Gråzonsproblematik och hybridkrigföring – påverkan på energiförsörjning

Daniel K Jonsson

FOI-R--4590--SE

Maj 2018

FOI

Daniel K Jonsson

Gråzonsproblematik och hybridkrigföring – påverkan på energiförsörjning

Bild/Cover: Daniel K Jonsson

Titel	Gråzonsproblematik och hybridkrigföring – påverkan på energiförsörjning
Title	Gray zone problems and hybrid warfare – impact on energy supply
Rapportnr	FOI-R--4590--SE
Månad/	Maj
Utgivningsår	2018
Antal sidor	82
ISSN	1650-1942
Kund	Energimyndigheten
Forskningsområde	5. Krisberedskap och samhällssäkerhet
FoT-område	Ej FoT
Projektnr	E13612
Godkänd av	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Gråzon brukar förstås som ett tillstånd mellan fred och krig. Gråzonsproblematik orsakas av ett antal kombinerade antagonistiska aktiviteter som angriparen avser inte ska att uppfattas som krigföring. Aktiviteterna kan exempelvis utgöras av politisk påverkan, manipulering av marknader, desinformation, informationspåverkan, stöd till ytterlighetsrörelser, maktdemonstrationer, illegal underrättelseinhämtning, hot och påtryckningar mot beslutsfattare, cyberangrepp och fysiska sabotage.

Att basera antagonistiska aktiviteter på gråzonsstrategi är inget nytt fenomen men dess aktualitet kan anses ha ökat, inte minst eftersom en sådan strategi underlättas av den informationsteknologiska utvecklingen men också för att icke-militära medel har getts ökad betydelse i ryskt strategiskt tänkande. Ett syfte med att använda gråzonsstrategi i en konfliktsituation, istället för militärt våld, är att vinna fördelar och uppnå politiska mål utan att mötas av eskalering och starka motåtgärder. Syftet kan också vara att testa, öva eller demonstrera vissa förmågor, eller att aktiviteterna utgör krigsförberedande åtgärder.

Det finns många alternativa tolkningar av vad gråzon innebär. Ett besläktat begrepp är hybridkrigföring. Om gråzonsbegreppet ska vara användbart i ett totalförsvarssammanhang krävs tydliga avgränsningar, exempelvis endast de aktiviteter som den kvalificerade statlige antagonisten genomför, eller ligger bakom via ombud, och som medför en sammantagen påtaglig samhällspåverkan.

Gråzonen innebär en rad utmaningar för krisberedskapen och totalförsvaret. Det civila försvarets särskilda regelverk aktiveras först vid höjd beredskap. Krisberedskapens aktörer, tillika det civila försvarets, måste därmed planera för att kunna hantera gråzon både med fredstida regelverk och regelverk för höjd beredskap.

Att möta gråzonshot handlar i första hand om att utveckla icke-militära motmedel. Ett sådant motmedel är att stärka förmågan att upprätthålla samhällets funktionalitet, vilket inte minst gäller energiförsörjningen. Robustare försörjningssystem ger ökad motståndskraft och höjer tröskeln för angrepp av

såväl militär- som gråzonskaraktär. Detta kräver ökad förståelse om samhällsfunktioners sårbarheter genom fördjupad sektorskunskap. Vidare krävs både samordning inom sektorer och sektorsövergripande samverkan för etablera en fungerande krishantering och för att kunna lösa det civila försvarets uppgifter. För att denna samverkan ska kunna få effekt måste den ske mellan aktörer med beslutsmandat, vilket i sin tur kräver i att sektorsansvaret tydliggörs.

Energi kan fungera som antingen ett mål eller ett medel i en konfliktsituation, exempelvis som mål för sabotage och cyberangrepp för att störa energiförsörjningen i sig eller som ett medel för politisk påverkan och utpressning. De internationella energimarknadernas karaktär, liksom de övergripande marknadsprinciperna, medför viss robusthet men också vissa sårbarheter. Sårbarheterna handlar bl.a. om ägandeförhållanden som kan ge en fientlig stat inflytande över infrastruktur och produktionsresurser samt att underleverantörsberoendet inom energisektorn kan medföra vissa säkerhetsrisker, exempelvis att känslig information sprids eller att verksamheter infiltreras. Det är dock svårt att avgöra om ett visst agerande på energimarknaden handlar om vanlig marknadskonkurrens eller om det finns ett underliggande syfte som en fientlig stat står bakom.

Digitaliseringen i energisektorn kan medföra vissa sårbarheter men även om cyberangrepp respektive fysiska sabotage är gråzonshot av olika karaktär får de liknande effekter i termer av störningar och avbrott om de realiseras. Exempel på konkreta hot är intrång i informations-, drift- och styrsystem, samt infiltration, insiders, kartläggning av nyckelpersonal, förberedelse för sabotage och annan underrättelseinhämtning.

Utformandet av strategier och åtgärder inom energiområdet som syftar till att hantera gråzonsproblematik bör ske integrerat med motsvarande planering för såväl fredstida krisberedskap som totalförsvar i höjd beredskap och krig. Det handlar således om att sträva efter en robustare energiförsörjning för hela hotskalan.

Nyckelord: gråzon, hybridkrigföring, krisberedskap, civilt försvar, totalförsvar, energiförsörjning, energisäkerhet

Summary

The gray zone is usually understood as a state between peace and war. Gray zone problems are caused by a number of combined antagonistic activities. The intention of the attacker is that the activities should not be perceived as warfare. A gray zone strategy could include activities such as influencing policy, market manipulation, disinformation, supporting political extremists, power demonstrations, illegal intelligence gathering, threats and pressure on decision makers, cyberattacks and physical sabotages.

Basing antagonistic activities on gray zone strategy is not a new phenomenon, but the actuality of this has increased, not the least since such a strategy is facilitated by the information technological development, but also since the role of non-military means has been given more importance in Russian strategic thinking. One purpose of exercising a gray zone strategy in a conflict situation instead of military violence, would be to gain benefits and to achieve political goals without meeting escalation and powerful countermeasures. The purpose could also be to test, practice or demonstrate certain abilities, or finally that the activities are in fact war preparations.

There are a number of alternative interpretations of the gray zone. A related concept is hybrid warfare. The gray zone concept needs to be clearly defined and delimited, in order to be useful in a total defence context, e.g. only the activities stage-managed by the qualified antagonistic state, resulting in obvious cumulative impact on society.

The gray zone creates a number of challenges for the crisis preparedness and the total defence. The special regulations for the civil defence are not activated until a state of heightened alert is declared. The crisis preparedness actors, also the civil defence actors, thus have to plan for handling the gray zone in the context of peacetime as well as wartime regulations.

The way gray zone threats can be met is primarily through non-military countermeasures. Some of these countermeasures aim at increasing the ability to maintain the functionality of society, not the least the energy supply. Robust supply systems increase the resilience of society and raise the threshold for aggressions of military as well as gray zone character. An increased understanding of the vulnerability of societal functions is needed in order to be able to increase robustness, which in turn requires increased knowledge on specific sectors. Moreover, both coordination within sectors and cooperation between sectors are required in order to establish a functioning crisis management and to be able to solve the civil defence tasks. In order to get desirable output from cooperation, cooperation must take place between actors with decision mandates, which in turn requires that sector responsibilities are clarified.

Energy can be a target or a mean in a conflict situation, e.g. a target for sabotage or cyberattack in order to disturb energy supply, or a mean for political pressure. International energy markets, as well as the overall market principles, have characteristics that support robustness but also entail some vulnerabilities. The vulnerabilities include e.g. ownership relations which could give a hostile state influence over infrastructure and production resources. Furthermore the subcontractor dependency in the energy sector could entail certain security risks, e.g. that confidential information is spread or that companies are be infiltrated. However, it is difficult to determine whether a certain action on the energy market is about ordinary market competition, or if there is an underlying purpose staged by a hostile state.

The digitalization in the energy sector could bring some vulnerabilities, but in spite of the fact that cyberattacks and physical sabotages are gray zone threats of different characters, the effects are similar in terms of disturbances and disruptions. Examples of other threats are intrusions in information, operation and control systems, and infiltration, insiders, surveying key personnel, sabotage preparations and other forms of intelligence gathering.

The design of strategies and measures to handle gray zone problems within the energy field should be integrated with peacetime contingency planning as well as with planning for total defence during hightened alert and war. Conclusively, the aim should be to strive for a more robust energy supply along the whole scale of threats.

Key words: grey zone, hybrid warfare, crisis prepardeness, contingency planning, civil defence, total defence, energy supply, energy security

Förord

Föreliggande rapport utgör ett kunskapsunderlag för planering och vidareutveckling av civilt försvar på energiområdet. Arbetet har finansierats av Energimyndigheten.

Inom ramen för det energipolitiska målet ”trygg energiförsörjning” arbetar Energimyndigheten med att skapa förutsättningar för, och att utveckla, ett robustare energisystem för hela hotskalan.[1] I den hotskalan ingår även så kallade ”gråzonshot”. Syftet med denna rapport är att öka kunskapen om gråzonshot mot energiförsörjningen och att höja medvetenheten kring dessa. Samtidigt är många av de resonemang som förs, liksom slutsatser som dras, i rapporten även tillämpbara på andra försörjningssystem, sektorer och samhällsfunktioner. Det är därför såväl FOI:s som Energimyndighetens förhoppning att föreliggande arbete kan komma till en bredare nytta, i utvecklingen av krisberedskapen och ett sammanhängande civilt försvar.

Energimyndigheten, Svenska kraftnät och andra energibranschaktörer har bidragit med oundgänglig underlagsinformation inför arbetet, samt bidragit med konstruktiva synpunkter på rapportutkast, liksom dialog om sekretesshantering och -bedömning (tillsammans med andra berörda myndigheter). Värdefulla synpunkter på rapporten har också getts av ett antal FOI-kollegor från enheten för Samhällets säkerhet, samt från FOI:s Rysslandsprojekt, RUFS. Författaren ansvarar dock för rapportens slutliga innehåll.

[1] Energimyndigheten 2018

Innehållsförteckning

1 Inledning

Gråzonen har blivit ett frekvent tema i hotbildsdiskussioner och totalförsvarssammanhang.[2] Gråzonen kan förenklat förstås som ett tillstånd mellan krig och fred eller en konfliktsituation som inbegriper användningen av olika maktmedel som i första hand inriktas mot det civila samhällets funktionalitet, vilket ibland också benämns som hybridkrigföring. Gråzonsproblematik och hybridkrigföring har fått ny aktualitet men är egentligen inga nya fenomen och det finns flera skäl till att vara skeptisk till användandet av begreppen.

För att kunna hantera angrepp av gråzonskaraktär, liksom att effekterna av angreppen inte ska få alltför stor effekt, behöver samhällsfunktionerna vara motståndskraftiga.[3] Särskilt i en situation som riskerar att eskalera och övergå i väpnad konflikt kan en robust energiförsörjning, liksom att övriga samhällsfunktioner är svåra att störa ut, spela en tröskelhöjande roll. Om det inte är möjligt att förlama samhället, och därmed också försvåra Försvarsmaktens och dess utländska samarbetspartners försvarsåtgärder, kan detta få en konfliktavhållande effekt.

Rapporten består av tre huvuddelar. Kapitel 2 reder ut begreppen gråzon och hybrid, främst i en internationell kontext. Gråzonsstrategiers olika karaktärsdrag, liksom tänkbara taktiker och metoder, lyfts sedan fram. Vidare diskuteras tolkningar av ryska förhållningssätt till (det som vissa analytiker i väst benämner som) gråzon och hybridkrigföring. Att särskilt fokus läggs på Ryssland motiveras av att arbetet har bedrivits inom ramen för utvecklingen av det svenska totalförsvaret, som regeringen har ålagt myndigheterna, för att möta det försämrade omvärldsläget som Ryssland anses vara huvudanledningen till.[4]

Kapitel 2 avslutas med en diskussion om gråzons- och hybridbegreppens relevans.

Kapitel 3 diskuterar gråzonsutmaningar utifrån en svensk kontext. Det handlar dels om generella utmaningar för samhällets säkerhet och krisberedskapen, dels om det civila försvarets utmaningar för att värna civilbefolkningen, att säkerställa de viktigaste samhällsfunktionerna och att stödja Försvarsmakten.

I kapitel 4 diskuteras energisektorns utmaningar avseende gråzonshot och hybridaktiviteter, dels baserat på tillgänglig internationell litteratur, dels baserat på ett scenariounderlag (Typfall 5) för planering för civilt försvar. Den avslutande delen i kapitel 4 (avsnitt 4.3) utgör en diskussion om gråzonsproblematik baserat på information från svenska energibranschaktörer

[2] Se t.ex. Försvarsberedningen 2017; Försvarsmakten 2017; Försvarsmakten 2018
[3] Försvarsberedningen 2017
[4] Se t.ex. Prop. 2014/15:109

och myndigheter. Energisystemens olika sårbarheter diskuteras, exempelvis de som digitaliseringen kan medföra. Marknadspåverkan, inflytande över strategisk infrastruktur, cyberhot, underrättelseinhämtning och infiltration är också hot som lyfts fram. De synpunkter som förekommer i avsnitt 4.3 behöver dock inte överensstämma med enskilda aktörers utan är författarens tolkningar och slutsatser.

Rapporten avslutas i kapitel 5 med slutsatser och rekommendationer dels för krisberedskapen och det civila försvaret i allmänhet, dels för energiberedskapen.

2 Gråzon och hybridkrigföring

Kapitel 2 fokuserar på begreppet gråzon och dess släktskap med hybridkrigföring och är av litteraturstudiekaraktär. Inledningsvis diskuteras begreppet gråzon (avsnitt 2.1) och gråzonsstrategier (2.2) innan besläktade koncept såsom hybridkrigföring mm. (2.3) lyfts fram. Sedan ges en mer konkretiserad hotbild avseende vilka aktiviteter som kan ingå, samt vilka taktiker som kan tillämpas, i en gråzonskonflikt (2.4). Därefter diskuteras tolkningar av ryska förhållningssätt (2.5) till gråzon och hybridkrigföring. Kapitlet avslutas med en kritisk betraktelse över användandet av gråzons- och hybridbegreppen (2.6).

2.1 Begreppet gråzon

”Gråzonen” har de senaste åren uppmärksammats i samhällsdebatten, i myndigheters kris- och krigsplanering, i hotbildsdiskussioner och i mer allmän säkerhetspolitisk forskning. I synnerhet har konceptet gråzonskonflikt (”gray zone conflict”) fått en ökande betydelse inom militär policy- och strategiutveckling, där den framtida hotmiljön beskrivs som ett ”kontinuum” eller spektrum av många olika typer av konflikter där traditionella militära medel undviks.[5] Ett flertal studier har i detta sammanhang utgått från begreppet hybridkrigföring (”hybrid warfare”) i stället för gråzon.[6] Hybridkrigföring och andra besläktade begrepp diskuteras vidare i avsnitt 2.3.

I definitioner brukar det ingå att gråzonskrigföringen har multidimensionell effekt,[7] dvs. att den med olika medel påverkar olika delar av samhället, och att det som sker är frukten av medvetna sammansatta handlingar.[8] Gråzonsproblematik kan ses som effekten av ett antal kombinerade antagonistiska aktiviteter som angriparen avser inte ska att uppfattas som krigföring. Aktiviteterna kan exempelvis utgöras av politisk, ekonomisk och psykologisk påverkan, desinformation, informationspåverkan, subversiv verksamhet, illegal underrättelseinhämtning, hot och påtryckningar mot beslutsfattare och cyberangrepp. Ofta betonas också medverkan av icke-statliga aktörer, en osäkerhet avseende vilka aktörer som är inblandade och vem som egentligen orkestrerar aktiviteterna. Gråzonens utmaningar anses dessutom vara beroende av hur hoten uppfattas.[9]

[5] Se t.ex. Banasik 2016; Echevarria 2016; Mazarr 2015; Wilson och Smitson 2016; Hermberg 2016; Jackson 2017; Wirtz 2017
[6] Se t.ex. Lanoszka 2016; Cederberg m.fl. 2017; Allen m.fl. 2017; Reisinger och Golts 2014
[7] T.ex. Hoffman 2016
[8] T.ex. Banasik 2016
[9] T.ex. Kapusta 2015

Gråzonsproblematik i sig är inget nytt fenomen eftersom stater har använt olika typer av gråzonstaktiker i någon mening sedan långt tillbaka.[10] De statliga aktörer som kan tänkas iscensätta gråzonsproblematik idag benämns ofta i den västliga litteraturen som ”revisionister”, eller ibland som ”revanschistiska stater”.[11] Det vill säga stater som vill förändra rådande säkerhetsordning och maktförhållanden och är villiga att agera mer expansivt än att bara sträva mot försvarsinriktad säkerhetsmaximering.[12] Denna typ av revisionister strävar efter att förändra fördelningen av tillgångar, inklusive territorium.[13] Revisionisterna anser att de antingen tidigare har blivit förfördelade eller att befintliga internationella normer och institutionella strukturer är orättvisa och att rådande förhållanden motverkar deras strävan att uppfylla sina egna rättmätiga mål.[14] I nordamerikansk säkerhetspolitisk diskurs brukar nutida exempel på tämligen offensiva revisionister exemplifieras som Iran, Nordkorea, Kina och Ryssland.[15] Därutöver kan även en rad andra stater i olika sammanhang betraktas som återhållsamma och moderata revisionister, exempelvis utvecklingsländer som vill kompensera för historiska eller nuvarande internationella förhållanden som upplevs som orättvisa.[16] Alla ”revisionister” är givetvis inte benägna att ta till aggressioner för att uppnå sina mål och att revisionister föredrar gråzonsstrategi framför andra tillgängliga medel finns det (mig veterligen) ingen forskning som kan belägga. Det är snarare så att det befintliga revisionistbegreppet har använts för att komplettera (och eventuellt bekräfta) utvecklingen av teori kring gråzon och hybridkrigföring. På motsvarande vis ses gråzon och hybrid i vissa sammanhang som en ny generation i krigföringens evolution (mer om detta i avsnitt 2.3).

Det bör också tilläggas att kopplingen mellan så kallade revisionister och gråzonsstrategi, som det beskrivs ovan, görs utifrån ett västligt perspektiv på internationell säkerhet. Man kan på goda grunder hävda att även västliga demokratier ägnar sig åt aktiviteter som andra stater kan uppfatta som gråzonsstrategi, exempelvis underrättelseinhämtning, informationspåverkan, ekonomisk maktutövning samt påverkan och informationsspridning. Exempelvis

[10] Michael Mazarr, som är en frontfigur i utvecklingen av den moderna hotbildsförståelsen, skriver (2015, p. 3): ”Concepts such as political destabilization, support for proxies and militias, information campaigns, and much more have been a staple of statecraft since the city states of Ancient Greece were vying for influence”.
[11] Se t.ex. Mazarr 2015; Severin 2018
[12] Zionts 2006
[13] Davidson 2002
[14] Mazarr 2015
[15] Se t.ex. Mazarr 2015; Wirtz 2017; Wilson och Smitson 2017; Jackson 2017
[16] Mazarr 2015

anser Ryssland att man från väst utsätts för ett slags hybridkrigföring med syfte att destabilisera det ryska samhället (se vidare avsnitt 2.5).[17]

Att använda gråzonsstrategi handlar grovt sett om att försöka uppnå politiska eller andra mål via tillgängliga maktmedel utan att eskalera en situation till krig eller annan kraftfull motreaktion.[18] Försvarsmakten uttrycker det som att ”…motståndaren strävar efter att kringgå grunderna för [den svenska] statens verktyg för institutionellt våld”.[19]

Samtidigt kan gråzonsaktiviteter vara just krigsförberedande. Gråzonsförloppet kan vara eskalerande och leda mot ett så kallat skymningsläge, dvs. en konfliktsituation där nästa steg kan förväntas vara användandet av militära medel (som antagonisten har tagit initiativet till och därmed har ett försteg). En gråzonssituation kan också förknippas med mer konstant intensitet (till skillnad från eskalerande) under en pågående konfliktsituation under en kortare eller längre tidsperiod. Slutligen skulle gråzonen kunna ses som ett tillstånd som betraktas som det nya normala, dvs. ”fred” = gråzon.[20]

2.2 Antagonistens gråzonsstrategier

Det finns många tänkbara syften för en stat att använda gråzonsstrategi gentemot en annan stat. Några exempel är:

- Att hantera inhemska problem och uppnå intern legitimitet genom extern expansion
- Att uppnå ekonomisk vinning och konkurrensfördelar
- Att störa, eller skapa inflytande över, andra länders funktionalitet och beslutsfattande
- Att undanröja uppfattade hot
- Att försvaga potentiella militära motståndare och därigenom skapa handlingsutrymme inför ett eventuellt militärt ingripande.

Även om syftet med gråzonsaktiviteter skulle vara krigsförberedande karakteriseras själva gråzonen av ett antagonistiskt agerande som syftar till att uppfattas, av den som utsätts liksom övriga omvärlden, som inom ramen för ”vanlig” internationell konkurrens och definitivt ligga under nivån för en väpnad konflikt. Detta brukar kallas för ”short-of-war strategies”[21], vilket nedan

[17] Se t.ex. Persson 2017
[18] Mazarr 2015
[19] Försvarsmakten 2018, s. 32
[20] Jonsson 2017
[21] Se t.ex. Wirtz 2017

benämns som gråzonsstrategier. Gråzonsaktiviteter och -taktiker benämns på motsvarande sätt som ”measures short-of-war”.[22] En misslyckad gråzonsstrategi är när den som utsätts väljer att eskalera en konflikt och svara med motsvarande eller högre nivå av maktmedel, exempelvis militärt våld. På omvänt vis kan man säga att framgångspotentialen för gråzonsstrategier bygger på offrets önskan att undvika fientligheter.

Gråzonsstrategi kan typiskt realiseras i tre, i vissa fall sammanhängande, inriktningar:[23]

- Att etablera ett fullbordat faktum (”fait accompli”)
- Att agera via ombud (”proxy warfare”)
- Att exploatera motpartens eventuella ovilja att omsätta avskräckning i handling.[24]

Ett ”fait accompli” kan materialiseras efter hand via små steg eller via ett tydligt kliv. Den amerikanske analytikern Van Jackson (2017) använder en tvådimensionell skala där ett fait accompli i ytterligheterna kan, å ena sidan, ske gradvis (”gradual”) eller som ett bestämt avgörande (”decisive”), å andra sidan utan tvång (”noncoersive”) eller med starka tvångsmedel (”highly coersive”). Den ryska olagliga annekteringen av Krim skulle kunna ses som ett exempel på ett tämligen tydligt och bestämt fullbordat faktum, med tydliga inslag av tvångsmedel. Men den ryska Krim-kampanjen uppvisade egentligen inte några kvalitativt nya inslag, som skulle kunna betraktas som gråzons- eller hybridmetoder, utan snarare möjliggjordes av god samordning mellan befintliga konventionella ryska militära och civila förmågor.[25]

Det mest typiska karaktärsdraget för en gråzonsstrategi är ändå att den aktör som använder sådan anser att det mest effektiva sättet att nå ett visst långsiktigt mål är en serie stegvisa förändringar snarare än ett stort kliv. Anledningen till detta är att följdeffekterna med det stora klivet anses svåra att förutse och därmed förknippade med högre risk.[26]

Vad gäller att agera via ombud så är väpnad krigföring genom ombud kanske inte det vi närmast associerar med gråzonen mellan krig och fred. Det som kan göra det till ”gråzon” är att den verkliga konfliktytan mellan parterna är dold trots att krigshandlingarna är högst reella och synliga. Men grundkonflikten

[22] Se t.ex. Harlow och Maerz 1991; Tierney 2006
[23] Wirtz 2017
[24] Min tolkning av ”exploitation of ambiguous deterrence situations”, Wirtz 2017, s. 107
[25] Severin 2018; Norberg m.fl. 2014
[26] Idén om stegvisa förändringar för att nå framgång knyter an till teorier om inkrementalism som effektiv metod för policyimplementering (främst utanför den utrikes- och säkerhetspolitiska sfären). Se t.ex. Lindblom 1959; Lindblom och Woodhouse 1993.

handlar då egentligen om något annat, t.ex. att skada tredje parts ekonomiska och strategiska intressen.

Väpnad krigföring via ombud får trots allt ses som ett specialfall i ett gråzonssammanhang men är vanligt förekommande i konflikter som karakteriseras av konventionell krigföring. Ett modernt exempel är de ryskstödda separatisterna i östra Ukraina. Andra exempel är olika grupperingar i Mellanöstern som stöds av Iran, exempelvis Hizbollah och Hamas.

Att agera via ombud, oavsett om våld används eller inte, kan handla om att exploatera befintliga inhemska etniska eller sociala spänningar. Det kan också omfatta tämligen modesta aktiviteter som att stödja politiska aktivister och ytterlighetsrörelser i ett annat land. Att samtidigt stödja flera ytterligheter som ligger i konflikt med varandra (t.ex. både höger- och vänsterextrema) kan vara logiskt om syftet är att polarisera, splittra och förstärka politiska och ideologiska konflikter.

Vad gäller exploatering av motpartens eventuella ovilja att omsätta avskräckning i handling, med syfte att förändra ”status quo”, kanske denna strategi bättre kan förstås som *förskjutning av jämvikt* eller *erosion*, via små stegvisa förändringar. Under det kalla kriget talade man om s.k. salamitaktik[27], dvs. att skära bort tunna, tunna skivor av korven så att det inte i stunden märks men att den ändå blir mindre och mindre. Det handlar om att stegvist och försiktigt flytta fram sina positioner där inget steg i sig kan motivera motparten att respondera kraftfullt men där stegen sammantaget – om de hade tagits i ett enda stort kliv – skulle ha mött en signifikant motåtgärd. I praktiken kan detta vara liktydigt med ett gradvist etablerande av ett fait accompli, rimligen utan användandet av alltför starka tvångsmedel. Ett exempel är den pågående kinesiska framflyttningen av positioner i Sydkinesiska sjön, där exempelvis den kinesiska militära närvaron har ökat, omtvistade små obebodda öar har militariserats och rev har byggts ut till öar för att hävda ökade territoriella anspråk.[28] Nära associerat till sådan jämviktsförskjutning är avsaknad av, eller otydliga, gränser för hur långt en sådan process kan gå innan motparten reagerar. Sådan gränser benämns ibland som ”red lines”.[29]

Det finns ett inbyggt dilemma i gråzonsstrategiers framgång. Ett bra resultat av ett agerande, utifrån angriparens perspektiv, är att antingen undvika betydande motåtgärder eller uppnå signifikanta resultat men det är sällan möjligt att uppnå bägge samtidigt.[30]

[27] Schelling 1966/2008
[28] Mazarr 2015; Wirtz 2017
[29] Se t.ex. Altman 2015
[30] Mazarr 2015

2.3 Är gråzon och hybridkrigföring samma sak?

Begreppen gråzon och hybrid används ibland synonymt. I Krigsvetenskapsakademins vitbok om ett nytt totalförsvar uppfattas gråzonen som den övergripande arenan för hybridkrigets alla områden.[31] Olika författare använder olika definitioner och begreppen används också olika beroende på om en viss analytikers fokus ligger på en potentiell motståndares aktiviteter eller på det egna landets skyddsåtgärder eller om hybridkrigföring ses som en strategi snarare än en ny form av krigföring.[32]

Hybridkrigföring används ofta för att beskriva en kombination av reguljär krigföring, icke-reguljär krigföring och andra typer av angreppsmetoder som exempelvis sabotage, desinformation, påverkansoperationer och cyberattacker. Följaktligen har ”hybrid” mycket gemensamt med förståelsen av ”gråzon” men samtidigt kan man på goda grunder hävda att all typ av krigföring är av hybrid natur.[33]

Hybridbegreppet började användas i början av 2000-talet och associerades då främst med upprorsliknande situationer och icke-statliga aktörer. Hybridkrigföring fick då en underförstådd negativ klang och benämningen användes för att beteckna motståndarens verksamhet som, i någon mening, ojuste och osportslig.

Sedan det ryska agerandet gentemot Ukraina från och med 2014 har hybridkrig i olika sammanhang förts fram som en ”ny typ av krigföring”. Begreppet hybridkrigföring infördes i Natos nomenklatur samma år. Samtidigt påtalar många analytiker att hybridkrigföring, liksom gråzonstaktiker, inte är något nytt fenomen. Det vi idag associerar med hybridkrigföring återfinns även i historiska konflikter, inte minst i 1900-talets världskrig. Hybridkrigföring är således inget nytt. Men Rysslands annektering av Krim har, oavsett om man bedömer det som ett resultat av hybridkrigföring eller något annat, kommit att bli en ny empirisk referenspunkt.[34]

Försök att sätta in hybridkrigföring i ett större sammanhang, genom att inordna företeelsen i en eskalerande konfliktskala, är exempelvis:[35] 1) gråzonskonflikt med mångtydig/svårförståelig (”ambiguous”) krigföring, 2) irreguljär krigföring

[31] Rosenius m.fl. 2017
[32] Lanoszka 2016
[33] Käihkö 2016
[34] Severin 2018
[35] Hoffman 2015

och terrorism, 3) hybridkrigföring, 4) begränsad konventionell krigföring, 5) storskalig konventionell krigföring (”major theatre”).

Alternativa perspektiv betonar istället att alla tillgängliga medel, däribland hybridkrigföring och andra okonventionella metoder som inte leder till eskalering är att betrakta som gråzonsverktyg, exempelvis irreguljär krigföring och terrorism men kanske också begränsad konventionell krigföring.[36] I det perspektivet är således allt innan kriget gråzon, och hybridkrigföring är en del av gråzonen.

Ett annat sätt att inordna hybridbegreppet är att använda teorier om att krigföring har utvecklats i olika generationer.[37] I den s.k. fjärde generationens krigföring (t.ex. under andra världskriget) vill angriparen engagera samtliga delar av motståndarens samhällsorganisation. Motståndaren behöver inte besegras militärt utan det räcker med att underminera samhällets stöd för fortsatt krigföring. Det som främst skiljer hybridkrigföring, som i detta sammanhang går under benämningen sjätte generationens krigföring, från tidigare generationers krigföring är att syftet med krigföringen inte främst är att besegra motståndaren eller erövra territorier utan att skapa ett politiskt labilt tillstånd.[38]

Vidare har hybridkrigföring som främst är informationsbaserad lanserats som s.k. hyperkrigföring, som bl.a. involverar automatiserade beslutsprocesser och snabba konfliktförlopp. Tankarna kring hyperkrigföring baseras på den ökade sårbarhet som följer av beroendet av uppkopplade digitaliserade styrsystem för samhällsfunktionalitet och sociala medier för informationsspridning.[39]

Hur förhåller sig då gråzonen till hybridkrigföring? Vad de flesta analytiker verkar vara överens om är att hybridkrigföring alltid är en kombination av olika element. ”Hybrid” handlar ju om någon form av blandning så i det perspektivet blir det således fel att tala om en enstaka ”hybridaktivitet”.[40] En kombination av flera gråzonstaktiker kan dock utgöra något som vi skulle kunna benämna som hybridkrigföring. Hybridkrigföring kan vara ett påtagligt inslag i en eskalerad situation, typiskt krig, medan gråzonsstrategi syftar till att inte eskalera situationen, åtminstone inte inledningsvis.

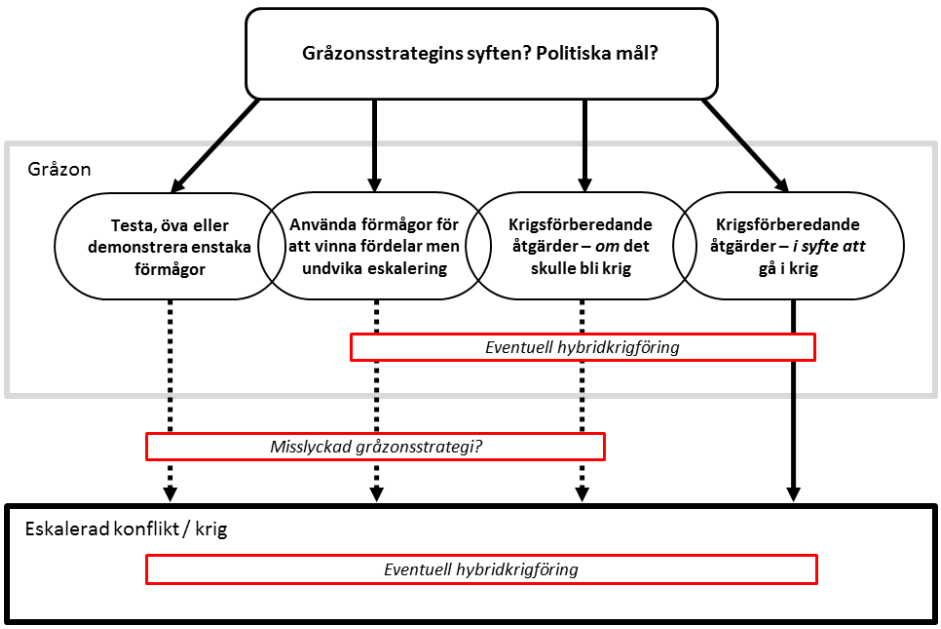
Inom amerikanska försvarskretsar kan man grovt sett säga att ”gråzonsproblematik” görs liktydig med de icke-kinetiska inslagen i hybridkrigföring. Ett kompletterande perspektiv är därför att förstå varianterna av hybridkrigföring som processer på två olika nivåer:[41]

[36] Mazaar 2015
[37] T.ex. Lind m.fl. 1989; 1994
[38] Käihkö 2016
[39] Allen 2017
[40] Se t.ex. Kofman och Rojansky 2015
[41] Severin 2018

Alla tillgängliga maktmedel och förmågor, dvs. såväl kinetiska som icke-kinetiska medel, används för skapa gynnsamma förutsättningar inför en eventuell senare öppen militär intervention med både reguljära och irreguljära förband.

Politiska, ekonomiska och psykologiska påtryckningsmedel i kombination med cyberangrepp och strategisk kommunikation används för att påverka ett land i viss riktning, vilket under kalla kriget benämndes som politisk krigföring och som vissa analytiker idag jämställer med gråzonsproblematik.

För att kunna förhålla sig till begreppen har jag valt att se gråzonen som ett tillstånd eller ett skede som kan iscensättas med olika övergripande, delvis överlappande, syften; t.ex. att testa och öva enstaka förmågor, att vinna något utan eskalering och/eller att skapa fördelar inför en eventuellt eskalerad situation, dvs. krigsförberedelser. Hybridkrigföring är då något som kan ingå dels i gråzonen, dels i en eskalerad konflikt eller krigssituation. Se Figur 1.



Figur 1. Gråzonsstrategins syften samt hybridkrigföring som möjligt inslag i såväl gråzon som eskalerad konflikt.

Ett sätt att se på kopplingen mellan gråzon och hybrid är således att när något vi uppfattar som hybridkrigföring sker under ett tillstånd som vi uppfattar som gråzon så är hybridkrigföringen en (stor eller liten) del av gråzonsstrategin och hybridkrigföringens olika inslag kan betraktas som sammansatta gråzonsaktiviteter (alternativt taktiker/metoder). Hybridkrigföring som involverar väpnade inslag och militära aktiviteter ökar rimligen risken för att motparten

responderar och därmed eventuellt eskalerar konflikten. Gråzonsstrategins syfte bör därmed inverka på vilka inslag som kan tänkas ingå i sådan hybridkrigföring.

Gråzonsstrategi är i sig ett slags risktagande. Eftersom eskalering i många fall ses som ett misslyckande är det rimligt att anta att de gråzonsaktiviteter som genomförs för att testa eller demonstrera förmågor eller för att vinna små fördelar åtminstone inte ska försämra förutsättningarna för egen krigföring – *om* man skulle tvingas gå i krig. Rimligtvis söks snarare synergier mellan de delvis besläktade syftena (se ovanstående Figur 1). Gråzonsstrategins alternativa syfte som mer renodlat krigsförberedande i syfte att gå i krig får betraktas mer som ett specialfall, synonymt med vad som brukar benämnas som skymningsläge.

2.4 Exempel på antagonistiska aktiviteter och taktiker i gråzon och hybridkrigföring

Gråzonen innebär särskilda utmaningar som skiljer sig från fredstida förhållanden men också från en krigssituation. Gråzonen kompliceras av att hoten kan vara otydliga och att det kanske saknas tillräcklig förvarning för olika skeenden. Mot bakgrund av detta blir vår förståelse av gråzonens olika inslag en förutsättning för att kunna planera inför, möta och agera på olika potentiella händelseutvecklingar. Vilka aktiviteter, liksom aktiviteternas intensitet, som är att betrakta som ”measures short-of-war” går inte att fastslå en gång för alla utan beror såväl på den aktuella kontexten som på hur de bemöts av den som utsätts för aktiviteterna.[42] Det vill säga, tolkningsföreträdet ligger hos försvararen. Om denne väljer att respondera kraftfullt så har ju gränsen (”red line”) för ”measures short-of-war” passerats.

Ett gråzonsläge kan se ut på olika vis eftersom syftet med de antagonistiska aktiviteterna kan variera. Det kan handla om att få ett land att justera sin utrikes-, säkerhets- eller handelspolitik, att hindra landet från att ta emot eller komma andra till hjälp, att försvaga landet inför en militär konflikt eller att belasta internationella samarbeten. Samtidigt kan gråzonen tolkas som ett slags allmänt lågintensivt grundläge med frekventa inslag av exempelvis påverkan och desinformation. Beroende på situation och syfte kan aktiviteterna få olika karaktär, exempelvis dolda för att skapa osäkerhet om vem som ligger bakom eller mer öppna för att mer tydligt hota och skrämmas, alternativt påvisa vissa egna förmågor.

Gråzonens karaktär påverkar således vilka aktiviteter och taktiker som kan betraktas som tänkbara. Detta styrs förutom av angriparens syften (t.ex. politiska och militärstrategiska intentioner) och tillgängliga maktmedel också av dennes uthållighet. Detta beror i sin tur på antaganden om den säkerhetspolitiska

[42] Mazarr 2015

kontexten. Det kan handla om status i pågående konflikter, samverkan och löften mellan olika parter samt dagsaktuella positioner av militära maktmedel men också om inrikes förhållanden. Dessa kan exempelvis utgöras av nuvarande regims handlingskraft och inrikespolitiska ställning samt den ekonomiska situationen, vilket i viss mån styrs av omvärldsfaktorer såsom oljeprisutveckling och hur enig det internationella samfundet kan tänkas vara avseende eventuella motåtgärder.

Exempel på konkreta ryska aktiviteter, taktiker och tillvägagångssätt, som kanske hellre associeras till hybridkrigföring snarare än gråzon, som U.S. Army Special Operations Command anser sig kunnat konstatera i Ukraina under 2013-2014, är följande:[43]

- Propaganda och desinformation via såväl traditionella som sociala medier, vilket inkluderat användandet av professionella skådespelare i nyhetsinslag, organiserade ”hacktivister” och skenbart oberoende bloggare
- Påverkan gentemot ukrainska politiker, statstjänstemän, poliser och militärer, samt deras anhöriga, via utpressning, mutor, hot, mord och kidnappning
- Organisering av och stöd till pro-ryska politiska partier, fackföreningar och paramilitära grupper
- Dold införsel av vapen och utrustning till pro-ryska styrkor samt införsel av icke-identifierbara ryska specialoperatörer (”små gröna män”) för att organisera och leda protestaktioner och paramilitära operationer, samt även organiserad införsel av paramilitära frivilligsoldater från utlandet
- Utfärdande av ryska pass till lokalbefolkning som påstås vara utsatta för ukrainska övergrepp.

Vidare har sedan 2015 ett antal cyberattacker drabbat Ukraina, gentemot exempelvis elförsörjningen, betalningssystemen, flygtrafiken, statsförvaltningen, media och sjukhus. Ytterligare tolkningar av ryska förhållningssätt till gråzons- och hybridkrigföring diskuteras i nästföljande avsnitt 2.5.

I en modell som FOI har vidareutvecklat som stöd till planering för civilt försvar (ursprungligen från Försvarsmaktens Militärstrategisk doktrin[44]) sorteras olika gråzonsinslag i termer av tänkbara maktmedel in i diplomatiska, politiska, ekonomiska och psykologiska maktmedel, liksom information, okonventionella metoder och slutligen militära maktmedel.[45]

[43] U.S. Army Special Operations Command 2015, s. 3
[44] Försvarsmakten 2016
[45] Modellen har bl.a. använts som stöd till Energimyndighetens planering för civilt försvar, se Jonsson m.fl. 2017.

Diplomatiska medel kan exempelvis vara fientlig retorik, restriktioner, utvisning av diplomater (persona non grata), avbrutna kontakter, ultimatum och hot om våld. Förutom faktiska angrepp kan enbart hot om användning av militära maktmedel vara ett sätt att påverka beslutsfattare och befolkning, vilket samtidigt gör det till ett psykologiskt maktmedel. Sådana hot skulle även kunna omfatta massförstörelsevapen.

Ekonomiska medel kan vara marknadspåverkan, sanktioner, avbrutna handelsförbindelser, ökat inflytande över strategisk infrastruktur, att störa ekonomisk infrastruktur och att överta svenska tillgångar utomlands samt angrepp på samhällskritisk infrastruktur. Politiska medel kan exempelvis vara politisk infiltration, stöd till ytterlighetsrörelser, subversiv verksamhet samt att påverka Sverige indirekt via påverkan på andra länder och organisationer (t.ex. EU).

Många av dessa aktiviteter överlappar varandra. Exempelvis kan iscensättande av terrorhandlingar ses som ett politiskt och ekonomiskt maktmedel som också kan förväntas ha psykologiska effekter, vilket också militära maktdemonstrationer, cyberaktivism, påtryckningar mot enskilda beslutsfattare och informationspåverkan kan förväntas ha. Informationspåverkan är inte bara en teknisk fråga utan underlättas om det utsatta landet karaktäriseras av öppenhet, t.ex. via yttrandefrihet och pressfrihet.[46]

På informationsarenan återfinns därutöver exempelvis cyberangrepp mot samhällsfunktioner, genom att exempelvis utnyttja de tekniska förutsättningarna för att störa och destabilisera dagens internetberoende infrastruktursystem. Därtill kommer cyberspionage mot företag och myndigheter samt nätattacker riktade mot företag, massmedier och myndigheter, exempelvis med syfte att kompromettera beslutsunderlagsdata.

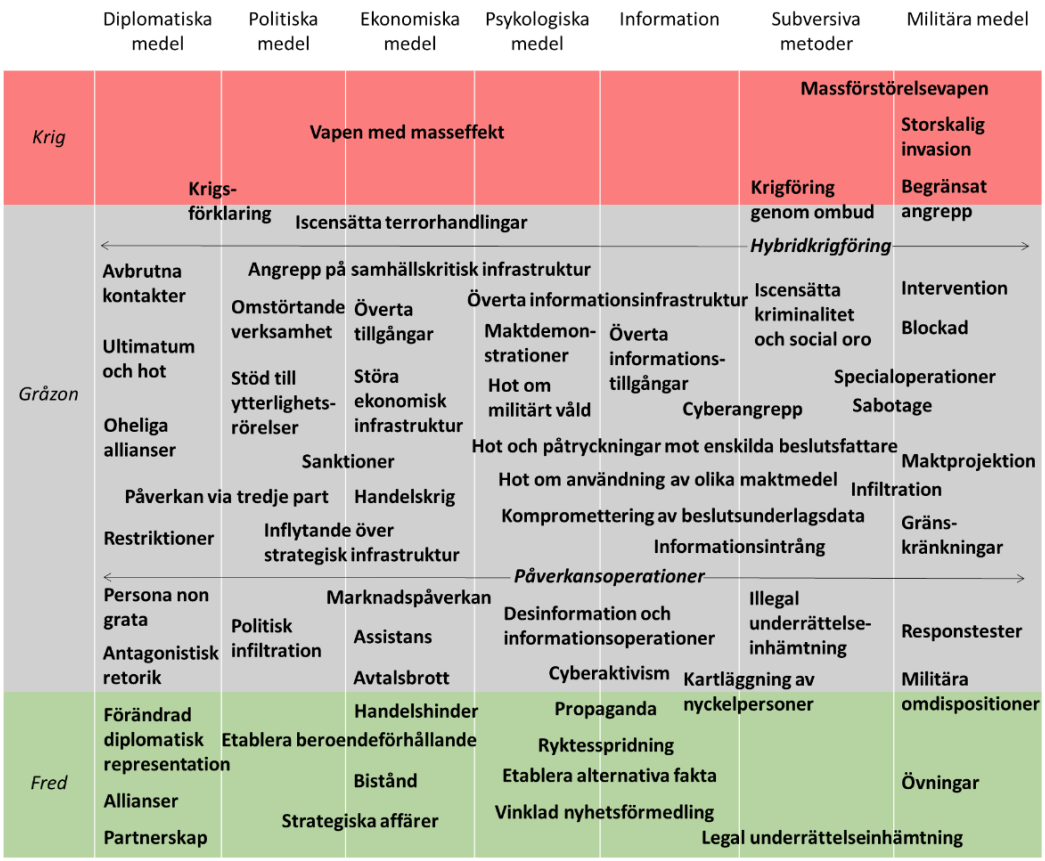
Illegal underrättelseinhämtning, personhot och sabotage kan ses som subversiva metoder mer eller mindre associerade med militära maktmedel såsom exempelvis specialoperationer, blockader samt angrepp/krigföring genom ombud. Ombud för angrepp kan i stort sett vara vem som helst i en gråzonssituation. Totalförsvarsplaneringen fokuserar på den externe statlige antagonisten men denne kan i gråzonen även utnyttja interna antagonister, exempelvis radikaliserade aktivister, kriminella grupperingar, internationell organiserad brottslighet samt terrorister. På motsvarande sätt som den externe antagonisten kan nyttja samhällets tekniska och infrastrukturella sårbarheter, exempelvis via sabotage, kan denne också nyttja intern antagonism för att uppnå sina politiska mål. Detta skapar ytterligare utmaningar och komplicerar den breda gråzonshotbilden ytterligare.

[46] Fooy 2016

Påverkansoperationer kan förstås som en samordnad användning och skräddarsydd blandning av diplomatiska aktiviteter, informationsoperationer, militära operationer och ekonomiska aktiviteter bortom en stats öppna, accepterade och lagliga aktiviteter för att uppnå sina politiska mål.[47] Det kan handla om försök att påverka politiskt beslutsfattande i en viss riktning, eller att förhindra beslut, samt att påverka den allmänna opinionen exempelvis genom desinformation, stöd till ytterlighetsrörelser och mer sammansatta informationsoperationer. Ibland sätts likhetstecken mellan *påverkansoperationer* och *informationspåverkan*. Det senare kan då omfatta en kombination av exempelvis manipulation, förfalskningar, diplomatiska utspel, militära aktiviteter, desinformation, propaganda, psykologisk krigföring, vilseledning och opinionsbildning.[48]

De exempel som diskuterats ovan åskådliggörs i Figur 2. Figuren ska dock inte ses som en vetenskaplig modell. Inordningen av olika aktiviteter och taktiker är inte alltid möjlig att göra på ett strikt och entydigt sätt, i synnerhet inte avseende maktmedelskategorier (kolumnerna). Dessutom bör det påtalas att vissa gråzonsaktiviteter kan vara tänkbara i såväl krig som fred. Figur 2 bör ses som ett hjälpmedel för att få en bred bild över tänkbara hot, som kan användas för att identifiera vilka kategorier av hot som är relevanta för en viss samhällssektor eller aktör. Påverkansoperationer liksom hybridkrigföring (se avsnitt 2.3) ses här som övergripande koncept som kan spänna över hela skalan av gråzonstaktiker.

[47] Försvarsmakten och Myndigheten för samhällsskydd och beredskap 2016
[48] Fooy 2016



Figur 2. Sammanfattande hotbildsöverblick med fokus på gråzonsaktiviteter.[49]

2.5 Tolkningar av ryska förhållningssätt till gråzon och hybridkrigföring

Begreppen gråzon eller hybridkrig används inte uttryckligen i den ryska militärdoktrinen.[50] I ryskt tänkande är de olika medel som vissa analytiker i väst förknippar med hybridkrigföring såsom hot, propaganda, vilseledning, olika

[49] Figuren baseras ursprungligen på Försvarsmaktens Militärstrategisk doktrin (2016) (Bild 3.3, s. 35), senare kompletterad med ”Exempel på möjliga medel för påverkan mot Sverige”, Gunnar Karlson (C MUST, Sälen 10 januari 2017). Därefter har den vidareutvecklats av FOI och finns i tidigare versioner i bl.a. Jonsson m.fl. 2017 och Jonsson 2017.

[50] Persson 2015

former av våldsanvändning, ekonomisk krigföring och militära maktdemonstrationer medel för att påverka en motståndare. Identifierade sårbarheter hos motståndaren, och de mål man vill uppnå avgör vilka medel som ska användas. Användandet av kombinationer av militära och icke-militära maktmedel benämns i rysk militärdoktrin snarare som ”icke-linjär” eller ”asymmetrisk” krigföring.[51]

Utifrån ryskt perspektiv är hybridkrigföring snarast något som väst praktiserade under 1900-talets kalla krig och sedermera ledde till upplösningen av Sovjetunionen, via ekonomisk och politisk destabilisering. Sovjetunionens fall har gjort stort avtryck på det ryska militära tänkandet. Insikten att staten inte kunde räddas trots de väpnade styrkornas storlek (inkl. kärnvapen) har lett till slutsatsen att icke-militära medel är lika viktiga som de militära resurserna.[52]

Koncept såsom ”färgrevolutioner”, ”kontrollerat kaos” och ”hybridkrig” betraktas av Ryssland som skapade av USA och Nato för att destabilisera det ryska samhället och staten liksom dess nära grannländer. De hot man i Ryssland diskuterar är exempelvis demoralisering av det ryska folket, utländsk ekonomisk kontroll och övertagande av tillgångar, samt fysisk förstörelse av system som är viktiga för rysk nationell säkerhet.[53] Med utgångspunkt från ett realpolitiskt synsätt, där ett ständigt internationellt nollsummespel pågår, anser sig Ryssland vara under angrepp från väst.[54]

Vilka är då omvänt de ryska målen, syftena och intentionerna som kan motivera motsvarande rysk gråzons- och hybridkrigföringsstrategi? Det kanske något förenklade och vanligt förekommande västliga synsättet är att sådana asymmetriska aktiviteter ligger den ryska ledningen närmare till hands, baserat på (den uppfattade ryska) synen att all mellanstatlig politik är ett kontinuerligt tillstånd av krigsliknande situationer.[55] Vidare anses användning av militära medel som en del av gråzonsstrategi och/eller hybridkrigföring ligga närmare till hands i rysk strategi jämfört med i västliga demokratier.[56] Militära insatser, eller mer eller mindre uttalade hot om sådana, ses mer självklart som tillgängliga policyinstrument gentemot grannländer och den strategin får anses som framgångsrik så länge som de västliga demokratierna inte responderar.

I analyser av det ryska agerandet betonas ofta att ekonomiska motiv och intressen visst kan spela roll men inte som enskild motivator.[57] Än viktigare anses att

[51] Persson 2016
[52] Persson 2017
[53] Se t.ex. Persson 2017; U.S. Army Special Operations Command 2015
[54] Westerlund 2017
[55] Se t.ex. Heier 2016
[56] Se t.ex. Banasik 2016
[57] Renz och Smith 2016a

stärka Rysslands identitet som stormakt, såväl externt som internt. Detta kan göras via olika strategier såsom att:

- Stärka de egna maktmedlen (t.ex. militär upprustning)
- Påvisa förmåga att kunna agera med högteknologiska medel bortom hemlandet (t.ex. militära insatser i Syrien)
- Öka inflytandet i det nära utlandet (t.ex. i Ukraina, Belarus, Moldavien och Kaukasienregionen[58])
- Sträva efter att försvaga tänkta militära motståndare (t.ex. minska Natos enighet kring vad som kan betraktas som artikel fem-situationer[59])
- Sträva efter att försvaga och splittra uppfattade politiska och värderingsmässiga motpoler (t.ex. stöd till ytterlighetsrörelser i olika EU-medlemsländer).

I en rapport från amerikanska RAND beskrivs motsvarande övergripande alternativa målsättningar med rysk hybridkrigföring som följande:[60]

- Erövra territorium utan att öppet använda konventionella militära medel
- Skapa förutsättningar för öppet konventionellt militärt agerande
- Påverka politik och förhållningssätt i andra länder.

De tillgängliga verktygen för hybridkrigföring anges i samma rapport som informationsoperationer, cyberoperationer, användandet av ombud, ekonomisk påverkan, politisk påverkan samt förtäckt verksamhet (t.ex. spionage, militära specialoperationer, utpressning, infiltration, subversion). Det som därtill huvudsakligen karaktäriserar rysk hybridkrigföring sägs vara följande:

- Att undvika öppen våldsanvändning eftersom eskalering inte är önskvärd om de politiska målen kan nås på annat sätt
- Att eftersträva ihärdighet och uthållighet även om intensiteten är låg
- Att anpassa medel och metod efter land och befolkning, dvs. att agera inom befintliga sociala, etniska och politiska ramverk.

Rysk hybridkrigföring brukar ofta associeras med generalstabschefen Valerij Gerasimovs artikel om icke-militära metoders roll i mellanstatliga konflikter. Gerasimov (2013) framhåller att icke-militära medel ofta är mer effektiva än

[58] Se t.ex. Hedenskog m.fl. 2018

[59] Atlantpaktens artikel 5 fastslår att ett angrepp på någon av medlemsstaterna ska ses som ett angrepp på hela alliansen. Nato-medlemmarna har därför ett gemensamt ansvar att ställa upp för varandra. Artikel 5 är formulerad så att medlemsländerna själva avgör hur de vill ge sitt stöd. Ett väpnat angrepp mot ett Natoland innebär därmed inte att samtliga medlemmar per automatik blir skyldiga att bistå med militära medel.

[60] Chivvis 2017

vapenmakt för att uppnå politiska och strategiska mål samt att rysk krigsvetenskap ligger efter den amerikanska avseende asymmetrisk krigföring.[61] Även om det inte finns något officiellt uttalat ryskt koncept som benämns som ”gråzonsstrategi” eller ”hybridkrigföring”[62] så tillmäts icke-militära medel idag en större vikt i rysk syn på militära konflikter. Den nuvarande ryska militärdoktrinen lyfter fram att nutida militära konflikter kännetecknas av militärt våld i kombination med icke-militära åtgärder såsom politiska, ekonomiska och informationsmässiga medel. Därtill framhålls användandet av specialoperationstrupp, irreguljära väpnade grupper, privata militära företag samt andra indirekta och asymmetriska metoder.[63]

Så när vissa västliga analytiker talar om ”rysk hybridkrigföring” så är det en egenhändig etikettering, som förvisso rent innehållsligt kan stämma överens med den officiella ryska synen. Ett exempel är Lanoszka (2016) som analyserar risken för rysk hybridkrigföring i de östra delarna av Europa genom att etablera fyra förutsättningar som var och en anses öka risken:

- Rysk lokal dominans avseende (främst) militära maktmedel (”local escalation dominance”)
- Rysk vilja att förändra ”status quo” (gentemot grannstaten eller i regionen)
- Att grannstaten är tämligen svag, exempelvis avseende avsaknad av ett robust civilsamhälle eller förekomst av etniska eller språkmässiga klyftor som kan exploateras
- Att grannstaten har etniska eller språkmässiga band till Ryssland.

Lanoszka diskuterar vidare olika syften med sådan eventuell hybridkrigföring. För exempelvis agerande gentemot de baltiska staterna skulle en sådan (hypotetisk) strategi kunna handla om att försvaga Natos vilja att verkligen fullfölja sina säkerhetsgarantier. För stater med nära politiska band till Ryssland (t.ex. Belarus) kan det snarare handla om preventivt agerande för att bibehålla politiskt inflytande och undvika framtida s.k. ”färgrevolutioner”.

Händelserna i Ukraina har bidragit till en rad analyser under senare år. Ett exempel är Renz och Smith (2016a) som fokuserar på Krim 2014 och inledningen av stridigheterna i östra Ukraina samma år. Deras slutsats är att det ryska ledarskapet visade förmåga att koordinera de olika instrument som möjliggjorde det framgångsrika utfallet, exempelvis informationsoperationer, cyberkrigföring liksom användandet av såväl proxy-soldater som specialförband. Vidare kunde just de ryska specialförbandens goda effektivitet i samband med övertagandet av Krim konstateras. Avslutningsvis konstateras att

[61] Persson 2013
[62] Persson 2015
[63] Hedenskog m.fl. 2017

maktdemonstrationer i form av omdispositioner och övningar av reguljära militära förband i närområdet, i större omfattning än någonsin under post-sovjettiden, var en central del av strategin.

Ett annat exempel på ”ryska hybridmetoder” beskriver den övergripande stegvisa strategin i linje med hur övertagandet av Krim gick till:[64]

- Agera med synbar legalitet
- Militära maktdemonstrationer
- Infiltrera ”små gröna män”
- Exploatera lokala sociala och etniska motsättningar
- Sprida propaganda.

Att upphöja observationen av ett enstaka skeende till strategi och rent av teori är problematiskt och begränsar generaliserbarheten och värdet av hur framtida ryska hybridhot ska förstås och analyseras. Vidare utpekas ibland ”riskområden” med geografisk närhet till Ryssland och en rysk minoritetsbefolkning, exempelvis Narvaområdet i Estland, Daugavpilsområdet i Lettland, norra Kazakstan eller Belarus.[65] Det finns en stor risk för feltolkningar när befintliga koncept, såsom hybridkrigföring, i efterhand matchas ihop med just händelseförlopp, såsom det ryska agerandet på Krimhalvön och i östra Ukraina. Kofman och Rojansky (2015) anför att händelserna ju inte behöver vara frukten av en steg för steg genomtänkt handlingsplan. De ryska operationerna i östra Ukraina benämns ofta som hybridkrigföring med stort beroende av konventionella militära medel men det är långt ifrån säkert att detta var grundplanen. En alternativ förklaring till händelseförloppets karaktär av militär konflikt är en mer eller mindre påtvingad eskalering när de ryska politiska målen inte kunde uppnås med i första hand propaganda och informationsoperationer, i andra hand intensifierad informationskrigföring, organisering och stöd till pro-ryska separatister, samt begränsade specialförbandsoperationer.[66]

Det bör avslutningsvis påtalas att det i säkerhetspolitisk debatt, tidskrifter och litteratur ofta förekommer svagt underbyggda slutsatser om hur det ryska ledarskapet tänker. Detta eftersom slutsatserna baserats på spekulation och andrahandskällor snarare än på empiri, bekräftade underrättelser och ryskspråkiga källor. Det finns en därför en uppenbar risk för rundgång av inte helt väl underbyggda slutsatser tills de etableras som sanningar.

[64] Reisinger och Golts 2014
[65] Se t.ex. Larrabee m.fl. 2017; Radin 2017
[66] Kofman och Rojansky 2015

I en finsk rapport[67] som bidrog till grundandet av det finska forskningscentrumet mot hybridhot betonas att för att förstå det (uppfattade) ryska hybridhotet krävs även samlad fördjupad kompetens avseende rysk ekonomi, politik, samhälle och historia liksom det ryska språket för att kunna tillgodogöra sig ryska källor (vilket är kompetenser som finns exempelvis inom FOI:s Rysslandsprojekt RUFS[68]). Vidare betonas, i den finska rapporten, riskerna med att se ”rysk hybridkrigföring” som ett nytt och övergripande strategikoncept som allt ryskt agerande ska tolkas in i. Rysk politik är mer komplex än så och om stora delar av rysk politik tolkas som en del i detta koncept så förloras den förståelse som kanske snarare har en historisk eller samhällelig förklaringsgrund.

2.6 Är gråzons- och hybridbegreppen relevanta?

Gråzonsproblematik och hybridkrigföring är egentligen inga nya fenomen och det finns all anledning att ifrågasätta användandet av begreppen[69] som kan tolkas som en ompaketering av något gammalt, i synnerhet när dessa börjar uppfattas som modeord. Det är i någon mening trendigt med gråzon och hybridkrig vilket påverkar såväl den allmänna debatten som politiken,[70] vilket i sin tur påverkar myndigheters inriktningar[71] och intressen och därmed även forskningen.[72]

Att konkretisera företeelser såsom exempelvis otillbörlig marknadspåverkan, illegal underrättelseinhämtning, operationer med specialförband utan nationsbeteckning, statsstödd propaganda, långsiktig politisk infiltration eller hot mot nyckelpersoner inom samhällsviktig verksamhet ger, å ena sidan, möjlighet till att med en betydligt större analytisk skärpa kunna adressera respektive hot. Detta jämfört med att klumpa ihop allt till ”gråzon”. Ett alltför avgränsat fokus, exempelvis att se cyberattacker som en enskild problematik, minskar, å andra sidan, möjligheten att se helheten i en (eventuellt) sammanhållen antagonistisk gråzonsstrategi som utgörs av en rad samordnade statsstödda aktiviteter.[73]

[67] Renz och Smith 2016b
[68] Se t.ex. Persson 2016
[69] Se t.ex. Kofman och Rojansky 2015; Käihkö 2016
[70] Se t.ex. Försvarsberedningen 2017
[71] Se t.ex. Försvarsmakten 2017
[72] Se t.ex. forskningsutlysning från Myndighetens för samhällsskydd och beredskap (2017): Civilt försvar med nya förutsättningar, med inriktning mot gråzonsproblematik (där för övrigt FOI beviljades anslag för projektet ”3 F för civilt försvar i gråzon: förståelse av hotbild, försvarsvilja och försörjningsförmåga”).
[73] Se t.ex. tal av försvarsminister Peter Hultqvist (2017) på konferens under temat ”Cyber Capabilities in Hybrid Warfare Scenarios”, där bl.a. cyberangrepp mot Estland (2007), Georgien (2008) och Ukraina (2014) lyfts fram som exempel.

Ett argument för gråzonens aktualitet som har förekommit sedan mitten av 1990-talet är att den logik som gällde under det kalla kriget – i termer av bipolaritet, maktbalans och geopolitisk rivalitet – inte är aktuell längre. Multipolaritet anses skapa mer jämna förutsättningar mellan stora och små makter, vilket därmed ska medföra förhållanden mer präglade av instabilitet och oförutsägbarhet, liknande en värld som föregick det första världskriget. Detta kan naturligtvis ifrågasättas, inte minst för att det första världskriget visade sig ha mycket lite gemensamt med en lågintensiv gråzonskonflikt och att den geopolitiska rivaliteten kan anses ha ökat sedan början på 2000-talet. Men poängen är att rationella aktörer i en multipolär värld *borde* undvika öppen militär konfrontation. Det är bland annat sådana resonemang som har underbyggt den vanligt förekommande slutsatsen att gråzonsoperationer kommer att utgöra den dominerande formen av mellanstatlig rivalitet under överskådlig tid.[74]

Men hur rationella kan egentligen konfliktaktörer vara? Det brukar sägas att kriget har en alldeles egen tvingande dynamik som svårligen låter sig planeras. Konfliktaktörer har olika mål och olika instrument till sitt förfogande för att nå dessa mål. De måste sedan välja hur och om de ska använda de olika instrumenten (inkl. militärt våld) utifrån hur de uppfattar situationen (de egna och motståndarens styrkor och svagheter). Frågan är då i vad mån det beslutsfattandet kan anses som rationellt givet att ingen aktör har tillgång till all information, att informationens korrekthet inte kan garanteras samt att beslutsfattandet påverkas av egna förutfattade meningar liksom motståndarens eventuella vilseledning.

Vidare kan man fråga sig vad multipolaritet egentligen betyder. Hur många aktörer krävs det för att det ska bli ”multi” och därmed minska sannolikheten för traditionella krig? I mångt och mycket lever 1900-talets institutioner och aktörer, liksom utrikes- och säkerhetspolitiska förhållningssätt, kvar även idag och därmed även makt- och rivalitetslogiken. Om gråzonskrigföring ska ses som det nya sättet att föra krig så är det ändå märkligt hur påtaglig användning av militära medel är i pågående konflikter, t.ex. i Syrien. Detta gäller även konflikter som ibland går under benämningen ”hybridkrig”, t.ex. kriget i Donbassregionen i Ukraina.

Det finns dock flera tungt vägande skäl till förnyad och förstärkt aktualitet för gråzonsproblematik i vår tid med anledning bl.a. av att kostnaden för direkt militär konflikt har ökat i och med fördjupade internationella ekonomiska beroenden.[75] Detta medför att aggressiva stater söker fler alternativa medel för att uppnå sina mål. Vidare har nya verktyg tillkommit, såsom cybervapen och andra tekniska och infrastrukturella möjligheter till avancerade informations- och påverkanskampanjer. Teknikutvecklingen och digitaliseringen, inte minst

[74] Se t.ex. Mazarr 2015
[75] Mazarr 2015

avseende kritiska samhällsfunktioner, har ökat antalet potentiella antagonister, deras geografiska räckvidd liksom deras potentiella mål.[76] Med *det svenska närområdet* åsyftas i regel den närmaste geografiska omgivningen men det svenska digitala närområdet är i själva verket globalt.

Trots belägg för gråzonshotens relevans och gråzonens aktualitet så betyder inte det att gråzonen ska ses som den ”viktigaste” hotbilden. Att ha gråzonen som dimensionerande planeringsförutsättning är direkt olämpligt, givet att vi bör planera för andra hot högre upp på hotskalan som inte bedöms som osannolika. Men det betyder inte att gråzonshotbilden bör utgå till förmån för hotet om väpnat angrepp och krig. Resonemang av karaktären ”klarar vi kriget så klarar vi allt” är inte giltiga givet hur dagens samhälle ser ut. Det är inte rimligt att anse att samhällsplaneringen snabbt skulle kunna ställas om och att de idag tillgängliga resurserna skulle kunna räcka till för att bygga om och re-organisera samhället till den robusthet och uthållighet som dikteras av krigets krav. Vidare är gråzonsproblematiken lika mycket en fråga för den vardagliga samhällsfunktionaliteten och krisberedskapen som för totalförsvaret.

Hur man än vänder och vrider på gråzonen återkommer man till den intuitiva förståelsen att det är något som ”ligger på gränsen”, som förknippas med osäkerhet och är något svårförståeligt som ändå återfinns mellan två kända storheter (krig och fred). Det mesta kan ju inrymmas i gråzonen, vilket skulle kunna göra begreppet till ett direkt olämpligt verktyg för förståelse av relevanta hot liksom hur vi skyddar oss mot dessa.

Min slutsats är trots allt att gråzonen är relevant men att det finns stor anledning till att vara skeptisk mot hur begreppet används. I ett beredskapsplaneringssammanhang är gråzonen inget annat än en delmängd av den sammantagna hotbilden, dvs. *den breda och heterogena antagonistiska hotbilden* vars bakomliggande syften måste förstås och vars innehåll måste konkretiseras och bemötas. När detta kan göras på ett nyanserat sätt finns det fog för att använda begreppet gråzon.

I ett totalförsvarssammanhang kan det också finnas en poäng med att nogsamt avgränsa gråzonen till de aktiviteter som den kvalificerade statsaktören genomför eller ligger bakom via ombud. Om all negativ samhällsbelastning, t.ex. vanlig kriminalitet, eller all påverkan som kan uppfattas som otillbörlig i någon mening, t.ex. affärsmässig lobbying, etiketteras som ”gråzon” blir begreppet oanvändbart.

[76] Cederberg m.fl. 2017

3 Gråzonsutmaningar för krisberedskap och civilt försvar

Kapitlet inleds i avsnitt 3.1 med en beskrivning av övergripande utmaningar för samhällets säkerhet i gråzon, som berör såväl den ordinarie krisberedskapen som det civila försvaret sammantaget. För att lösa det civila försvarets uppgifter, inom olika samhällssektorer, finns en rad specifika utmaningar i en gråzonssituation, vilka översiktligt diskuteras i avsnitt 3.2.

3.1 Övergripande utmaningar för samhällets säkerhet

Utmaningarna i gråzonen finns på flera nivåer. Under gråzonen kan det tänkas föreligga en redan ansträngd säkerhetspolitisk situation i närområdet, vilket i sig är utmanande, men kanske inget direkt konkret militärt hot mot Sverige som motiverar höjd beredskap.

Den av regeringen beslutade återupptagna planeringen av ett sammanhängande totalförsvar, som berör Försvarsmakten, Myndigheten för samhällsskydd och beredskap och civila myndigheter, kan förstås vara liktydigt med planering för höjd beredskap.[77] Därmed finns en risk för att planeringen för att hantera gråzonsproblematik faller mellan de stolar som krisen respektive kriget utgör.

Det civila försvaret ska baseras på den ordinarie krisberedskapen.[78] Om höjd beredskap inte råder innebär det en viss typ av utmaning. Det civila försvarets särskilda regelverk aktiveras först vid höjd beredskap. Detta innebär sannolikt att det som sker inom ramen för en gråzonssituation, åtminstone inledningsvis, ska hanteras av samma aktörer och inom i stort sett samma organisatoriska former som i fred. Tillgängliga verktyg för hantering är därmed desamma i fred inom ramen för regelverket avseende krishantering, dvs. till skillnad från under höjd beredskap då exempelvis förfogande för att tillgodose totalförsvarets behov kan tillämpas. Krisberedskapens aktörer, tillika det civila försvarets, måste därmed planera inför gråzon avseende både fred och höjd beredskap.

Detta talar sammantaget för en i högre grad gemensam planering och organisation för fredstida krisberedskap och det civila försvaret. Detta behov uttrycks också av Försvarsberedningen som föreslår att det civila försvarets uppgifter, att värna civilbefolkning, upprätthålla de viktigaste

[77] Se Prop. 2014/15:109; SFS 2015:1052; SFS 2015:1053
[78] Prop. 2014/15:109

samhällsfunktionerna, samt stödja Försvarsmakten, bör kompletteras och förtydligas i en riktning som ligger närmare krisberedskapen.[79]

Gråzonen är komplex och förknippas med en rad osäkerheter, exempelvis vem som ligger bakom en viss aktivitet och om det överhuvudtaget är någon som ligger bakom det som händer. Gråzonens karaktär av otydlighet och osäkerhet gör att det kan vara svårt att etablera en allmänt vedertagen förståelse av vad som händer, både för beslutsfattare och allmänhet. Dessutom är det svårt att avgöra när situationen motiverar extraordinära åtgärder för att hantera en viss händelse. De enskilda hoten som förknippas med gråzonen kan kanske hanteras var för sig men en effektiv strategisk hantering kräver överblick och sektorsövergripande samverkan.[80] Enskilda sektorsaktörer varken kan eller bör ha huvudansvaret för att respondera gentemot en kvalificerad antagonistisk statsaktör.

Som tidigare beskrivits är det utifrån angriparens perspektiv svårt att *både* undvika betydande motåtgärder *och* att uppnå signifikanta resultat om den utsatta har möjlighet att genomföra motåtgärder. Men eftersom det i en gråzonssituation kan vara svårt att motivera extraordinära åtgärder är preventivt tröskelhöjande arbete viktigt. Det handlar bl.a. om att göra samhällskritiska infrastruktursystem mer robusta. Tröskeleffekt används i militära sammanhang som en avskräckningsmetafor, vilken i viss mån också kan vara giltig för det civila försvaret. Om insatsen, och kanske även upptäcktsrisken, ökar för att ett angrepp mot en civil infrastruktur ska få avsedd verkan kan den ökade robustheten verka avhållande. Avskräckning handlar om att höja angriparens ekonomiska och politiska kostnader för angrepp liksom att skapa förutsättningar för att minimera den potentiella vinsten ett angrepp kan medföra. Fysisk avskräckning i termer av militär förmåga eller robust infrastruktur utgör bara en del av den svenska avskräckningskapaciteten, därtill kommer exempelvis olika former av internationell säkerhetssamverkan som gör att ett angrepp är förenat med ett högre risktagande.[81] Ömsesidiga internationella säkerhetsberoenden samt möjligheten att ge och ta emot såväl civil som militär hjälp är konfliktavhållande, givet angriparens ovilja till de ökade kostnader en eskalering skulle innebära.

För att kunna planera för en adekvat krisberedskap och ett civilt försvar är det avgörande att förstå vilka slags hot som kan drabba Sverige i ett gråzonsläge samt att gråzonen kan ha olika karaktär. Den förståelsen är viktig bland annat för att samhällets aktörer ska kunna genomföra förberedelser samt prioritera vilka

[79] Försvarsberedningen (2017) (s. 83) föreslår såväl ett förtydligande som en utvidgning av uppgifterna. De ursprungliga uppgifterna föreslås kompletteras med: upprätthålla en nödvändig försörjning, upprätthålla samhällets motståndskraft mot externa påtryckningar och bidra till att stärka försvarsviljan, bidra till att stärka samhällets förmåga att förebygga och hantera svåra påfrestningar på samhället i fred, samt med tillgängliga resurser bidra till förmågan att delta i internationella fredsfrämjande och humanitära insatser.

[80] Palmgren 2017

[81] Se t.ex. Westerlund 2017

åtgärder som ska genomföras. Efter ett par decenniers nedmontering av försvaret är hotbildsförståelsen begränsad, vilket är en utmaning i sig. Förutom en ökad förståelse för vilka olika slags hot som samhället kan utsättas för, behövs också en ökad förståelse för vilka motåtgärder som finns tillgängliga samt hur metoder för att bemöta de nya hoten kan etableras på olika nivåer i samhället. Bland annat underlättar detta för myndigheter och beslutsfattare att identifiera risker och samverkansbehov under ett gråzonsläge. Det gäller exempelvis hur och när myndigheters och andra berörda aktörers agerande behöver anpassas för att motverka olika hot eller när extraordinära åtgärder är motiverade. En fördjupad förståelse kan också utmynna i nya förhållningssätt och ny lagstiftning för att skapa förutsättningar för agerandet i ett gråzonsläge, liksom synliggörande av vilka risker som är förknippade med en sådan utveckling, bland annat vad gäller transparens och ingrepp i grundläggande samhälleliga besluts- och styrningsfunktioner.

En besläktad utmaning är hur man möter hot mot de egna samhälleliga värdena utan att begränsa eller göra avkall på desamma. Ett exempel från informationskrigföringen är att ett försvar som innebär att försöka blockera antagonistens desinformation eller narrativ riktade till utländska medborgare[82] kan betraktas som en inskränkning av det demokratiska samhällets öppna karaktär.

Hotförståelse är således viktigt men att ensidigt studera motståndarens aktiviteter, agerande och beteende kan vara vanskligt eftersom det kan vara svårt att se hur de olika inslagen hänger ihop i en sammanhållen strategi. Det är dock frestande att göra det eftersom det leder tanken mot att det kanske skulle kunna gå att förutse vad som kan inträffa härnäst. Men en framgångsrik gråzonsstrategi är av sin natur svårbegriplig. Vissa hävdar till och med att gråzonskrigföring inte har någon beröring med gängse strategiförståelse.[83] Andra menar att man ska försöka göra gråzonsstrategier begripliga genom att analysera motståndarens syfte snarare än att fokusera på agerandet.[84]

Det som normalt omfattar den ordinarie civila krisberedskapens hotbilder bör i viss mån också ingå i gråzonshotbilder, men inte med samma utgångspunkt. Den externa antagonisten kan exempelvis skapa ”olyckor”, infrastrukturella störningar, smittspridning och underblåsa social oro. Antagonister kan inte skapa extrema väderhändelser, klimatförändringar eller naturkatastrofer men sådana händelser kan ändå exploateras, när de väl uppstår, av såväl interna som externa antagonister, exempelvis i form av samhällsbelastande kriminalitet eller för att minska allmänhetens förtroende för myndigheter och regering.

[82] Hellman och Wagnsson 2017
[83] Elkus 2015
[84] Wilson och Smitson 2017

De samtidiga utmaningarna att hantera störningar, klargöra läget och att initialt förstå vem den egentlige antagonisten är, liksom vilket mål denne har, karaktäriserar gråzonen. Vidare kan ett gråzonsförlopp vara tämligen utdraget i tid, vilket utmanar samhällets uthållighet oavsett om förloppet är eskalerande eller inte.

3.2 Utmaningar med att lösa det civila försvarets uppgifter

Gråzonen medför en rad utmaningar för civila försvaret.[85] Det civila försvarets uppgifter är att att värna civilbefolkningen, att upprätthålla de viktigaste samhällsfunktionerna, samt att stödja Försvarsmakten. En särskild utmaning för ansvariga myndigheters möjligheter till styrning och snabb respons är att mycket samhällsviktig verksamhet huvudsakligen är privat, exempelvis godstransporter, apotek och läkemedelstillverkning, banker, energi, mobiltelefoni och internet, dagligvaruhandel samt privat hälso- och sjukvård.

Även om gråzonsaktiviteternas påverkan på samhällets funktionalitet skulle vara begränsade så kan även mindre störningar i lokala tekniska system bidra till förstärkta störningar i andra större system. Exempelvis påverkar störningar i elförsörjningen och data- och telekommunikationerna indirekt även samhällsviktiga funktioner såsom livsmedelsförsörjningen, betalningssystemen, VA-systemen, fjärrvärmen och transportlogistiksystemen, som i sin tur får ytterligare spridningseffekter. Även samhällsfunktioner med reservkraft kan påverkas av mindre men återkommande elavbrott om nytt bränsle inte hinner fyllas på i tid innan nästa elavbrott uppstår. Det kan exempelvis gälla avloppsreningsverk, trafikledningscentraler, sjukhus samt jordbruksanläggningar och lager i livsmedelskedjan.

Även begränsade tekniska störningar kan få psykologiska effekter om oro och rädsla breder ut sig. Informationskampanjer, desinformation, falska meddelanden och psykologiska påverkansoperationer kan påverka allmänhetens förtroende för samhällets styrning och därmed försvarsviljan, vilket kan ses som en del av målet, liksom en förutsättning för, att värna civilbefolkningen.

En eventuell ökning av ”olyckor”, i en gråzonssituation skulle direkt påverka civilbefolkningen men ökar också arbetsbelastning för polis, räddningstjänst och akutsjukvård, vilket indirekt minskar möjligheten att värna civilbefolkningen.

[85] Parallellt med arbetet med föreliggande rapport har FOI på uppdrag av MSB tagit fram ett gråzonsscenario, Typfall 5: Utdragen och eskalerande gråzonsproblematik (Jonsson 2018). Utmaningarna för det civila försvaret som beskrivs i avsnitt 3.2 i denna rapport baseras på avsnitt 2.3-2.5 i Jonsson 2018. I avsnitt 4.2 i föreliggande rapport diskuteras specifikt energisektorns utmaningar i relation till Typfall 5. Själva scenariobeskrivningen återfinns som bilaga i denna rapport.

Vissa uppgifter som i vanliga fall åläggs polis, räddningstjänst och akutsjukvård kan komma att nedprioriteras. I ett skede där särskilt utsatta människor är i behov av extra resurser från redan hårt belastad kommunal vård- och omsorgspersonal kan andra kommunala samhällsfunktioner komma att nedprioriteras. Oavsett anledning till eventuella sjukdomsutbrott i ett gråzonsläge drabbas indirekt samhällets funktionalitet av sjukfrånvaro då samhällsfunktioner blir underbemannade.

Särskilt störningar i el- och värmesystem, om de inträffar under de kalla årstiderna, har direkt påverkan på civilbefolkningens hälsa. Behov av evakuering av särskilt utsatta kan uppkomma, vilket binder upp personella resurser som kanske hade behövts bättre på annat håll. Elavbrott i kombination med störningar i leveransen av reservkraftsbränsle påverkar exempelvis sjukvård och avloppsrening, vilket också i nästa led kan drabba civilbefolkningens hälsa. Eventuell avsaknad av varmvatten kan medföra sämre hygien och därmed ökad risk för smittspridning och eventuella sjukdomsutbrott, vilket medför direkt påverkan på civilbefolkningen.

Uppkomst av eventuell desinformation i en gråzonssituation som måste dementeras tar myndigheternas resurser i anspråk och kan också undergräva myndigheternas trovärdighet i att kommunicera läget framöver, då en faktisk höjning av hotnivån och därmed beredskapen kan bli aktuell. Att nå ut med korrekt och saklig information kan i sin tur mildra indirekta effekter av störningar, exempelvis hamstring av livsmedel och drivmedel. Där spelar bl.a. mediesektorns funktionalitet en viktig roll. Mediers förmåga att nå ut med saklig och opartisk information är överhuvudtaget en viktig beståndsdel i det psykologiska försvaret. Begränsad möjlighet till pålitlig nyhetsförmedling kan skapa oro och otrygghet, öka ryktesspridning samt öka möjligheten att medvetet sprida falsk information. En annan viktig del i ett psykologiskt försvar är att identifiera, analysera och möta informationskampanjer, vilket försvåras av störningar i informationsinfrastrukturen. Å andra sidan försämras då även möjligheten att iscensätta informationskampanjer och sprida falsk information.

Om störningar i betalningssystemen skulle uppkomma i en gråzonssituation så påverkas människors möjligheter att anskaffa förnödenheter och därmed också deras fysiska hälsa. Om det inte är möjligt att anskaffa förnödenheter på normal väg kan snatterier, småstölder och inbrott komma att öka. Detta ökar arbetsbördan för ordningsmakten, vilket i sin tur indirekt kan påverka möjligheterna att värna civilbefolkningen.

Störningar som drabbar data- och telekommunikationer skapar följdeffekter som direkt kan påverka människors hälsa, exempelvis att läkemedel inte går att hämta ut. Om möjligheten att nå ut med information från myndigheter, liksom etablerad nyhetsförmedling, blir begränsad kan ryktesspridning, liksom möjligheten att medvetet sprida falsk information, komma att öka.

Eventuella större störningar som drabbar elförsörjningen samt data- och telekommunikationen kan skapa stora följdeffekter i en rad sektorer. Det kan gälla det elektroniska recepthanteringssystemet för utskrivna läkemedel, bankers internetservicefunktioner, livsmedelskedjornas beställningssystem och lagersaldon, den spårbundna kollektivtrafikens signalsystem, informations- och nyhetsförmedlingen etc. I ett förlopp där samhällsfunktioner upphör och exempelvis medför akut vatten- och livsmedelsbrist, finns uppenbara risker för civilbefolkningens fysiska välmående.

Att hantera stora infrastrukturella störningar samt att återställa funktionalitet är en utmaning oavsett händelseförlopp. Sådana insatser måste kunna ledas och försörjas med materiella resurser samt kompetens och arbetskraft. Till skillnad från läget vid en ”naturlig” kris kan en antagonist på olika sätt försöka att ytterligare försvåra hanterings- och återställningsarbete, exempelvis genom att störa ledningsfunktioner.

Upprätthållandet av Försvarsmaktens förmågor är åtminstone delvis beroende av tjänster som produceras i civila sektorer. Det handlar bland annat om el, drivmedel, transporter av personal och materiel, tele- och datakommunikationer, livsmedel, läkemedel och sjukvård, samt finansiella tjänster. Dessa sektorer bemannas av människor ur civilbefolkningen, vars relativa välmående och möjligheter att ta sig till sina arbetsplatser är en förutsättning för att stöd till Försvarsmakten ska kunna realiseras. Fysiska störningar och angrepp mot dessa samhällsfunktioner, liksom eventuell underbemanning, påverkar givetvis negativt möjligheten för det civila samhället att tillgodose Försvarsmaktens behov.

Det bör noteras att om det inte råder höjd beredskap i en viss gråzonssituation så är det kanske i första läget så att det förväntas att Försvarsmakten ska stödja krisberedskapen och det civila samhället, snarare än att Försvarsmakten ska ta emot stöd. Försvarsmaktens stöd till det civila samhället kan exempelvis handla om flygtransporter av reservdelar och reparationsmateriel för återställning av infrastruktur eller att hemvärnsförband bistår polis och räddningstjänst. Försvarsmaktens stöd till samhället måste hela tiden vägas mot utförandet av de egna uppgifterna och detta kan leda till behov av samordning mellan militära och civila resurser.

4 Gråzonshot och utmaningar inom energiområdet

Det övergripande syftet med detta kapitel är att bidra till en översiktlig gråzonshotbild för energiområdet. Hotbilden ska fungera som:

- Ett verktyg för att diskutera de problem som kan uppkomma i hotbilden med energibranschens aktörer
- Ett stöd till Energimyndighetens omvärldsbevakning, hur den ska fokuseras och vidareutvecklas
- Ett underlag inför planering av energiberedskapsåtgärder.

Kapitlet är indelat i tre delar. Först sammanfattas aktuell litteratur om energi och gråzon/hybridkrigföring (4.1). Sedan diskuteras energisektorns utmaningar utifrån gråzonsscenariot Typfall 5 (4.2). Slutligen förs en diskussion om gråzonshot och relaterade sårbarheter baserat på information från svenska energibranschaktörer och myndigheter (4.3).

4.1 Energi och gråzon/hybrid i aktuell litteratur

Litteraturen kring gråzonskonflikt och hybridkrigföring som på ett relevant sätt berör energiområdet är begränsad. Energi lyfts dock ibland fram som en aspekt som kan vara både ett mål och ett medel i en gråzonskonflikt,[86] inte minst vad gäller observationer från Ukrainakonflikten.[87] Energi som mål handlar exempelvis om sabotage mot elförsörjningen. Energi som medel kan exempelvis vara att använda det s.k. energivapnet i termer av politisk utpressning genom att hota med att avbryta energileveranser.[88]

Uppdelningen av energi som mål respektive medel kan dock inte alltid göras på ett strikt sätt. Exempelvis kan ett sabotage mot en viss del av energiförsörjningen, som därmed synbart blir ett mål, egentligen syfta till det övergripande målet att sprida oro och rädsla samt försvaga landet.

Vad gäller litteratur om energiförsörjningstrygghet i allmänhet finns inom risk- och krisforskningen en stor mängd studier med fokus på främst icke-antagonistiska hot. Noterbart är att lejonparten av forskningen fokuserar på analyser av, eller beredskap inför att möta, enskilda avgränsade händelser snarare

[86] Se t.ex. Mazarr 2015, som exemplifierar användandet av olika maktmedel i gråzonen som ”from cyberattacks to information campaigns to energy diplomacy” (s. 2).
[87] T.ex. Reisinger och Golts 2014; Renz och Smith 2016a;
[88] Se t.ex. Smith Stegen 2011

än över tid utdragna krisförlopp. Detta gäller energiområdet i allmänhet[89] och elområdet i synnerhet.[90] Det finns dock exempel på studier med ett mer utdraget tidsperspektiv, exempelvis inom den s.k. peak oil-teorin[91] eller studier av försörjning i krigszoner.[92] Ännu ovanligare är studier som fokuserar på energi och antagonistiska hot,[93] särskilt avseende långvariga störningar. Fördjupade analyser av specifika gråzons- och hybridtaktiker mot/via energi är därmed också en bristvara men det finns ändå ett antal studier från senare år, med viss slagsida mot analyser av förmodat ryskt agerande. Dessa studier tenderar att fokusera på antingen cyberhot mot energiförsörjningen eller energi som ett politiskt och/eller ekonomiskt maktmedel.

Det är rimligt att anta att ett antal stater har skapat en egen cyberförmåga som inte bara ska kunna agera defensivt utan även offensivt. Att cyberkrigföring är en aktivitet som inte bara är legitim i en konfliktsituation utan även kan användas för att skapa bättre förutsättningar inför en eventuell framtida konflikt, är ett förhållningssätt som brukar tillskrivas flertalet stormakter, inte minst USA och Ryssland.[94] Därtill bedöms det att betydelsen av synbart fristående, men regeringsfinansierade, hackergrupper ökar.[95] Dessa ombud för andra stater är många och byter skepnader liksom metoder. Det handlar exempelvis om datastölder, förstörelse av data, införsel av skadlig mjukvara, scanning av SCADA-system, dvs. industriella informations- och styrsystem, övertagande av system samt s.k. spear-phishing, ransomware, zero-day och watering holes.[96] Exempel på cyberhackergrupper som tros ha koppling till den ryska regeringen och som har angripit olika energisystem i bl.a. Ukraina och USA är Sandworm team (olika alias: Telebots, Electrum, BlackEnergy) och Koala team (olika alias: Energetic Bear, Dragonfly).[97]

När det handlar om digitala gråzonshot mot energiförsörjningen kan dessa inordnas på tre olika nivåer:[98]

1. Hög nivå: Cyberkrigföring i termer av stora, sällsynta och potentiellt mycket skadliga cyberattacker som genererar fysisk förstörelse och möjligen skadade och dödade människor.

[89] Se t.ex. Hughes och Ranjan 2013; Robinson 2003
[90] Se t.ex. de Nooij m.fl 2007; de Nooij m.fl 2009; Veloza och Santamaria 2016
[91] Se t.ex. Kjärstad och Jonsson 2009; Aleklett m.fl 2010
[92] Se t.ex. Pilav 2012
[93] Se dock t.ex. Holmgren m.fl. 2007; Pilav 2012; Stulberg 2017; Andersson och Westerdahl 2017
[94] Se t.ex. Antonovich 2011; Giles 2016
[95] Connell och Vogler 2017
[96] Se fördjupad förklaring på begrepp på exempelvis svenska datatermgruppen: www.datatermgruppen.se
[97] Se t.ex. Estonian Foreign Intelligence Service 2018; Greenberg 2017a
[98] Muller m.fl 2018

2. Mellannivå: Cyberspionage/cyberangrepp som använder digitala verktyg för att stjäla information, störa eller skapa avbrott i systemen eller skapa förutsättningar för den högre nivån av sabotage.
3. Lägre nivå: Vardagsbruset som de flesta aktörer utsätts för rutinmässigt i termer av mindre ambitiösa scannings- och intrångsförsök via oskyddade ingångar i system samt kriminella aktiviteter med ekonomiska syften, t.ex. försök till bedrägeri via epost eller virus.

Exempel på angrepp på den högre nivån är de digitala sabotagen som drabbade Ukrainas elsektor 2015 och 2016 (som Ryssland tros ligga bakom). Angriparen fick 2015 fäste i systemen via en s.k. trojan som aktiverades när en falsk epost-bilaga öppnades och lyckades därmed infiltrera de nätverk som sammanband kontorssystemen med de digitala styrsystemen av kraftverk. År 2016, då säkerheten hos de enskilda företagen hade förbättrats, angreps istället själva elnätet via intrång i en i systemet centralt belägen kraftstationsnod. En skadlig s.k. modulär mjukvara med kapacitet till stor fysisk förstörelse, liksom även med möjlighet att användas vid ytterligare tillfällen, infördes i kraftöverföringssystemet. Säkerhetsforskare bedömer att bägge incidenterna, men i synnerhet den senare, hade potential att skapa betydligt större skador och elavbrott än vad som skedde och att det primära syftet därmed antagligen i första hand var att demonstrera angriparens egen förmåga (se även Figur 1, avsnitt 2.3).[99]

Ytterligare ett exempel på angrepp på den högre nivån är Stuxnet-angreppet (som USA/Israel tros ligga bakom) mot den iranska urananrikningsanläggningen i Natanz. Angreppet skadade anläggningens centrifuger trots att inte styrsystemen till dessa var kopplade till internet. Man tror därför att infiltrationen skedde via antingen en s.k. insider, en infekterad bärbar dator som tillhörde servicepersonal eller via infekterade USB-minnen.[100]

Ett exempel på angrepp på mellannivå (som Rysslands militära underrättelsetjänst tros ligga bakom[101]) är den ransomeware,[102] bl.a. med namnen Petya, ExPetr, Goldeneye och NotPetya, som 2017 fick stor spridning bland främst ukrainska företag, däribland energibolag. Spridningen påbörjades dagen innan den ukrainska självständighetsdagen och syftet föreföll inledningsvis vara ekonomisk cyberkriminalitet. Det visade sig dock att den skadliga mjukvaran

[99] Greenberg 2017b; Muller m.fl. 2018
[100] Zetter 2014
[101] Nakashima 2018; Vendil Pallin 2018
[102] Ransomware är skadeprogram som smittar en dator, låser den och begär en lösensumma för att låsa upp den.

egentligen inte var någon ransomware utan en datamask[103] som raderade data från hårddiskarna på de infekterade datorerna. Angriparna hade lyckats sprida den skadliga mjukvaran genom att infiltrera ett visst bokföringssystem med tillhörande mjukvara, som enligt ukrainsk lag är ett av två alternativ som måste användas av landets alla näringslivsaktörer.[104]

Ytterligare ett exempel på angrepp på mellannivån är den s.k. Shamoon-attacken, mot det statliga saudiska oljebolaget Saudi Aramco (som Iran tros ligga bakom). Ett virus drabbade cirka 30 000 datorer inom företaget, som tillfälligt slutade fungera, och orsakade därmed stora avbrottskostnader men inga kända fysiska skador.[105]

De digitala angreppen mot energiförsörjningen har bidragit till ökat fokus på såväl hotförståelse som att kartlägga sårbarheter, exempelvis i Norges oljeindustri.[106] Men energi och gråzon berör mer än bara cyberfrågan. Energi kan användas för att uppnå politiska mål och omvänt kan politiskt agerande ha syftet att ekonomiskt gynna den egna energibranschen. Möjligheten att använda dessa maktmedel varierar mellan olika länder. I exempelvis Saudiarabien och Ryssland är möjligheterna relativt sett stora eftersom petroleumindustrin och staten är nära sammanflätade.

Det har skrivits mycket om det s.k. ryska energivapnet, dvs. att använda hot om avbrutna eller begränsade energileveranser som utpressningsmedel, i synnerhet under den senaste perioden av relativt sett höga energipriser (fram till slutet av 2014).[107] Föreställningen om den ryska energiexporten som ett potentiellt hot baseras i första hand på tolkningar av rysk policy snarare än på empiri. Redan 2003 fastslog den ryska energistrategin att energi bör användas som ett verktyg för inrikes- och utrikespolitisk implementering.[108] Den nu gällande strategin från 2009 betonar en effektiv användning av energiresurserna för att bland annat kunna stärka Rysslands utrikespolitiska position.[109] I vidareutvecklingen av rysk energipolicy befästs denna bild via uttalanden om att olje- och gaspolitiken inte bara bör vara en signifikant del av rysk utrikespolitik utan det enskilt viktigaste instrumentet.[110] Vidare beskrivs att energipolitikens huvudprioritet är att använda

[103] En datamask, eller internetmask, är en form av datorvirus som själv sprider sig från dator till dator över Internet. Det som skiljer en mask från övriga datorvirus är att den inte behöver hjälp av någon oförsiktig användare. Maskar utnyttjar därför oftast istället någon slags säkerhetsbrist för att kunna spridas vidare.
[104] Kramer 2017; Cherepanov 2017; Muller m.fl. 2018
[105] Kello 2017; IISS 2013
[106] Muller m.fl. 2018
[107] Se litteraturöversikter i t.ex. Sonnsjö 2014; Månsson 2014
[108] Energy Strategy of the Russian Federation 2003
[109] Ministry of Energy of the Russian Federation 2010
[110] Margelov 2011

den stora ryska energipotentialen för att främja internationella ekonomiska och politiska relationer med syfte att säkra ryska geopolitiska och geoekonomiska intressen i Europa och i grannländer.[111]

Då som nu råder oenighet bland bedömare om energivapnets effektivitet. Somliga hävdar att så länge som motparten är en välfungerande och ekonomiskt utvecklad stat så kan aldrig energivapnet få någon särskilt stor effekt.[112] Andra menar att energivapnet både har stor potential och dessutom har varit flitigt och framgångsrikt använt gentemot Ukraina, men även indirekt mot väst, sedan 2014.[113] Man kan dock slå fast några aspekter som spelar roll avseende om energivapnet skulle kunna ha potentiell verkan eller inte:

- Om energiråvaran är ledningsbunden (t.ex. naturgas) eller icke-ledningsbunden (t.ex. LNG och olja), vilket i sin tur ger olika marknadsförutsättningar och därmed möjlighet till alternativa leverantörer
- Effekter på kort respektive lång sikt, för såväl angriparen som den stat (eller de stater) som blir utsatta
- Om en enskild stat, t.ex. Ukraina, blir utsatt eller om det drabbar flera och större stater med möjlighet till samverkan och solidaritet, t.ex. EU
- Hur energisituationen i övrigt ser ut för den stat som blir utsatt, t.ex. alternativa energikällor, distributionsvägar, energieffektivitet, energianvändningsmönster, industristruktur etc.

En vanligt förekommande slutsats bland bedömare är att Ryssland sammantaget är mer beroende av energiintäkter från EU än vad EU är beroende av rysk energi.[114]

I Ukrainakonflikten har energi fungerat som både mål och medel. Under 2014, i konfliktens inledning, stängdes den ryska gastillförseln till Ukraina under 180 dagar samtidigt som kolgruvor, transportleder och kraftverk i närheten av stridszonen stängdes ner, attackerades eller förstördes. Ukraina svarade med att stänga elektriciteten till den av Ryssland annekterade Krimhalvön. Numera finns dock en överenskommelse som syftar till säkra såväl Ukrainas koltillförsel som Krims elförsörjning.[115]

Annekteringen av Krim har i sig en energirelaterad innebörd. Det ukrainska energibolaget som verkade på Krim, Chornomornaftogaz, har nationaliserats av

[111] Institute of Energy Strategy 2018
[112] Se t.ex. Bartuska 2017
[113] Gonchar och Chubyk 2017
[114] Se litteraturöversikt i Jonsson och Sonnsjö 2013, kap. 4
[115] Gonchar och Chubyk 2017

den ryska staten, inklusive dess land- och havsbaserade energiråvarutillgångar. Dessa, framför allt, gastillgångar, har relativt sett ringa betydelse utifrån ett ryskt perspektiv men desto större betydelse för Ukrainas inhemska energiförsörjning. Vidare sträcker sig gasfälten från Krimhalvön och sedan västerut utmed den ukrainska kusten. Utvinningsplattformarna på gasfälten skulle kunna användas av militära styrkor i händelse av en utökad konflikt.[116]

Sammantaget kan man hävda att energiaspekter på olika sätt har ingått i hela skalan av maktmedel som Ryssland har använt gentemot Ukraina i den pågående konflikten,[117] dvs. diplomatiska, politiska, ekonomiska, psykologiska, information, subversiva metoder och militära medel (se Figur 2, avsnitt 2.4). Ryssland har strävat efter att minska Ukrainas trovärdighet som ett tillförlitligt transitland, bl.a. i diplomatiska sammanhang men även i form av informationsspridning med innebörden att Ukraina olovligen tillskansar sig stora volymer gas avsedd för europeiska konsumenter. Ukrainska försök att öka sin självförsörjningsgrad har också mötts av propaganda, bl.a. har det italienska företaget Enis prospekteringen av utvinning av s.k. shale-gas i Ukraina, liksom ukrainsk kärnbränsleförsörjning via amerikanska Westinghouse (som för övrigt tillverkas på anläggningen i Västerås), beskrivits som ett stort risktagande och att katastrofer i termer av att ett andra Tjernobyl är att vänta. Vidare har de ukrainska energirelaterade ekonomiska kostnaderna stundom varit stora, på grund av unilateralt satta gaspriser på en betydligt högre nivå än vad övriga Europa betalat. Förlusten av kapital- och energitillgångar har varit kännbar. Vidare har cyberangrepp och fysiska sabotage mot elförsörjningen skapat ekonomisk belastning liksom negativa psykologiska effekter. Slutligen har såväl konventionella militära medel som väpnade inslag i hybridkrigföringen, exempelvis via ombud, använts för att förstöra energianläggningar och energiråvarutillgångar.

Många av källorna i detta avsnitt fokuserar på (förmodat ryska) angrepp mot Ukraina. Det bör påtalas att källmaterialet endast undantagsvis är vederbörligt vetenskapligt granskat. Med det sagt är det ändå intressant att Ukrainaexemplet kan ses från något olika perspektiv. Å ena sidan kan man anse att det som har hänt i Ukraina inte är direkt överförbarbart som sannolika hot mot den svenska energiförsörjningen givet att en väpnad konflikt faktiskt pågår där. Andra väsentliga skillnader, jämfört med Sverige, är Ukrainas historiska, politiska och geografiska belägenhet. Men å andra sidan finns det bedömare som menar att (de förmodat ryska) aktiviteterna gentemot Ukraina lika väl kan ses som indirekt riktade mot väst. Detta i termer av att Ukraina fungerar som ett slags testlaboratorium för framtida cyberangrepp riktade mot väst och/eller som ett objekt för demonstration av förmågor.[118] Att testa gråzonskrigföring, med syfte

[116] Rühle och Grubliauskas 2015
[117] Slobodian 2016
[118] Greenberg 2017b

att undvika eskalation, är i det avseendet lämpligt gentemot en part man redan befinner sig i eskalerad konflikt med. Eskalationen får då inga egentliga konsekvenser (se Figur 1, avsnitt 2.3).

Vid sidan av pågående konflikter i exempelvis Ukraina och Mellanöstern råder det lyckligtvis brist på aktuell empiri avseende gråzons- och hybridkrigföring gentemot energiförsörjningen eller med hjälp av energi som maktmedel. Ett sätt att ändå belysa den potentiella problematiken är med hjälp av scenarier. Ett exempel är hur ett framtida Europa med ett moderniserat och mer sammankopplat elnät med hög grad av introducering av s.k. smarta elmätare skulle blir mer sårbart och därmed utsatt för nya typer av cyberhot.[119] Ett annat exempel är scenariot ”Sweden under attack!” som utgör ett synkroniserat angrepp på kritisk energi- och informationsinfrastruktur.[120] De enskilda delattackerna i det scenariot medför egentligen inte så särskilt allvarliga konsekvenser – de är för övrigt baserade på öppet dokumenterade inträffade incidenter – men när de inträffar skräddarsytt och synkroniserat blir effekterna på samhällets funktionalitet mycket stora. Ytterligare ett scenarioexempel, ”Typfall 5”, diskuteras i nästföljande avsnitt.

4.2 Diskussion om energisektorns utmaningar baserat på Typfall 5: Utdragen och eskalerande gråzonsproblematik

På uppdrag av MSB har FOI utvecklat ett antal så kallade typfall som grund för planering för civilt försvar.[121] Det senaste femte typfallet är ett scenario som illustrerar en utdragen och eskalerande gråzonsproblematik. Typfallet belyser ett förlopp som skulle kunna leda till ett så kallat skymningsläge, dvs. en konfliktsituation där nästa steg kan förväntas vara öppna stridshandlingar.

Det råder i scenariot en ansträngd säkerhetspolitisk situation i närområdet men det föreligger inledningsvis inget direkt konkret militärt hot mot Sverige som motiverar höjd beredskap. De inledande händelserna innebär en rad utmaningar för samhället i termer av cyberangrepp i mindre skala, sabotage och påverkad information. Propaganda och desinformation sprids samtidigt som underrättelseverksamheten ökar i Sverige. Med tiden innebär de upprepade infrastrukturella störningarna en ökad samhällsbelastning över en rad sektorer samt upplevd otrygghet bland befolkningen.

När situationen eskalerar ytterligare via intensiva påverkanskampanjer, fartygsrelaterade olyckor och omfattande cyberangrepp är samhällsutnötningen

[119] Paillard 2017
[120] Schmidt-Felzmann 2016
[121] Lindgren 2014; Jonsson 2018

påtaglig. Försörjningssystemen fungerar inte, påtryckningar och hot sker mot beslutsfattare och rädslan bland befolkningen gör att många lämnar städerna medan andra reser från Sverige.

Händelseförloppet är tämligen utdraget i tid, drygt nio månader, och de säkerhetspolitiska spänningarna i närområdet ökar över tiden för att i scenariots avslutande faser inbegripa begränsade stridshandlingar i något av de nordisk-baltiska grannländerna. Givet att den säkerhetspolitiska situationen är ansträngd och eskalerar mot en eventuell regional konflikt skulle syftet exempelvis kunna vara att lamslå svenskt beslutsfattande, att få Sverige att avbryta bilaterala och internationella samarbeten, att förhindra att Sverige tar emot tredje part, samt att skapa handlingsutrymme för ett militärt ingripande mot Sverige eller något nordiskt-baltiskt grannland. De parallella utmaningarna att hantera störningar, klargöra läget, återställa samhällets funktionalitet och mildra de negativa effekterna av störningarna, liksom att förstå antagonistens mål, karaktäriserar denna typ av scenario. Händelseförloppet i sin helhet återfinns i denna rapports bilaga.

Vilka utmaningar innebär då ett sådant scenario för energibranschen liksom närmast ansvariga myndigheter?[122]

För det första så sker olika slags cyberangrepp och fysiska sabotage mot energiförsörjningens olika delar i princip över hela scenarioförloppet. Inledningsvis handlar det främst om angrepp mot lokala försörjningssystem, vilket exempelvis skulle kunna vara fjärrvärme och avgränsade delar av elförsörjningen. Störningar och avbrott innebär givetvis alltid någon slags utmaning för de aktörer som ansvarar för att upprätthålla funktionalitet. Samtidigt finns det inget i denna inledande del av scenariot som borde innebära problem avseende att få tillgång till teknisk personal och reparationsmateriel. En kanske större utmaning är att få energibranschens aktörer att förstå och sätta de olika enstaka incidenterna i ett större sammanhang och agera utifrån den kunskapen, exempelvis att skärpa säkerhetsrutiner och öka bevakningen. Givet att underrättelseinhämtningen mot landet som helhet ökar krävs vaksamhet och kanske även förändrade säkerhetsarrangemang för enskilda objekt i energisystemen liksom för nyckelpersoner i energisektorn.

Upprepade störningar över tid är givetvis belastande men så länge som den negativa säkerhetssituationen inte har eskalerat ytterligare medför det sannolikt inte heller i detta senare skede några större problem avseende personaltillgång. Däremot kan skenande kostnader vara en stor belastning för somliga aktörer som i slutändan kan komma att påverka försörjningstryggheten. Det kan också vara så

[122] De utmaningar som uppstår för civilbefolkningen, Försvarsmakten och övriga samhällsviktiga funktioner, som en följd av energibortfall och -störningar beskrivs översiktligt i Jonsson 2018, avsnitt 2.3-2.5.

att det börjar bli brist på vissa typer av reparationsmateriel, beroende på vad som har varit de specifika målen för angreppen/sabotagen.

Att informationsmiljön och människors psykologi påverkas i detta scenario kan innebära indirekta effekter på energiområdet som är ganska svåra att förutse. Ökad oro skulle exempelvis kunna leda till hamstring av drivmedel och andra bränslen i ett rätt så tidigt skede av händelseutvecklingen.

Med tiden ökar belastningen på försörjningsystemen, inte minst för el och drivmedel. Eftersom även Sveriges grannländer är drabbade måste det antas att det börjar råda brist på såväl teknisk personal som reparationsmateriel. Även om enskilda privata aktörer i detta skede säkert gör allt de kan för att återställa funktionalitet får man anta att behovet av övergripande samordning och prioriteringar är mycket stort, vilket ytterst faller på ansvariga myndigheter.

I detta skede sker också antagonistisk påverkan på det internationella planet, exempelvis via vissa EU-länder, vilket indirekt kan påverka svensk energiförsörjning. Det kan exempelvis handla om svenska energiföretags möjlighet till utländska underentreprenörers tjänster, enskilda utländska kompetenser eller inköp av nödvändiga komponenter. I det internationella sammanhanget – där även andra länder än Sverige är drabbade av gråzonsaktiviteter – skulle man också kunna tänka sig en situation där energi blir en säkerhetspolitisk bytesvara mot något Sverige i denna situation uppfattar sig sakna, t.ex. vissa militära resurser eller garantier om militärt stöd i utbyte mot ökad svensk export av el eller drivmedel (trots egen bristsituation).

I typfallets senare skeden påverkas energiförsörjningen svårt. Incidenter och sabotage gentemot fartyg och hamnar påverkar främst drivmedelsförsörjningen och omfattande cyberangrepp i kombination med fysiska sabotage skulle kunna innebära ett storskaligt nationellt/nordiskt elavbrott under en tid. En sådan händelse skulle under alla omständigheter innebära en stor utmaning för såväl hela samhället som energiaktörerna. Att detta också sker under vad man får utgå ifrån är störda förhållanden förstärker denna utmaning. Med störda förhållanden avses i detta sammanhang dels att även andra infrastruktursystem, t.ex. telekommunikationer och transport, är drabbade, dels att även grannländerna är drabbade, dels att antagonisten kanske avser att försvåra återställningsarbetet genom exempelvis upprepade cyberangrepp eller åtgärder som hotar reparationspersonalens liv och hälsa, t.ex. minering av kraftledningsgator.

I scenariots slutliga skede är rädslan bland befolkningen stor. Hur enskilda personer agerar i en sådan här krissituation är det svårt att spekulera i. Om många människor lämnar städerna för landsbygden skulle det, åtminstone teoretiskt sett, kunna innebära att det är svårt att möta efterfrågan av el, drivmedel och bränslen, vars försörjningssystem är designade utifrån normallägets tämligen urbaniserade demografi. Att prioritera sin egen och sin familjs fysiska säkerhet framför sina arbetsuppgifter är i många avseenden ett förståeligt beteende. Men det får

naturligtvis negativa återverkningar inom såväl energiaktörernas som övriga samhällsaktörers verksamheter.

Scenariot avslutas med att antagonisten erbjuder Sverige bistånd i form av bl.a. drivmedel, reparationsmateriel och teknisk personal, och i synnerhet till vissa hårt drabbade kommuner vid Östersjökusten. Denna situation illustrerar, på ett kanske något övertydligt sätt, ett avvägningsdilemma mellan humanitära aspekter och samhällsfunktionalitet, å ena sidan, och säkerhetspolitiska och militärstrategiska risker, å andra sidan. En rimlig slutsats är att ett sådant beslut varken kan eller bör fattas av enskilda kommuner eller energibranschaktörer.

4.3 Diskussion om gråzonshot baserat på information från svenska branschaktörer och myndigheter

Den översiktliga gråzonshotbilden för energiområdet kompletteras i detta avsnitt med information från svenska branschaktörer och myndigheter. Detta avsnitt inleds med en diskussion om behovet av att bejaka informationsspridning men samtidigt hantera sekretess, följt av en beskrivning av den metod som har tillämpats i denna rapport för att åstadkomma detta. Därefter diskuteras hot och sårbarheter, bl.a. utifrån olika perspektiv på marknad, aktörer, teknik och individer.

Som tidigare har beskrivits, ska den sammantagna hotbilden kunna fungera som ett diskussionsunderlag för energisektorns olika aktörer liksom hur närmast berörda bevakningsansvariga myndigheter ska inrikta omvärldsbevakningen. Avsnittet utgör ett av flera underlag inför planering av energiberedskapsåtgärder och bör betraktas som ”work in progress”. Ny kunskap om gråzonshot genereras, liksom nya indikationer ackumuleras, kontinuerligt över tiden. För en enskild aktör utgör indikationer och observationer endast en delmängd av den sammantagna hotbilden. Det finns därför ett behov av att tillgängliggöra mer sammantagen information för att öka medvetenheten om hotbilden hos berörda aktörer, vilket i sin tur kan bidra till såväl förbättrade skyddsåtgärder som ytterligare observationer.

Att identifiera och medvetandegöra antagonistiska hot och relaterade sårbarheter medför ett särskilt dilemma vad gäller informationshantering. Att höja medvetandet om hoten hos berörda aktörer är en grundförutsättning för att överhuvudtaget kunna gå vidare mot etablering av skyddsåtgärder. Detta kräver ett visst mått av öppenhet. Samtidigt kan en öppen identifiering av olika hot leda till att den potentielle antagonisten förbättrar sina metoder eller väljer andra mål för angrepp.

Inom exempelvis cyberspionaget kan man se att antagonisternas metoder utvecklas ett steg före skyddsåtgärderna. När skyddsåtgärder för ett objekt

genomförs så förändras antagonistens tillvägagångssätt. Det kan exempelvis handla om att när en viss aktör ökar skyddet för vissa system så väljer antagonisten att istället söka sårbarheter hos underleverantörer för att därigenom få en väg in i systemen.

Att öka förståelsen för hur system kan påverkas samt hur de potentiellt påverkar varandra är givetvis viktigt. Men det kan också vara en poäng att utåt sett visa att vi gör dessa analyser – att visa att vi har kunskap om vårt eget samhälle, är medvetna om våra sårbarheter och att vi aktivt arbetar med dem. Det kan sända tröskelhöjande signaler gentemot antagonisten men samtidigt medför det då, som sagt, en risk för att denne börjar använda mer sofistikerade metoder.

Ökad öppenhet och kunskapsspridning om aktuella hot ligger i tiden och är något som också försiktigt bejakas av de svenska säkerhets- och underrättelsetjänsterna, liksom behovet av att möta hot genom myndighetssamverkan.[123] Det handlar om balansgången mellan behovet av kunskapsspridning och risken att röja arbetsmetoder, källor, det sammantagna kunskapsläget och våra åtgärder för att reducera såväl hot som sårbarheter. Ett exempel på motsvarande balansgång är redovisningarna av Försvarsmaktens perspektivstudiearbete, som består av såväl öppna som hemliga delar.

4.3.1 Metod för balansgång mellan sekretess och öppenhet

I det följande kommer ett antal exempel på gråzonshot och underliggande problematik att diskuteras. Informationen kommer ursprungligen från ett antal olika myndigheter och aktörer inom energibranschen. Exakt vilka dessa källor är anges inte i denna öppna rapport eftersom angivna exempel skulle kunna sammanlänkas med inträffade aktörsspecifika händelser, ge en indikation om vilka iscensatta hot eller tester avseende förmågor som inte har upptäckts, eller ge en alltför tydlig bild av specifika befintliga sårbarheter.

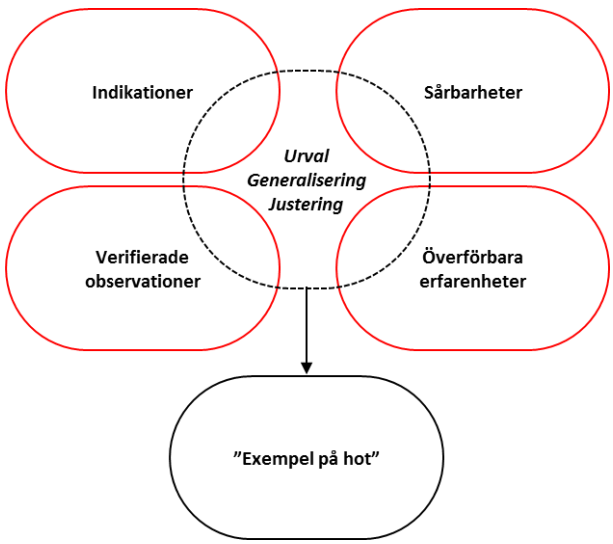
I den metod som används här, för att hantera sekretess och samtidigt bejaka kunskapsspridning, anges exempel från ursprungligen fyra kategorier (förknippade med olika grader av sekretess, alternativt öppen information):

- Inträffade händelser i form av indikationer, dvs. man ser att något har hänt men har ingen tydlig helhetsbild avseende exempelvis om det är en medveten handling eller inte, vilket syftet är eller vem som egentligen ligger bakom.
- Inträffade händelser i form av verifierade observationer, dvs. man har en hyfsat klar bild av vad som har hänt, eller händer, och vem antagonisten med hög sannolikhet är.

[123] Se t.ex. Säkerhetspolisens årsbok 2016 (utgiven mars 2017)

- Tänkbara potentiella hot baserade på bedömda befintliga och framtida sårbarheter.
- Tänkbara potentiella hot baserade på överförbara erfarenheter i andra relevant jämförbara system, sektorer eller länder.

Vilka exempel eller resonemang som tillhör vilken kategori anges av sekretesskäl inte. Det ursprungliga insamlade underlaget är att betrakta som delvis hemligt men ingen enskild hemlig uppgift förekommer i denna rapport.[124] Detta säkerställs genom att generalisera och/eller justera exempel så dessa inte kan kopplas till specifika händelser, förhållanden, aktörer eller system. Vidare görs urvalet av exempel med hänsyn till dels att man inte ska kunna skapa sig en helhetsbild av befintlig kunskap, dels att den sammantagna diskussionen i sig, ska kunna vara öppen. Se principskiss Figur 3.



Figur 3. Metod för urval av exempel på hot, med hänsyn till sekretess.

Texten som följer utgör därmed generaliserade beskrivningar av ”exempel på hot” liksom de allmänna omständigheter som skapar förutsättningar för att realisera hot (snarare än konkreta sårbarheter, såvida de inte är allmänt uppenbara). Läsaren kan uppleva viss frustration på grund av brist på konkretion, tydlighet, avsaknad av helhetsbild och att det inte går att utläsa om exempel utgör verkliga händelser eller endast tänkbara hot, vilket dock är nödvändigt med hänsyn till sekretess.

[124] Texten har innan publicering genomgått en vederbörlig sekretessbedömning.

4.3.2 Hot, sårbarheter och marknadsförutsättningar

Givet insamlade indikationer och observationer av gråzonsaktiviteter skulle man kunna hävda att vi redan idag befinner oss i gråzonen men samtidigt är detta långt ifrån det som förknippas med en eskalerad gråzonsproblematik, motsvarande exempelvis den problematik som beskrivs i Typfall 5 (se föregående avsnitt 4.2). Eftersom den diskussion som förs i detta avsnitt i första hand baseras på empiri från nuläget så bör aktiviteter som exempelvis underrättelseinhämtning, infiltration, cyberhot och marknadspositionering främst förstås som gråzonsaktiviteter på en lägre nivå. Det kan handla om förberedelser inför en *eventuell* eskalerad gråzonssituation (eller väpnad konflikt), dvs. skapa förutsättningar för ett framtida agerande. Det kan också handla om att testa, öva eller demonstrera förmågor till gråzonskrigföring (se Figur 1, avsnitt 2.3).

Det finns olika sätt att karakterisera och kategorisera hot och gråzonsaktiviteter. Översikten över exempel på gråzonshot i avsnitt 2.4 sorterar olika medel i diplomatiska, politiska, ekonomiska, psykologiska, militära etc. När man studerar en enskild sektor finns behov av mer konkretion samtidigt som det blir mer uppenbart att hoten och dess effekter hänger ihop. Exempelvis kan underrättelseinhämtning vara en förberedelse för ett fysiskt intrång där viss utrustning ansluts i syfte att skapa förutsättningar för ett framtida cyberangrepp som i sin tur leder till ett fysiskt sabotage av någon anläggning som medför psykologiska effekter hos befolkningen men också kan fungera som ett indirekt hot mot Sverige som i slutändan kan påverka politiskt beslutsfattande. Exemplet ger också insikten att teknisk säkerhet långt ifrån bara handlar om teknik.

En mer avgränsad indelning av gråzonsaktiviteter är att betrakta underrättelseverksamhet, sabotage, terrorism, övrig kriminalitet och subversion som de primära säkerhetshoten. Dessa kan i sin tur leda till en rad olika effekter (snarare än att se dessa som hot i sig), exempelvis ekonomisk belastning, avbrott i försörjningssystem, social oro och ”vanlig” kriminalitet, befolkningens förtroende för myndigheter eller påverkan på beslutsfattare.

Eftersom underlaget till detta avsnitt till stor del härrör från aktörer inom energisektorn hamnar därmed fokus av naturliga skäl på hot mot just deras verksamheter. Men energi kan som tidigare beskrivits både vara ett mål och ett medel i en konfliktsituation, t.ex. ett medel för att påverka den politiska debatten. Ett exempel skulle kunna vara att en antagonist har som mål att främja splittring i svensk politik genom att sätta en fråga med polariserande potential på agendan, exempelvis kärnkraftens vara eller icke vara. Om denne då placerar något radioaktivt material i anslutning till ett kärnkraftverk, som uppmäts och upptäcks, så skulle det kunna väcka liv i debatten utan reell anledning. Här finns också möjlighet för antagonisten att underblåsa debatten via ryktesspridning, desinformation och stöd till politiska grupperingar. Frågan skulle stjäla utrymme från andra politiska frågor och potentiellt kunna påverka utgången av ett val.

I det följande diskuteras hot, sårbarheter och förutsättningar för dessa utifrån följande rubriker:

- Marknadsprinciperna ger förutsättningar för såväl funktionalitet som sårbarhet
- Ägarskapsförhållanden som kan ge antagonistiskt inflytande över kritisk infrastruktur
- Underleverantörsberoendet skapar olika sårbarheter
- Marknadskonkurrens eller antagonistiskt agerande?
- Tekniska och fysiska hot av olika karaktär men med liknande effekter
- Metoder för intrång i informations-, drift- och styrsystem
- Standardisering är ett verktyg för ökad säkerhet som också kan innebära potentiella sårbarheter
- Digitaliseringen kan medföra sårbarheter via ogenomtänkt outsourcing och alltför snabbt införande av nya applikationer
- Infiltration, insiders och annan underrättelseinhämtning

Marknadsprinciperna ger förutsättningar för såväl funktionalitet som sårbarhet

I vår öppna samhällskonstruktion finns inbyggda förutsättningar för realiserandet av vissa hot. Det handlar bl.a. om bejakandet av näringsfrihet, den fria äganderätten liksom övriga villkor för affärsverksamhet.

En marknad är alltid utsatt för ett maktspel och syftet med att försöka påverka en marknad kan vara olika, t.ex. att kortsiktigt höja priset på vissa energiråvaror, att ackumulera kapital eller att skapa strategiska fördelar inför en mer ansträngd säkerhetspolitisk situation. Man kan, oavsett vilken påverkan man talar om, konstatera att energimarknaderna är ”lämpliga” mål för att i slutändan kunna påverka politiskt beslutsfattande eftersom energins centrala roll i det moderna samhällets funktionalitet är odiskutabel.

De internationella marknadsprinciperna är i någon mening överordnade nationell lagstiftning. Utländskt inflytande över svensk strategisk infrastruktur är idag oundvikligt. Ett totalförsvarsperspektiv handlar ändå om någon slags strävan efter oberoende – att ha egen förmåga att upprätthålla de viktigaste samhällsfunktionerna. Fungerande samhällsfunktioner förutsätter fungerande försörjningssystem, inte minst för energi. Försörjningssystemen levererar om marknaderna fungerar och inte alltför enkelt kan påverkas på ett otillbörligt sätt.

Ett trivialt konstaterande är att strävan efter oberoende inte kan drivas av de enskilda privata energimarknadsaktörerna utan att frågan ligger på betydligt högre nivå. De enskilda företagen har en viktig roll i totalförsvaret men huvuddelen av själva ansvaret kan inte läggas över på dem.

Ägarskapsförhållanden som kan ge antagonistiskt inflytande över kritisk infrastruktur

En fungerande marknad kräver konkurrens för att vara effektiv. Därmed ska marknaden vara öppen för alla relevanta aktörer. Marknadsfriheten gäller således i högsta grad även frihet avseende ägande och ägarskapsförhållanden.

Ägandet av kritisk infrastruktur har sedan 1990-talet i allt större grad förflyttats till privata aktörer. Detta har setts som en naturlig del av den pågående omregleringen av bland annat elmarknaden. På senare tid har kontrollen av den kritiska infrastrukturen i allt högre grad pekats ut som en potentiell riskfaktor som kan utnyttjas för att påverka ett annat land såväl i krig som i ett gråzonsläge. Antagonistiskt inflytande genom ägande via ombud skulle kunna innebära att beslut tas på företagsekonomisk grund som kan minska elnätets resiliens. På motsvarande sätt kan ett sådant ägande också fungera som ett potentiellt politiskt påverkansmedel.

Nya ägarskapsförhållanden behöver inte vara något problem men kan skapa svårigheter vad avser exempelvis tillsyn. Trenden av ”finansifiering” och att ”värdepapperisera” tillgångar gör att ansvariga myndigheter kan få svårt att både möta och identifiera en relevant motpart. Det kan exempelvis röra sig om utländska pensions- och värdepappersfonder eller riskkapitalbolag som investerar i en mindre andel av ett elnät. Ett annat problem är att ägandet kan anonymiseras via olika bolagskonstruktioner som är kopplade till varandra. Det är främst i det fallet det kan finnas oro för att det bakom ägandet skulle kunna finnas en potentiell antagonist som vill skapa handlingsutrymme inför en eventuell konfliktsituation. Det skulle exempelvis kunna gälla bolag med skyldighet att beredskapslagra en viss mängd oljeprodukter.

Nya ägarförhållanden avseende infrastruktur tillhör normala förändringar inom energiområdet. I affärslogiken ingår det ofta att bjuda in fler parter vid ett uppköp, t.ex. riskkapitalister, med syfte att dels sprida risker, dels att få möjliga framtida samarbetsparter. Det handlar om att skapa strategiska allianser, vilket kan manifesteras i exempelvis delägarskap i kraftverksanläggningar. Gemensamma affärer är nätverksbyggande och skapar såväl förtroendebaserade som företagsekonomiskt motiverade beroenden i termer av riskdelning och försäkran om framtida stöd, vilket i sin tur gynnar försörjningstryggheten men medför också vissa risker. Ett från början rent affärsmässigt samarbete med en viss aktör skulle på sikt kunna utvecklas till något annat.

Underleverantörsberoendet skapar olika sårbarheter

I hotbildssammanhang associeras i regel riskerna med utländskt inflytande över samhällskritisk infrastruktur med större anläggningar och infrastruktursystem. Dessa system baseras på såväl komponenter som kompetenser som de enskilda aktörerna inte själva tillverkar eller innehar, oavsett om de är svenska eller inte.

De potentiella problemen med inflytande handlar således inte bara om ägarskap utan även om underleverantörer av komponenter, hårdvara och teknikstöd. Idag råder en globaliserad komponent- och underleverantörsmarknad som aktörerna behöver ha legala och organisatoriska medel för att kunna hantera.

Ett elbolag i Sverige, exempelvis, köper en modul från ett större och väletablerat utländskt företag, som består av komponenter som tillverkas i en fabrik i ett tredje land, som innehåller integrerad datorkod från en mjukvaruleverantör i fjärde land, som i sin tur skrivits av programmerare i ett femte land. Kedjereaktionen till följd av det svenska elbolagets inköp av utrustning, och därtill följande potentiella säkerhetsrisker, är svår att överblicka.

Det finns en uppenbar målkonflikt mellan underleverantörsberoende och säkerhetsskydd. Det handlar bland annat om att bolag som lämnar offerter kan tänkas göra det enbart för att inhämta information utifrån upphandlingsunderlaget, som exempelvis innehåller kravställningar som kan beröra nivåer av säkerhetsskydd eller kritiska systemfunktioner. Den typen av agerande behöver dock inte ha ett bakomliggande antagonistiskt motiv utan kan lika väl handla om kommersiella aktörers omvärldsbevakning. Affärslogiken handlar om att få det som motsvarar ens uppställda krav för ett så lågt pris som möjligt. Där är det mycket svårt att avgöra om offererande aktör drivs är rena affärsintressen eller om det skulle kunna finnas andra bakomliggande syften.

Entreprenörer som de svenska energiaktörerna är beroende av kommer ofta från andra länder. Det gäller inte minst den tekniska personal som behövs vid återställande av raserad nätinfrastruktur. I en eskalerad situation är det rimligt att anta att det blir konkurrens om dessa resurser och kanske till och med att företagen ”drar hem” personal om hotfulla omständigheter råder. Men företagen skulle också kunna bli ”tvingade hem”, antingen av företagets hemlands myndigheter eller av företagets ägare (med kopplingar till antagonisten).

Marknadskonkurrens eller antagonistiskt agerande?

Det som komplicerar förståelsen för om ett visst agerande ska ses som marknadskonkurrens eller ett antagonistiskt agerande är att på marknaden finns inga ”motståndare” utan alla är marknadsaktörer, dvs. konkurrenter och samarbetspartners. Det som ytterligare komplicerar denna förståelse är att ett visst agerande i nuläget inte alls behöver ses som ett hot men att agerandet skapar förutsättningar för iscensättandet av hot i en framtid som befinner sig längre upp på gråskalan. Det innebär att potentiella ombud för framtida gråzonsaktiviteter i dagsläget kanske inte alls är medvetna om att de är tilltänkta ombud. Det kan exempelvis handla om nya ägarskapsförhållanden, uppköp av infrastruktur eller etablering av leverantörsberoenden. Detta kan ses som fullt rimliga marknadsageranden som görs i vinstdrivande syften men också som aktioner med syfte att understödja en framtida avancerad gråzonskrigföring där en

samarbetspartner kan utsättas för påtryckningar att agera som antagonistiskt ombud.

Ökat potentiellt antagonistiskt inflytande över strategisk infrastruktur i form av direkt eller indirekt ägarskap över produktions-, distributions- eller driftsresurser som medför ett starkt beroendeförhållande kan ses som en förberedelse för en eskalerad gråzonskonflikt. Detta kan också omfatta påverkan via tredje land och skapa förutsättningar för att få bättre effekt av annan otillbörlig marknadspåverkan.

Det finns givetvis en risk för en överdriven alarmism och att man helt i onödan misstänkliggör marknadsaktörer med koppling till vissa stater. Oron kan kanske ses som mer befogad om ett specifikt marknadsagerande förefaller uppenbart märkligt utifrån kommersiella grunder. Kommersiella aktörer som ger sig in i rena förlustaffärer, t.ex. ägande och drift av infrastruktur med dåliga affärsförutsättningar, skulle kunna ha en underliggande agenda som motiverar ett sådant ologiskt agerande. Men det behöver inte vara så – dåligt underbyggda investeringsbeslut och bristande affärsmannaskap kan lika gärna vara förklaringen.

Därutöver finns uppenbara skillnader mellan olika länders marknadsvillkor, politikens inflytande över näringslivet samt vad som betraktas som nationella intressen. I en mer eskalerad gråzonssituation är det inte orimligt att anta att krav kan ställas på vissa fullt fungerande och vinstdrivande marknadsaktörer, med kopplingar till fientlig stat, att bli ombud för gråzonskrigföring.

Tekniska och fysiska hot av olika karaktär men med liknande effekter

Tekniska hot såsom olika former av cyberhot särskiljs ibland från fysiska sabotage. Men även digitala medel kan användas för att åstadkomma fysiska sabotage, exempelvis genom att ta över styrningen av systemkomponenter och överbelasta dessa. Hoten hänger ihop, inte minst också för att hot om sabotage, eller cyberangrepp, kan vara ett medel för ekonomisk utpressning eller för att försöka påverka svensk politik och svenskt beslutsfattande.

För att kunna genomföra fysiska sabotage kan underrättelseinhämtning på förhand krävas. En sådan inhämtningsoperation kan också kombineras med tester av den utsatta aktörens beredskap, exempelvis genom att dölja en sådan inhämtning som ett inbrott eller en stöld. Att hoten hänger samman förstås också genom att ett fysiskt intrång kan göras med det bakomliggande syftet att få tillgång till informationssystem eller skapa framtida förutsättningar för detta. Inbrott där ingenting har stulits eller stölder av utrustning eller material (t.ex. kopparkablar) som sedan dumpas skulle kunna indikera ett underliggande antagonistiskt syfte. Även det som i förstone ser ut som simpel skadegörelse men som vid närmare undersökning ser ut att ha gjorts med en precision som kräver

tekniska kunskaper kan vara en motsvarande indikation, vilket då är liktydigt med ett riktat sabotage.

Samtidigt finns det väsentliga skillnader mellan digital och fysisk antagonism. Det finns anledning att tro att många stater har sänkt ribban för när genomförandet digitala angrepp kan motiveras, medan man fortfarande drar sig för att göra fysiska angrepp, inte minst på grund av risken att ertappas och identifieras. Möjligheterna att använda ombud, t.ex. hackergrupper, kan ses som större vid digitala angrepp jämfört med vid fysiska angrepp, vilket ger en helt annan möjlighet för fientligt sinnad stat att förneka inblandning.

Vidare kan ett digitalt angrepp inledas via ett intrång i en liten anläggning men sedan skalas upp mot större anläggningar när man väl befinner sig inom systemet. Dessutom kan angreppet ske från vilken plats som helst på jorden. För att nå samma effekt med ett fysiskt angrepp måste man som antagonist inte bara vara på plats (eller använda kinetiska fjärrstridsmedel) utan måste också gå direkt på de stora anläggningarna, som i regel åtnjuter en högre skyddsnivå.

Detta knyter an till vad som bör betraktas som ”skyddsvärt” – att inte ensidigt fokusera på skyddsvärden i formen av enskilda objekt utan snarare på funktionalitet. En enskild mindre delkomponent, betraktas kanske inte som ett objekt med särskilt skyddsvärde. Ett större kraftverk ses däremot självklart som något skyddsvärt. Men ett stort antal av dessa mindre delkomponenter i ett distribuerat system, från samma tillverkare med samma inbyggda sårbarheter och möjligheter till fjärrstyrning, som hackas samtidigt kan sammantaget vara liktydigt med att slå ut ett kraftverk. Definitionen av vad som är skyddsvärt bör därför omformuleras.

Metoder för intrång i informations-, drift- och styrsystem

Cyberhoten och andra IT-relaterade hot kan ha olika ofta sammankopplade syften, t.ex. att förstöra komponenter, få åtkomst till styrsystem, orsaka avbrott, inhämta information, plantera skadlig mjukvara, exempelvis s.k. malware eller ransomware. Olika medel för detta är exempelvis;

- Att hacka sig in i system utifrån på distans
- Att efter fysiskt intrång koppla upp sig på utrustning och därefter hacka sig in
- Att utnyttja redan färdighackad utrustning som aktören har köpt och installerat
- Att infiltrera organisationen med personer som får access till system
- Att utnyttja personer med befintlig access till system.

Det två sistnämnda punkterna, som omfattar mer individrelaterade frågor, diskuteras mer utförligt nedan. Att utnyttja redan färdighackad utrustning, dvs.

korrupt hårdvara diskuterades ovan i samband med beroendet av underleverantörer.

Oavsett väg in i systemen och vad syftet med intrånget är, så finns en rad uppenbara generella sårbarheter att exploatera.

Standardisering är ett verktyg för ökad säkerhet som också kan innebära potentiella sårbarheter

Standardiseringstrenden berör allt ifrån fysiska komponenter, till operativsystem i kontorssystem, till särskilda programmoduler. I begynnelsen av digitaliseringen utvecklade ofta företag egna individuellt anpassade system liksom egen datorkod (med eller utan hjälp av konsulter), för exempelvis nätstyrning. Det är inte ekonomiskt rationellt att arbeta så idag. Det innebär att många aktörer idag använder samma typ av systemlösningar som, å ena sidan, medför kollektiv säkerhetsnytta när systemen kontinuerligt förbättras men, å andra sidan, att gemensamma kvarstående, eventuellt ännu inte identifierade, sårbarheter kan exploateras.

Standardisering av IT-säkerhetsarkitektur är något positivt och bedrivs ofta som ett led i kvalitetsarbete som syftar till att skapa mer homogena och tillförlitliga systemlösningar. Ökad tillförlitlighet och bred användning av väl beprövade säkerhetslösningar är rationellt. Den potentiella sårbarheten som standardiseringen ändå innebär ligger mer på samhällelig nivå eftersom eventuella säkerhetsluckor finns hos många aktörer. Skadlig mjukvara som distribueras brett kan därmed få stora samhälleliga skadeverkningar när den aktiveras i olika system hos olika aktörer som använder samma IT-säkerhetsstandard eller samma typ av administrativa stödsystem (se exemplet i avsnitt 4.1, från Ukraina 2017, där en skadlig datamask spreds via ett visst bokföringssystem).

Digitaliseringen kan medföra sårbarheter via ogenomtänkt outsourcing och alltför snabbt införande av nya applikationer

Till det tekniska perspektivet hör också att den ökade digitaliseringen kräver en utvecklad typ av specialistkompetens som energiföretagen inte alltid har möjlighet att integrera i den egna verksamheten. I linje med strävan mot ökad effektivisering genom specialisering, inom såväl energiområdet som i de flesta andra branscher, anlitas istället konsulter och underleverantörer. Dessa löser inte bara väldefinierade tekniska problem enligt detaljerade beställningar utan tar i olika hög grad ansvar för viss funktionalitet över tid. Man kan därmed säga att delar av elförsörjningen outsourcas. Detta riskerar att minska elleverantörernas insyn och kompetens vad gäller säkerhetsfrågor och försvåra ansvariga myndigheters tillsyn, i synnerhet om utländska underleverantörer anlitas.

Styr- och driftsystemen anses oftast som det mest skyddsvärda för att kunna upprätthålla leveranssäkerhet. Sammankoppling av olika datorsystem utgör därmed en potentiell säkerhetsrisk. När kontorssystem, med lägre skydds- och säkerhetskrav, direkt eller indirekt sammankopplas med styr- och driftsystem kan det fungera som en väg in för att direkt påverka försörjningssystemen.

I det sammanhanget är också risken för intrång via nya applikationer relevant. Det gäller exempelvis de nya smarta elmätarna. Detta är inte bara en teknisk fråga. Även om leverantörerna av elmätarna lyckas etablera en tillfredställande säkerhetsnivå avseende exempelvis kryptering så blir säkerheten beroende av hur dessa kommer att användas. De framtida möjligheterna till fjärrstyrning och informationsinsamling kan skapa nya säkerhetsrisker. Vidare finns en risk vid själva installationen av elmätarna som görs av underleverantörer, som då måste få tillgång till kryptonycklarna. I takt med att fler och fler nya elmätare installeras har underleverantörerna åtminstone i dagsläget svårt att täcka behovet av installationspersonal, vilket medför att de rekryterar personal eller anlitar bemanningsföretag utanför Sverige.

Outsourcing utgör i sig inget problem. Om outsourcing leder till att energileverantörerna förlorar överblicken över de egna systemens säkerhetsarrangemang, som de ansvarar för, så är det däremot problematiskt. Nya applikationer är i sig inte heller något problem. Problemet är om ny och omogen teknik implementeras alltför snabbt utan att ha utsatts för tillräcklig riskanalys och testning.

De hot som teknikutvecklingen medför ligger i mångt och mycket utanför energibranschaktörernas kontroll och kompetens. Aktörerna är i första hand tekniktillämpare medan många hot har sitt ursprung på teknikutvecklingssidan. Därvidlag skulle aktörerna kunna betraktas som beställare snarare än ”aktörer”. Hoten i tillämpningskedjan handlar i högre grad om medvetna eller omedvetna mänskliga handlingar.

Infiltration, insiders och annan underrättelseinhämtning

Personer på insidan av en verksamhet som agerar på annans uppdrag, s.k. insiders, kan utgöra ett hot mot en energibranschaktörs verksamhet på olika sätt, t.ex. inhämtning av information som berör systemfunktionalitet och sårbarheter, förberedande av fysiskt sabotage eller cyberangrepp samt kartläggning av nyckelpersonal.

Det behöver inte bara handla om insiders som söker fast anställning på företagen utan även praktikanter, tillfälligt sommaranställda och examensarbetare, som exempelvis kan utgöras av gäststudenter från utlandet. Detta gäller även underentreprenörer, leverantörer av utrustning och andra kommersiella samarbetspartners till den primärt berörda aktören.

Det har tidigare beskrivits att utländska företag, som svenska företag samarbetar med, teoretiskt sett skulle kunna utsättas för påtryckningar av hemlandets myndigheter i syfte att ge samarbetet en ny agenda, trots att de inledningsvis hade rent kommersiella intressen. På motsvarande sätt kan även enskilda individer utsättas för påtryckningar och därmed bli insiders även om det egna syftet inte var det från början. Att undvika dessa typer av hot, exempelvis via säkerhets- och bakgrundskontroller, är ingen lätt uppgift för de svenska aktörerna, som dels behöver kompetent personal oavsett var de kommer ifrån, dels inte vill bli förknippade med någon slags diskriminering. Och givetvis kan en insider också ha svenskt ursprung.

Insiders kan skapa sig möjligheter till underrättelseinhämtning som kanske inte är möjlig på annat sätt men inhämtning kan också ske via synbart legitima tillvägagångssätt såsom exempelvis inbokade studiebesök på anläggningar eller oanmälda besök av ”allmänt intresserade”. Det kan också handla om arrangerade affärsmöten där man ger sken av att vara intresserade av framtida samarbeten men egentligen har syftet att inhämta information om exempelvis företagets system, teknik, säkerhetsnivåer, arbetsrutiner och nyckelkompetenser.

Antagonistisk kartläggning av nyckelpersonal är det svårt att skydda sig emot såsom samhället ser ut idag och givet all personlig och professionell information som finns tillgänglig via öppna källor. Dessutom kan vissa brister i säkerhetsmedvetenhet inom organisationerna medföra att synbart trivial information om anställda lämnas ut eller synliggörs på hemsidor. Vidare underlättas personkartläggning av webbtjänster såsom Facebook och LinkedIn, som också kan användas för att söka bilateral kontakt. Kontaktsökande kan också ske via direkta inbjudningar till, eller vid medverkan i, konferenser, kurser, utbildningar och andra professionella forum. Personkartläggningens specifika syften kan man bara spekulera i men skulle kunna ses som förberedelser inför riktad påverkan eller planering, alternativt iscensättande, av något annat slags hot.

Energisektorn är kunskapsintensiv. Branschaktörerna behöver en rad specifika kompetenser och förmågor för god funktionalitet och rationell utveckling på en konkurrensutsatt marknad. Därmed utgör kompetent personal (gärna med internationell erfarenhet), liksom kostnadseffektiva underleverantörer och underentreprenörer, nödvändiga förutsättningar för företagens framgång. Ett problem är att det inte är möjligt att genomföra säkerhetsprövning och registerkontroll på personal som inte bor i Sverige. Det finns inga system för att efterfråga registerkontroll från myndighet i annat land.

De krav som regering och riksdag ställer på totalförsvaret och dess aktörer måste på något sätt kunna speglas i kravställningen gentemot underleverantörer, samt vid outsourcing och s.k. funktionsupphandlingar. För energiföretag finns reglering men det behövs också tydliga riktlinjer och lämplig reglering för underleverantörer som vill leverera till energibranschens aktörer.

5 Slutsatser och rekommendationer

Gråzonsbegreppet kan vara användbart men bör användas restriktivt, beroende på syfte, samt avgränsas till de aktiviteter som den kvalificerade statsaktören genomför eller står bakom

Gråzonsbegreppet är relevant på flera sätt. Även om gråzonsaktiviteter är något man kan se historiskt så har aktualiteten ökat, dels har kostnaden för direkt militär konfrontation ökat (i och med fördjupade internationella ekonomiska beroenden), dels har möjligheterna ökat genom nya verktyg (såsom cybervapen). Ett skäl till att begreppet ofta används i Sverige beror sannolikt på att lagstiftningen, åtminstone i dagsläget, gör en tydlig skillnad på normalläge och höjd beredskap, respektive fred och krig. Gråzonsbegreppet fyller därmed ut ett potentiellt tomrum – en gråzon. I den förståelsemodell som lagstiftningen speglar synliggörs inte på samma sätt antagonistiska alternativa syften såsom att testa, öva och demonstrera icke-militära angreppssätt, att vinna fördelar utan att eskalera en konflikt, eller att skapa fördelar inför en eventuell militär konfrontation.

Oprecis användning av begreppet gör att det mesta kan inrymmas i gråzonen, vilket är olämpligt. Enskilda hot bör adresseras för vad de verkligen är snarare än att klumpas ihop i gråzonen. Man skulle kunna anse att begreppet främst hör hemma på centrala myndigheters nivå, som både har behovet av att se helheten samt ansvarar för att bemöta den samlade hotbilden, medan andra aktörer bör fokusera på de specifika hoten (exempelvis cyberintrång) för att kunna kraftsamla för att skydda sig mot dessa. Samtidigt kan förståelse för den sammantagna hotbilden vara en förutsättning för att upptäcka och identifiera hot samt att skydda sig mot dessa.

När är det lämpligt respektive olämpligt att tala om ”gråzon”? Ett sunt förhållningssätt är att i olika sammanhang kritiskt fråga sig varför man själv, eller andra, använder gråzonsetiketten:

- Är det för att man gör observationer som verkligen är nya eller kläds dessa bara i annan skrud?
- Är det för att denna nytolkning av hotbilden ger oss bättre förutsättningar att möta hoten?
- Är det ett modeord, som uppfattas som något nytt och spännande, som används som ett lobbyverktyg för att sätta försvars- och krisberedskapsfrågor på agendan?
- Är det för att gråzon verkligen är motståndarens strategi eller använder vi begreppet slentrianmässigt när något skeende är oklart och svårbegripligt?

- Är det för att gråzonen känns som en lagom utmanande hotbild, inte lika otäck som kriget där många civila aktörer kanske uppfattar sin roll som överspelad?
- Är det kanske till och med gråzonen mellan våra myndigheters och krisberedskapsaktörers ansvarsområden som avses, medvetet eller omedvetet? Det utgör i sådana fall en helt annan betydelse, som visserligen den kvalificerade antagonisten kan komma att utnyttja.

I ett beredskapsplaneringssammanhang är gråzonen endast en delmängd av den sammantagna hotbilden. I ett totalförsvarssammanhang bör gråzonen avgränsas till de aktiviteter som den kvalificerade statlige antagonisten genomför eller ligger bakom via ombud, vilket visserligen är svårt eftersom gråzonen präglas av osäkerhet.

Gråzonshot bör främst mötas med icke-militära motmedel, såsom förmåga att upprätthålla samhällets funktionalitet

Verktyg för att möta gråzonsaggression är nödvändiga för att inte gråzonsstrategierna ska lyckas och därmed ge incitament till ytterligare aktiviteter. Gråzonen synliggör i viss mån ett tomrum mellan försvararens fredstida utrikespolitik och diplomati respektive tillgängliga militära försvarsåtgärder. I grund och botten handlar ju gråzonsstrategi om att exploatera motpartens önskan om att inte eskalera konflikten och att inte bli tvungen att använda militära medel. Utmaningen med att möta gråzonshot handlar därmed i första hand om att fylla detta tomrum och främst utveckla icke-militära motmedel.[125]

Ett sådant motmedel är att stärka förmågan att upprätthålla samhällets funktionalitet, vilket bland annat ställer krav på energiförsörjningen. Mer robusta infrastruktursystem kan i det sammanhanget ha en tröskelhöjande effekt. Ett motsvarande begrepp är motståndskraft.[126]

Robusta försörjningssystem ger motståndskraft och höjer tröskeln för angrepp

Motståndskraft genom robusta försörjningssystem, och därigenom förmåga att upprätthålla samhällets funktionalitet, kan förstås via tre nivåer:

För det första, motståndskraft, som höjer tröskeln för angrepp, höjer också insatsen för antagonisten och ökar kanske även upptäcktsrisken. Det blir därmed ”dyrare” och kanske inte alls meningsfullt att angripa och därmed får motståndskraften en konfliktavhållande och fredsfrämjande effekt. Även om angriparen primärt inte har intresse av att skapa störningar och avbrott i

[125] Hermberg 2016
[126] Se t.ex. Försvarsberedningen 2017

exempelvis försörjningsystemen kan sådana förutsättningar bidra till ökad sårbarhet för politisk utpressning. Ett sådant perspektiv ger vid handen att vår första försvarslinje är just de system som samhällets funktionalitet är beroende av.

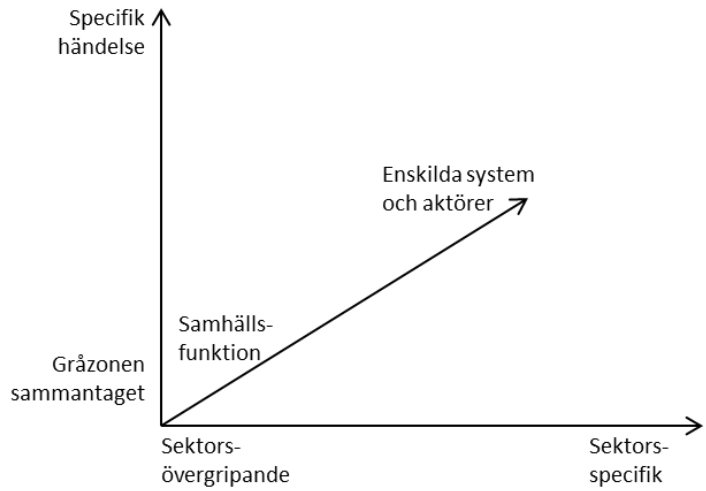
För det andra så kan de kritiska samhällsfunktionerna och då i synnerhet motståndskraftiga försörjningssystem komma att spela en särskilt viktig tröskelhöjande roll för att undvika att en eskalerad gråzonssituation övergår i väpnad konflikt. Om inte samhällets stöd till Försvarsmakten, som möjliggör militära försvarsåtgärder och väpnad strid, kan ryckas undan kan detta få en krigsavhållande effekt hos motparten.

För det tredje är det i en eskalerad konfliktsituation osannolikt att Sverige agerar ensam. Samhällets funktionalitet utgör basen för Försvarsmaktens möjligheter att verka men beroendet av denna funktionalitet gäller i ännu högre grad för förband från utländska samarbetspartners som inte är på hemmaplan och därmed inte har tillgång till egen basal försörjningsinfrastruktur eller fasta installationer. Detta betonar ytterligare vikten av samhällets förmåga att leverera funktionalitet via motståndskraftiga försörjningssystem, för att Sverige ska kunna fungera som värdland.

Öka förståelsen om samhällsfunktioners sårbarheter genom fördjupad sektorskunskap snarare än ett alltför ensidigt fokus på övergripande krisberedskapsprinciper

Hur ska då tröskeln kunna höjas och samhällsfunktionernas motståndskraft stärkas? Det handlar om att kunna navigera i såväl hotbilden som i de egna sårbarheterna. Identifiering av hot kan ta sin utgångspunkt i en förståelse av den som hotar och dennes strategier, tillgängliga verktyg och uttalade mål men också genom att observera beteendet.[127] Vägen till ökad förståelse om sårbarheter sitter ofta i detaljerna så ett ensidigt fokus på övergripande krisberedskapsprinciper räcker inte. Det krävs också fördjupning på enskilda aktörer, system, sektorer och specifika gråzonshändelser. Sammanfattningsvis handlar det om att ha förmåga att kunna skifta perspektiv och röra sig i det tredimensionella rum som Figur 4 illustrerar.

[127] Cederberg m.fl. 2017



Figur 4. Dimensioner att beakta för ökad förståelse kring gråzonshot och samhällsfunktioners sårbarhet.[128]

Ett alltför ensidigt fokus på förmågebyggande längs någon utvald dimension i figuren, eller i några utvalda ytterändar ger en krisberedskap och ett civilt försvar som kommer att halta. Tekniska strukturer, försörjningsråvaror, ekonomiska resurser och aktörer, liksom institutioner, normer och lagar är byggstenar för krishanteringsförmåga som måste samspela och matcha varandra.[129] Detta kan sammantaget utgöra krisberedskapens och det civila försvarets sammantagna organisation (eller ”systemet”) som också måste vara adaptiv och kunna agera flexibelt. Den kvalificerade antagonisten är en motspelare som inte avser anpassa sin taktik och strategi till att passa våra organisatoriska strukturer, snarare tvärtom.

Gråzonsproblematiken tydliggör att det inte handlar om att prioritera mellan antingen fredstida försörjningstrygghet eller kriget – en robustare försörjning behövs för hela hotskalan

Även om förståelsen av ”gråzonen” som ett tillstånd mellan fred och krig är ospecifik och starkt förenklad för den med sig en viktig pedagogisk poäng. Nämligen att det är svårt att planera för fungerande försörjningssystem eller andra samhällsviktiga verksamheter under störda förhållanden utifrån en enstaka dimensionerande hotbild, eller att tvingas prioritera mellan konkurrerande

[128] Utvecklad utifrån Veibäck m.fl. 2016
[129] Veibäck m.fl. 2016

hotbilder. Gråzonens spännvidd och mångfald, på energiområdet liksom andra områden, överbryggar de binära tillstånden krig respektive fred.

Strävan efter en robusthet som är giltig under alla förhållanden är därmed central. Energimyndigheten uttrycker detta som att ”…planeringen för civilt försvar är en planering för hela hotskalan, där säkerhet, skydd och förmågor måste byggas integrerat för både krisberedskap och höjd beredskap”.[130]

Regeringens och centrala myndigheters styrning av den återupptagna totalförsvarsplaneringen kan inte låta sig begränsas av befintliga förvaltningsformer och nuvarande lagfästa begrepp, såsom ”höjd beredskap”, utan måste anpassas efter den aktuella hotbilden.

Omdefiniera vad som ska anses som skyddsvärt, från objekt till funktionalitet

Uppdaterad säkerhetsskyddslagstiftning kan också vara relevant i detta sammanhang. Definitionen av vad som är ”skyddsvärt” bör bli bredare. Detta bör innebära att förståelsen för vad som är att betrakta som ”rikets säkerhet” breddas från det primärt försvarsinriktade mot att även omfatta samhällets säkerhet och funktionalitet. Det innebär också att fler aktörer jämfört med idag får ansvar för säkerhetsskydd. Ett första steg är att etablera en medvetenhet om att även civil infrastruktur kan ha ett särskilt skyddsvärde.

Vidare är det inte görligt att som förr ensidigt fokusera på skyddsvärden i formen av enskilda objekt eftersom funktionalitet är det centrala. Funktionalitet måste betraktas utifrån ett systemperspektiv som omfattar exempelvis beroenden mellan olika system och system i system.

Detta är komplext och snarare än att ge sig på den sannolikt omöjliga uppgiften att försöka säkra samtliga viktiga komponenter behövs också ett ”good enough”-perspektiv. Nivån på detta ”good enough” måste sättas i relation till såväl hotbilden som beroendena mellan olika samhällsfunktioner och försörjningsystem. Beroendena måste förstås och därmed även insikten om att en ansträngd gråzonssituation sannolikt inte påverkar endast en sektor i taget, vilket kräver sektorsövergripande samverkan.

Tydliggör sektorsansvaret samt bejaka samordning och samverkan

Såväl planering för upprätthållande av funktionalitet som planering för extraordinära åtgärder, inom ramen för att lösa det civila försvarets uppgifter, kräver både samordning inom sektorer och sektorsövergripande samverkan. För

[130] Energimyndigheten 2018, s. 2

att denna samverkan ska kunna få effekt måste den ske mellan aktörer med beslutsmandat, vilket i sin tur kräver i att sektorsansvaret tydliggörs.[131]

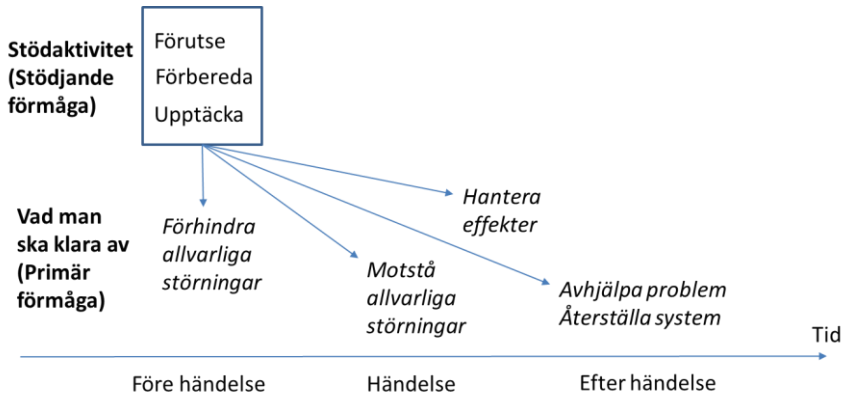
Planering kräver beslut, såvida inte ”planeringen” enbart har ett kunskapsuppbyggande syfte. För att ge effekt i ökad totalförsvarsförmåga via konkreta planer och åtgärder krävs beslut som bara enskilda myndigheter kan fatta. Samtidigt är samhällets funktionalitet en intim sammanflätning av beroenden mellan olika sektorer och mellan aktörer inom samma sektor. Därför krävs samordning och samverkan, liksom informationsdelning. Men själva planeringen måste till största del göras vid de bevakningsansvariga myndigheterna som har beslutsmandaten.

Samordning och informationsdelning inom sektorer bidrar bl.a. till etablerandet av en gemensam förståelse för den aktuella hotbilden, vilket är en förutsättning för samordnade åtgärder. Detta kräver dock att hotbilden gentemot respektive sektor kartläggs och hålls uppdaterad.

Energiberedskapens olika förmågor bör ta höjd för gråzonshot i den sammantagna störnings- och hotbilden

För att öka samhällsfunktionernas motståndskraft krävs sammantaget förmåga att kunna förhindra allvarliga störningar och motstå dessa om händelser likväl inträffar, samt att kunna hantera effekterna av störningarna och slutligen avhjälpa problemen och/eller återställa systemen. Det gäller såväl energiförsörjningen som övriga samhällsviktiga funktioner. Detta kan benämnas som primära förmågor. För detta krävs s.k. stödjande förmågor i termer av att kunna förutse hot, förbereda sig inför hot samt upptäcka händelser som kan leda till allvarliga störningar. Se Figur 5.

[131] Se t.ex. Denward m.fl. 2017



Figur 5. Översikt över stödjande respektive primära förmågor.[132]

För att etablera den stödjande förmågan som krävs för att kunna möta gråzonsproblematik med primära förmågor behövs empiri, omvärldsbevakning och framsyn (exempelvis via scenariometoder) som bygger upp hotbildsförståelsen. Det vill säga ”att förutse”, liksom att identifiera energisystemens sårbarheter. Kapitel 4 i denna rapport är ett av flera sätt att utveckla de stödjande förmågorna inom energisektorn, genom ökad medvetenhet om gråzonshot.

Nästa steg handlar om att öka förmågan att upptäcka hot iscensatta av en kvalificerad statsaktör och förbereda sig inför dessa. Ytterligare nästa steg är att finna sätt att öka förmågan att hantera dessa händelser, dvs. de primära förmågorna.

Energibranschen prioriterar leveranssäkerhet men hotskalan bör utvidgas och därmed även möjligheterna att upptäcka och identifiera gråzonshot

Man ska ha klart för sig att de privata och offentligt ägda aktörer som sammantaget utgör energibranschen redan idag gör vad de kan för att skydda sina verksamheter och därmed sin lönsamhet – oavsett hot. Att förebygga störningar och avbrott samt att snabbt kunna återställa funktionalitet är därmed oftast prioriterat framför att grundligt analysera huruvida ett problem beror på antagonistiska aktiviteter eller inte, och än mindre om antagonisten är en kvalificerad statsaktör eller bara en enskild hacker.

Detta medför ett analytiskt dilemma – incidenter finns det gott om men empirin används inte primärt för att utveckla hotförståelsen. Prioriteringen att återställa snarare än att utreda händelsens bakgrund ger visserligen energiförsörjningen en

[132] Veibäck m.fl. 2016

styrka genom robusthet oavsett hot. Detta förhållningssätt kan dock påverka det förebyggande arbetet negativt då inte hotbilden till fullo förstås liksom hur hotbilden skulle kunna utvecklas i ett mer ansträngt säkerhetspolitiskt läge. För det är uppenbart att det ena inte kan utesluta det andra. Att fokusera på leveranssäkerheten ger följdfrågan: vilka är förutsättningarna för leveranssäkerhet i *alla* rimligt tänkbara lägen? En relevant och sammantagen hotbild som speglar hela hotskalan bidrar till att bättre förstå dessa förutsättningar.

Förmågan att upptäcka och identifiera gråzonshot förutsätter fördjupad samverkan mellan underrättelsetjänst, säkerhetstjänst, civila myndigheter och privata aktörer

Underrättelse- och säkerhetsmyndigheternas uppdrag är att upptäcka, identifiera och varna för hot. Det sistnämnda medför ett behov av informationsspridning till civila myndigheter och privata aktörer.[133] Omvänt behöver information om eventuella gråzonsaktiviteter, kanske endast i form av indikationer, som de privata aktörerna erfar vidarebefordras till myndigheterna.

Energimyndigheten redovisar till regeringen att ”…omvärldsbevakning och –analys behöver stärkas och fördjupas tillsammans med andra omvärldsbevakande myndigheter”.[134] Detta är en ståndpunkt som kan vidimeras utifrån denna rapports slutsatser.

Höj medvetenheten om gråzonshot bland privata energibranschaktörer genom att bejaka informationsspridning – men med hänsyn till sekretess

Samlad information om hot och sårbarheter förknippas i regel med sekretess och därmed är den informationen inte på ett givet sätt tillgänglig för privata branschaktörer. Samtidigt är det just hos dessa aktörer som medvetenheten behöver höjas. Den grad av öppenhet som då krävs måste därför vägas mot riskerna med att vi blottar delar av vår kunskap. Där har bevakningsansvariga myndigheter, såsom Energimyndigheten och Svenska kraftnät, en viktig roll gentemot branschen.

Vidare styrs branschen av kommersiella intressen och för en enskild aktör kan röjandet av egna sårbarheter innebära konkurrensnackdelar gentemot andra aktörer. Att ha förståelse för och tillgodose de privata aktörernas behov av affärssekretess är därmed också en viktig uppgift för ansvariga myndigheter.

Det behövs således en väl avvägd informationsspridning. Man skulle kunna tala om behovet av ett minsta gemensamma kunskapsläge, dvs. en övergripande

[133] Severin 2018
[134] Energimyndigheten 2018, s. 10

hotbild bestående av väl övervägt utvalda men relevanta exempel snarare än den sammantagna befintliga kunskapen om kända hot och sårbarheter. Om specifik information som sprids öppet skulle leda till ett förändrat tillvägagångssätt hos motståndaren just avseende den informationen så är det att betrakta som en ”kostnad” som kan uppvägas av nyttan som kunskapsspridningen överlag förväntas ha. Men detta gäller just information om exempel på hot. Exempel på sårbarheter, som inte är alldeles uppenbara för en extern betraktare, är däremot något som betingar ett högre skyddsvärde.

Metoden för balansgången mellan sekretess och öppenhet som beskrivs i avsnitt 4.3.2 skulle kunna fungera som en utgångspunkt för hur medvetandegörande och informationsspridning bland privata aktörer ska hanteras i framtida beredskapsarbete, i såväl energisektorn som i andra samhällsviktiga verksamheter.

De privata aktörernas kärnverksamhet är inte ”rikets säkerhet” och det innebär också att kunskapen om det antagonistiska riskperspektivet och totalförsvarets behov kan vara begränsad. Men även inom myndigheter, länsstyrelser och kommuner har perspektivet *höjd beredskap och krig*, som på olika sätt skiljer sig från det fredstida krisperspektivet, varit frånvarande under en längre tid. Istället för att inkludera allt på en gång finns det anledning att börja höja medvetandet genom att försöka förstå de grundläggande logiska skillnaderna mellan olika typer av hot. Det mest grundläggande är att vårt preventiva agerande gentemot antagonistiska hot påverkar motparten, dvs. inte bara påverkar effekten av iscensatta hot utan också påverkar själva hoten.

Referenser

Aleklett, K., Höök, M., Jakobsson, K., Lardelli, M., Snowden, S., Söderbergh, B. 2010. The peak of the oil age-analyzing world energy production reference scenario in world energy outlook 2008. Energy Policy, 38, 1398-1414

Allen, J., Breedlove, P.M., Lindley-French, J., Zambellas, G. 2017. Future war NATO? From hybrid war to hyper war via cyber war. Supporting Paper of the GLOBESEC NATO Adaptation Initiative

Altman, D. 2015. Red Lines and Faits Accomplis in Interstate Coercion and Crisis. Ph.D. Thesis, Cambridge, MA: Massachusetts Institute of Technology

Andersson, M., Westerdahl, L. 2017. Sveriges elförsörjning – hur möter vi en ökande sårbarhet? I: Hull Wiklund, C., Faria, D., Johansson, B. (red.). Strategisk Utblick 7. FOI-R--4454--SE. Totalförsvarets forskningsinstitut

Antonovich, P. 2011. Cyberwarfare: Nature and content. Military Thought, 20(3), 35-43

Banasik, M. 2016. Unconventional war and warfare in the gray zone: the new spectrum of modern conflicts. Journal of Defense Resources Management, 7:1, 37-46

Bartuska, V. 2017. The energy weapon that could not. Assessing the European security in the stand-off with Russia, 2014-2015. In Hajek, J. (ed.), Hybrid Threats: Overcoming ambiguity, building resilience. NATO Energy Security Centre of Excellence. No. 11, 2017, 25-32

Cederberg, A., Eronen, P., Mustonen, J. 2017. Regional cooperation to support national hybrid defence efforts. Hybrid CoE Working Paper 1. The European Centre of Excellence for Countering Hybrid Threats

Cherepanov, A. 2017. TeleBots are back: supply-chain attacks against Ukraine. Welivesecurity.com, 2017-06-30

Chivvis, C.S. 2017. Understandning Russian ”hybrid warfare” – and what can be done about it. Testimony (CT-468) presented before the House Armed Services Committee, March 22 2017. RAND Corporation

Connell, M., Vogler, S. 2017. Russia’s Approach to Cyber Warfare. CNA Analysis & Solutions, March 2017. Center for Naval Analyses

Davidson, J.W. 2002. The roots of revisionism: Fascist Italy, 1922-39. Security Studies, 11:4, 125-126

De Nooij, M., Koopmans, C., Bijvoet, C. 2007. The value of supply security. The costs of power interruptions: Economic input for damage reduction and investment in networks, Energy Economics, 29, 277-295

De Nooij, M., Lieshout, R., Koopmans, C. 2009. Optimal blackouts: Empirical results on reducing the social cost of electricity outages through efficient regional rationing. Energy Economics, 31, 342-347

Denward, C., Larsson, P., Stenérus Dover, A.S. 2017. Sektorsansvar. Ansvarssystem eller semantik? FOI-R--4542--SE. Totalförsvarets forskningsinstitut

Echevarria II, A.J. 2016. Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy. Strategic Studies Institute and U.S. War College Press

Elkus, A. 2015. 50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense. War on the Rocks (December 15th, 2015)

Energimyndigheten 2018. Trygg energiförsörjning för civilt försvar. Energimyndighetens redovisning av regeringsuppdrag 2015-12-10 Ju2015/00054/SSK, Ju2015/00055/SSK, Ju2015/00067/SSK (delvis), Ju2015/09669/SSK samt redovisning av uppdrag nr 6 i regleringsbrev för budgetåret 2017 avseende Statens energimyndighet, Regeringskansliet 2016-12-20, M2016/02922/S (delvis). Dnr 2018-1862, 2018-02-14

Energy Strategy of the Russian Federation 2003. Ryska Federationen

Estonian Foreign Intelligence Service 2018. International Security and Estonia 2018

Fooy, F. 2016. Vem ska jag tro på? Vårt försvar. Nr. 3, Oktober 2016, 20-21

Försvarsberedningen 2017. Motståndskraft. Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021-2025. Regeringskansliet, Försvarsdepartementet, Ds 2017:66

Försvarsmakten 2016. Militärstrategisk doktrin, M7739-354028

Försvarsmakten 2017. Försvarsmaktens delredovisning av perspektivstudien 2016-2018, FM2015-13192:12

Försvarsmakten 2018. Tillväxt för ett starkare försvar. Slutredovisning av Försvarsmaktens perspektivstudie 2016-2018. FM2015-13192:15, 2018-02-22

Försvarsmakten och Myndigheten för samhällsskydd och beredskap (MSB) 2016. Sverige kommer att möta utmaningarna. Gemensamma grunder (grundsyn) för en sammanhängande planering för totalförsvaret. FM2016-13584:3, MSB 2016-25

Gerasimov, V. 2013. The value of science is in the foresight: New challenges demand rethinking the forms och methods of carrying out combat operations. Voyenno-Promyshlennyy Kurier, jan-feb 2013, 23-29

Giles, K. 2016. Handbook of Russian Information Warfare. Fellowship Monograph 9. NATO Defence College

Gonchar, M., Chubyk, A. 2017. Energy in new generation warfare. Learned lessons from Russia's hybrid war against Ukraine. In Hajek, J. (ed.), Hybrid Threats: Overcoming ambiguity, building resilience. NATO Energy Security Centre of Excellence. No. 11, 2017, 33-39

Greenberg, A. 2017a. Hackers gained direct access to US power grid controls. Wired magazine, May Issue

Greenberg, A. 2017b. How an entire nation became Russia's test lab for cyberwar. Wired magazine, July Issue

Harlow, G.D., Maerz, G.C. (eds.). 1991. Measures Short of War: The George F. Kennan Lectures at the National War College, 1946-1947, Washington, DC: National Defense University Press

Hedenskog, J., Holmquist, E., Norberg, J. 2018. Security in the Caucasus: Russian policy and military posture. FOI-R--4567--SE. Totalförsvarets forskningsinstitut

Hedenskog, J., Malmlöf, T., Norberg, J., Oxenstierna, S., Persson, G., Vendil Pallin, C., Westerlund, F. 2017. "Ryssland", i Rossbach, N.H., Sundberg, A. (red.), FOI:s underlag inför nästa försvarspolitiska inriktningsbeslut, Bilaga 1, 25-35. Dnr. FOI-2016-1544

Heier, T. 2016. The logic of asymmetry: Russia's approach towards NATO. In Haaland Matláry, J. & Heier, T. (eds.). Ukraine and Beyond: Russia's Strategic Security Challenge to Europe, 265–287. Palgrave Macmillan

Hellmann M., Wagnsson, C. 2017. How can European states respond to Russian information warfare? An analytical framework, European Security, 26:2, 153-170

Hermberg, N.M. 2016. The danger of the gray zone: flawed responses to emerging unconventional threats. Small wars journal, December 6, 2016

Hoffman, F.G. 2016. The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War. The Heritage Foundation, 2016 Index of US Military Strength (2015), 25-36

Holmgren, Å.J., Jenelius, E., Westin, J. 2007. Evaluating strategies for defending electric power networks against antagonistic attacks. IEEE Transactions on power systems, 22:1, 76-84

Hughes, L., Ranjan, A. 2013. Event-related stresses in energy systems and their effects on energy Security, Energy, 59, 413-421

Hultqvist, P. 2017. Tal av försvarsminister Peter Hultqvist på AFCEA TechNet Europe conference 2017 (engelska). Upplands Väsby, 10 oktober 2017

IISS 2013. The cyber attack on Saudi Aramco. International Institute of Strategic Studies.

Institute of the Energy Strategy 2018. Energy Strategy of the RF Concept till 2030 (project).

Jackson, V. 2017. Tactics of strategic competition. Gray Zones, Redlines, and Conflicts before War. Naval War College Review, 70:3, 39-61

Jonsson, D.K. 2017. Att använda scenarier i planering för civilt försvar. FOI-R--4434--SE. Totalförsvarets forskningsinstitut

Jonsson, D.K. 2018. Typfall 5: utdragen och eskalerande gråzonsproblematik. Komplettering av hotbildsunderlag i utvecklingen av civilt försvar. FOI Memo 6338. Totalförsvarets forskningsinstitut

Jonsson, D.K., Johansson, B., Lindgren, F., Veibäck, E., Bergstrand, M. 2017. Scenariobaserad planering för civilt försvar inom energiområdet. FOI-R--4356--SE. Totalförsvarets forskningsinstitut,

Jonsson, D.K., Sonnsjö, H. 2013. EU:s framtida energisäkerhet i en föränderlig omvärld. Scenarioanalys för Försvarsmakten. FOI-R--3627--SE. Totalförsvarets forskningsinstitut

Kapusta, P. 2015. The Gray Zone. Special Warfare 28, no. 4, 18-25

Karlson, G. 2017. Exempel på möjliga medel för påverkan mot Sverige. Presentation i Sälen 10 januari 2017

Kello, L. 2017. The virtual weapon and international order. Yale University Press, New Haven

Kjärstad, J., Jonsson, F. 2009. Resources and future supply of oil, Energy Policy, 37, 441-464.

Kofman, M., Rojansky, M. 2015. A closer look at Russia's "Hybrid War". Kennan Cable, No. 7, April 2015

Kramer, A.E. 2017. Ukraine cyberattack was meant to paralyse, not profit, evidence shows. The New York Times, 2017-06-20

Käihkö, I. 2016. All krigföring är av hybrid natur. Statsvetenskaplig tidskrift. 118:4, 623-641

Lanoszka, A. 2016. Russian hybrid warfare and extended deterrence in eastern Europe, International Affairs 92:1, 175-195

Larrabee, F.S., Pezard, S., Radin, A., Chandler, N., Crane, K., Szayna, T.S. 2017. Russia and the West after the Ukrainian crisis. RAND Corporation, RR-1305-A

Lind, W., Nightengale, K., Schmitt, J., Sutton, J., Wilson, G. 1989. The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette, 73:10, 22-26

Lind, W., Schmitt, J., Wilson, G. 1994. Fourth Generation Warfare: Another Look. Marine Corps Gazette. December 1994, 34-37

Lindblom, C.E. 1959. The Science of Muddling Through. Public Administration Review, 19:2, 79-88

Lindblom, C.E., Woodhouse, E.J. 1993. The Policy-making Process. Prentice Hall, Englewood Cliffs, New Jersey

Lindgren, F. 2014. Hotbildsunderlag i utvecklingen av civilt försvar. FOI Memo 5089. Totalförsvarets forskningsinstitut

Margelov, M. 2011. Chairman of the Foreign Affairs Committee of the Council of the Russian Federation. Speech, November 2011

Mazarr, M.J. 2015. Mastering the Gray Zone: Understanding a Changing Era of Conflict, Strategic Studies Institute and U.S. Army War College Press

Ministry of Energy of the Russian Federation 2010. Energy strategy of Russia. For the period up to 2030. Decree No. 1715-r of the Government of the Russian Federation. Institute of Energy Strategy

Muller, P.L., Gjesvik, L., Friis, K. 2018. Cyber-weapons in international politics. Possible sabotage against the Norwegian petroleum sector. NUPI Report 3/2018, Norwegian Institute of International Affairs

Myndigheten för samhällsskydd och beredskap (MSB) 2017. Utlysning av forskningsmedel: Civilt försvar med nya förutsättningar. 2017-06-15, Dnr. 2017-6313

Månsson, A. 2014. Energi och konflikter: översikt och analytiskt ramverk. I Jonsson, D.K. (red.), Energi, säkerhet och konflikt i ett framtidsperspektiv, s. 65-87. FOI-R--3813--SE. Totalförsvarets forskningsinstitut

Nakashima, E. 2018. Russian military was behind “NotPetya” cyberattack in Ukraine, CIA concludes. The Washington Post, 12 January

Norberg, J., Westerlund, F., Franke U. 2014. The Crimea Operation: Implications for Future Russian Military Interventions, i Granholm, N., Malminen, J., Persson, G. (red.), A Rude Awakening: Ramifications of Russian Aggression towards Ukraine, s. 41-50. FOI-R--3892--SE. Totalförsvarets forskningsinstitut

Paillard, C.A. 2017. Hybrid threats on energy infrastructures and supply lines. In Hajek, J. (ed.), Hybrid Threats: Overcoming ambiguity, building resilience. NATO Energy Security Centre of Excellence. No. 11, 18-25

Palmgren, A. 2017. Gråzonsproblematik. Försvarshögskolan, 2017-01-25

Persson, G. 2013. Säkerhetspolitik och militär-strategiskt tänkande, i Hedenskog, J., Vendil Pallin, C. (red.), Rysk militär förmåga i ett tioårsperspektiv – 2013, s. 71-88. FOI-R--3733--SE. Totalförsvarets forskningsinstitut

Persson, G. 2015. Mellan krig och fred – militärstrategiskt tänkande i Ryssland, i Dalsjö, R., Korkmaz, K., Persson, G. (red.), Örnen, Björnen och Draken: Militärt tänkande i tre stormakter, s. 46-64. FOI-R--4103--SE. Totalförsvarets forskningsinstitut

Persson, G. (ed.) 2016. Russian Military Capability in a Ten-Year Perspective 2016, FOI-R--4326--SE. Totalförsvarets forskningsinstitut

Persson, G. 2017. The War of the Future: A Conceptual Framework and Practical Conclusions Essays on Strategic Thought. Russian Studies, Nato Defence College, 03/17 – July 2017

Pilav, A. 2012. Before the war, war, after the war: urban imageries for urban resilience. Disaster risk science, 3:1, 23-37

Prop. 2014/15:109. Försvarspolitisk inriktning – Sveriges försvar 2016-2020

Radin, A. 2017. Hybrid warfare in the Baltics: Threats and potential responses. RAND Corporation, RR-1577-PAF

Reisinger, H., Golts, A. 2014. Russia's hybrid warfare: Waging war below the radar if traditional collective defence. Research paper no. 105, NATO Defence College, November 2014

Renz, B., Smith, H. 2016a. Russia and hybrid warfare – going beyond the label. Aleksanteri Papers 1/2016, Aleksanteri Institute, University of Helsinki

Renz, B., Smith, H. 2016b. After 'hybrid warfare', what next? – Understanding and responding to contemporary Russia. Publication of the Government's analysis, assessment and research activities 44/2016, Statsrådets kansli (Finland)

Robinson, N. 2003. Fuel Protests: Governing the Ungovernable? Parliamentary Affairs, 56, 423-440

Rosenius, F., m.fl. 2017. Ett nytt totalförsvar. En vitbok från KV21 (Krigsvetenskap i det 21:a århundradet). Kungl. Krigsvetenskapsakademin, Stockholm

Rühle, M., Grubliauskas, J. 2015. Energy as a tool of hybrid warfare. Research paper no. 113, NATO Defence College, April 2015

Schelling, T.C. 1966/2008. Arms and Influence. New Ed. 2008, New Haven: Yale University Press

Schmidt-Felzmann, A. 2016. "Sweden under attack!" Lessons from the past incidents for coping with a comprehensive synchronized attack on critical energy

and information infrastructure. NATO SPS Advanced Research Workshop: May 18-20, 2016 in Stockholm

Severin, M. 2018. Tidig förvarning och icke-militära angreppssätt. Utmaningar för underrättelsetjänsten. FOI-R--4577--SE. Totalförsvarets forskningsinstitut

SFS 2015:1053. Förordningen om totalförsvar och höjd beredskap

SFS 2015:1052. Förordning om krisberedskap och bevakningsansvarigas ansvar vid höjd beredskap

Slobodian, N. 2016. Energy instruments of "hybrid warfare". Partner perspectives, Statfor Worldview, 7 mars 2016

Smith Stegen, K. 2011. Deconstructing the 'energy weapon': Russia's threat to Europe as a case study. Energy policy 39(10), 6505-6513

Sonnsjö, H. 2014. Att förstå energisäkerhet genom internationella relationer. I Jonsson, D.K. (red.), Energi, säkerhet och konflikt i ett framtidsperspektiv, s. 45-64. FOI-R--3813--SE. Totalförsvarets forskningsinstitut

Stulberg, A.N. 2017. Natural gas and the Russia-Ukraine crisis: Strategic restraint and the emerging Europe-Eurasia gas network. Energy Research & Social Science 24, 71-85

Säkerhetspolisen 2016. Årsbok, utgiven mars 2017

Tierney, J.J. 2006. Chasing Ghosts: Unconventional Warfare in American History. Washington, DC: Potomac Books

U.S. Army Special Operations Command 2015. "Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014 (Unclassified version).

Veibäck, E., Johansson, B., Jonsson, D.K., Sonnsjö, H., Mittermaier, E., Stenérus Dover, A-S. 2016. Energi och förmåga. Analytiska perspektiv och empiriska erfarenheter inom drivmedelsområdet. FOI-R--4241--SE. Totalförsvarets forskningsinstitut,

Veloza, O.P., Santamaria, F. 2016. Analysis of major blackouts from 2003 to 2015: Classification of incidents and review of main causes. Electricity, 29, 42-49

Vendil Pallin, C. 2018. Russian "cyber troops" and Information Warfare. Paper for PANEL 4:15 – Politics: Russian disinformation and its effects in Europe, BASEES Conference 2018, Cambridge

Westerlund, F. 2017. Vad avskräcker Ryssland från angrepp? Rysk syn på svensk avskräckningspolitik. Kungl. Krigsvetenskapsakademin 2017:4, 137-156

Wilson, I., Smitson, S. 2016. Solving America's gray-zone puzzle. Parameters, 46:4. 55-67

Wirtz, J.J. 2017. Life in the “Gray Zone”: observations for contemporary strategists. Defense & Security Analysis, 33:2, 106-114

Zetter, K. 2014. Countdown to Zero Day: Stuxnet and the launch of the World’s first digital weapon. Crown/Archtype

Zionts, D.M. 2006. Revisionism and its variants: Understanding state reactions to foreign policy failure. *Security Studies*, 15:4, 632-633

Bilaga: Typfall 5: Utdragen och eskalerande gråzonsproblematik

Utdrag ur Jonsson, D.K. 2018. Typfall 5: utdragen och eskalerande gråzonsproblematik. Komplettering av hotbildsunderlag i utvecklingen av civilt försvar. FOI Memo 6338. Totalförsvarets forskningsinstitut. Avsnitt 2.2 Situation och händelseförlopp.

I Sverige, liksom i de nordisk-baltiska grannländerna, har under senare tid ett tämligen stort antal svårförklarliga olyckor inträffat. Detta bidrar till en ökad arbetsbelastning för polis, räddningstjänst och akutsjukvård. Därtill sker en rad dolda angrepp såsom mindre cyberangrepp och fysiska sabotage på samhällsfunktioner där man försöker dölja spåren och/eller rikta misstankarna åt annat håll. Angreppen förefaller ske främst mot ”lågt hängande frukter” såsom lokala försörjningssystem samt enstaka samhällsaktörer och företag, snarare än mot strategiska mål. Förekomsten av förvrängd information och korrupta data i system som används av beslutsfattare, operatörer och specialister inom en rad samhällssektorer ökar, vilket tyder på avancerade dataintrång. Påverkan på samhällets funktionalitet är tämligen begränsad men bland allmänheten sprider sig ändå viss oro.

Spridandet av propaganda via internetaktivister och alternativa medier, som sedan ibland oreflekterat sprids vidare i svenska traditionella medier, förmedlar en skev bild av Sverige. Den svenska allmänheten utsätts för mångtydiga fakta och ibland ren desinformation i frågor som berör bl.a. ordning och trygghet, migration och integration, traditionella värderingar, krisberedskap och försvar, samt utrikes- och säkerhetspolitik. Dessa informationsoperationer, som i första hand utnyttjar vårt öppna samhälles informationsinfrastruktur i termer av internets sociala medier och bloggar, liksom indirekt TV, radio och tidningar, får viss negativ påverkan på allmänhetens förtroende för myndigheter och politiker.

Främmande makts underrättelseverksamhet i Sverige och dess grannländer ökar med tiden. Det gör även en allt mer konfrontativ diplomatisk retorik i kombination med spridning av propaganda via statskontrollerade medier.

De upprepade infrastrukturella störningarna, som nu pågått i flera månader, sliter på samhället. Verksamheter når övertidstak för anställda, får brist på reparationsmaterial och överskrider budget. Myndighetsbeslut drar ut på tiden pga. försvårad informationsdelning beroende på störda IT-system. De periodvisa störningarna i lokal och regional elförsörjning, liksom i data- och telekomsystemen, bidrar tillförstärkta störningar i andra försörjningssystem och

samhällsfunktioner. Eftersom även Sveriges grannländer är drabbade förstärks problemen ytterligare av gränsöverskridande effekter.

Den upplevda otryggheten bland människor leder till indirekta effekter såsom exempelvis att det råder brist på vissa livsmedel pga. hamstring. Fler övergår också till att använda kontanter pga. störningar i betalkortssystemen, vilket leder till kontantbrist på vissa håll. Primärvården belastas av lokala utbrott av magsjuka. Räddningstjänsten belastas av en ökning av bränder pga. att människor använder uttjänta eldstäder samt lagar mat över öppen eld på exempelvis balkonger, när värme- och elsystem fallerar. Polisen belastas av ökade ordningsstörningar och ökad gängkriminalitet liksom av alltmer våldsamma uppgörelser mellan olika gäng som helt plötsligt förefaller blivit tyngre beväpnade. Vidare kan en markant ökning av den organiserade brottslighetens aktiviteter på den ekonomiska arenan konstateras, såsom bidragsfusk, skattebrott och penningtvätt. Särskilt drabbad är bank- och finanssektorn som utsätts för cyberrelaterade utpressningsförsök via s.k. ransomeware-attacker.

Ett falskt pressmeddelande som ser ut att komma från Säkerhetspolisen, avseende ökat terrorhot mot Sverige, får stor spridning i sociala medier. Dessutom förekommer motsvarande inlägg på sociala medier som kan tolkas som att de kommer från pålitliga källor såsom Sveriges Radio och Krisinformation.se. Detta skapar oro och förvirring och tar myndigheternas kommunikationsresurser i anspråk.

När den ansträngda situationen har varat i ungefär ett halvår blir främmande makts diplomatiska utspel allt mer aggressiva med indirekta hot om militärt våld. Påverkansoperationer på den internationella nivån intensifieras för att förhindra en gemensam hållning, främst inom EU. Denna påverkan sker bl.a. via diplomatiska framstötar, ekonomiskt bistånd, fördelaktiga handelsavtal, hot om indragna energileveranser och personliga kontakter. Sverige och de nordisk-baltiska grannländerna vill gemensamt med EU peka ut och vidta sanktionsåtgärder mot antagonisten men EU är politiskt splittrat. Vidare bidrar den svenska parlamentariska situationen, med en svag minoritetsregering och ett tämligen polariserat politiskt klimat, till att det är svårt att nå konsensus avseende hur Sverige ska bemöta hoten. Främmande makt underblåser den politiska splittringen genom att stödja ytterlighetsrörelser på såväl höger- som vänsterkanten, liksom att försöka påverka enskilda politiker inom etablerade partier.

Det är ovanligt kallt för årstiden så den individuella och lokala krisberedskapen sätts på svåra prov när störningarnas intensitet fortsätter att öka. Samhällsutnötningen och bristen på information om ”vad som egentligen händer?” ger påtagliga psykologiska effekter. Teorier om inhemsk terrorism och att händelserna skulle vara frukten av en konspiration för att få Sverige att överge sin traditionella säkerhetspolitik får visst fäste, vilket också underblåses av

främmande makts informationsoperationer via såväl statskontrollerade medier som sociala medier och somliga svenska debattörer.

Ökningen av fartygsrelaterade incidenter, svårförklarliga olyckor och konstaterade sabotage gör att redare i allt större utsträckning undviker hamnar och farleder i anslutning till Östersjön, inte minst pga. höjda försäkringspremier. Produktionen i viss tillverknings- och förädlingsindustri har dock redan stagnerat pga. brist på insatsvaror och komponenter till följd av IT-relaterade störningar i transportlogistiksystemen.

Ett omfattande cyberangrepp inträffar. Detta drabbar såväl Sverige som de närmaste grannländerna och under några dagar fungerar inte betalningssystemen, ledningssystemen för flyg- och tågtrafik samt mobiltelefonin. Den svenska krisberedskapen prövas hårt då också de fysiska sabotagen mot de nationella försörjningssystemen eskalerar. Störningarna som drabbar just el- och drivmedelsförsörjningen skapar stora följdeffekter i andra system, exempelvis påverkas både primärproduktionen av livsmedel och kylkedjan vid transporter, vilket får stora konsekvenser för möjligheten att distribuera färskvaror och frysta livsmedel. Störningarna påverkar därmed försörjningen av såväl inhemskt producerade som importerade livsmedel. Vissa skador som följd av sabotagen kommer att ta lång tid att reparera och därmed att återställa funktionalitet. Det är svårt att leda och samordna verksamheter och åtkomsten till elektroniska styrsystem är mycket begränsad. Därtill är det osäkert om hela VMA-systemet fungerar som planerat.

Försök till påtryckningar mot olika beslutsfattare ökar via epost, brev och hembesök. Här drabbas inte bara myndighetspersoner utan även nyckelpersonal inom privat samhällsviktig verksamhet. Företag med leveransavtal med Försvarsmakten förefaller vara hårdast drabbat av hot om våld och sabotage.

Det rapporteras från ett nordiskt-baltiskt grannland om sociala oroligheter mellan olika etniska grupper samt att några slags beväpnade lokala miliser gör sporadiska angrepp mot myndighetskontor och polisen. Samtidigt ökar främmande makts militära övningsverksamhet och omdispositioner i närområdet, liksom kränkningar av svenskt luftrum och sjöterritorium. Efter nio månaders störningar och svår samhällsansträngning är nu rädslan allmänt utbredd inom den svenska befolkningen och många som har möjlighet lämnar städerna och beger sig till släktingar eller fritidshus ute i landet. Vissa väljer till och med att lämna Sverige. Detta inte minst på grund av att en snar akut livsmedelsbrist kan skönjas. Ransonering förbereds men hamstringen av det som fortfarande finns tillgängligt eskalerar, liksom priserna. Solidariteten med andra i närmiljön är dock stor och många människor hjälper varandra i denna ansträngda situation medan andra inriktar sig på att skydda sina egna resurser, med våld om så är nödvändigt.

Befolkningen i allmänhet känner stor frustration och uttrycker starkt missnöje, vilket underblåses av främmande makts intensifierade propaganda och ryktesspridning, som bl.a. förmedlar bilden av att förnödenheter undanhålls befolkningen till förmån för Försvarsmakten och dess utländska samarbetspartners. Upplopp och plundring förekommer i flera svenska städer.

Vaga nyhetsrapporter, samt en flodvåg av tvetydig information på sociala medier, om stridshandlingar i det nordisk-baltiska grannlandet når den oroliga svenska allmänheten och de utarbetade svenska beslutsfattarna. Främmande makt varnar den svenska regeringen för att besluta om höjd beredskap, och därigenom ytterligare öka spänningen i närområdet, men kommer samtidigt med ett erbjudande. Sverige erbjuds humanitärt bistånd, och då i synnerhet vissa svårt drabbade kommuner vid Östersjökusten, i form av direktinförsel av förnödenheter, drivmedel, reparationsmateriel och teknisk personal.

ISSN1650-1942

www.foi.se