcka, identifiera och varna för framväxande hot mot Sverige. Fokus ligger på antagonistiska hot och risker i gränslandet mellan fred och krig; hot som ofta går under samlingsbenämningen hybrid- eller gråzonsproblematik. Hotens diffusa karaktär innebär att de kan vara svåra att upptäcka, karaktärisera och överskåda. Situationen ställer krav på nationella underrättelse- och säkerhetstjänsters förmåga att skapa en sammanhängande lägesbild ur ett skenbart osammanhängande förlopp.

Det försämrade omvärldsläget har aktualiserat behovet av fördjupad samverkan mellan säkerhetstjänst, underrättelsetjänst och civila aktörer. Omvärldsutvecklingen har även ökat behovet av att kontinuerligt försörja samhällsaktörer utanför säkerhetssektorns kärna med öppen information om hotutvecklingen och förändringar i terrängen.

Studien konstaterar att det finns tydliga paralleller mellan den samtida diskussionen om hybrid- och gråzonshot och de diskussioner som fördes inom underrättelsetjänsten om riskerna med det ’icke-militära angreppet’ på 1960-talet. I frågan om hur förvarningsfrågan kan inkorporeras inom ramen för totalförsvarskonceptet kan det därför finnas anledning att tillvara erfarenheter från historien.

Nyckelord: Tidig förvarning, underrättelsetjänst, säkerhetstjänst, indikatorer, gråzonsproblematik, hybridkrigföring, lägesbild, totalförsvar.

Summary

The combination of novel societal vulnerabilities and powerful technologies has meant that non-military measures short of war have gained renewed relevance in interstate conflicts. Actors seeking to challenge the status quo and exert influence over other countries' policies, today have many options for doing so without crossing the threshold of armed aggression.

This pilot study provides a broad introduction to these challenges and the implications facing Swedish intelligence and security services in their mission to detect, identify, and warn against emerging threats against Sweden.

The study focuses on antagonistic threats in the grey area between peace and war; activities often referred to as 'grey zone' or 'hybrid' threats. These activities tend to be difficult to detect, attribute and assess, and in order to enhance situational awareness, intelligence agencies need to find ways to link seemingly disparate occurrences into a coherent whole.

The complex and multifaceted threat situation highlights the need for enhanced interagency cooperation and information sharing between civilian and military agencies. For relevant signals to travel upstream, the report stresses the need to continually provide lower-level authorities with open source information relating to threat development and potential aggressors' modus operandi.

The study notes that the contemporary debate on hybrid warfare in Sweden bears strong resemblances with challenges facing Swedish intelligence agencies in the 1960's. Important lessons could thus be drawn from studying how Sweden organised its intelligence sharing apparatus in preparation for a 'non-linear attack' during the Cold War.

Keywords: Intelligence analysis, security services, early warning, indicators, grey zone threats, hybrid warfare, measures short of war, situational awareness, non-linear warfare, Total Defence

Innehållsförteckning

Förord

FOI har på uppdrag av Försvarsdepartementet, inom ramen för projektet Försvarspolitiska studier, analyserat hur den koordinerade användningen av icke-militära maktmedel inverkar på underrättelse- och säkerhetstjänstens uppgift att upptäcka, identifiera och varna för framväxande hot och förändringar i omvärlden. Innehållet i rapporten har granskats i enlighet med FOIs interna granskningsregler.

Författaren vill inledningsvis rikta ett varmt tack till John Rydqvist, FOI, och Jan Leijonhielm, FHS, som har granskat rapporten och bidragit med kloka kommentarer och idéer löpande under skrivprocessen. Tack även till Jonas Clausen Mork och Fredrik Westerlund samt till de kolleger och externt inbjudna gäster som generöst delade med sig av sina erfarenheter vid granskningsseminariet i januari 2018.

Michael Jonsson
Projektledare

Mars 2018

1 Inledning

Det säkerhetspolitiska läget i norra Europa har under den senaste tioårsperioden försämrats successivt. Kriget i Georgien, annekteringen av Krim och Rysslands militära stöd till rebeller i östra Ukraina har förändrat den försvarspolitiska dynamiken runt Östersjön i grunden. Rysslands åsidosättande av det rustningsbegränsande kärnvapenavtalet INF aktualiserar åter betydelsen av kärnvapenhot för närområdet och förstärker bilden av ett Ryssland som är berett att utmana den rådande europeiska säkerhetsordningen. Insikten om att Sverige skulle bli indraget i en konflikt i vårt närområde har föranlett ett förnyat fokus på nationella försvarsförmågor.[1] Att öka krigsförbandens duglighet är åter Försvarsmaktens högsta prioritet.[2]

Men den militära hotdimensionen utgör bara en del av problembilden. Den typ av lågintensiva och multidimensionella påverkansoperationer som riktats mot bland annat Georgien och Estlands infrastruktur, ekonomi och befolkning har föranlett en intensiv diskussion om strategi, operationskonst och det moderna krigets karaktär. Vad är krig? Och vilken roll spelar ett lands försvarsmakt i en tid när icke-militära maktmedel får en tillsynes alltmer central roll i mellanstatliga konflikter?

Även Sverige är kontinuerligt utsatt för verkan av strategiska maktmedel. Överbefälhavare Michael Bydén har refererat till detta som en ”komplex hybridkrigföring där man försöker utnyttja våra svagheter, där man försöker ge sig på oss inte bara med militära medel […]”.[3] Försvarsminister Peter Hultqvist har i sin tur talat om att Sverige befinner sig ”mitt i en gråzonsproblematik”.[4]

Den här typen av sammansatta hot som syftar till att destabilisera motståndarens samhällsfunktioner kan av olika anledningar vara svåra att upptäcka, karaktärisera och analysera. Situationen ställer krav på förmåga hos den angripne att skapa en sammanhängande lägesbild ur ett skenbart osammanhängande förlopp. Omvärldsutvecklingen har därför gett upphov till en internationell diskussion om tidig förvarning. Flertalet tankesmedjerapporter och policydokument understryker vikten av att västerländska underrättelsetjänster

[1] Bringéus (2016), *Säkerhet i en ny tid: Betänkande av utredningen om Sveriges försvars- och säkerhetspolitiska samarbeten*, SOU 2016:57; Försvarsmaktens delredovisning av perspektivstudien 2016–2018, HKV 2016-12-01 (FM2015-13192:9), bilaga 1 s. 4
[2] Regeringens proposition 2014/15:109, Försvarspolitisk inriktning - Sveriges försvar 2016–2020
[3] Lönnaeus (2016), ’ÖB: Ryska cyberattacker mot Sverige varje dag’, Sydsvenskan 10 februari
[4] Peter Hultqvist uttalande under seminarium i Almedalen, ’Höjd Beredskap – ett verktyg för samhällsstörningar i gråzonen?’, 3 juli 2017

vässar sin förmåga att identifiera och tolka tecken och signaler som kan indikera att ett ”hybridangrepp” är under uppsegling.[5] Nato har inlett en satsning på att stärka sin förmåga till tidig förvarning (early warning) och lägesbildsuppfattning (situational awareness), och EU har inrättat en Hybrid Fusion Cell inom analyscentret EU INTCENT.[6] Förmågan att identifiera och hantera antagonistiska hot och påtryckningsförsök som faller under tröskeln för väpnat angrepp listas som en av de viktigaste åtgärderna för att stärka Natos försvar mot vad organisationen sedan 2014 valt att kalla hybridkrigföring.[7]

I ljuset av det försämrade säkerhetsläget och de diversifierade säkerhetshoten finns det anledning även för Sverige att se över landets samlade kapacitet att identifiera, värdera och delge information kopplat till olika typer av antagonistiska aggressionsformer.

Föreliggande rapport syftar till att diskutera och problematisera begreppet tidig förvarning i denna kontext, det vill säga när statliga aktörer söker störa normalläget med hjälp av så kallade ”hybridmetoder”.

1.1 Syfte och avgränsning

Studiens övergripande målsättning är att identifiera utmaningar som så kallad hybrid- och gråzonsproblematik medför för svensk underrättelse- och säkerhetstjänst i deras uppdrag att upptäcka, identifiera och varna för framväxande hot mot Sverige.

Ansatsen är bred och rapporten gör inga anspråk på att ge en uttömmande bild av läget. Rapporten bör betraktas som en förstudie som syftar till att reda ut grundläggande begrepp, rama in problemet och identifiera möjliga vägar framåt.

Rapportens fokus är hot som emanerar från stater eller statsstödda antagonister, även om analysen kommer att visa att denna gränsdragning inte nödvändigtvis

[5] Se till exempel Fägersten (2017), ’Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence’, i Hamilton (red), *Forward Resilience: Protecting Society in an Interconnected World Working Paper Series,* SAIS and Center for Transatlantic Relations; Ducaru (2016), ‘Framing NATO’s Approach to Hybrid Warfare’, i Iancu Niculae et al (red), *Countering Hybrid Threats: Lessons Learned from Ukraine* (IOS Press); Pernik och Jermalavicius (2017), ‘Resilience as Part of NATO’s Strategy: Deterrence by Denial and Cyber Defense’, i Daniel Hamilton (red), *Forward Resilience: Protecting Society in an Interconnected World, Working Paper Series,* SAIS and Center for Transatlantic Relations

[6] European Commission Press Release (2017), Security and defence: Significant progress to enhance Europe's resilience against hybrid threats – more work ahead, 19 juli

[7] NATO Wales Summit Declaration, 5 september 2014

är självklar. Sverige utgör en viktig referenspunkt men texten diskuterar fenomenet förvarning, ”hybridoperationer” och samhällssäkerhet på ett mer allmängiltigt plan.

Studiens fokus på icke-militära maktmedel i gränslandet mellan fred och krig innebär att den rör sig i en begränsad del av det totala konfliktspektrumet som omfattar olika typer av krigföring. Studien kommer således inte att gå in på den teknisk-militära dimensionen av förvarning, där t.ex. sensorer utfärdar taktisk förvarning för kvalificerade fjärrstridsmedel. Den kommer heller inte att gå in på detaljer avseende specifika underrättelsemetoder eller indikatorer.

1.2 Metod

Studien har karaktären av en översiktlig litteraturstudie där underlaget som redovisas baseras på öppna källor.

Ämnets karaktär innebär att det finns naturliga begräsningar i vilka källor och vilket material som kan ligga till grund för analysen. Dessa begränsningar utgörs primärt av den höga sekretessnivå som omgärdar underrättelse- och säkerhetstjänstverksamhet, inte minst vad gäller metoder och tillvägagångssätt. Den akademiska litteraturen om svensk samtida underrättelsetjänst är dessutom relativt begränsad i omfattning. Materialet som ligger till grund för rapporten utgörs av akademisk litteratur, forskningsrapporter, utredningar samt, i förekommande fall, memon vars sekretesstämpel har hävts.

1.3 Disposition

Rapporten tar sin utgångspunkt i begreppen *hybridkrigföring* och *gråzonsproblematik,* två begrepp som har präglat den västerländska försvarsdebatten under de senaste åren. Del två redogör för ett antal empiriska referenspunkter som har inverkat på den konceptuella förståelsen av begreppen samt beskriver hur fenomenen tolkats i en svensk kontext. Syftet med avsnittet är dels att reda ut betydelsen av två omtvistade begrepp som används på olika sätt i debatten, dels att redogöra för logiken bakom varför icke-militära maktmedel fått en allt mer central roll i mellanstatliga konflikter. En slutsats är att det inte rör sig om några nya tillvägagångssätt eller strategier, men att ny teknik, nya geostrategiska kontexter samt ökade samhälleliga sårbarheter aktualiserar behovet av att tänka bortom den binära förståelsen av krig och fred som präglat svensk försvarsplanering under många år.

Del tre konkretiserar den teoretiska diskussionen om hybridkrig och gråzonsproblematik genom att redogöra för två samtida konfliktscenarier som illustrerar hur icke-militära maktmedel initialt kan tänkas användas i ett

angrepp mot Sverige. Avsnittet diskuterar för- och nackdelar med att arbeta med scenariobaserad planering för olika samhällsaktörer, samt riskerna med att låsa fast sig i en tolkningsram i studiet av potentiella motståndares agerande.

Del fyra redogör för skillnaderna mellan strategisk och taktisk förvarning samt kopplar samman diskussionen om icke-militära angreppsformer med underrättelsetjänstens uppdrag att varna för fientlig verksamhet mot nationen. Avsnittet diskuterar kopplingen mellan indikatorer och förvarning ur ett antal infallsvinklar. Den traditionella tanken om *tidig förvarning* för väpnat angrepp ställs mot idén om *tidig upptäckt* respektive *tidig åtgärd/reaktion.*

Del fem diskuterar hur den koordinerade användningen av icke-militära påverkansmedel kan anses inverka på svensk underrättelse- och säkerhetstjänsts arbete med att upptäcka och varna för framväxande antagonistiska hot av mer diffus karaktär. Behovet av en ökad medvetenhet om fenomenet utanför säkerhetssektorns kärna, sektorsövergripande samverkan samt nära dialog mellan underrättelsetjänst och beslutsfattare lyfts som viktiga aspekter.

Del sex presenterar studiens slutsatser och förslag på vidare forskning.

2 Centrala begrepp

Innan vi påbörjar en diskussion om tidig förvarning finns det ett behov av att redogöra för de omvärldsförändringar som drivit på diskussionen om behovet av förbättrade och mer integrerade förvarningssystem. Detta kommer att göras med utgångspunkt i två centrala begrepp som används för att beskriva de potentiella hotscenarier som länder runt om i Europa nu förbereder sig på för att kunna hantera; hybridkrigföring och gråzonsproblematik. Syftet här är inte att ge en fullständig historisk tillbakablick, men en viss orientering i begreppsfloran är nödvändig för att därefter kunna knyta an till diskussionen om vad detta kan innebära för nationella underrättelsetjänsters arbete.

2.1 Hybridkrigföring

Begreppet hybridkrigföring fördes in i Natos nomenklatur under toppmötet i Wales 2014 och associeras i dag primärt med rysk strategi i allmänhet och landets agerande i Ukraina i synnerhet. Ser man till begreppets utveckling över tid blir det dock tydligt att olika konflikter runt om i världen har använts som utgångspunkt för att förklara och definiera vad hybridkrigföring är. Natos generalsekreterare Jens Stoltenberg har med hänvisning till Rysslands agerande på Krim beskrivit hybridkrigföring som den mörka spegelbilden av Natos *comprehensive approach*; ” vi använder en kombination av militära och icke-militära medel för att stabilisera länder. Andra använder det för att destabilisera dem”.[8] Men det finns inget doktrinärt stöd för hybridkrigföring i Ryssland. Här talar man snarare om icke-linjär krigföring.

När ryska militärteoretiker talar om hybridkrig är det inte för att karaktärisera det egna tillvägagångssättet utan för att beskriva något som bedrivs av väst. Arabiska våren och upptakten till Maidanrevolten ses från ryskt håll som exempel på en form av amerikansk hybridkrigföring där subversion och färgrevolutioner används för att störta oönskade regimer. Även Sverige har anklagats av rysk underrättelsetjänst för att delta i hybridkriget mot Ryssland.[9]

[8] Öppningsanförande av Natos generalsekreterare Jens Stoltenberg vid NATO Transformation Seminar, 25 mars 2015

[9] Galeotti (2016), *Hybrid War or Gibridnaya Voina? Getting Russia’s non-linear Military Challenge Right*, (Mayak Intelligence) s. 24; Sverige pekas ut i hybridkrig mot Ryssland, Svenska Dagbladet, 22 dec 2017.

Paradoxalt nog betraktas hybridkrigföring alltså som något Ryssland måste utarbeta strategier för att möta.[10]

Begreppet har under dess 15-åriga historia använts för att beskriva vad som vid olika tillfällen uppfattats som ”nya” tillvägagångssätt från vitt skilda aktörer, inklusive tjetjenska rebeller, Iran, Hizbollah, IS och Kina. Det faktum att empiri från konflikter runt om i världen löpande har modifierat den konceptuella analysen och förståelsen för vad hybridkrigföring är har sannolikt bidragit till den förvirring som omgärdar begreppet i dag.[11] Idén om hybridkriget har enligt en analytiker blivit ett ”Frankensteins monster” som antar nya former beroende på vilken rapport eller PowerPoint-presentation man tar del av.[12] Av detta skäl finns det anledning att backa tillbaka och i en kort historisk tillbakablick redogöra för hur förståelsen för begreppet hybridkrigföring har utvecklats över tid.

Initialt fokus på icke-statliga aktörer

Tidiga definitioner av hybridkrigföring utgick från observationer av icke-statliga aktörers krigsteknik. William J. Nemeths studie av tjetjenska rebeller, *Future War and Chechnya: A Case for Hybrid Warfare* från 2002 var en av de första analyserna som diskuterade konceptet hybridkrig.[13] Nemeth argumenterade för att det tjetjenska samhället var en hybrid mellan ett traditionellt, klanbaserat samhälle och en modern stat; en spänning som reflekterades i tjetjenernas krigföring. Tjetjenernas ”militära hybridstyrkor” tillämpade en kombination av traditionell gerillakrigföring, modern informationsteknologi och sofistikerade informationsoperationer i sin kamp mot det militärt överlägsna Ryssland. Det finns de som menar att Tjetjenernas tillvägagångssätt och syn på krigets allsidiga natur kan ha influerat dagens ryska strateger.[14]

En annan inflytelserik empirisk referenspunkt är Libanonkriget som utkämpades under 34 dagar mellan Israel och Hizbollah 2006. Det faktum att Hizbollah lyckades hålla Israels armé stången överraskade många, inklusive den amerikanske officeren Frank G. Hoffman som beskrev de av Iran uppbackade Hizbollahstyrkorna som en sammansmältning av en konventionell

[10] McDermott (2016), ‘Gerasimov Calls for New Strategy to Counter Colour Revolution, *Eurasia Daily Monitor,* Vol. 13 Is. 46

[11] Se Reichborn-Kjennerud & Cullen (2016), “What is Hybrid Warfare?”, Norwegian Institute of international Affairs, NUPI Policy Brief

[12] Kofman (2016) ‘Russian Hybrid Warfare and Other Dark Arts’, *War on the Rocks,* 11 mars

[13] Nemeth (2002), ‘Future war and Chechnya: a case for hybrid warfare’, Monterrey CA, the Naval Postgraduate School

[14] Racz (2014) ‘Russia’s Hybrid Warfare in Ukraine’, The Finnish Institute of International Affairs, Report 43, s. 30

armé och en klassisk gerillastyrka; ett tydligt exempel på ett modernt ”hybrid-hot”.[15] Kombinationen av Hizbollahs decentraliserade kommandostruktur, effektiva kommunikationskampanj och inte minst betydande tillgång till moderna vapensystem representerade en ny typ av utmaning som västerländska försvarsplanerare måste ta höjd för.[16]

Hoffman fick stöd av auktoriteter inom det amerikanska försvarsetablissemanget och en debatt uppstod om att USA:s försvarsplanerare måste överge idén att hot kommer att presentera sig i prydliga kategorier. Framtidens krig, menade man, kommer att vara ”hybrida”; där adjektivet hybrid skulle fånga förändringarna i motståndarens organisation, taktik och teknik.[17]

De inledande diskussionerna om hybridkrigföring fokuserade alltså på de kinetiska aspekterna av kriget. Taktik, operationskonst och tillgång till potenta vapen stod i fokus för analysen. Hybridkrigföring tillämpades av innovativa och amorfa icke-statliga grupper som använde vapen som tidigare varit förbehållna stater och som tillämpade en kombination av urskillningslöst våld och kriminell störning. Det var samtidens version av gerillakrigföring.[18] De allt mer potenta icke-statliga aktörerna bidrog till att sudda ut skiljelinjen mellan, och användbarheten av, de två analytiska kategorierna reguljär och irreguljär krigföring.

Rysslands annektering av Krim blev ny empirisk referenspunkt

Efter Rysslands annektering av Krim 2014 fick hybridkrigsbegreppet medialt genomslag, samtidigt som den konceptuella analysen skiftade fokus. Från att tidigare ha fokuserat på icke-statliga aktörers krigföringsteknik diskuterades nu begreppet i termer av hur staten Ryssland kombinerade militära maktmedel med desinformationskampanjer, cyberattacker samt ekonomisk och energirelaterad utpressning i syfte att uppnå strategiska effekter. Att annekteringen kunde genomföras utan att några skott avlossades medförde att den västerländska diskursen om hybridkrigföring fick ett tydligare fokus på den statliga, centrala koordineringen av civila påverkansmedel, samt på användandet av proxy-styrkor.

[15] Hoffman (2006) “Lessons from Lebanon: Hezbollah and Hybrid Wars”, *Foreign Policy Research Institute*
[16] Hoffman (2007), *Conflict in the 21st Century: The Rise of Hybrid wars*, (Potomac Institute for Policy Studies)
[17] Mattis & Hoffman (2005), ’Future warfare: The rise of hybrid wars’. *Proceedings Magazine,* vol. 131/11/ s. 18–20
[18] Nemeth (2002) s. 29

För analytiker som bevakat rysk militär förmåga under många år stod det dock klart att få inslag i Krim-kampanjen var kvalitativt nya.[19] Operationen genomfördes med hjälp av sedan länge beprövade metoder i kombination med ny teknologi och förbättrad koordinering mellan civila och militära myndigheter. Undantaget var möjligtvis den stora andelen kontrakterade militärer relativt andelen värnpliktiga som deltog i operationen.[20]

Det som skedde i Ukraina hade i varierande grad redan skett i andra postsovjetiska stater. Ett särskilt intressant exempel är Georgien som sedan självständigheten 1991 har utsatts för ett brett spektrum av påtryckningar från Ryssland. Den ryska verktygslådan som använts i Georgien har inkluderat subversiva element, etablerandet av pro-ryska NGO:s och mediekanaler, inflytelseagenter, ekonomisk utpressning, cyberattacker samt konventionellt militärt våld. Georgien kan i viss mån sägas ha fungerat som en slags prövosten för rysk icke-linjär krigföring.[21]

Hybridkrigets fokus på sårbarheter

På ett konceptuellt plan har hybridkrigföring beskrivits som själva koordineringen av kinetiska och icke-kinetiska maktmedel som skräddarsys för att utnyttja specifika svagheter i motståndarens nationella system. Hybriditeten tros skapa positiva synergieffekter för den som tillämpar krigföringen där helheten blir större än summan av de enskilda delarna. För att uppnå avsedd effekt krävs i praktiken en stark kommandostruktur som styr kampanjen centralt.[22] Den centrala koordineringen av maktmedel kan liknas vid en termostat, där temperaturen kan höjas och sänkas beroende på hur scenariot utvecklar sig.

Hur en ”hybridkampanj” designas och vilken relativ vikt de olika maktinstrumenten ges kan sägas vara beroende av tre faktorer:

1. Hotaktörens förmågor (och kapacitet att synkronisera olika maktmedel)
2. Dennes politisk-strategiska målsättningar
3. De upplevda sårbarheterna hos mållandet

[19] Maigre (2015), ‘Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO’, *German Marshall Fund of the United States*

[20] Norberg, Westerlund & Franke (2014), ‘The Crimea Operation: Implications for Future Russian Military Interventions’, i Granholm, Malminen, & Persson (red.), *A Rude Awakening: Ramifications of Russian Aggression towards Ukraine,* FOI-R--3892--SE, s. 48

[21] Se Nilsson (2018) ‘Russian Hybrid Tactics in Georgia’, Institute for Security and Development, The Silk Road Studies Program

[22] Cullen & Reichborn-Kjennerud (2016b), ‘Countering Hybrid Warfare, Baseline Assessment’, Multinational Capability Development Campaign (MCDC), s. 17

Varje sådan ”hybridoperation” kommer följaktligen att vara beroende dels av den aggressiva aktörens förmågor och målsättning, dels av hur dessa förmågor och målsättningar kan matchas mot mållandets unika kontext och sårbarheter. Detta är naturligtvis inget nytt; militär strategi handlar i grunden om att kombinera olika maktmedel och använda sin styrka mot motpartens svagheter så att de egna målen kan främjas. Omvärldsutvecklingen visar dock att dessa mål i allt mindre utsträckning uppnås genom att avväpna en motståndare på slagfältet.

I takt med att vårt beroende av globala försörjningsflöden inom livsmedel, bränsle, energi, data och kapital ökar har den tredje punkten ovan, mållandets sårbarheter, fått nya dimensioner. Genom att slå ut eller utsätta kritiska samhällsfunktioner för hårt tryck kan ett land påverkas att agera i en för hotaktören fördelaktig riktning. Om angriparen har lyckats penetrera ett kritiskt system kan det dessutom räcka med att signalera att man förfogar över *möjligheten* att angripa systemet. Försvararen och dennes allierade blir på så sätt medvetna om att en eskalation kan vara förenad med stora kostnader.[23]

En angripare kan även försöka utnyttja andra icke-fysiska sårbarheter, till exempel befintliga motsättningar mellan grupper i mållandets samhälle, kryphål i lagar eller inbyggda trögheter i demokratiska beslutsprocesser (t.ex. det kollektiva beslutsfattandet som kännetecknar Nato och EU). Nyckeln till en lyckad hybridkampanj är att anpassa den till den specifika kontext som råder i mållandet. Detta innebär att en hybridkampanj i land A inte nödvändigtvis kan användas för att förutsäga hur en kampanj ser ut i land B.

Sammanfattning

Det som i den västerländska debatten beskrivs som ”hybridkrigföring” kan sammanfattningsvis betraktas som sammanblandningen av två separata (men ibland överlappande) processer.

Det rör sig dels om en process som har många likheter med traditionell krigföring, där olika kinetiska och icke-kinetiska maktmedel används för att "mjuka upp" slagfältet inför en militär intervention där både reguljära och irreguljära förband sedermera deltar. Den andra processen har ett större fokus på politiska, ekonomiska och psykologiska påtryckningsmedel som i dag kan

[23] Denna strategiska användning av cyberoperationer användes enligt rysslandsforskaren Steven Blank både i Georgien och Ukraina, se Blank (2017), ’Cyber War and Information War á la Russe’, i Understanding Cyber Conflict: 14 Analogies, Perkovich & Levite (red). Se också Hollis (2011), ’Cyberwar Case Study: Georgia 2008’, *Small Wars Journal*

kombineras med cyberangrepp och strategisk kommunikation för att över tid påverka ett land att röra sig i en viss riktning.[24]

Det senare tillvägagångssättet, som under kalla kriget gick under benämningen *politisk krigföring*, har i den samtida debatten fått ett nytt namn: gråzonsproblematik.

2.2 Gråzonsproblematik

Parallellt med diskussionen om hybridkrigföring har en likartad men bredare debatt förts inom amerikanska försvarskretsar om "The Gray Zone". I viss mån kan man säga att hybridkrigföringens icke-kinetiska dimension passerar som ”gråzonsproblematik” i USA. Debatten drivs av övertygelsen att USA:s strategiska motståndare i ökande grad söker underminera och urholka landets politiska, militära och ekonomiska makt på den internationella arenan. Begreppet ”gråzonskonflikt” seglade upp på den amerikanska dagordningen runt 2015 och har sedan dess blivit ett samlingsnamn för de säkerhetsutmaningar som landets försvarsmakt bedöms stå inför, primärt i operationsområden utanför det amerikanska fastlandet.[25]

Företrädare för de amerikanska specialförbanden, USSOCOM, har förutspått att majoriteten av de hot som USA kommer att behöva hantera under de kommande åren karaktäriseras av att de utspelar sig just i den juridiska och militärstrategiska gråzonen mellan acceptabel internationell konkurrens och öppen militär krigföring; i mellanrummet mellan traditionell diplomati och öppen militär aggression.[26] Att begreppet har fått så pass stor uppmärksamhet beror sannolikt på att tillvägagångssättet neutraliserar mycket av västvärldens militära förmågor. Som en amerikansk officer ska ha uttryckt saken: ”vi har spenderat miljarder på att förbereda oss på fel slags krig”.[27]

Begreppet ”gråzonskonflikter” används i den amerikanska kontexten för att beskriva kampanjer längre ner på konfliktspektrumet där aktörer på ett subtilt och nyanserat sätt använder olika typer av tvångsmedel för att uppnå politiska

[24] Se Galeotti (2016), *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear Military Challenge Right*, (Mayak Intelligence)

[25] Se till exempel ‘Not at Peace and Not at War: An Exploration of “Gray Conflicts’ (2015), *Joint Strategy Review*; USSOCOM White Paper (2015), ‘The Gray Zone’, *US Special Operations Command;* Warburg (2016).’Perceiving Gray Zone Indications’, *US Army Special Operations Command,* Patricia DeGennaro (2016), ‘The Gray Zone and intelligence Preparation of the Battle Space, Small Wars Journal, Aug. 17

[26] General Votel, (2015). ‘Statement of General Joseph L. Votel, US Army Commander US Special Operations Command’

[27] Anonym citerad i Galeotti (2016), *Hybrid War or*… s. 9

målsättningar utan att korsa gränsen för konventionell krigföring. Karaktäristiskt för denna typ av antagonistiska hot är att de präglas av stor otydlighet och begränsad våldsanvändning. I brittiska försvarskretsar använder man begreppet *ambigous warfare* (tvetydig krigföring) för att beskriva i princip samma sak.[28]

Det kan röra sig om situationer där militära maktdemonstrationer, samhällsstörande operationer och desinformationskampanjer på olika nivåer nyttjas i syfte att skapa förvirring och passivitet, eller för att övertyga eller tvinga mållandet att agera i strid med dess nationella kärnintressen. Genom att agera dolt eller förneka inblandning (s.k. *plausible deniability*), kan den aggressiva parten öka osäkerheten avseende vem som ligger bakom aggressionerna samt vad syftet är.[29] Bevisbördan att man över huvud taget är utsatt för ett angrepp hamnar hos den angripna parten. Tillvägagångssättet syftar till att underminera motståndarens beslutsprocess och möjlighet att använda legitimt våld som svar.[30] En annan viktig aspekt är att de länder som ska försvara sig från denna typ av moraliskt och juridiskt tveksamma strategier kan ha tydliga begränsningar vad gäller svängrum för vedergällning; att svara med samma slags metoder är ofta inte ett alternativ för demokratiska stater. Detta ger angriparen en komparativ fördel.

Inget nytt fenomen

Politisk destabilisering, stöd till proxy-styrkor och informationskrigföring tillhör några av de mest klassiska verktygen för staters maktutövande. I skuggan av kalla krigets ömsesidiga hot om vedergällning med massförstörelsevapen fördes maktkampen under tröskeln för regelrätt krig med hjälp av propaganda, underrättelseoperationer och taktiska ombud.[31] Den dolda kraftmätningen bröts genom Sovjetunionens sammanbrott, men har nu återigen aktualiserats, om än i en ny strategisk kontext.

Michael J. Mazarr från den amerikanska tankesmedjan RAND har argumenterat för att så kallade gråzonskonflikter har fått förnyad relevans på senare år. ”Revanschistiska stater” som Kina, Iran och Ryssland söker i dag utnyttja asymmetriska förhållanden genom att successivt förskjuta gränserna för status quo utan att provocera fram en militär sammandrabbning med det än så länge

[28] Mumford & McDonald (2014), ’Ambigous Warfare’, Rapport producerad för Development, Concepts and Doctrine Centre (DCDC)
[29] Wirtz (2017), ‘Life in the Gray Zone: Observations for Contemporary Strategists’, *Defense & Security Analysis,* Vol. 33, No. 2
[30] Mumford & McDonald (2014), s. 3
[31] Se Kennan (1991), *Measures Short of War: The George F. Kennan Lectures at the National War College, 1946-1947*, Washington, DC: National Defense University Press

militärt överlägsna USA.[32] Asymmetrin kan spela på förmågor, men även viljan att använda våld och engagera de egna trupperna.

Vidare har teknikutvecklingen medfört en komprimering av tids- och rumsförhållanden. Kraftfulla cybervapen, digitaliseringen av informationsarenan och civila verktyg som drönare och kustbevakning erbjuder nya möjligheter för de aktörer som vill utöva påverkan utan att exponera den egna personalen. Påverkansoperationer i form av digitala sabotage, terror och psykologisk krigföring kan genomföras under radarn och på distans.

Icke-linjära eskalationsförlopp

Denna typ av gråzonsstrategier utmanar även vår traditionella förståelse av hur ett krisförlopp utvecklas över tid. Idén om en gradvis eskalerande kris som stegras successivt enligt en given eskalationstrappa, och som matchas av det gradvisa införandet av beredskapsåtgärder, är ett tankemässigt arv från kalla kriget som inte nödvändigtvis kan appliceras på den här typen av scenarier.[33] Gråzonsstrategier bygger på idén om att långsamt förskjuta styrkeförhållandena genom en lång rad aktiviteter och begränsade provokationer, snarare än att driva på tydliga förändringar som riskerar att trigga igång en kraftfull motreaktion från den angripne parten (eller dennes allierade). En annan möjlig målsättning är att utnyttja brist på redundans hos försvararen och på så sätt orsaka utnötning eller utmattning över tid.

Strategin att hålla sig under sådana trösklar och ”röda linjer” kallas ofta *salami-slicing*, där den aggressiva aktören flyttar fram sina positioner långsamt och där varje steg eller provokation i sig självt upplevs som relativt harmlös.[34] Sammantaget och över tid kan dock agerandet innebära att status quo gradvis nöts ner och den aggressiva partens intressesfär utvidgas. Kinas successiva maktförskjutning i Sydkinesiska havet, där landet byggt upp artificiella öar med militära installationer, är ett exempel på ett sådant tillvägagångssätt.[35]

En annan mer militaristisk strategi som kan tillämpas inom ramen för gråzonskonflikter är att mycket snabbt förändra fakta på marken innan den angripne hinner uppfatta vad som har hänt. Här blir förvarningstiden mycket kort. Fait accompli-strategin bygger på en abrupt förändring i status quo där den angripne plötsligt står inför fullbordat faktum. Det blir således den

[32] Mazarr (2015), *Mastering the Gray Zone: Understanding a Changing era of Conflict,* Strategic Studies Institute, U.S. Army War College, s. 3

[33] Se Connable, Campbell & Madden (2016), *Stretching and Exploiting Thresholds for High-Order War. How Russia, China, and Iran Are Eroding American Influence Using time-Tested Measures Short of War* (Rand Corporations: Santa Monica), s. 9-15

[34] Schelling (1966), *Arms and Influence* (New Haven, CT: Yale University Press), s. 66-68

[35] Haddick (2014), ‘America has No Answer to China’s Salami-Slicing’, *War on the Rocks,* 6 februari

angripne, och inte angriparen, som lämnas med beslutet om huruvida det är värt att eskalera konflikten och tillgripa våld för att ta tillbaka det som har förlorats.[36] Rysslands annektering av Krim är ett exempel på ett sådant tillvägagångssätt. Genom att snabbt skapa en ny situation som förverkligats med minimalt antal döda presenterades Ukraina och Nato med alternativet att eskalera, något som Ryssland mycket riktigt bedömde inte låg i Natos intresse.

Gråzonens trösklar är inte givna

Det är i sammanhanget viktigt att påpeka att det inte *a priori* finns några givna trösklar eller röda linjer som särskiljer gråzon från fred eller krig. Tolkningen av motståndarens agerande ligger i betraktarens ögon. Röda linjer är koppade till politisk vilja. Om den aggressiva parten förnekar sin formella inblandning i en konflikt, samtidigt som den angripna parten inte vill förklara krig på grund av att ett sådant ställningstagande är förenat med stora risker, kan även en väpnad konflikt utkämpas i "gråzonen". Ett exempel är de sedan 2014 pågående striderna i östra Ukraina. Ryssland förnekar direkt inblandning, trots att överväldigande bevis talar för motsatsen. Samtidigt refererar den ukrainska regeringen till den nationella försvarsoperationen som en "Anti-terrorist Operation".[37]

Att dra linjer i sanden och medge för världen att man befinner sig i krig är beslut som baseras på politiska och militärstrategiska avvägningar. När kostnaderna att fatta ett sådant beslut överstiger fördelarna kan även en konflikt med tusentals dödsoffer utkämpas i "gråzonen".

Den svenska kontexten

I den svenska försvarspolitiska debatten har begreppet "gråzon" primärt diskuterats i termer av ett juridiskt ingenmansland mellan krig och fred. I regeringsformens femtonde kapitel "Krig och krigsfara" redogörs för hur regering och riksdag ska organisera sig i händelse av krig. Här slås det fast att Försvarsmakten får agera för att möta ett väpnat angrepp eller förhindra kränkningar av rikets territorium.[38] Sveriges beredskapslagar är skrivna med utgångspunkt i en binär förståelse för krig och fred, där krig förstås som ett väpnat angrepp och där fred är avsaknaden av detsamma. Skrivningarna är en rest från det andra världskriget, då kriget förväntades komma i form av en militär invasion över havet eller inmarsch via Nordkalotten med efterföljande ockupation. När underrättelsetjänstens larmklocka ljöd skulle Försvarsmakten

[36] Se Altman (2015), 'Red Lines and Faits Accomplis in Interstate Coercion and Crisis', avhandling från Cambridge, MA: Massachusetts Institute of Technology
[37] 'Förutsättningar för krisberedskap och totalförsvar i Sverige' (2017), Försvarshögskolan, Crismart
[38] 15 kap. 13 § RF

mobiliseras för att bjuda motstånd.[39] Men den juridiska gråzon i vilken många av dagens konflikter utspelar sig skapar praktiska problem för de aktörer som har i uppdrag att skydda Sveriges territoriella integritet och suveränitet.

Robert Dalsjö och Thomas Hultmark argumenterar i artikeln *Hur uppnå verkan i kris och gråzon?* att det nya omvärldsläget kräver att Försvarsmakten utformar nya riktlinjer för hur man ska agera i gråzonen mellan krig och fred, och gör upp med ingrodda föreställningar från den strategiska timeouten; "En sådan föreställning är att 'om det inte är krig så är det fred'. I fred dominerar då produktionsperspektivet, verksamhet vardagar 9 till 5, verksamhetsplanering, arbetstidsbestämmelser, personalvård, etc. Att det faktiskt kan bli aktuellt med mycket skarp verksamhet, fastän fred råder, blir då kontraintuitivt."[40]

I ett försök att nyansera den binära uppdelningen mellan krig och fred har Försvarsmaktens nya militärstrategiska doktrin (MSD-16) introducerat begreppet "gråzonsproblematik".[41] Doktrinen nämner begreppet ett dussintal gånger, vilket kan jämföras med föregående doktrin från 2011 samt Försvarsmaktens operativa doktrin från 2014 där begreppet "gråzon" inte nämns alls.[42]

I MSD-16 beskrivs gråzonsproblematik som "de strategiska otydligheter som uppstår mellan fred och krig". I doktrinen konstateras det att Sverige är kontinuerligt utsatt, ofta subtilt, för verkan av strategiska maktmedel. Underförstått är att gråzonen är ett läge som infaller när den aggregerade intensiteten och allvaret i dessa aggressioner ökar. Det är dock inte möjligt att med någon exakthet specificera när detta läge inträffar. Karaktäristiskt för denna typ av situation är att det råder en "spänning mellan inre och yttre säkerhet".[43]

Det svenska samhället är indelat enligt en juridisk och förvaltningsmässig modell där det finns en tydlig ansvarsuppdelning för att hantera inre respektive yttre säkerhet. Denna modell svarar inte nödvändigtvis upp mot de förändringsprocesser som den moderna krigföringen genomgått, eller mot våra potentiella motståndares bild av kriget som fenomen. Den ryska icke-linjära krigföringen har till exempel ett mer holistiskt förhållningssätt till internationellt maktutövande. Här dras inga tydliga gränser mellan krig och fred. Den

[39] Ekman (2000), *Den militära underrättelsetjänsten: Fem kriser under det kalla kriget* (Stockholm: Carlssons förlag), s. 16

[40] Dalsjö och Hultmark (2017), "Hur uppnå verkan i krislägen och gråzon", *Kungl. Krigsvetenskapsakademiens Handlingar och Tidskrift* Vol. 2, s. 155

[41] Försvarsmakten (2016), Militärstrategisk doktrin (MSD-16) s. 37

[42] Jmf. Försvarsmakten, Operativ doktrin 2014; Militärstrategisk Doktrin 2011 (MSD-12). Begreppet "hybridkrigföring" diskuteras dock i båda dokumenten.

[43] Försvarsmakten (2016), Militärstrategisk doktrin (MSD-16) s. 37. Värt att notera är dock Försvarsmaktens Perspektivstudier (PERP) har diskuterat gråzonen som begrepp, bl.a. i Försvarsmaktidé och målbild. Årsrapport från Perspektivplanering 2000-01, Försvarsmakten, s. 74

ryska doktrinen omfamnar idén om att militära operationer samspelar med ett lands övriga maktmedel i strävan att uppnå en viss politisk effekt.[44]

Att gråzon som begrepp har introducerats i Sveriges militärstrategiska doktrin kan ses som försök att rikta uppmärksamhet mot det faktum att krig, liksom fred, har många gråskalor samt att all krigföring, i viss mån, är hybrid.[45]

2.3 Slutsatser

Begreppen hybridkrigföring och gråzonsproblematik är två försök att begripliggöra konflikter som utmanar den traditionella västerländska synen på krig och krigföring; en syn som traditionellt sett har varit fokuserad på striden. Begreppen är försök att teoretisera och generalisera svårtolkade och sammanlänkande aggressionsformer som suddar ut gränserna mellan reguljär och irreguljär, civilt och militärt, krig och fred. Att begreppet har fått så pass stor uppmärksamhet beror sannolikt på att tillvägagångssättet neutraliserar stora delar av västvärldens militära förmågor.

De ord vi använder för att beskriva verkligheten runt omkring oss påverkar vårt sätt att tänka, vilket i förlängningen inverkar på hur vi planerar och förbereder oss för att möta den.[46] I bästa fall hjälper begrepp som hybridkrig och gråzonsproblematik oss att tänka klart kring det faktum att det finns, och alltid har funnits, ett spektrum av gråskalor som täcker in utrymmet mellan djupaste fred och väpnad strid. I värsta fall bidrar dessa språkliga nybildningar till att underminera vår förståelse av krigets komplexitet. Det kan dessutom finnas en risk att introduktionen av nya etiketter och prefix överbetonar dragen av förändring, vilket kan förleda oss att tro att det är något fundamentalt nytt som måste hanteras.[47]

Slutligen kan det konstateras att det inte finns någon allmänt accepterad definition av varken gråzonsproblematik eller hybridkrigföring, eller vilka slags maktmedel som ingår i problembilden. Och kanske är det mindre viktigt att enas om en sådan. Alltför detaljerade definitioner av fenomen riskerar att

[44] Hedenskog, Persson & Vendil Pallin (2016), 'Russian Security Policy', i Persson (red), *Russian Military Capabilities in a Ten-Year Perspective*, FOI-R--4326--SE, s. 114

[45] För ett resonemang om detta, se Käihkö (2016), 'All krigföring är av hybrid natur', Statsvetenskaplig tidskrift. No 4

[46] För en diskussion om etikettering och ordval i försvarsplanering, se Smith (2003), 'Guerrillas in the Mist: Reassessing Strategy and Low Intensity Warfare', Review of International Studies, Vol 29, no 1, s. 19-37

[47] För en kritik av begreppen, se till exempel Elkus (2015), '50 Shades of Gray. Why the Gray Wars Concept Lacks Strategic Sense', *War on the Rocks*, 15 december; Giles (2016), 'Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power, Chatham House, Research Paper

bli inaktuella så fort en aktör utvecklar sina förmågor och tillvägagångssätt. Däremot kan det vara värdefullt att gå bortom abstraktionerna och konkretisera hur sådana hypotetiska scenarier kan gestalta sig i olika kontexter. Här kan scenarier och *typfall* tjäna som diskussionsunderlag för hur olika samhällsfunktioner kan tänkas påverkas i en kris- eller krigssituation. Nästa avsnitt kommer att redogöra för två sådana typfall som har tagits fram av FOI i syfte att stödja uppbyggnaden av det civila försvaret.

3 Scenarier för gråzon och hybridhot

Det försämrade säkerhetspolitiska läget har föranlett ett ökat fokus på den svenska totalförsvarsförmågan. Med utgångspunkt i en beskrivning av hur ett modernt krig kan yttra sig har FOI på uppdrag av bl.a. Myndigheten för Samhällsskydd och Beredskap (MSB) tagit fram ett antal scenarier i syfte att konkretisera och nyansera hur olika typer av angrepp (militära som icke-militära) skulle kunna se ut, samt vilka effekter de skulle kunna få på samhället.

Två av dessa scenarier har särskild relevans för denna rapport då de präglas primärt av användningen av icke-militära maktmedel och stor osäkerhet.

Den eskalerande hybridkonflikten

Detta typfall redogör för en situation där en statlig angripare använder ett brett spektrum av öppna och dolda maktmedel för att betvinga svenska politiker och den breda opinionen att agera i en för motståndaren viktig säkerhetspolitisk fråga.[48] Scenariot utgår från en situation som karaktäriseras av ökade spänningarna i Östersjön och där motståndarens diplomatiska retorik gentemot Sverige blir allt mer fientlig. Försvarsmaktens incidentberedskap prövas via återkommande responstester och desinformation kopplat till svensk försvars- och säkerhetspolitik får spridning i svenska medier. Störningar på kritisk infrastruktur sammanfaller med svenska utrikespolitiska utspel och krisberedskapen prövas hårt av tillsynes isolerade olyckor och omfattande cyberattacker som slår mot betalsystemet och mobiltelefoninätet. En ökning av oförklarliga bränder belastar räddningstjänsterna och social oro sprider sig med kravaller och upplopp som följd. Efter att milismän utan nationalitetsbeteckning hamnat i direkt strid med polis och hemvärn i olika landsändar anbefaller regeringen slutligen höjd beredskap och ber om internationell hjälp. Morgonen därpå briserar ett mindre taktiskt kärnvapen i Norrland; ett vapen som felaktigt påstås tillhöra Sveriges internationella partner vars flygvapen ska ha samövat med svenska förband i närheten av platsen.

Scenariot avslutas i och med att antagonisten uppmanar det svenska folket att stå upp för sin 200-åriga tradition av neutralitet genom att avbryta allt internationellt militärt samarbete samt att verka för en kärnvapenfri zon i Norden och Östersjöregionen.

[48] Jonsson (2017), 'Att använda scenarier i planeringen för civilt försvar', FOI-R--4434--SE

Typfall 5: Utdragen och eskalerande gråzonsproblematik

Detta typfall beskriver ett eskalerande förlopp som pågår under nio månader och som präglas av tillsynes isolerade olyckor, sabotage och cyberangrepp. Det är inledningsvis svårt att bedöma vad antagonistens intentioner är i scenariot. Möjliga syften skulle kunna vara att lamslå svenskt beslutsfattande eller att skapa handlingsutrymmen för ett militärt ingripande. Samtidigt som det är oklart vad det är som egentligen händer fungerar de intensifierade störningarna som en larmklocka om möjlig eskalation.[49]

Händelseförloppet inleds med en rad svårtolkade incidenter på lokal nivå som slår mot elförsörjning, telekommunikationer och transportsystem. Primärvården belastas av lokala utbrott av magsjuka och polisens resurser knyts upp av en påtaglig ökning i gängkriminalitet och allmänna ordningsstörningar. Bank- och finanssektorn drabbas i ökande grad av utpressningsförsök och ransomeware-attacker.

Ett falskt pressmeddelande som varnar för förhöjt terrorhot får stor spridning i sociala medier. Desinformation om att Försvarsmakten undanhåller mat från befolkningen till förmån för sina utländska samarbetspartners leder till upplopp och plundring, samtidigt som förtroendet för myndigheter och politiker sjunker. Den säkerhetspolitiska situationen i området försämras kraftigt och paras med en allt mer konfrontativ diplomatisk retorik från främmande makt. Händelseförloppet eskalerar när ett omfattande cyberangrepp slår mot bland annat flyget och tågtrafikens ledningssystem, samtidigt som de fysiska sabotagen mot nationella försörjningssystem ökar i omfattning. Även Sveriges grannländer drabbas av liknande angrepp. Scenariot avslutas med att tvetydig information om stridshandlingar i ett nordiskt-baltiskt grannland når utarbetade beslutsfattare via sociala medier. Samtidigt som regeringen varnas av främmande makt för att höja beredskapen, erbjuds Sverige en ”hjälpande hand” i form av förnödenheter till utsatta regioner runt Östersjökusten.

3.1 Scenariometodikens för- och nackdelar

Scenarierna som beskrivits ovan karaktäriseras av de parallella utmaningarna som samhällsaktörer kan komma att stå inför i händelse av en utdragen kris, det vill säga; hantera störningar, överblicka läget, återställa samhällsfunktionalitet och mildra de negativa effekterna av störningarna. Genom att på ett strukturerat och metodiskt sätt definiera ett utfallsrum som spänner över mer eller mindre sannolika händelseutvecklingar kan scenarier stödja det

[49] Jonsson (2018), ’Typfall 5: Utdragen och eskalerande gråzonsproblematik. Komplettering av hotbildsunderlag i utvecklingen av civilt försvar’, FOI Memo 6339

planeringsarbete som krävs för att samhället ska kunna hantera effekterna av ett möjligt angrepp. Genom att levandegöra hotbilder och synliggöra osäkerhetsfaktorer kan scenariobaserad planering även bidra till att öka den mentala och politiska medvetenheten bland relevanta aktörer, och i bästa fall nyansera djupt rotade idéer om hur framtiden kan komma att gestalta sig. Detta kan i sin tur bidra till att korta reaktionstiden vid omvälvande händelser.

Samtidigt som scenarier kan ge värdefull vägledning är det dock sannolikt att denna vägledning inte kommer att överensstämma med den framtid som slutligen materialiseras. Scenarier kan inte täcka upp för alla tänkbara händelseförlopp; överraskningsmomentet kan aldrig elimineras. Detta gör scenariobaserade metoder till ett tveeggat svärd.

Förförståelse och kognitiv dissonans

Gemensamt för många så kallade varnings- och underrättelsemisslyckanden genom historien är att beslutsfattare och analytiker har utgått från en felaktig tolkningsram i studiet av potentiella hot. Historien är full av exempel på hur mentala föreställningar om motståndarens drivkrafter, begränsningar och planer påverkat vilka slags signaler som plockats upp samt vilka som ignorerats.[50]

Ett klassiskt exempel är attacken på Pearl Harbor. Under tiden som ledde fram till attacken utgick USA:s försvarsmakt från en teori om att ett eventuellt angrepp mot den amerikanska flottbasen skulle komma inifrån. Det fanns en oro att japaner boendes på Hawaii skulle genomföra sabotage eller terroristattacker mot både civila och militära mål, såsom radiomaster, bondgårdar och flottbaser. Inkommande underrättelser och beslutsunderlag filtrerades således genom den tolkningsramen. För att underlätta övervakning ställdes flygplanen vingspets mot vingspets; en åtgärd som fick ödesdigra konsekvenser när angreppet visade sig komma från skyn.[51]

Kontentan är att alltför starka och detaljerade föreställningar om hotbilder riskerar att låsa fast betraktaren i en tolkningsram som i sin tur påverkar perceptionen av pågående förlopp. Denna logik kan appliceras på dagens diskussioner om gråzons- och hybridproblematik. Efter Rysslands annektering av Krim har forskare och militära strateger i väst sökt hitta sätt att strukturera ”rysk hybridkrigföring” enligt en linjär förklaringsmodell. En modell som har fått stor spridning delar in det ryska tillvägagångssättet i åtta faser, där fas 1-4 karaktäriseras av olika icke-kinetiska påverkansoperationer som syftar till att ”mjuka upp” landet i fråga genom att undergräva statens funktion och folkets

[50] Wohlstetter (1962), *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press)
[51] Silver (2012), *The Signal and the Noise: Why Most Prediction Fail – But Some Don't* (London: Penguin Books)

förtroende för densamma. Därefter går operationen in i ett mer kinetiskt skede. Fas 4–8 karaktäriseras av subversiva aktiviteter initierade av ryska special-förband, blockader, etablerandet av no-fly zoner, telekrigföring och attacker med fjärrstridsmedel mot kritisk infrastruktur. Reguljära förband i form av ”fredsbevarande styrkor” sätts enligt modellen in först i den sjätte fasen. Motståndarlandet ska vid den punkten redan befinna sig i upplösnings-tillstånd.[52]

I takt med att teorin om ”hybridkriget” och dess olika eskalerande faser får genomslag finns det en naturlig risk att det skapas mentala föreställningar om hur ett potentiellt angrepp från Ryssland skulle kunna gestalta sig. Detta kan i sin tur medföra en risk för att signaler som bekräftar förutfattade meningar plockas upp och förstärks, samtidigt som andra, potentiellt mer relevanta, sorteras bort. Starka psykologiska krafter underblåser vår benägenhet att se det vi vill eller förväntar oss att se. Men att utgå från att en potentiell angripare kommer att agera stereotypt är att bädda för överraskningar.

Att arbeta med utgångspunkt i antaganden om hur olika antagonister kan tänkas agera under vissa givna betingelser är en beprövad arbetsmetod inom underrättelsetjänsten, där indikatorer tas fram med utgångspunkt i analyser om fiendens förväntade agerande. Frågan är dock hur effektivt ett sådant deduktivt förhållningssätt är som förvarningsstrategi i en tid där antalet möjliga an-greppsformer är oräkneliga, och där en aktörs agerande i tidigare konflikter inte nödvändigtvis är applicerbart på den egna samhälleliga kontexten. Innan vi påbörjar en diskussion om detta ska vi först redogöra för några grund-läggande antaganden om överraskning och tidig förvarning.

[52] Se Bērziņš (2014), ‘Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy’, Policy paper No 2, *National Defence Academy of Latvia Center for Security and Strategic Research*, s. 6

4 Den tidiga förvarningens syfte och mål

Den främsta uppgiften för många underrättelsetjänster har traditionellt sett varit att anta rollen som vakthund; att larma i händelse av ökad fientlig aktivitet mot landet. Den ideala varningen avseende yttre aggressioner är detaljerad, utfärdad i god tid och möjliggör för beslutsfattare att välja mellan olika konfliktförebyggande åtgärder. En varning som utfärdas med ’god framförhållning’[53] kallas ofta *strategisk varning* och bygger i grunden på en förmåga till ackumulerad kunskapsuppbyggnad i fred om olika aktörers förmågor och intentioner.

Med utgångspunkt i en väl förankrad normalbild är målet att så tidig som möjligt upptäcka indikationer på potentiellt hotande verksamhet i omvärlden som är av strategisk betydelse.[54] Strategisk förvarning kan förstås i termer av ett långsiktigt riskhanteringsverktyg. En väl fungerande förvarningsförmåga bidrar till att skapa flexibilitet i resursanvändning och kan bidra till att en nation inte har en onödigt hög och kostsam beredskap under perioder som karaktäriseras av fred och stabilitet. Tidiga indikationer på att omvärldsläget är på väg att försämras kan i bästa fall överbrygga förmågegap genom att trigga igång beredskapshöjande, diplomatiska eller offensiva åtgärder som syftar till att förebygga, avvärja eller dämpa effekterna av uppkomna hot. Men att i för stor utsträckning förlita sig på att få förvarning innebär alltid ett strategiskt risktagande.

Som exempel på en långsiktig strategisk förvarning kan nämnas den öppna rapporten *Det kaukasiska lackmustestet* som publicerades veckorna efter den rysk-georgiska konflikten 2008.[55] Målet med rapporten var att dra ett antal tentativa slutsatser om vilka konsekvenser kriget kunde få för omvärlden och i förlängningen svensk säkerhetspolitik som vid tidpunkten präglades av den strategiska timeouten. Rapportförfattarna menade att kriget 2008 utgjorde ett lackmustest som visade att Ryssland nu valt väg. Det rysk-georgiska kriget gav en tidig indikation på den nya världsordningens karaktär och funktionssätt. [56]

Exemplet illustrerar ett centralt problem i förvarningssammanhang, nämligen utmaningen för beslutsfattare att i realtid bedöma vilka prognoser och

[53] En tidsangivelse som sällan definieras i litteraturen.
[54] United States Army Functional Concept for Intelligence 2020-2040 (2017), s. 9
[55] Larsson (red) (2008), ‘Det kaukasiska lackmustestet: Konsekvenser och lärdomar av det rysk-georgiska kriget i augusti 2008), FOI-R--2563--SE
[56] Ibid s. 3

varningar som är relevanta och vilka som inte är det. Det är först i efterhand, när dammet har lagt sig, som irrelevant brus, falsklarm och motstridiga uppgifter med säkerhet kan sorteras bort.

Tidig förvarning för ett nära förestående angrepp kallas ofta *taktisk förvarning*. För att en taktisk varning över huvud taget ska nå fram och få någon effekt krävs det att alla delprocesser i en komplex händelsekedja klaffar. Först och främst måste det finnas observerbara bevis som varslar om att motståndaren kan komma att agera i en viss kritisk riktning. Dessa antydningar måste inte bara vara av sådan art att de kan fångas upp och flaggas av underrättelsetjänstens informationsinhämtning (en inhämtning som styrs av den politiska inriktningen); analysfunktionen måste dessutom göra en korrekt tolkning av dess innebörd och relevans. Denna varseblivning måste sedan formuleras och kommuniceras på ett klart och tydligt sätt till jäktade beslutsfattare. Här är budbärarens förtroende avgörande. Om underrättelsetjänsten har kommit med för många falsklarm riskerar detta förtroende att undergrävas. Ett centralt steg i varningen är att de beslutsfattare som delges informationen inte bara uppskattar betydelsen och värdet av uppgifterna; det måste även finnas tid, förmåga, och inte minst politiskt momentum för att kunna vidta adekvata åtgärder.[57] Om något i händelsekedjan brister brukar man tala om ett underrättelsemisslyckande, även om det i många fall de facto handlat om ett policymisslyckande.

Det finns ett omfattande forskningsfält som redogör för alla de kognitiva och organisatoriska fallgropar som bidrar till att varningar inte utfärdas i tid eller lämnas utan åtgärd. Det råder viss enighet om att förvarning inte huvudsakligen handlar om förmågan att identifiera avvikelser och slå larm inför hotande faror. Istället är det övergången från analys och varseblivande till insikt och reaktion som är den kritiska punkten i förvarningskedjan.

Helt avgörande är även vem som är mottagaren av förvarningen samt vilka möjligheter denne har att reagera på ett meningsfullt sätt. [58] I studiet av varningar är det därför viktigt att hålla isär analysproblemet (dvs. underrättelsetjänstens förmåga att upptäcka och delge information) från varningrespons problemet (dvs. beslutsfattarnas förmåga att uppfatta och agera på varningen). Utan respons är varningen meningslös.

---

[57] Omand (2010) *Securing the State* (London: C. Hurst & Co)

[58] Se till exempel Agrell (2008), *Förvarning och Samhällshot,* (Studentlitteratur: Lund) s. 250; Kovacs (1997), 'The Nonuse of Intelligence', *International Journal of intelligence and Counterintelligence,* Vol. 10, No. 4; Betts (2009), 'Surprise Despite Warning: Why Sudden Attacks Succeed' i Christopher Andrew, Richard Aldrich och Wesley K. Warks (eds), *Secret intelligence: A Reader* (New York: Routledge); Kam (1988), *Surprise Attack: the Victim's Perspective* (Cambridge, Mass and London: Harvard University Press)

Händelsekedjan som redogjordes för ovan är en förenklad beskrivning av ett varningsförlopp. Varningen är i regel inte något entydigt och momentant, något som i ena stunden saknas för att i andra stunden föreligga i färdig form. Varning bör snarare betraktas som en sammanflätad väv av ständigt pågående parallella processer.[59] Tidig förvarning för väpnat angrepp är, precis som överraskning, en fråga om gradskillnader. Angrepp sker mycket sällan från en klarblå himmel.

Den traditionella metoden för att erhålla varning för angreppshot var länge *Indications & Warning*; en metod som togs fram av den amerikanska underrättelsetjänsten under kalla kriget och som syftade till att varna för nära förestående angrepp från Sovjetunionen. I följande avsnitt diskuteras och problematiseras denna metod och dess tillämpning på förlopp med varierande grad av intensitet som karaktäriseras av användning av icke-militära maktmedel.

4.1 Indikatorbaserade förvarningsmetoder

Även om det under kalla kriget fanns en rädsla för att bli utsatt för sovjetisk subversion och *aktiva åtgärder* var det trots allt hotet om krig i dess mer eller mindre traditionella form som dominerade försvarsplaneringen.[60] I den här kontexten dominerade de indikatorbaserade förvarningsmetoderna, på engelska *Indications & Warning*. Förvarningsmetodiken bygger i korthet på att underrättelsetjänsten med utgångspunkt i kunskap om motståndarens doktrin, militära kapacitet och agerande i tidigare konflikter genererar en mängd mer eller mindre sannolika hotscenarier. Med utgångspunkt i dessa scenarier försöker analytikerna steg för steg förutsäga vilka åtgärder motståndaren rimligtvis måste vidta för att ta sig till det tänkta slutmålet, samt vilka upptäckbara signaler dessa steg kan tänkas generera.

Förhoppningen är att löpande bevakning av dessa indikatorer kan ge tidiga ledtrådar om att något av de föridentifierade hotförloppen är på väg att materialiseras, vilket i sin tur kan trigga igång mobiliserande eller konfliktavvärjande åtgärder i det egna landet. Förvarningspotentialen ligger här i att det är för kostsamt och påfrestande för en militär organisation att upprätthålla en konstant hög beredskap. De militära, ekonomiska eller politiska förberedelser som ett land bedöms behöva genomföra inför ett angrepp behöver således vara tillräckligt distinkta för att fungera som larmklocka för försvararens underrättelsetjänst. I teorin ska de bästa indikatorerna fungera

[59] Agrell (2008), s. 250
[60] Brodin (1978), 'Surprise Attack: The Case of Sweden', *Journal of Strategic Studies,* Vol. 1, No.1, pp. 98-110

som varningslampor; ju fler som tänds desto högre sannolikhet för ett annalkande angrepp. [61]

För svensk underrättelsetjänsts under kalla kriget såg många underrättelseproblem relativt likartade ut år efter år. Synen på nationell säkerhet utgick från nationen som idé och geografisk företeelse och behovet av underrättelse- och säkerhetstjänst var tämligen statiskt. Kalla krigets förvarningssystem och -metoder byggde på idén om en tydligt definierad, extern fiende vars agerande åtminstone delvis var förutsägbart (och övervakningsbart). Inhämtare och analytiker visste på förhand vilken slags information som var särskilt intressant och inkommande information antingen bekräftade eller falsifierade antaganden om motståndarens förväntade beteende.

I dag arbetar Sverige liksom de flesta andra länder med ett betydligt bredare säkerhetsbegrepp, delvis som en konsekvens av att ett ökande antal opportunistiska aktörer ger uttryck för maktanspråk i en multipolär värld. En annan förklaring till den ökande komplexiteten är det invecklade och bräckliga försörjningsschema som samhällets funktionalitet är uppbyggd kring. Ett exempel på ett sådant intrikat system är den svenska elförsörjningen vars styrsystem traditionellt sett har varit isolerat från omvärlden, men som i dag involverar en stor mängd nationella och internationella aktörer.[62] Ett allvarligt avbrott inom elförsörjningen kan få förödande och svåröverblickbara konsekvenser för stora delar av samhället; konsekvenser som i viss mån kan jämföras med ett väpnat angrepp. Väger man in hela försörjningskedjan är antalet möjliga hotscenarier oräkneliga.

I takt med att hotbilden som moderna samhällen står inför ökar i komplexitet har allt fler länder rört sig bort från det klassiska tillvägagångssättet med att övervaka potentiella hotaktörer och gått mot ett mer inåtblickande, risk- och sårbarhetsfokuserat synsätt på säkerhet.[63] I den samtida förvarningsdebatten har det höjts röster för att den klassiska Indications & Warning-metodologin delvis har spelat ut sin roll.[64] Rapporter från Nato, EU och US Army Special Operations Command argumenterar för att västerländska underrättelsetjänster bör anta ett mer induktivt förhållningssätt till inhämtning och analys, där

[61] Grabo (2004), *Anticipating Surprise: Analysis for Strategic Warning* (Washington, DC: Joint Military Intelligence College)
[62] Andersson & Westerdahl (2017), 'Sveriges elförsörjning Hur möter vi en ökad sårbarhet?' FOI Memo 6173
[63] Se t.ex Hulnick (2005), 'Indications and warning for homeland Security: Seeking a new paradigm', International Journal of intelligence and Counter intelligence, Vol. 18, No 4, s. 605; Treverton (2011), 'Comparing Early Warning Across Domains', Försvarshögskolan; Omand (2010) Securing the State
[64] Giles (2016)

nationens egna sårbarheter, snarare än den potentielle angriparens förväntade beteende, sätts i centrum för inhämtning och analys.[65]

Den långsiktiga förmågan att stå emot och absorbera störningar mot samhällskroppen är en mätare på ett samhälles motståndskraft, dess *resiliens*. Vikten av att bygga resiliens på samhällelig nivå genom att öka robustheten i kritiska nätverk, infrastruktur och finansiella system understryks i Nato och EU:s strategier mot hybridhot.[66] Här bedöms underrättelsetjänster kunna spela en viktig roll, både genom att identifiera, övervaka och hantera samhälleliga sårbarheter.[67] Detta perspektiv på samhällssäkerhet sätter *tidig upptäckt*, snarare än *tidig förvarning,* i centrum.

4.2 Tidig förvarning vs. tidig upptäckt

Skillnaderna mellan tidig förvarning och tidig upptäckt kan illustreras genom en mycket förenklad jämförelse mellan terroranalytikerns och cyberanalytikern funktion.[68] I båda fallen vill analytikern hitta trender och tendenser på ett så tidigt stadium som möjligt för att förhindra eller förebygga hotet. Men skillnaden i hotets karaktär inverkar på vilken typ av signaler som är av intresse för respektive analytiker, samt *när* i förhållande till angreppets initiering som varningen utfärdas.

Terroranalytikern letar efter indikatorer som ger ledtrådar om att en attack kan vara nära förestående. Hon bevakar misstänkta terrorceller och söker efter avvikelser i kommunikations- och rörelsemönster. Om terroranalytikerns varning ska vara användbar måste den utfärdas *innan* själva attacken har inträffat. Varningens syfte är således att förhindra att attacken över huvud taget inträffar genom att gärningsmannen grips eller tågstationen utryms. På så sätt påminner det om underrättelsetjänstens larmklockefunktion inför ett väpnat angrepp. Om varningen kommer *efter* att bomberna släppts över staden är den inte mycket värd.

För cyberanalytikern är utgångspunkten något annorlunda. Här är utsikterna relativt små för att kunna identifiera indikatorer innan ett angrepp över huvud taget har ägt rum. Utmaningen består snarare i att identifiera indikationer på

[65] Se till exempel United States Army Special Operations Command (2016), 'White Paper - Perceiving Gray Zone Indications' och European Union (2016)
[66] Se till exempel 'Joint Framework on countering hybrid threats a European Union response' (2016), European Commission
[67] Fägersten (2017)
[68] Resonemanget är lånat från rapporten 'Comparing Early Warning Across Domains' (2011), sammanställd av Gregory F. Teverton efter en workshop om tidig förvarning på Försvarshögskolan där svenska och internationella experter deltog.

att ett angrepp redan har initierats, eller att ett virus har planterats i ett system. Cyberangrepp kan förbli oupptäckta i flera månader, ibland år, beroende på angriparens mål. De signaler som primärt är av intresse är således de som framträder när ett slags angrepp redan har initierats. Eftersom angriparens identitet och syfte ofta är höjt i dunkel blir cyberanalytikerns primära uppgift att attribuera attacken, det vill säga knyta angreppet till en specifik aktör, samt att utreda varför angreppet genomförts. Utmaningen innan angreppet har initierats består snarare i att säkerställa att systemen är robusta och motståndskraftiga så att angrepp kan förebyggas så långt som möjligt. En liknande logik kan appliceras på hybridhot.

En viktig skillnad mellan militära och icke-militära maktmedel är att den senare hotkategorin är mer diffus. Dold sabotageverksamhet mot kritisk infrastruktur, påverkansoperationer i informationsmiljön och ekonomisk utpressning är inte självmarkerande på samma sätt som militär våldsutövning. Eftersom dess former och effekter kan vara svåra att mäta och kvantifiera kan det därför vara svårt att över huvud taget upptäcka att man är utsatt för ett slags angrepp. Metaforen med grodan som inte hoppar ur det långsamt upphettade vattnet gör sig påmind. Dessa svårigheter förstärks givetvis i de fall angriparen genom vilseledning eller användning av ombud försöker dölja eller förneka ansvar för sitt agerande.

Eftersom många av de icke-militära maktmedlen används även inom ramen för fredstida konkurrensförhållanden kan det dessutom vara svårt att tolka syftet med en handling. Ryms handlingen inom ramen för ”normal” mellanstatlig konkurrens eller ska den betraktas som antagonistisk? Rör det sig om en begränsad påverkansoperation eller ska handlingen förstås i ett större regionalt sammanhang? Handlar det om förbekämpning inför ett stundande väpnat angrepp eller är syftet snarare att testa Sveriges beslutsamhet? Med andra ord: Vad är det som händer? Vem ligger bakom? Och vad är syftet?

Givet de icke-militära maktmedlens diffusa karaktär kan det sammanfattningsvis finnas en poäng att skilja mellan två typer eller förhållningssätt till varningen som fenomen: *tidig förvarning* som syftar till att ge beslutsfattare och centrala samhällsfunktioner möjlighet att avvärja ett förestående angrepp och *tidig upptäckt* som syftar till att begränsa angreppets skadeverkan och hantera följdeffekterna av densamma.

5 Analys och diskussion – utmaningar för underrättelsetjänsten

Mot bakgrund av det som har diskuterats ovan finns det anledning att fundera djupare kring hur den koordinerade användningen av icke-militära påverkansmedel kan anses inverka på underrättelse- och säkerhetstjänstens uppgift att upptäcka, identifiera och varna för framväxande hot mot Sverige. Några möjliga utmaningar och möjligheter diskuteras nedan.

5.1 Lärdomar från historien

Det första som bör framhållas är att frågan om förvarning kopplat till icke-militära angrepp är långt ifrån ny för svensk underrättelsetjänst. Redan under 1960-talet fördes diskussioner om vilka åtgärder som borde vidtas för att förbereda regeringen, Försvarsmakten och underrättelsetjänsterna för att hantera ett svårtolkat angrepp mot Sverige som åtminstone inledningsvis präglades av icke-militära maktmedel av subversiv karaktär.

Fiktiva underrättelserapporter från en högkvartersövning genomförd 1966 tecknar en bild av hur underrättelsetjänsten vid tidpunkten föreställde sig hur ett sådant angrepp skulle kunna se ut samt vilka maktmedel som kunde tänkas användas för att ”mjuka upp” Sveriges försvarsvilja samt påverka landets beslutsfattare i ett internationellt krisläge. Övningsscenariot utgår från ett läge där spänningarna mellan Nato och Warszawapakten ökar successivt och där oron sprider sig över Europa.[69] Efter att stormakternas förhandlingar bryter samman inleds en utdragen fas som präglas av omfattande propaganda och spridning av falska dokument i svenska medier.

Övningens fiktiva underrättelserapporter redogör för en lång rad oförklarliga och tillsynes isolerade incidenter på lokal nivå såsom haverier, demonstrationer mot regeringen, strejker, sabotage, inbrott på ambassader, mystiska olyckor samt plötsliga salmonellautbrott. Det rapporteras om en intensifierad aktivitet bland regeringskritiska organisationer (vilka KGB och GRU vid tidpunkten bedömdes utöva visst inflytande över) samt en ökad social oro bland befolkningen. Samtidigt varnar Sovjetunionen Sveriges regering för att eventuella mobiliseringsåtgärder skulle uppfattas som en “ovänlig handling”.

[69] Scenariot i övningen Malcolm redogörs för i Hjort (2002), ”Den farliga fredsrörelsen. Säkerhetstjänsternas Övervakning av Fredsorganisationer, Värnpliktsvägrare och FNL-grupper 1945-1990”, SOU 2002:90, Del 2

Scenariot sträcker sig över en 13 månader lång krisperiod; ett läge som i dag sannolikt skulle benämnas som ett *gråzonsläge*. De fiktiva rapporterna ger vid handen att det finns starka misstankar om att det är Sovjetunionen som ligger bakom den subversiva aktiviteten, men eventuella kopplingar till främmande makt kan inte ledas i bevis. Drygt ett år efter att scenariot påbörjats invaderar Sovjetunion Sverige via Finland.[70]

Mot bakgrund av de ökade spänningarna som präglade Östersjöregionen under 1960-talet[71] fördes diskussioner inom den svenska underrättelsetjänsten om hur olika angreppsformer, däribland icke-militära sådana, skulle hanteras. Vilka indikationer kunde underrättelsetjänsten tänkas få inför ett sådant angrepp, och hur skulle förvarningsfrågan hanteras i en situation som präglades av ett långsamt eskalerande förlopp med hög potential för tvära omkast? Att frågan var prioriterad framgår av promemorian ”Möjligheter att lämna indikatorer på sovjetiskt anfall” från sommaren 1962, författad av dåvarande chefen för B-byrån, Birger Elmér samt Bertil Wenblad. [72]

För att kunna skapa en gemensam situationsförståelse i ett sådant scenario underströks vikten av nära samarbete mellan den militära underrättelsetjänsten och säkerhetstjänsten. En av säkerhetsunderrättelsetjänstens viktigaste uppgift i förvarningssystemet var vid tidpunkten att lämna delunderlag för beslut om beredskapshöjande åtgärder.[73] Försvarsstabens säkerhetsavdelning utgick från antagandet att den presumtive angriparen inför ett ”väpnat eller annan form av angrepp” ofrånkomligen skulle behöva komplettera sitt underrättelseunderlag inom flera olika områden. Man räknade således med att den säkerhetshotande verksamheten inför en förestående operation skulle öka i sådan grad att det skulle kunna uppmärksammas.[74]

Men eftersom Sovjetunionen bedömdes ha kapacitet att använda ekonomiska, politiska och psykologiska betvingelsemedel som omfattade ”alla aspekter av det utvalda mållandets samhälle” behövde varningsfrågan betraktas ur ett ännu bredare perspektiv. Sverige rekommenderades därför ta ett helhetsgrepp på varningsfrågan och utreda huruvida en varningsmekanism kunde införas där en varning från en sektor innebar larm för övriga sektorer. ”Varningsfrågan”, föreslår memot från 1962, ”bör betraktas som en totalförsvarsfråga”.

I dag, drygt 50 år senare, är den strategiska kontexten en annan. Hotbilden skiljer sig på flera viktiga punkter och vårt samhälle har genomgått stora

[70] Hjort (2002) s. 312–324
[71] Bland annat som en följd av den finska ”Notkrisen” 1961.
[72] Ekman (2000), *Den militära underrättelsetjänsten: Fem kriser under det kalla kriget* (Stockholm: Carlssons förlag), s. 196, not 98
[73] Ekman (2000). s 194, not 96
[74] Ibid.

förändringar, inte minst vad gäller hur staten och näringslivet är organiserat. Likväl finns det uppenbara paralleller mellan de diskussioner som fördes om icke-militära angrepp för ett halvt sekel sedan och dagens diskussioner om ”hybridhot”.[75] Likheterna mellan *Typfall 5* som redogjordes för i kapitel tre och scenariot i övningen Malcolm från 1966 är slående.

I ljuset av dessa historiska paralleller finns det anledning att titta närmare på vilka erfarenheter av förvarning som finns bevarade i våra arkiv. Ett exempel på en sådan fråga är hur förvarningsmekanismen inkorporerades inom ramen för totalförsvarskonceptet. Värt att notera är att samverkansforumet Totalförsvarets chefsnämnd (TCN) inrättades 1962, samma år som underrättelsetjänsten eftersökte ökad samverkan med övriga totalförsvaret. TCN upplöstes 2000.[76]

5.2 Behovet av sektorsövergripande samverkan

Ett axiom som ofta upprepas är att erfarenheter från gårdagens totalförsvarsplanering inte kan direktöversättas till dagens kontext. Detta gäller naturligtvis även i frågor som rör underrättelsetjänstens förutsättningar att inhämta, analysera och delge information kopplat till antagonistiska hot. En jämförelse mellan hur staten och industrin var organiserad då och nu ger vid handen att Försvarsmakten och det offentliga i dag har helt andra förutsättningar för att på egen hand och inom ramen för den egna verksamheten upptäcka, överblicka och åtgärda olika typer av antagonistiska hot och angreppsförsök. Många av de ”sensorer” som Försvarsmakten eller andra delar av det offentliga tidigare förfogade över har i dag privatiserats och återfinns i näringslivets regi.

Det försämrade omvärldsläget har därför aktualiserat behovet av fördjupad samverkan och utökat informationsutbyte mellan underrättelse- och säkerhetstjänster å ena sidan och aktörer som inte har rikets säkerhet som sin kärnverksamhet å den andra. Det rör sig om en bredare krets samhällsaktörer, inklusive myndigheter, kommuner, mediebolag, företag och finansinstitut. Här finns det även en viktig internationell dimension som bör tas om hand.

[75] Severin (2017), “Intelligence in an age of ambiguity – How a time-tested warning method can be applied on Russia’s “new” way of war”, Masteruppsats vid King’s College London, Department of War Studies

[76] Totalförsvarets chefsnämnd (TCN) utgjorde mellan 1962 och dess nedläggning 2000 ett centralt organ inom totalförsvaret. Där fanns cheferna för alla de myndigheter som hade en nyckelroll i totalförsvaret, t.ex. Överstyrelsen för ekonomisk beredskap, Räddningsverket, Televerket, Vattenfall mm.

En nyligen genomförd intervjustudie med företag inom fyra olika branscher visar att privata näringsidkare genom sina tjänster och uppdrag förfogar över information som kan vara av vikt och intresse för totalförsvaret.[77] Ett sådant exempel är anställda inom säkerhetsföretag som registrerar avvikelser i den dagliga bevakningen av samhällsviktiga anläggningar. Ett annat exempel är företag inom e-hälsa som genom ny teknik har tillgång till realtidsdata kopplat till plötsligt uppkomna sjukdomsutbrott.

Förmågan att kunna föregripa snabba förändringar i samhället i ett krisläge aktualiserar frågor om hur näringslivet i egenskap av sensorer i samhället kan nyttjas i större utsträckning för att stödja totalförsvaret i att upptäcka och motverka antagonistiska hot och försök till destabilisering. I arbetet med att kartlägga samhällets sårbarheter finns det därför goda skäl att noga utreda vilken slags information underrättelse- och säkerhetstjänsterna kan tänkas behöva från olika sektorer samt hur denna information ska samlas in. En fungerande samordning kan främja förmågan att skapa en strategisk lägesbild, men kan även bidra till en ökad förmåga att taktiskt hantera enskilda incidenter inom ramen för fredstida krishantering.

För att kritisk information på lokal nivå ska kunna komma rätt aktör till del krävs det emellertid att företag och myndigheter själva är medvetna om att informationen är kritisk och att andra parter är i behov av den. Den allt mer komplexa hotbild som har vuxit fram aktualiserar därför behovet av att totalförsvarssystemet och näringslivet kontinuerligt försörjs med insikter och kunskap om hotutvecklingen och förändringar i terrängen. Behovet av att i förebyggande syfte utbilda och medvetandegöra en bredare krets samhällsaktörer innebär att information om hotbilder och omvärldsutveckling kan behöva tillgängliggöras och anpassas för distribution utanför underrättelsesystemet.

Denna trend, där information och bedömningar som under det kalla kriget var förbehållet en liten krets underrättelsemän och beslutsfattare nu delvis delas med aktörer över hela samhällsspektrat har beskrivits som ett paradigmskifte inom underrättelsetjänsten. David Omand, f.d. chef för den brittiska underrättelsemyndigheten GCHQ, har beskrivit det i termer av ett skifte från den hemliga staten (the Secret State) till den beskyddande staten (the Protective State).[78]

[77] Branscherna är Bevakning och säkerhet, IT och telekom, Bygg och entreprenad, Kyl- och frystransporter. Se Olsson, Ryghammar & Lundén (2017), 'Näringslivets syn på roller och ansvar i totalförsvaret', FOI-R--4551--SE, s. 27; 45–46

[78] Omand (2010), s. 9

Vem äger helhetsbilden?

I tider av ökad samverkan finns det sannolikt behov av att fastställa tydliga rutiner vad gäller ansvarsområden, roller, mandat och administration; vem ansvarar för vad, vem rapporterar vad till vem, och – inte minst – vilken myndighetsfunktion äger den tvärsektoriella helhetsbilden? För att samverkan ska fungera effektivt i kris och krig bör fungerande processer och fora vara på plats i fredstid.

Inrättande av olika typer av *fusion centers* på nationell och internationell nivå var efter 11 september ett sätt att integrera underrättelse- och säkerhetstjänsters bedömningar med varandra. Med hjälp av avidentifierad information på aggregerad nivå kan centren bidra till att skapa sektorsövergripande helhetsperspektiv, identifiera informationsluckor och öka förståelsen för orsakssammanhang. Ett annat syfte med centren är att snabbt kunna svara på uppkomna behov från beslutsfattare kopplat till frågor om terrorhot.[79] I frågan om hur förvarningsfrågan kan inkorporeras inom ramen för totalförsvarskonceptet finns det möjligen inspiration att hämta från Nationellt centrum för terrorhotbedömning (NCT).[80] Att skapa nya institutionaliserade samarbeten är dock mycket resurskrävande och måste vägas noga mot förväntad nytta.

Vikten av säkra kommunikationsvägar

En förutsättning för att underrättelse- och säkerhetstjänsten ska kunna samverka och dela information med externa aktörer är att det finns tillgång till robusta och säkra kommunikationsvägar. Driftsäkra system för delgivning av elektronisk information med hög sekretess mellan försvarsunderrättelsesystemet och krisberedskapsmyndigheter betraktas som en grundförutsättning för att de ökade samverkansbehoven ska kunna mötas. Det finns redan i dag ett uttalat behov bland berörda myndigheter om utbyggda kommunikationsvägar mellan underrättelsetjänsterna (den inre kärnan) och krisberedskapsmyndigheter (den yttre kärnan). Avsaknaden av ett effektivt system utgör i dag en begränsande faktor för effektiv informationsdelning.[81]

För verksamheter som kringgärdas av hög sekretess är frågor om tillit och förtroende viktigt.[82] Ovan nämnda intervjustudie pekar på att svenska underrättelseproducenter till viss del saknar förtroende för civila aktörer vad gäller förmågan att förstå och hantera komplex och känslig underrättelseinformation. Studien drar slutsatsen att möjligheterna till samverkan mellan

[79] Se Persson (2013), Fusion Centres – Lessons Learned. En studie av samverkansfunktioner på underrättelse- och säkerhetstjänstområdet, Försvarshögskolan, CATS

[80] I arbetsgruppen som etablerades 2009 ingår personal från Säkerhetspolisen, FRA och Must.

[81] Normark, Thunholm & Viksten (2017), 'Kartläggning av förutsättningar för delgivning av hemlig information', FOI-R--4418--SE

[82] Se t.ex. Omand (2010), s. 300–302; Persson (2013), s. 14-17

underrättelseproducerande myndigheter och andra krisberedskapsmyndigheter påverkas av både sociala och strukturella faktorer.[83]

Sårbarhetsanalyser, normalbilder och tröskelvärden

En annan förutsättning för att civila aktörer ska kunna bidra till att skingra dimman i ett gråzonsläge är att det finns en kännedom om vad som utgör normalt respektive onormalt läge. Studiet av anomalier, det vill säga signifikanta förändringar i normalläget, är en grundläggande förutsättning för tidig förvarning.

De icke-militära maktmedlens potential att orsaka avsevärd skada aktualiserar behovet av att med utgångspunkt i genomgripande sårbarhetsanalyser etablera normalbilder för ett brett spektrum av samhällets funktioner och verksamheter, även sådana som faller utanför det traditionella säkerhetsbegreppet. Med utgångspunkt i dessa normalbilder kan ”trösklar” och brytpunkter etableras (till exempel; normalt läge/försämrat läge/krisläge). På förhand etablerade tröskelvärden kan bidra till förmågan att följa och uppfatta gradvisa försämringar i flera olika sektorer, samt att skapa en överskådlighet vad gäller allvarlighetsgraden i ett potentiellt angrepp: Vilka sektorer är drabbade och vilka tecken finns på att angreppet är koordinerat?[84] Tröskelvärden kan även fylla ett pedagogiskt syfte när förändringar ska kommuniceras till beslutsfattare.

5.3 Spänning mellan inre och yttre säkerhet

Som har konstaterats tidigare kommer ett potentiellt icke-militärt angrepp mot Sverige inte att uppfattas endast om sökljuset är riktat utåt, mot den presumtive angriparen. För att förstå angreppets nyanser och omfattning behöver denna information kompletteras med bedömningar av status i den ”inre miljön”. Mot bakgrund av detta finns det anledning att anta att ett tilltagande intresse för så kallad ”gråzonsproblematik” (t.ex. främmande makts stöd till våldsbejakande oppositionsgrupper, sabotage, spionage och subversion mm) matchas med ett ökat intresse för både civila och militärt inriktade säkerhetstjänsters samlade bedömningar av läget. Här uppstår möjligen en utmaning vad gäller statens inriktning och styrning av de olika underrättelsemyndigheterna. Som Normark et al konstaterar bedriver de brottsförebyggande myndigheterna ett underrättelsearbete som primärt syftar till att tillgodose sina egna behov. Detta kan jämföras med den strategiska försvarsunderrättelseverksamheten som har ett

[83] Normark et al (2017), s. 45

[84] För ett resonemang om sårbarhetsövervakning i realtid och behovet av trösklar, se Cullen & Reichborn-Kjennerud (2016a), ‘Countering Hybrid Warfare, Analytical framework’, *Multinational Capability Development Campaign (MCDC)*, s. 20

tydligare uppdrag att löpande delge information och bedömningar till uppdragsgivare inom Regeringskansliet. Dessa ingångsvärden vad gäller rapporteringskrav påverkar respektive myndighets metodik, organisation och resursanvändning.

Regeringens krav på att myndigheter ska delta i återuppbyggandet av totalförsvaret har bidragit till en utveckling där fler aktörer efterfrågar ökad samverkan med relevanta underrättelsemyndigheter. Representanter från FRA, Must och Säkerhetspolisen vittnar om en tydlig efterfrågeökning kopplat till hemlig information.[85] Förfrågningar om såväl skriftlig som muntlig rapportering kommer i ökande takt från bevakningsansvariga myndigheter samt från delar av Regeringskansliet, men även från internationella samarbetspartners och EU. Begränsade resurser innebär dock att underrättelsemyndigheterna ständigt måste prioritera vilka informationsbehov som kan och bör tillgodoses. En möjlig konsekvens av dessa prioriteringar är att viktig information inte kommer andra myndigheter till del i tid.[86]

Detta aktualiserar frågor om inriktningen för olika underrättelsemyndigheters grunduppdrag. Kan befintliga underrättelse- och säkerhetstjänststrukturer möta ökande behov av delgivning och samverkan? Finns det anledning att göra tillägg eller ändringar i grunduppdrag och resurstilldelning så att efterfrågan på muntliga och skriftlig avrapportering kan mötas?

5.4 Varningssignaler och brus

I ett scenario där användandet av strategiska maktmedel antar allt större och allvarligare proportioner finns det anledning att anta att motståndaren med hjälp av vilseledande åtgärder kommer att söka utmatta svenska resurser, fördröja motreaktioner, försämra situationsförståelsen och påverka beslutsfattares möjlighet och förmåga att agera i en viss riktning. I en sådan situation kommer underrättelsetjänstens avnämare sannolikt att efterfråga underrättelseprodukter som kan stödja varseblivningen så att Regeringskansliet i sin tur kan bedöma vilket juridiskt, politiskt och militärt handlingsutrymme som föreligger.

Försvarsberedningen konstaterar i sin rapport att den avgörande frågan i ett sådant läge är huruvida regeringen kan identifiera att det handlar om en antagonistisk statlig aktör samt om det föreligger krigsfara. Det är denna varseblivning som ligger till grund för beslut om huruvida skärpt beredskap

[85] Normark et al (2017), s. 32
[86] Ibid. s. 44

ska tillkännages.[87] En beredskapshöjning skulle innebära en betydande påverkan på samhällets funktioner, samtidigt som det skulle ge statsmakten utökade legala möjligheter att försvara landet. Ett regeringsbeslut om skärpt eller höjd beredskap skulle dessutom ha en kraftig signaleffekt gentemot medborgarna, den presumtive angriparen och tredje part; en signal med potentiellt eskalerande potential. Beslut om höjd beredskap måste därför ”hamna rätt”.[88]

I ett sådant läge finns det en risk för att motståndaren vidtar åtgärder i syfte att stressa och vilseleda svensk lägesbildsuppfattning. Underrättelsetjänsterna översköljs dagligen av ett omfattande brus bestående av mer eller mindre diffusa varningssignaler om potentiella hot och förändringar i omvärlden.[89] I internationella krislägen tenderar denna typ av brus att öka.[90] Underrättelse-resurser riskerar således att bindas upp av en strid ström av motstridiga och ofullständiga uppgifter om skiftande företeelser som först i efterhand kan avskrivas som irrelevanta eller som uttryck för vilseledningsförsök. Detta ställer krav på underrättelsetjänsterna att se mönster där sådana finns, dvs. bedöma huruvida tillsynes isolerade incidenter utgör delar i en sammansatt kampanj som syftar till att uppnå specifika mål. Nästan lika viktigt blir att kunna avfärda misstankar om incidenterna har mer triviala eller vardagliga förklaringar.

Att avvakta i väntan på mer och bättre underrättelser kan i ett sådant spänt läge framstå som ett attraktivt alternativ för beslutsfattare. Men som Försvars-beredningen mycket riktigt konstaterar i sin senaste rapport: Gråzons-problematiken ställer stora krav på beslutsfattande och agerande.[91] Det som historiskt har kännetecknat lyckade överrasknings- och vilseledningsförsök är att den angripne, trots förvarning, inte har dragit de riktiga slutsatserna eller sett konsekvenserna av att inte agera på de observerade förberedelserna i tid och med tillräcklig kraft.[92] Att utarbeta strategier för hur påverkansförsök från främmande makt och icke-militära angreppssätt ska förebyggas och mötas på taktisk, operativ och strategisk nivå blir om möjligt än viktigare än förmågan

[87] Motståndskraft. Inriktning av totalförsvaret och utformningen av det civila försvaret 2021–2025, s. 68

[88] Tal av Björn von Sydow, FOI-dagen, september, 2017

[89] Säkerhetspolisen uppgav till exempel att myndigheten under början av 2017 hanterade 6 000 underrättelserapporter i månaden.

[90] Ett historiskt exempel är invasion av Tjeckoslovakien 1968 som föregicks av att Warszawapakten skapade ett för Natos analytiker övermäktigt informationsbrus. Se Betts (1980-1981), ’Surprise Despite Warning: Why Sudden Attacks Succeed’, Political Science Quarterly, vol. 95, no 4, s. 565

[91] Motståndskraft – Inriktning av totalförsvaret och utformningen av det civila försvaret 2021–2025, Ds 2017:66, s. 66

[92] Se Furustig, Ljunggren, Unge (2001), ’Skydd mot strategisk vilseledning. Del 1: Definitioner, metoder, diskussioner’, FOI-R--0294--SE, s. 36

att upptäcka och överblicka dem. En god lägesbild är en förutsättning för tidig förvarning. Men utan respons är varningen meningslös.

6 Slutsatser

Kombinationen av kraftfull teknik och nya samhälleliga sårbarheter innebär att kalla krigets *politiska krigföring* som utkämpades under tröskeln för väpnat angrepp har fått nya dimensioner. Icke-linjära angreppssätt som skräddarsys för att matcha mållandets samhälleliga sårbarheter har i dag potentialen att orsaka betydande skada på såväl kort som lång sikt. Genom att slå ut eller utsätta viktiga samhällsfunktioner för hårt tryck, alternativt signalera att man förfogar över *möjligheten* att göra det, kan en angripare söka påverka andra länders utrikes- och säkerhetspolitik till en förhållandevis låg politisk och ekonomisk kostnad. De icke-militära hotens diffusa karaktär innebär att de kan vara svåra att upptäcka, karaktärisera och överskåda. Det försämrade säkerhetsläget i Sveriges närområde ställer underrättelsetjänsten och beslutsfattare inför nygamla utmaningar.

Rapporten har visat att det finns paralleller mellan dagens diskussion om hybridkrigföring och oron för det ”icke-militära angreppet” på 1960-talet. Flera av de åtgärder som diskuterades inom den svenska underrättelsetjänsten under kalla kriget har viss relevans än i dag. Omvärldsutvecklingen har åter aktualiserat behovet av ett tätt samarbete mellan underrättelsetjänst och säkerhetstjänst samt mellan underrättelsetjänster och civila aktörer (t.ex. myndigheter, finansinstitut och mediehus). Att involvera aktörer utanför säkerhetssektorns kärna kan bidra dels till förmågan att på ett tidigt stadium upptäcka och förstå försåtliga mönster i samhället, dels till att skapa den strategiska helhetsbild som nationella beslutsfattare har att förhålla sig till. Hotens karaktär aktualiserar även frågor om vilken myndighetsfunktion som är bäst lämpad att omhänderta den tvärsektoriella helhetsbilden, samt på vilket sätt varningsfrågan kan inkorporeras i totalförsvarskonceptet.

Den traditionella idén om tidig förvarning bygger på föreställningen om en gradvis eskalerande kris som stegras successivt och som kan mötas av gradvisa beredskapshöjande åtgärder. Indikatorbaserade förvarningsmetoder är i sin tur uppbyggda kring idén om en på förhand definierad hotprocess med tydliga orsakssamband där varningslampor tänds allteftersom krisen eskalerar. Den specifika typ av hot som har diskuterats i denna rapport karaktäriseras av stor osäkerhet och otydlighet och utmanar således både den traditionella förståelsen för krisförlopp liksom traditionella metoder för tidig förvarning.

Som illustrerades av övningsscenariot från 1966 finns det en tradition att tolka en ökning av subversiv aktivitet som ett preludium, en slags upptakt, till det väpnade angreppet. Men givet de icke-militära maktmedlens potential att orsaka avsevärd skada finns det kanske anledning att ompröva detta antagande.

Som rysslandsforskaren Mark Galeotti nyligen har påpekat; subversion, propaganda och påtryckningsförsök från Ryssland bör inte förstås i termer av ett preludium till krig. Det bör snarare förstås som kriget självt.[93]

Denna översiktliga litteraturstudie har identifierat generella utmaningar som så kallad hybrid- och gråzonsproblematik kan medföra för svensk underrättelse- och säkerhetstjänst. Det kan konstateras att den samtida underrättelselitteraturen kopplat till denna specifika typ av frågeställning är relativt begränsad. Detta är något förvånande givet det stora intresse som hybridkrigföring och gråzonsproblematik som fenomen har tilldragit sig på senare år. Det finns således behov av mer och fördjupad metodutveckling och forskning på området. Det pågår i dag nationella, bilaterala och multilaterala projekt som syftar till att förbättra och modifiera länders och organisationers förmågor att uppfatta och varna för angrepp av icke-militär karaktär. Att samla preliminära resultat och utreda hur andra länder och organisationer närmar sig frågor om sensorer, indikatorer och förvarning kan bidra till viktiga erfarenheter i det fortsatta arbetet med att förbättra Sveriges möjligheter att förebygga och möta icke-militära påverkan- och angreppsförsök från främmande makt.

[93] Galeotti (2018), 'I'm Sorry for Creating the 'Gerasimov Doctrine'', *Foreign Policy,* 5 mars

7 Litteraturförteckning

Agrell, Wilhelm (2008), *Förvarning och Samhällshot,* (Studentlitteratur: Lund)

Agrell, Wilhelm (2012), *Underrättelseanalysens metoder och problem* (Gleerups: Malmö)

Altman, Daniel (2015), *Red Lines and Faits Accomplis in Interstate Coercion and Crisis*, avhandling från Cambridge, MA: Massachusetts Institute of Technology

Andersson, Maria & Lars Westerdahl (2017), ’Sveriges elförsörjning - Hur möter vi en ökad sårbarhet?’ FOI Memo 6173

Asp, Viktoria, Emmelie Andersson, Linnéa Arnevall & Rickard Blomstrand (2017), ’Förutsättningar för krisberedskap och totalförsvar i Sverige’, Försvarshögskolan, Crismart

Bērziņš, Jānis (2014), ‘Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy’, National Defence Academy of Latvia Center for Security and Strategic Research

Betts, Richard K. (2009), ’Surprise Despite Warning: Why Sudden Attacks Succeed’, i Christopher Andrew, Richard Aldrich & Wesley K. Warks (red), *Secret Intelligence: A Reader* (New York: Routledge)

Blank, Steven (2017), ‘Cyber War and Information War á la Russe’, i George Perkovich & Ariel Levite (red), *Understanding Cyber Conflict: Fourteen Analogies*, Georgetown University Press

Bringéus, Krister (2016), 'Säkerhet i en ny tid: Betänkande av utredningen om Sveriges försvars- och säkerhetspolitiska samarbeten', SOU 2016:57

Brodin, Katarina (1978), ‘Surprise Attack: The Case of Sweden’, *Journal of Strategic Studies,* Vol. 1, No.1, pp. 98-110

Connable, Ben, Jason H. Campbell & Dan Madden (2016), *Stretching and Exploiting Thresholds for High-Order War. How Russia, China, and Iran Are Eroding American Influence Using Time-Tested Measures Short of War*, (Rand Corporations: Santa Monica)

Cullen, Patrick J. & Erik Reichborn-Kjennerud (2016a), ‘Countering Hybrid Warfare, Analytical Framework’, *Multinational Capability Development Campaign (MCDC)*

Cullen, Patrick J. & Erik Reichborn-Kjennerud (2016b), ‘Countering Hybrid Warfare, Baseline Assessment’, *Multinational Capability Development Campaign (MCDC)*

Dalsjö, Robert & Thomas Hultmark (2017), 'Hur uppnå verkan i krislägen och gråzon', *Kungl. Krigsvetenskapsakademiens Handlingar och Tidskrift,* Vol. 2

Degennaro, Patricia (2016), ’The Gray Zone and Intelligence Preparations of the Battle Space, Small Wars Journal, http://smallwarsjournal.com/print/50009

Ducaru, Sorin Dumitru (2016), ‘Framing NATO’s Approach to Hybrid Warfare’, i Niculae, Iancu et al (red), *Countering Hybrid Threats: Lessons Learned from Ukraine* (IOS Press)

Ekman, Stig (2000), *Den militära underrättelsetjänsten: Fem kriser under det kalla kriget* (Stockholm: Carlssons förlag)

Elkus, Adam (2015), ’50 Shades of Gray. Why the Gray Wars Concept Lacks Strategic Sense’, *War on the Rocks,* 15 december

European Commission (2016), ‘Joint Framework on countering hybrid threats a European Union response’, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018

European Commission (2017), Press Release: Security and defence: Significant progress to enhance Europe's resilience against hybrid threats – more work ahead, 19 juli, http://europa.eu/rapid/press-release_IP-17-2064_en.htm

Furustig, Hans, Boris Ljunggren & Wilhelm Unge (2001), ’Skydd mot strategisk vilseledning. Del 1: Definitioner, metoder, diskussioner’, FOI-R--0294--SE

Fägersten, Björn (2017), ’Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence’, i Daniel Hamilton (red), *Forward Resilience: Protecting Society in an Interconnected World Working Paper Series,* SAIS and Center for Transatlantic Relations

Försvaret av Sverige – Starkare försvar för en osäker tid, SOU 2014:20

Försvarsmakten (2014), Operativ doktrin (OPD-14)

Försvarsmakten (2016), Militärstrategisk doktrin (MSD-16)

Försvarsmaktens delredovisning av perspektivstudien 2016-2018, HKV 2016-12-01 (FM2015-13192:9)

Försvarsmaktsidé och målbild Årsrapport från Perspektivplanering 2000-01, https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/perspektivplan/rapport5.pdf

Galeotti, Mark (2016), *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear Military Challenge Right*, (Mayak Intelligence)

Galeotti, Mark (2018), 'I'm Sorry for Creating the 'Gerasimov Doctrine'', *Foreign Policy,* 5 mars

Giles, Keir (2016), 'Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power', Chatham House Research Paper

Grabo, Cynthia (2004), *Anticipating Surprise: Analysis for Strategic Warning* (Washington, DC: Joint Military Intelligence College)

Haddick, Robert (2014), 'America has No Answer to China's Salami-Slicing', War on the Rocks, 6 februari, https://warontherocks.com/2014/02/america-has-no-answer-to-chinas-salami-slicing/

Hedenskog, Jakob, Gudrun Persson & Carolina Vendil Pallin (2016), 'Russian Security Policy', i Persson (red), *Russian Military Capabilities in a Ten-Year Perspective,* FOI-R--4326--SE

Hjort, Magnus (2002), "Den farliga fredsrörelsen. Säkerhetstjänsternas Övervakning av Fredsorganisationer, Värnpliktsvägrare och FNL-grupper 1945-1990", SOU 2002:90, Del 2

Hoffman, Frank G. (2006) 'Lessons from Lebanon: Hezbollah and Hybrid Wars', Foreign Policy Research Institute

Hoffman, Frank G. (2007), *Conflict in the 21st Century: The Rise of Hybrid wars* (Potomac Institute for Policy Studies)

Hollis, David (2011), 'Cyberwar Case Study: Georgia 2008', *Small Wars Journal*, http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Hulnick, Arthur S. (2005), 'Indications and Warning for Homeland Security: Seeking a New Paradigm', *International Journal of Intelligence and Counter Intelligence*, Vol. 18, No 4

Joint Strategy Review (2015), 'Not at Peace and Not at War: An Exploration of "Gray Conflicts', USSOCOM White Paper

Jonsson, Daniel K. (2017), 'Att använda scenarier i planeringen för civilt försvar', FOI-R--4434--SE

Jonsson, Daniel K. (2018), ’Typfall 5: Utdragen och eskalerande gråzonsproblematik. Komplettering av hotbildsunderlag i utvecklingen av civilt försvar’, FOI Memo 6339

Kam, Ephraim (1988), *Surprise Attack: the Victim’s Perspective* (Cambridge, Mass and London: Harvard University Press)

Kennan, George F. (1991), 'Measures Short of War: The George F. Kennan Lectures at the National War College’, 1946-1947, (Washington, DC: National Defense University Press)

Kofman, Michael (2016) ‘Russian Hybrid Warfare and Other Dark Arts’, War on the Rocks, 11 mars, https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/

Kovacs, Amos (1997), ‘The Nonuse of Intelligence’, *International Journal of Intelligence and Counterintelligence,* Vol. 10, No. 4

Käihkö, Ilmai (2016), ‘All krigföring är av hybrid natur’, *Statsvetenskaplig tidskrift.* No 4

Larsson, Robert L. (red) (2008), ‘Det kaukasiska lackmustestet: Konsekvenser och lärdomar av det rysk-georgiska kriget i augusti 2008’, FOI-R--2563--SE

Lönnaeus, Olle (2016), ‘ÖB: Ryska cyberattacker mot Sverige varje dag’, Sydsvenskan 10 februari

Maigre, Merle (2015), ‘Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO’, German Marshall Fund of the United States

Mattis, James & Frank G. Hoffman (2005), ’Future Warfare: The Rise of Hybrid Wars’, *Proceedings Magazine,* Vol. 131/11

Mazarr, Michael J. (2015), *Mastering the Gray Zone: Understanding a Changing era of Conflict, Strategic Studies Institute*, (U.S. Army War College)

McDermott, Roger (2016), ‘Gerasimov Calls for New Strategy to Counter Color Revolution, *Eurasia Daily Monitor,* Vol. 13 Is. 46

Motståndskraft – Inriktning av totalförsvaret och utformningen av det civila försvaret 2021-2025, Ds 2017:66

Mumford, Andrew & Jack McDonald (2014), ’Ambigous Warfare’, Rapport producerad för Development, Concepts and Doctrine Centre (DCDC)

Nemeth, William J. (2002), *Future War and Chechnya : a Case for Hybrid Warfare*, (Monterrey CA, the Naval Postgraduate School)

Nilsson, Niklas (2018), 'Russian Hybrid Tactics in Georgia', Institute for Security and Development, The Silk Road Studies Program

Norberg, Johan, Fredrik Westerlund & Ulrik Franke (2014), 'The Crimea Operation: Implications for Future Russian Military Interventions', i Niklas Granholm, Johannes Malminen, & Gudrun Persson (red.), *A Rude Awakening: Ramifications of Russian Aggression towards Ukraine,* FOI-R--3892--SE, Stockholm, 2014

Normark, Magnus, Per Thunholm & Runar Viksten (2017), 'Kartläggning av förutsättningar för delgivning av hemlig information', FOI-R--4418--SE

Olsson, Matilda, Charlotte Ryghammar & Jenny Lundén (2017), 'Näringslivets syn på roller och ansvar i totalförsvaret', FOI-R--4551--SE

Omand, David (2010) *Securing the State* (London: C. Hurst & Co)

Pernik, Piret & Tomas Jermalavicius (2017), 'Resilience as Part of NATO's Strategy: Deterrence by Denial and Cyber Defense', i Daniel Hamilton (red), *Forward Resilience: Protecting Society in an Interconnected World,* Working Paper Series, SAIS and Center for Transatlantic Relations

Persson, Gudrun (2013), 'Fusion Centers – Lessons Learned. En studie av samverkansfunktioner på underrättelse- och säkerhetstjänstområdet', Försvarshögskolan, CATS

Persson, Gudrun (red) (2016) *Russian Military Capabilities in a Ten-Year Perspective,* FOI

Racz, Andras (2014) 'Russia's Hybrid Warfare in Ukraine', *The Finnish Institute of International Affairs,* Report 43

Regeringens proposition 2014/15:109, Försvarspolitisk inriktning – Sveriges försvar 2016–2020

Reichborn-Kjennerud, Erik & Patrick Cullen (2016), 'What is Hybrid Warfare?', Norwegian Institute of International Affairs, NUPI Policy Brief

Schelling, Thomas (1966), *Arms and Influence* (New Haven, CT: Yale University Press)

Severin, Malin (2017), "Intelligence in an age of ambiguity – How a time-tested warning method can be applied on Russia's "new" way of war", Masteruppsats vid King's College London, Department of War Studies

Silver, Nate (2012), *The Signal and the Noise: Why Most Prediction Fail – But Some Don't* (London: Penguin Books)

Smith. M.L.R. (2003), 'Guerrillas in the Mist: Reassessing Strategy and Low Intensity Warfare', *Review of International Studies,* Vol 29, No 1

Treverton, Gregory F. (2011), 'Comparing Early Warning Across Domains' Försvarshögskolan

United States Army Functional Concept for Intelligence 2020-2040 (2017)

United States Army Special Operations Command (2016), 'White Paper - Perceiving Gray Zone Indications'

Wirtz, James (2017), 'Life in the Gray Zone: Observations for Contemporary Strategists', *Defense & Security Analysis,* Vol. 33, No. 2

Wohlstetter, Roberta (1962), *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press)

Votel, Joseph L. (2015). 'Statement of General Joseph L. Votel, US Army Commander US Special Operations Command, Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilties. House Armed Services Committee Subcommittee on Emerging Threats and Capabilities'

FOI

ISSN1650-1942

www.foi.se