Strategisk verktygslåda mot hybridhot

Ett ramverk för gemensam problemförståelse

JESSICA APPELGREN, SEBASTIAN BAY,
JOHANNES MALMINEN, ERIK ZOUAVE

FOI-R--4816--SE
ISSN 1650-1942 Maj 2020

Jessica Appelgren, Sebastian Bay, Johannes Malminen, Erik Zouave

Strategisk verktygslåda mot hybridhot

Ett ramverk för gemensam problemförståelse

Titel	Strategisk verktygslåda mot hybridhot – Ett ramverk för gemensam problemförståelse
Title	Strategic toolbox for hybrid threats - A framework for common understanding of the problem
Rapportnr/Report no	FOI-R--4816--SE
Månad/Month	Maj
Utgivningsår/Year	2020
Antal sidor/Pages	48
ISSN	1650-1942
Kund/Customer	Utrikesdepartementet
Forskningsområde	Krisberedskap och civilt försvar
FoT-område	Inget FoT-område
Projektnr/Project no	B12520
Godkänd av/Approved by	Malek Finn Khan
Ansvarig avdelning	Försvarsanalys

Bild/Cover: Shutterstock

Sammanfattning

Den säkerhetspolitiska situationen präglas idag av instabilitet och oförutsägbarhet. Antagonistiska aktörer använder konventionella och okonventionella metoder på ett samordnat sätt för att uppnå särskilda mål i fredstid. Sverige behöver öka sin förmåga att motverka dessa så kallade hybridhot.

Utifrån EU:s gemensamma ram för att motverka hybridhot föreslås ett ramverk för en svensk strategisk verktygslåda. För att konkretisera den teoretiska diskussionen om hybridhot och det föreslagna ramverket presenteras ett fiktivt scenario med hybridangrepp mot Sverige. Scenariot redogör både för händelseutvecklingen och möjliga motåtgärder.

Med ramverket för en strategisk verktygslåda mot hybridhot som utgångspunkt redogörs för ett antal förslag på hur Sveriges förmåga att motverka hybridhot kan stärkas. Bland annat föreslås en nationell strategi för hybridhot, förstärkt övningsverksamhet, etablering av en nationell förstärkningsresurs, utveckling av kommunikativ beredskap, en översyn av lagstiftningen för att motverka hybridhot samt förstärkt erfarenhetshantering.

Nyckelord: hybridhot, hybridkrigföring, gråzon, påverkanskampanj, informationspåverkan.

Summary

Instability and unpredictability are key characteristics of the present security situation. In peacetime, antagonistic actors use conventional and unconventional means in a coordinated way to achieve specific goals. Sweden needs to increase its ability to counter these so called hybrid threats.

Based on the EU framework for countering hybrid threats, a framework for a Swedish strategic toolbox is proposed. In order to operationalise the theoretical discussion on hybrid threats, and the proposed framework, the report presents a fictitious scenario with hybrid threats aimed at Sweden. The scenario describes both the course of events and possible countermeasures.

With the framework for a strategic toolbox for countering hybrid threats as a starting point, a number of suggestions for strengthening Sweden's ability to counter hybrid threats are presented. Suggestions such as a national strategy for mitigating hybrid threats, enhanced exercises, the establishment of a national reinforcement capacity, the development of communicative preparedness, a review of relevant legislation for countering hybrid threats, and improved capabilities for hybrid threat investigation and evaluation.

Keywords: hybrid threats, hybrid warfare, grey-zone, influence campaign, information influence.

Innehåll

1 Inledning 7
1.1 Syfte 7
1.2 Metod 8
1.3 Disposition 8
2 Hybridhot 9
2.1 Ny säkerhetspolitisk hotbild 9
2.2 Perspektiv på hybridhot inom EU och Nato 9
2.3 Svenska perspektiv på hybridhot 10
2.4 Begreppets innebörd 12
2.4.1 Kombination av olika medel 12
2.4.2 Samordnat för att nå strategiska mål 13
2.4.3 Direkta angrepp eller genom ombud 13
2.4.4 Förnekbarhet och svårighet att se helheten 13
2.5 Förslag till begreppsanvändning 13
2.6 Hybridhot och hybridangrepp 15
2.7 Hybridangrepp eller hybridkrig? 15
3 Verktygslåda mot hybridhot 17
3.1 Målsättningar 17
3.1.1 Före, under och efter angrepp 18
3.2 Principer 19
3.2.1 Legalitet 19
3.2.2 Tillsammans med andra 20
3.3 Strategier 20
3.3.1 Reducera egna sårbarheter 20
3.4 Roller och ansvar 21
3.4.1 Krisberedskapssystemet 21
3.4.2 Rättsväsendet 22
3.4.3 Det militära försvaret 23
3.4.4 Totalförsvaret och höjd beredskap 23

3.4.5 Behov av speciallagstiftning? 24
3.4.6 Behov av omorganisering? 24
3.5 Förmågor 25
3.5.1 Motståndskraft 25
3.5.1.1 Medvetenhet 26
3.5.1.2 Detektion 26
3.5.1.3 Attribution 27
3.5.1.4 Strategisk kommunikation 27
3.5.1.5 Erfarenhetshantering 27
3.5.1.6 Nationell förstärkningsresurs 28
3.5.2 Motåtgärder 28
3.6 Verktyg 29
3.6.1 Militära verktyg 29
3.6.2 Politiska verktyg 30
3.6.3 Ekonomiska verktyg 31
3.6.4 Civila verktyg 31
3.6.5 Informationsverktyg 32
4 Scenario med hybridhot 33
4.1 Ett fiktivt scenario 33
4.2 Fiktiv hantering av scenariot 34
5 Vägen framåt 37
6 Slutnoter 38

1 Inledning

Det försämrade säkerhetspolitiska läget ställer ökade krav på svensk förmåga att motverka antagonistiska hot. Myndigheter, regioner och kommuner har återupptagit planeringen för civilt försvar för att öka svensk förmåga att motstå ett väpnat angrepp. Ökade resurser läggs även på att motverka organiserad brottslighet, extremism, cyberangrepp och informationspåverkan. Samtidigt saknas det en sammanhållen strategi för att motverka ett av de hot som i stor utsträckning kommit att dominera den säkerhetspolitiska debatten de senaste fem åren; hybridhot.

I den allmänna debatten, hos myndigheter, inom forskningen och i litteraturen används en rad olika begrepp för att beskriva samma eller liknande företeelser som det vi i denna rapport har valt att kalla hybridhot – exempelvis hybridkrigföring, icke-linjär krigföring, gråzonsproblematik och påverkanskampanjer. När ett fenomen – oavsett om det är nytt eller gammalt – uppmärksammas på bred front är det vanligt att begreppsförvirring uppstår. Begreppsförvirringen är en del i processen för att förstå och hantera fenomenet.

1.1 Syfte

Det säkerhetspolitiska samtalet har under de senaste åren präglats av diskussioner om hur stater kan möta hybridhot. Den europeiska unionen (EU), Nordatlantiska fördragsorganisationen (Nato) och ett antal stater i vårt närområde har tagit fram råd och riktlinjer inom området, men hitintills har det saknats ett sammanhållet grepp om hur dessa utmaningar påverkar Sverige och hur de bäst bör hanteras.

Alla länder har olika syn på vad som hotar och vad som är hotat, gränsdragningar mellan inre och yttre säkerhet, militärt och civilt. Denna rapport är ett försök att konceptualisera hybridhot utifrån en svensk kontext. Genom att strukturera målsättningar, principer, strategier, förmågor och verktyg utifrån en svensk kontext hoppas vi kunna bidra till en ökad förståelse för Sveriges säkerhetspolitiska och strategiska verktygslåda för att motverka hybridhot och möta hybridangrepp.

Rapporten riktar sig huvudsakligen till svenska beslutsfattare och tjänstemän på strategisk nivå.

Totalförsvarets forskningsinstitut (FOI) har för detta projekt beviljats projektstöd från Utrikesdepartementet (UD).

1.2 Metod

Rapporten bygger huvudsakligen på analys av ett antal rapporter, artiklar, studier och policydokument om hybridhot. Särskild vikt har lagts vid de råd och rekommendationer som utarbetats av EU, det Europeiska kompetenscentret för motverkandet av hybridhot (Hybrid CoE) samt av Multinational Capability Development Campaign (MCDC) Hybrid Warfare Project.

För att öka förståelsen för olika aktörers begreppsanvändning, rollfördelning och samordning genomfördes en nationell konferens om hybridhot ur ett säkerhetspolitiskt och strategiskt perspektiv. Vid konferensen deltog bland andra Regeringskansliet, Myndigheten för Samhällsskydd och Beredskap (MSB), Försvarsmakten, Polismyndigheten, Säkerhetspolisen (Säpo), Sveriges Riksbank, Riksgälden, Tullverket och Försvarets radioanstalt (FRA).

Författarna har även besökt och samverkat med en rad kunskapscentrum såsom the European Center of Excellence for Countering Hybrid Threats (Hybrid CoE), NATO Strategic Communications Center of Excellence (StratCom CoE) och the Development, Concepts and Doctrine Center (DCDC) för att diskutera frågeställningar och utmaningar inom området hybridhot.

Slutligen har författarna genomfört interna seminarier för att med stöd av sakkunniga experter analysera policy, begreppsanvändning och verktyg utifrån en svensk kontext.

1.3 Disposition

Rapporten beskriver inledningsvis vad hybridhot och hybridangrepp är, den säkerhetspolitiska kontexten och möjliga antagonister.

Utifrån denna genomgång föreslår rapporten ett ramverk för en svensk verktygslåda för att motverka hybridhot och möta hybridangrepp, samt diskuterar verktygslådans olika beståndsdelar.

Huvudfokus för rapporten ligger på Sveriges nationella strategier och de verktyg som Regeringskansliet och dess departement redan har till sitt förfogande för att motverka hybridhot. Genomgången beskriver såväl det svenska rättsliga ramverket för att motverka hybridhot som nu gällande ansvarsfördelning för hantering av hybridangrepp. För att konkretisera såväl hybridhot som möjliga verktyg för att motverka ett hybridangrepp så presenteras därefter ett fiktivt scenario för att möta hybridangrepp.

Med den föreslagna verktygslådan som utgångspunkt redovisas tankar kring den svenska verktygslådans styrkor och svagheter samt förslag på hur förmågan kan stärkas.

2 Hybridhot

Detta kapitel redogör för den förändrade säkerhetspolitiska hotbild som bidragit till att hybridhot kommit att ta en allt större plats på den säkerhetspolitiska dagordningen. Kapitlet beskriver även fenomenet hybridhot och etablerar den begreppsförståelse som används i rapporten.

2.1 Ny säkerhetspolitisk hotbild

Idag utmanar ett antal stater västvärldens traditionellt dominerande ställning i det internationella systemet. När framväxande stormakter vill ta större plats och ha mer inflytande ökar konkurrensen och konfliktytorna i det internationella systemet. Sammantaget har detta medfört en tilltagande polarisering och bristande tilltro till demokratiska institutioner, och demokratin befinner sig nu på tillbakagång i ett flertal länder.[1]

Den säkerhetspolitiska situationen har förändrats och försämrats sedan början av 2000-talet och präglas idag av instabilitet och oförutsägbarhet.[2] Det faktiska trendbrottet går det att tvista om, men Georgienkriget i augusti 2008 beskrivs ofta som en vändpunkt.[3] Om Georgienkriget var trendbrottet, ses idag Rysslands angrepp mot Ukraina och annektering av Krim 2014 som den faktiska vattendelaren där Ryssland fullt ut påvisade en vilja och förmåga att använda sig av alla till buds stående medel – inklusive militära – för att nå sina mål.[4]

Sedan annekteringen av Krim har Rysslands användning av hybridangrepp i olika former fått en hel del uppmärksamhet. Belysande exempel är Rysslands försök att påverka det amerikanska presidentvalet 2016, mordförsöket på den ryske före detta underrättelseofficeren Sergej Skripal och hans dotter i Storbritannien med hjälp av ett kemiskt stridsmedel samt cyberangreppet mot Organisationen för förbud mot kemiska vapen (OPCW) 2018.

Rysslands påtagliga likgiltighet inför överenskomna internationella normer och spelregler har förändrat Sveriges säkerhetspolitiska hotbild.[5]

Det centrala i den säkerhetspolitiska utvecklingen är hur en rad konventionella och okonventionella metoder nu används på ett sammansatt sätt för att påverka andra länder.[6]

2.2 Perspektiv på hybridhot inom EU och Nato

I Europeiska unionens gemensamma ram för att motverka hybridhot beskrivs hybridhot som en blandning av tvångsåtgärder och omstörtande verksamhet som en aktör, genom både konventionella och okonventionella metoder, på ett samordnat sätt använder för att uppnå särskilda mål. Detta gör aktören utan att

överskrida gränsen för krigföring, men genom att utnyttja den angripna statens svagheter och skapa osäkerhet för att försvåra den utsatta statens beslutsfattande.[7]

Enligt Nato är hybridhot en kombination av militära och icke-militära, såväl dolda som öppna, metoder. Exempelvis desinformation, cyberattacker, ekonomiska påtryckningar, utplacering av oregelbundna väpnade grupper och användning av reguljära styrkor. Nato menar att hybridhot används för att göra gränsen mellan krig och fred oskarp och för att så ett frö av tvivel hos den angripna staten.[8]

Natos kunskapscentrum för strategisk kommunikation (NATO StratCom CoE) beskriver hybridhot som nyttjandet av en bredd av verktyg, koordinerade, synkroniserade och medvetet riktade mot demokratiska stater och institutioners inneboende sårbarheter. Hybridhot anses exploatera gränsen mellan upptäckt och attribution och mellan krig och fred. Angriparen försöker påverka olika former av beslutsfattande på både lokal, regional och internationell nivå för att uppnå egna mål på den angripnes bekostnad.[9]

Det europeiska kompetenscentret för motverkande av hybridhot (Hybrid CoE) beskriver också hybridhot som samordnade och synkroniserade åtgärder som medvetet riktas mot demokratiska staters och institutioners systemiska sårbarheter. Syftet med hybridhot beskrivs som att påverka beslutsfattande på alla samhälleliga nivåer och undergräva den angripna staten för att uppnå egna strategiska mål. Enligt kunskapscentret utmanar hybridhot, förutom gränsdragningar mellan krig och fred, också gränsdragningar mellan internt och externt, nationell och internationell, och mellan vän och fiende.[10]

2.3 Svenska perspektiv på hybridhot

I den försvarspolitiska propositionen från 2015 använder regeringen begreppet påverkanskampanj för att beskriva en sammanhållen och centralt styrd verksamhet som nyttjar ett brett spektrum av såväl öppna som dolda kanaler. En påverkanskampanj, enligt propositionen, ”kan inkludera politiska, diplomatiska, ekonomiska och militära maktmedel, både öppet och dolt, för att nå så stor effekt som möjligt. […] Det kan kompletteras med falska dokument, smutskastning och hot, inklusive med militära medel, styrkedemonstrationer samt dolda operationer såsom fiktiva personer i sociala medier, falska dokument, frontorganisationer eller planterade nyheter. På detta sätt kan exempelvis vinklad, vilseledande eller oriktig information förmedlas som påverkar mottagarens vilja, förståelse, beteenden och attityd.” [11]

Regeringen bedömer i propositionen att Sverige bör utveckla sin förmåga att identifiera och möta påverkanskampanjer samt att berörda myndigheter och aktörer måste ha förmåga att kunna hantera påverkanskampanjer i fred och vid höjd beredskap. [12]

Försvarsberedningen använder i sina rapporter Motståndskraft[13] och Värnkraft[14] såväl hybridhot som ett antal andra begrepp för att beskriva en breddad hotbild där militära och icke-militära maktmedel används för att påverka vårt beslutsfattande och uppnå politiska och militära syften.[15] Försvarsberedningen hänvisar bland annat till ”ryktesspridning, motsägelsefull information, vilseledning och överraskning” där angriparen strävar efter att försvåra eller omöjliggöra vårt beslutsfattande och agerande.[16]

I Försvarsmaktens militärstrategiska doktrin (MSD 16)[17] används hybridhot och ett antal andra begrepp för att beskriva en hot- och riskbild som är bredare än den traditionellt militära. MSD 16 beskriver att den traditionella förståelsen av krig och fred utmanas när stater skapar allianser med icke-statliga aktörer för att utvidga det strategiska handlingsutrymmet och för att dölja sitt agerande och undvika att situationer eskalerar.[18]

I Försvarsmaktens och MSB:s gemensamma grundsyn används inte begreppet hybridhot, men myndigheterna konstaterar att ”Sverige kan utsättas för öppna och dolda påtryckningar som utövas med olika medel som politiska, psykologiska, ekonomiska och militära”. Påverkansoperationer beskrivs som ”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”.[19]

Säpo och Must använde tidigare begreppet påverkansoperation för att beskriva ”[s]amordnad och förnekbar verksamhet som initieras av en statsaktör […], huvudsakligen genom spridande av vilseledande eller oriktig information, ofta kompletterad med annan för ändamålet särskilt anpassat agerande.”[20]

Den militära underrättelse- och säkerhetstjänsten (Must) beskriver i sin senaste årsrapport hur Ryssland utvecklar och använder icke-militära och militära medel som kombineras för att uppnå bestämda mål.[21] Must använder begreppet ickelinjär krigföring för att beskriva när ”icke-militära och militära medel kombineras för att uppnå ett bestämt mål utifrån en specifik situation.”.[22] Säpo använder i sin senaste årsbok påverkansoperationer för att beskriva ”vilseledande eller oriktig information som sprids via sociala och traditionella medier.”[23]

Säkerhetspolisen använder inte heller benämningen hybridhot i sina senaste årsböcker, men fastslår att ”hotet mot Sverige är bredare och djupare än tidigare och kommer i många skepnader.” Hotet beskrivs som öppen och dold påverkan av främmande makt vilken riktar sig mot grundläggande individuella rättigheter, ekonomi, det politiska oberoendet och mot den territoriella suveräniteten.

Säpo nämner bland annat desinformation och strategiska uppköp av värdefull infrastruktur, teknik eller kunskap som två av flera metoder främmande makt använder. Vidare poängteras att ”oförutsägbarheten ökat och främmande makt agerar mer aggressivt i samhället, under tröskeln för väpnad konflikt.”[24]

MSB använder begreppen informationspåverkan, påverkanskampanj och påverkansaktivitet. Informationspåverkan definieras som ”potentiellt skadlig kommunikation som främmande makt eller deras ombud ligger bakom (medvetet eller omedvetet). [...] Informationspåverkan kan genomföras som enskilda aktiviteter eller som en del av en större påverkanskampanj.” Påverkanskampanj definieras som ”[…] en från främmande makt koordinerad verksamhet som innefattar vilseledande eller oriktig information eller annat för ändamålet särskilt anpassat agerande och som syftar till att påverka beslut av politiska eller andra svenska offentliga beslutsfattare, opinioner hos hela eller delar av den svenska befolkningen, beslut eller opinioner i ett annat land, där Sveriges suveränitet, målen för vår säkerhet eller andra svenska intressen kan komma att påverkas menligt.”[25]

Regeringen använder löpande i sin externa kommunikation såväl hybridhot[26] och hybridkrig [27] som påverkansoperationer [28] och påverkanskampanjer [29] för att beskriva i huvudsak snarlika fenomen.

2.4 Begreppets innebörd

Såväl inom EU och Nato, som inom Sverige, används hybridhot för att beskriva flera olika fenomen. Såsom redovisats ovan används även andra begrepp mer eller mindre synonymt för att beskriva likartade fenomen. Denna varierande, och föränderliga, användning av begrepp för att beskriva vad som i huvudsak kan betraktas som samma fenomen påvisar att det saknas gemensamma, eller vedertagna, definitioner inom detta område.

Men även om det saknas en allmänt accepterad definition så tycks många trots allt vara överens om vilken typ av hotbild det handlar om. Nedan listas några av hybridhotens mest centrala och vanligast förekommande teman.

2.4.1 Kombination av olika medel

Ordet ”hybrid” betyder korsningsform eller något som består av skilda arter,[30] vilket låter oss förstå att hybridhot utgörs av en kombination av flera olika maktmedel. Oaktat om det därför ska anses fel att benämna enstaka händelser eller separata medel för hybridhot,[31] verkar i alla fall de flesta anse att hybrid innebär att mer än en metod används.[32]

Antagonistens val och kombination av maktmedel beror på antagonistens intention och kapacitet, samt vilka tillfällen som presenterar sig i form av sårbarheter hos den stat som angrips.

Eftersom förmågan att kombinera konventionella och okonventionella maktmedel vanligtvis är central för begreppsdefinitionen så anses antagonisten ofta vara en stat, en statsliknande aktör, eller dess ombud.[33] I Sverige pekas ofta Ryssland och Kina, eller dess ombud, ut som möjliga antagonister med intention och kapacitet att utföra ett hybridangrepp mot Sverige.[34]

2.4.2 Samordnat för att nå strategiska mål

Maktmedel kan anpassas så att intensiteten höjs eller sänks genom att antalet maktmedel som används ökas eller minskas. Detta styrs av vilka effekter som eftersträvas.[35] Ett eller flera maktmedel kan användas för att uppmuntra en specifik attityd eller beteende – eller för att bestraffa andra attityder eller beteenden.[36]

Användningen av olika maktmedel kan koordineras för att uppnå ett syfte eller en målsättning. Det kan handla om specifika målsättningar, såsom att påverka en annan stats besluts- och handlingsförmåga eller att uppnå ekonomisk vinning. Det kan också röra sig om bredare mål såsom att långsiktigt undergräva demokratiska värderingar och rådande styrelseskick.[37]

Oavsett vilka målsättningar angriparen kan tänkas ha, kan de uppnås genom att på olika sätt utnyttja eller angripa en stats sårbarheter, det vill säga de skyddsvärden som en stat inte kan skydda på grund av bristande medvetande, resurser eller exponering. Kritiska funktioner och sårbarheter i en stat och dess samhälle kan finnas över ett brett spektrum av områden.[38] Det kan handla om tekniska sårbarheter i IT-system, sårbarheter kopplade till skydd av nyckelpersoner eller sårbarheter i mediesystem, opinionsbildning eller kognition.[39]

2.4.3 Direkta angrepp eller genom ombud

Hybridangrepp kan utföras direkt eller indirekt genom ombud som både medvetet, omedvetet eller genom hot och tvång tjänar angriparens intressen. Allt från underrättelse- och säkerhetstjänster, kriminella nätverk, företag och föreningar kan användas för att dölja vem som ligger bakom ett angrepp.[40] Användningen av ombud, i form av statliga eller icke-statliga aktörer, gör det möjligt för angriparen att undvika upptäckt och därmed även undvika en riktad motreaktion.

2.4.4 Förnekbarhet och svårighet att se helheten

Hybridangrepp kan skräddarsys för att undvika detektion och attribution för att i så stor utsträckning som möjligt ligga under tröskeln för en kraftfull motreaktion från den angripna staten. Detta gör att det kan vara både svårt och ta lång tid att tolka och förstå om och hur enskilda händelser hänger ihop och vem de utförs av.[41]

2.5 Förslag till begreppsanvändning

Ett antal olika aktörer använder olika begrepp och definitioner för att beskriva antagonistisk samordning av konventionella och okonventionella metoder för att påverka stater. Även om flertalet definitioner är påfallande lika så är det lika tydligt att det inte finns samstämmighet krig begreppsanvändningen, varken nationellt eller internationellt. I Sverige använder flera av de centrala aktörerna olika begrepp. Påverkanskampanj, påverkansoperation, icke-linjär krigföring, hybridhot och gråzonsproblematik är de mest frekvent förekommande.

Det är kanske inte avgörande att alla använder samma begrepp så länge det finns samförstånd om de utmaningar begreppen relaterar till. Risken är dock att den breda begreppsfloran gör diskussionen svårbegriplig eller missvisande, vilket riskerar att leda till att samverkan kring hybridhot försvåras, undergrävs eller permanent fastnar i en begreppsdiskussion. Att i denna situation föreslå ett begrepp och en definition som alla kan ställa sig bakom är troligen inte möjligt.

Vi konstaterar att både EU och Nato använder sig av begreppet hybridhot.[42] Även ett antal länder som Sverige har ett nära säkerhetspolitiskt samarbete med, såsom Finland,[43] använder sig av begreppet. Detta indikerar att hybridhot internationellt har etablerat sig som en gängse term för att beskriva det aktuella fenomenet inom den kontext Sverige vanligen agerar. Eftersom hybridhot inte kan mötas enbart nationellt, utan i mångt och mycket är beroende av internationell samordning, underlättar det troligen såväl nationellt som internationellt om Sverige använder samma begrepp som våra samarbetsparters.

En definition av hybridhot, för en svensk strategisk verktygslåda, föreslås därför utgå ifrån EU:s definition av hybridhot. Samtidigt är det viktigt att understryka att eftersom hotet hela tiden förändras, behöver vi kontinuerligt ompröva våra definitioner i takt med att hotet förändras.[44]

För att definiera hybridhot krävs ett antal avvägningar för att avgränsa det hot vi avser utifrån aktör, intention, kapacitet och tillfälle – en sådan definition bör också vara tydligt avgränsad mot andra typer av hot. Definitionen kan vara antingen snäv eller bred.

En snäv definition av hybridhot utgår från att hotaktören är en stat med betydande kapacitet att kombinera öppna och dolda metoder, militära och icke-militära, syftande till att påverka andra stater (direkt eller indirekt) genom att utnyttja stater eller målgruppers inneboende sårbarheter. Den avgränsar hybridangrepp till staters komplexa koordinerade angrepp på andra stater för att tydliggöra att det inte rör sig om enbart diplomati, subversion eller desinformation.

En bred definition speglar en övergripande problemförståelse och kan vara relevant även om mål och metoder utvecklas. En bred definition är politisk snarare än analytisk, då den bidrar till problemförståelse snarare än att vara ett praktiskt redskap för att identifiera och motverka hybridangrepp.

Vårt förslag till begreppsanvändning för denna rapport utgår ifrån en bred definition. En sådan definition är inte användbar för alla aktörer, alla tillfällen och för alla syften. Vi tror dock att en bred definition passar vårt föreslagna ramverk för att motverka hybridhot och möta hybridangrepp eftersom ramverket syftar till att skapa en helhetssyn snarare än att etablera en metod för att identifiera hybrid-angrepp.

2.6 Hybridhot och hybridangrepp

I denna rapport används **hybridhot** för att beskriva **en aktörs intention, kapacitet och möjliga tillfällen att använda konventionella och okonventionella metoder på ett samordnat sätt för att nå sina målsättningar i fredstid**. Verkställande av hotet benämns **hybridangrepp**. Exempel på hybridhot är bland annat samordnad användning av cyberangrepp, valmanipulation, desinformationskampanjer och underrättelseoperationer. Militära maktmedel kan förekomma i begränsad utsträckning; exempelvis i form av militär underrättelseinhämtning, fram- och omgruppering av militära förband eller andra åtgärder som projicerar hot.

Med aktör avses här en stat eller dess ombud, som har förmåga att kombinera konventionella och okonventionella metoder. Konventionell ska i denna definition förstås som öppna och direkta metoder; exempelvis diplomati, ekonomiska sanktioner och konventionella militära metoder. Med okonventionell avses metoder som är dolda, asymmetriska eller indirekta; exempelvis subversion, underrättelseoperationer, informationspåverkan, användning av ombud. I krigföringssammanhang kan okonventionell även syfta på vapensystem som använder kemiska, biologiska, radiologiska och nukleära tekniker, men detta är inte vad som åsyftas i detta sammanhang.

I vanligt språkbruk är ett hot antingen en varning om en negativ påföljd riktat mot ett objekt, eller en inneboende fara för negativ utveckling hos en person eller ett objekt.[45] I sådana sammanhang särskiljs ofta hotet (varningen eller kapaciteten) från aktiviteten (verkställandet av hotet).

I denna rapport definierar vi hot utifrån ett säkerhetsskyddsperspektiv, det vill säga att hot är en sammanvägning av angriparens intention, kapacitet och tillfälle.[46] Eftersom hotet är aktörsdrivet, ska det ses som en funktion av antagonistens medvetna agerande. **Intention** består av den uttalade eller påvisade vilja som angriparen innehar för ett angrepp.[47] **Kapacitet** är tillgängliga resurser för ett angrepp, vilket kan bestå av exempelvis personal, organisation, ekonomi och utrustning.[48] **Tillfälle** är tids- och rumsaspekter, det vill säga när en angripare har möjlighet att realisera angrepp.[49]

2.7 Hybridangrepp eller hybridkrig?

En central del av hybridbegreppet är hur det förhåller sig till begreppen krig och fred. En skiljelinje som framträder i diskussioner är i vilken utsträckning väpnat angrepp ska införlivas i definitionen, och i vilken mån ett hybridangrepp ska förstås som ett förstadium till krig.

Krig och fred är rättsliga begrepp som, förvisso utan att definieras, används i svensk författning. Sverige är enligt vår grundlag i fred fram tills dess att regeringen förklarar att riket är i krig. Regeringen får avge en sådan krigsförklaring

vid väpnat angrepp mot landet, i annat fall krävs riksdagens medgivande.[50] Även om företeelsen idag kan anses vara föråldrad då formella krigsförklaringar i praktiken inte längre används, medför den viktiga nationella rättsverkningar för Sverige. Är Sverige i krig blir vissa författningar automatiskt tillämpliga, medan vissa andra för fredstid anpassade författningar upphör att gälla.[51] De utredningar och förarbeten som ligger till grund för idag gällande grundlag kom fram till att det varken var möjligt eller eftersträvansvärt att definiera de händelser eller handlingar som kan anses innebära att krig råder, utan det ansågs att det är regeringens konstitutionella ansvar att avgöra vad krig är.[52]

Begrepp som inkorporerar suffixet ”-krig” eller ”-krigföring” används ofta för att beskriva situationer där icke-militära maktmedel nyttjas för att stödja väpnad strid. Begrepp som inkorporerar ”-hot” eller ”-angrepp” används ofta för att beskriva påverkan där militära maktmedel endast delvis ingår.

Utifrån en svensk kontext finns det fördelar med en tydlig begreppsanvändning kopplat till frågan om ”-hot” eller ”-krig”. Svensk lagstiftning gör en tydlig distinktion mellan krig och fred, vilket medför att användandet av ”-krig” eller ”-krigföring” medför betydande legala konsekvenser. Det är viktigt att notera att det i Sverige redan finns en omfattande verktygslåda för att förbereda inför, och att hantera, kriget – i form av totalförsvaret.

Det finns ett betydande internationellt regelverk för hur krig får föras – krigets lagar. För att inte utarma det internationella regelverket bedömer vi att det finns anledning att begränsa användningen av benämningen ”-krig” eller ”-krigföring” för att beskriva maktmedel som nyttjas i fredstid och som kanske inte innebär våldsanvändning.

En möjlig lösning på gränsdragningsproblematiken är att särskilja begreppsanvändningen av hybridhot och hybridkrigföring utifrån en svensk definition av krig och fred. Utifrån en sådan uppdelning kan hybridkrigföring definieras som konventionella och okonventionella metoder en aktör använder på ett samordnat sätt för att uppnå sina målsättningar under väpnad konflikt eller i en utsträckning som är att betrakta som ett väpnat angrepp. Exempel på hybridkrigföring är då väpnat angrepp mot Sverige understöds av sanktioner, subversion och informationspåverkan. Om Sverige utsätts för hybridkrigföring råder krig.

Gränsdragningen utifrån en sådan definition blir således skarp och understryker att det är regeringen, möjligen med riksdagens godkännande, som avgör om en händelseutveckling ska klassificeras som hybridkrigföring.

3 Verktygslåda mot hybridhot

Ett sätt att konkretisera hanteringen av hybridhot är att betrakta alla Sveriges tillgängliga resurser för att motverka hybridhot och möta hybridangrepp som verktyg i en verktygslåda. För att kunna använda verktygen behövs även målsättningar, principer, strategier, roller och ansvar. En verktygslåda innehåller alltså inte bara verktyg, utan även instruktionsböcker.

Nedan presenteras ett förslag för hur ett ramverk för en svensk strategisk verktygslåda för hantering av hybridhot skulle kunna se ut. Indelningen har inspirerats av EU:s gemensamma ram för att motverka hybridhot[53] med efterföljande riktlinjer.[54] Verktygslådan tar även hänsyn till andra relevanta aktörers tillvägagångssätt för att möta hybridhot, såsom MCDC Hybrid Warfare Project.[55] Däremot utgår förslaget från ett svenskt perspektiv och vad som skulle kunna anses vara användbart för svenska förhållanden.

Vårt förslag är att verktygslådan bör innehålla målsättningar, principer, strategier, roller och ansvar samt förmågor och verktyg.

- Målsättningar – VAD som ska uppnås och vad som ska värnas.
- Principer och strategier – HUR vi ska motverka hoten och bemöta angreppen.
- Roller och ansvar – VEM som gör vad för att motverka hoten och bemöta angreppen.
- Förmågor och verktyg – MED VAD ska vi motverka hoten och bemöta angreppen.

3.1 Målsättningar

Sveriges säkerhet handlar om mer än att enbart skydda landets territorium – ytterst ska säkerhetspolitiken garantera Sveriges politiska oberoende och självständighet.[56] Målen för Sveriges säkerhet är att värna befolkningens liv och hälsa, samhällets funktionalitet, miljö och ekonomiska värden, förmågan att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter samt nationell suveränitet.[57]

Målen för Sveriges säkerhet är styrande för såväl totalförsvaret som den svenska krisberedskapen. Totalförsvar är den verksamhet, bestående av militärt och civilt försvar, som behövs för att förbereda Sverige för krig, försvara Sveriges territorium och bidra till stabilitet och säkerhet i norra Europa.[58] Sveriges krisberedskap syftar till att värna målen för Sveriges säkerhet genom att skapa en förmåga att före, under och efter en kris förebygga, motstå och hantera krissituationer.[59]

Utifrån målen för Sveriges säkerhet har regeringen bestämt att målen för samhällets krisberedskap ska indelas i ett förebyggande perspektiv och ett hanterande perspektiv med målsättning att minska risken för olyckor och kriser som hotar vår säkerhet, värna människors liv och hälsa samt grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter genom att upprätthålla samhällsviktig verksamhet och hindra eller begränsa skador på egendom och miljö om olyckor och krissituationer inträffar. [60]

Statliga myndigheter har ett ansvar för att minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter under fredstida krissituationer och höjd beredskap, vilket medför att detta även gäller för hybridhot.[61]

Krisberedskapsarbetet ska också utgöra en utgångspunkt för arbetet med det civila försvaret, vilket innebär att värna civilbefolkningen, säkerställa de viktigaste samhällsfunktionerna och bidra till Försvarsmaktens förmåga vid ett väpnat angrepp eller krig i Sveriges närområde.[62]

Vår definition av hybridhot utgår från metoder som används i fred. Därmed är det definitionsmässigt målen för krisberedskapen snarare än målen för totalförsvaret som är vägledande för motverkande av hoten och bemötandet av angreppen. Det bör dock övervägas om målen för krisberedskapen är fullgoda målsättningar även vid hybridangrepp och om eventuella överlapp eller brister gentemot de mål som gäller för totalförsvaret finns. Det bör även utredas hur bemötande av hybridangrepp påverkas ifall regeringen fattar beslut om höjd beredskap och aktiverar totalförsvaret (se avsnitt om legala grunder).

Det saknas idag specifika målsättningar för att motverka hybridhot. Detta kan behöva utredas, och det är rimligt att anta att ett antal myndigheter behöver utveckla särskilda målsättningar för arbetet med att motverka hybridhoten och möta hybridangrepp.

3.1.1 Före, under och efter angrepp

Utöver att möta och motverka, går det att i enlighet med MCDC Hybrid Warfare Project dela in mål för bemötandet i faserna före, under och efter ett angrepp.[63]

Före ett angrepp är målbilden att förberedelser och förebyggande arbete bygger motståndskraft genom att reducera sårbarheter och öka förmågan att hantera effekterna av hybridhot. Förberedelser och förebyggande arbete bör avskräcka en antagonist från att angripa Sverige. Om ett angrepp sker så ska det säkerhetsskyddande arbetet vara tillräckligt effektivt för att angreppet inte fullt ska kunna verkställas och syftet med angreppet därmed inte uppnås.

Under ett angrepp har avskräckning och eget förbyggande arbete delvis eller helt misslyckats. Målbilden är nu att Sverige effektivt ska kunna identifiera, motstå och hantera angreppet. Sverige kan också behöva säkerställa att EU handlar gemensamt, och om så krävs, mobiliserar tillgängliga verktyg till stöd för Sverige och europeiska intressen. I detta arbete är den svenska utrikespolitiken av betydande vikt.[64]

Efter ett angrepp är målbilden att återställning efter angreppet har skett, att effekten av angreppet, såväl kortsiktigt som långsiktigt, har minimerats och att antagonisten ska ha avskräckts från ytterligare angrepp. Detta gäller såväl fysiska angrepp som informationspåverkan mot beteenden och attityder hos svenska och utländska målgrupper.

3.2 Principer

De förslag till principer som presenteras nedan bygger huvudsakligen på ett svensk synsätt på internationella relationer såsom uttryckt i den senaste utrikespolitiska deklarationen,[65] samt på generella råd och rekommendationer som etablerats av MCDC Hybrid Warfare Project,[66] EU:s gemensamma ram för att möta hybridhot[67] och *Hybrid Threats: A Strategic Communications Perspective* publicerad av Natos kunskapscentrum för strategisk kommunikation.[68]

Sverige bör utgå ifrån principer som grund för hanteringen av hybridhot.[69] Dessa principer kan förslagsvis ta sin utgångpunkt i vårt demokratiska styrelseskick, legalitetsprincipen (att all offentlig makt ska utövas i enlighet med lagen),[70] respekten för de mänskliga rättigheterna och det svenska synsättet att

> ”ett välfungerande internationellt samarbete och folkrätten är grunden för en världsordning där rättsstaten, regler och avtal går före den starkes rätt.”[71]

3.2.1 Legalitet

All svensk verksamhet för att motverka hybridhot måste respektera de grundläggande rättigheterna, inkluderat skyddet av personuppgifter, yttrandefriheten, informationsfriheten och föreningsfriheten.[72] Grundvalen för internationella relationer är att eventuella tvister ska lösas med fredliga medel; det är förbjudet för stater att använda, eller att hota om att använda, våld i deras förbindelser med varandra.[73]

Verktyg för att möta ett hybridangrepp kan exempelvis vara ekonomiska sanktioner, utvisning av diplomater eller straffrättsliga åtgärder.[74] Medan det finns ett brett utbud av potentiella motåtgärder, avråder Europarådet från motåtgärder som bryter mot den Europeiska konventionen om mänskliga rättigheter och understryker att alla motåtgärder måste vara lagliga, proportionella och nödvändiga i en demokrati.[75]

Konsekvensen av dessa utgångspunkter är troligen att Sverige inte kommer att använda sig av vissa verktyg som angriparen kan tänkas använda mot oss, till exempel subversiv verksamhet.

3.2.2 Tillsammans med andra

Även om stater är enskilt ansvariga för frågor som rör nationell säkerhet,[76] står många EU-stater inför en gemensam eller likartad problembild när det gäller hybridhot. EU är Sveriges viktigaste utrikes- och säkerhetspolitiska arena och regeringen beskriver i senaste utrikesdeklarationen att ”ingen annan aktör [än EU] är i så stor utsträckning en garant för svensk ekonomi, säkerhet och fred”.[77] Det finns en möjlighet för Sverige att åberopa den så kallade solidaritetsklausulen (artikel 222 i EUF-fördraget[78]) och be andra medlemsstater om hjälp ifall en allvarlig kris till följd av hybridangrepp behöver hanteras.[79]

Samordnade insatser på EU-nivå, genom EU:s politik och instrument, med utgångspunkt i europeisk solidaritet kan vara avgörande för små nationers förmåga att hantera hybridhot från resursstarkare motståndare.[80]

Sverige säkerhetspolitiska linje bygger på en aktiv utrikes- och säkerhetspolitik i kombination med fördjupade försvarssamarbeten, i synnerhet med Finland.[81] Sverige har nära relationer med övriga länder i Norden, Baltikum, EU och Storbritannien samt en nära säkerhetspolitisk relation med USA.[82]

3.3 Strategier

Utifrån en förståelse av hybridhot behöver Sverige utveckla en strategi för att motverka hybridhot. Hur denna strategi ser ut är i grunden beroende av nationella förutsättningar och prioriteringar och kan innefatta allt från att inte göra något alls, till en strategi som i sin ytterlighet bygger på förmåga till kraftfull vedergällning för att avskräcka eller bestraffa en angripare militärt.

Den strategi som utvecklas kommer delvis att vara beroende av en förståelse och bedömning av ett specifikt hot samt hotaktörens förmåga och bevekelsegrunder. Samtidigt krävs en övergripande strategi för att motverka hybridhot som bygger på svenska målsättningar, strukturer och principer.

Utöver en övergripande strategi lyfter EU[83], MCDC[84], Hybrid CoE[85] och StratCom CoE[86] två strategiska prioriteringar som är särskilt viktiga: Att reducera egna sårbarheter och att säkerställa egen förmåga att detektera hybridhot. Detektion hanteras i avsnittet om förmågor.

3.3.1 Reducera egna sårbarheter

En utgångspunkt för hanteringen av hybridhot är god förståelse av det egna samhällets styrkor och svagheter.[87] En antagonist kan komma att anpassa sitt förhållningssätt och inrikta sig på områden där riskkalkylen framstår som fördelaktig för syftet som ska uppnås. För att förvägra antagonister angreppspunkter är det därför viktigt att betrakta oss själva och åtgärda de sårbarheter en antagonist annars riskerar att angripa.[88]

Ett öppet demokratiskt samhälle kommer alltid att kunna utsättas för hybridangrepp, men god självkännedom om nationella, regionala och lokala förutsättningar ökar möjligheterna att motverka hybridhot. Utifrån kunskap om vårt eget samhälles styrkor och svagheter går det att genomföra ett långsiktigt arbete för att åtgärda våra sårbarheter.[89]

Till skillnad från kriser och samhällsstörningar som är icke-antagonistiska (exempelvis naturkatastrofer) är det förmodligen svårare att förutspå ett optimalt bemötande av hybridangrepp, eftersom antagonisten medvetet kommer att utnyttja de sårbarheter som finns i den svenska organisationen och samordningen.

Att identifiera svenska styrkor och svagheter ur en möjlig motståndares perspektiv är svårt. Däremot finns det goda möjligheter att utveckla scenarier, samt genomföra övningar och penetrationstester som systematiskt prövar och utvecklar vår motståndskraft och förmåga att möta hybridangrepp. Sådana övningar skulle kunna ge uppslag till viktiga förstärkningsåtgärder och prioriteringar i verksamheten.[90,91]

3.4 Roller och ansvar

Fredstida kriser och samhällsstörningar ska hanteras i enlighet med likhets-, ansvars- och närhetsprincipen, samt det geografiska områdesansvaret. För situationer som krigsfara och krig har Sverige beredskap i grundlag och annan författning som möjliggör balanserade förändringar i styrningen av landet och som underlättar samhällets omställning. Beroende på vilket begrepp som används för att definiera en situation blir alltså olika lagrum tillämpliga. Det här avsnittet syftar till att gå igenom de rättsliga premisser under vilka Sverige kan möta hybridhot.

3.4.1 Krisberedskapssystemet

Enligt nu gällande lagstiftning är hybridhot och hybridangrepp primärt en utmaning för samhällets krisberedskap och rättsväsendet. Sverige har en starkt decentraliserad krisberedskap, baserad på samverkan och samordning mellan självständiga myndigheter, självstyrande kommuner och regioner, ideella organisationer och näringsliv. Fredstida kriser och samhällsstörningar hanteras alltså inom ramen för ordinarie regelverk och förvaltningsstrukturer och grundar sig på likhets-, ansvars- och närhetsprincipen och på det geografiska områdesansvaret.[92]

Ansvarsprincipen innebär att den som har ansvar för en viss verksamhet under normala förhållanden har samma ansvar även i kris och är ålagt att samverka med andra aktörer.[93] Närhetsprincipen innebär att krisen ska hanteras där den inträffar och av närmast berörda aktörer. Likhetsprincipen innebär att samhället, så långt det är möjligt, ska fungera på samma sätt vid störningar som vid normala förhållanden. Det geografiska områdesansvaret är uppdelat på lokal, regional och

nationell nivå och innebär att utpekade aktörer har ett ansvar inom ett geografiskt område för inriktning, prioritering och samordning av tvärsektoriella åtgärder inför, under och efter en kris.[94]

På lokal nivå ansvarar kommunerna för delar av krisberedskapen och ska exempelvis inom ramen för sitt geografiska områdesansvar se till att kommunens aktörer samverkar och uppnår samordning under extraordinära händelser.[95]

På regional nivå är länsstyrelserna geografiskt områdesansvariga myndigheter och fungerar som den sammanhållande länken mellan olika aktörer inom länet och gentemot såväl andra län som nationell nivå. Länsstyrelserna är ansvariga för att sammanställa en samlad regional lägesbild i respektive län och ska ha en tjänsteman i beredskap (TiB) som initierar och samordnar det inledande arbetet för att upptäcka, verifiera, larma och informera vid allvarliga kriser som rör länet.[96]

På nationell nivå är regeringen geografiskt områdesansvarig, vilket innebär att det är regeringens uppgift, med stöd av Regeringskansliet, att på övergripande nationell nivå säkerställa effektiv krishantering. Regeringen ska också kommunicera med allmänheten, media och med internationella aktörer.[97]

Stora delar av det operativa krisarbetet har regeringen delegerat till berörda myndigheter där ansvaret för ledning och samordning ligger.[98] Statliga myndigheter ska genom sin verksamhet minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter under kris.[99] Myndigheter ska samverka vid kris och MSB ska stödja andra myndigheter med samordning, kommunikation, prioritering och lägesbildsarbete. MSB ska även kunna stödja och effektivisera krishanteringen, samt bistå Regeringskansliet med underlag och information i samband med kriser.[100]

Vissa bevakningsansvariga myndigheter har ett särskilt ansvar för att planera och vidta förberedelser för att skapa förmåga att hantera en kris, att förebygga sårbarheter och att motstå hot och risker. Myndigheterna ska samverka med länsstyrelser, andra statliga myndigheter, kommuner, regioner och näringsliv samt hålla regeringen informerad om händelseutvecklingen, tillgängliga resurser och åtgärder vid kriser. Dessa myndigheter har också ett ansvar att vidta de ytterligare förberedelser som krävs inom respektive ansvarsområde vid höjd beredskap.[101]

Näringslivet är också en viktig del av samhällets krisberedskap eftersom mycket av den verksamhet som är samhällsviktig idag drivs av privata företag. Näringslivets roll i krisberedskapen är dock i mångt och mycket oreglerad.[102]

3.4.2 Rättsväsendet

Rättsväsendet (polis, åklagare, domstol och kriminalvård) upprätthåller den enskildes rättssäkerhet och rättstrygghet genom att förebygga och bekämpa brottslig verksamhet, utreda brott, verkställa påföljder och ge stöd till brottsoffer.[103]

Hybridangrepp innefattar ofta aktiviteter som kan betraktas som brottslig verksamhet, såsom spionerі, olaga hot, olovlig underrättelseverksamhet, dataintrång och allmänfarlig verksamhet.[104] Detta medför att rättsväsendet har ett betydande ansvar för att förebygga, identifiera, utreda och lagföra verksamhet inom ramen för hybridhot. Det handlar både om att hantera specifika händelser såväl som att kartlägga och bidra till en övergripande lägesbild. Säkerhetspolisen har dessutom ett särskilt ansvar för att förebygga, förhindra och upptäcka verksamhet som innefattar brott mot rikets säkerhet.[105]

Polisen ansvarar för att bemöta all våldsanvändning som utförs av icke-statliga aktörer, eller till synes icke-statliga aktörer i Sverige.[106] Försvarsmaktens ansvar är tydligt avgränsat till främmande makts kränkningar av den svenska territoriella integriteten. Polisen har dock nyligen uttryckt ett behov av att utöka möjligheterna till stöd från Försvarsmakten till att omfatta fler situationer än vad nu gällande ordning medger – huvudsakligen för att stärka polisens förmåga att hantera hybridangrepp.[107] Förändringen är angelägen eftersom nuvarande regelverk skapar osäkerhet kring Försvarsmaktens möjlighet att stödja polisen för att möta ett hybridangrepp som inte kan attribueras till främmande makt.

3.4.3 Det militära försvaret

I fred ska Försvarsmakten försvara Sverige och främja svensk säkerhet, bland annat genom att bidra till att förebygga att konflikter uppstår, förvärras eller sprids. För att verka avhållande mot angrepp på Sverige ska Försvarsmakten upprätta och vidmakthålla en militär tröskel som avskräcker ett angrepp. Vid inre och yttre irreguljära och subversiva hot ska Försvarsmakten kunna nyttja delar av sin förmåga för att stödja andra aktörer. Försvarsmakten ska även kunna lämna stöd till det civila samhället i händelse av samhällsstörningar,[108] samt att bedriva omvärldsbevakning och upptäcka och identifiera yttre hot mot Sverige och svenska intressen.[109]

Om Sverige utsätts för hybridangrepp i form av begränsade kränkningar av den territoriella integriteten så möts dessa av Försvarsmakten, som har ett stående uppdrag att använda våld för att hävda Sveriges territorium under fred och neutralitet.[110] Denna rätt till våldsanvändning gäller endast vid kränkningar utförda av en annan stat eller vad som åtminstone kan antas vara en annan stat.

3.4.4 Totalförsvaret och höjd beredskap

Skulle Sverige utsättas för allvarliga hybridangrepp, även utan att krigshandlingar nödvändigtvis inletts, skulle åtgärder för att höja försvarsberedskapen i hela eller vissa delar av landet kunna behövas. I en sådan situation blir det totalförsvaret, det vill säga både det militära och det civila försvaret, som ska hantera hybridangreppen om det föreligger krigsfara.[111]

Regeringen kan besluta om skärpt eller högsta beredskap i händelse av krigsfara, ifall det råder utomordentliga förhållanden på grund av att det är krig utanför Sveriges gränser, eller på grund av att Sverige tidigare har befunnit sig i krig eller krigsfara.[112]

Under samma förutsättningar som ger regeringen rätt att besluta om höjd beredskap, kan regeringen också besluta att de så kallade fullmaktslagarna ska tillämpas. Det är lagar som till exempel möjliggör omdisponering av personella och materiella resurser och ingripanden i näringslivets och enskilda medborgares fri- och rättigheter.[113]

Vid höjd beredskap ska bevakningsansvariga myndigheter inrikta sin verksamhet på uppgifter av betydelse för totalförsvaret, hålla regeringen informerad om händelseutvecklingen, om vidtagna och planerade åtgärder och lämna underlag till Försvarsmakten. [114] Ordinarie verksamhet ska myndigheterna fortsätta med så långt det är möjligt, med hänsyn till personal och övriga förhållanden.[115] Länsstyrelsen ska som högsta civila totalförsvarsmyndighet inom länen verka för att största möjliga försvarseffekt uppnås. MSB företräder civilt försvar på nationell nivå och ska stödja myndigheters samordning av åtgärder vid höjd beredskap.[116]

3.4.5 Behov av speciallagstiftning?

Det pågår en diskussion om huruvida nuvarande krisberedskapslagstiftning är tillräcklig för att samhällets aktörer ska kunna vidta lämpliga åtgärder för att möta antagonistiska hot i fredstid.[117] Det finns historiska exempel på krissituationer som krävt ett effektivt beslutsfattande eller en anpassning av arbetsformer där befintlig lagstiftning inte upplevts tillräcklig. Viss hantering av dessa kriser har då skett utanför lagen, det har bland annat handlat om att enskilda statsråd fattat beslut för regeringens räkning eller ingripit i myndighetsutövning. Att offentlig makt ska kunna utövas i strid med lagen och ändå anses vara godtagbar på grund av situationens krav, så kallad konstitutionell nödrätt, har avfärdats i grundlagsutredningar och liknande, men har ofta accepterats i praktiken.[118]

Vid tidigare grundlagsutredningar[119] har det konstaterats att krishantering inte bör innefattas i grundlagen. Det har antingen ansetts onödigt eller så har enighet inte uppnåtts om vilka situationer sådana regler ska täcka in. Vilken reglering som behövs i annan författning än grundlag övervägdes däremot inte. Vi bedömer att det finns behov av att ytterligare utreda huruvida viss speciallagstiftning måste utformas för att tydliggöra roller och ansvar för att motverka och möta hybridangrepp.

3.4.6 Behov av omorganisering?

En fråga som ofta ställs är om det nuvarande svenska krishanteringssystemet, som i grunden skapades för att hantera icke-antagonistiska händelser, är tillräckligt för att motverka hybridangrepp? Klarar systemet av att detektera, analysera, samordna och styra ett stort antal departement och myndigheter för att prioritera och koordinera en konsekvensbegränsning av ett angrepp – såväl som att samordna svenska

och multilaterala motåtgärder för att påverka en motståndare att avstå från, eller upphöra med, angreppet?

Den i skrivande stund pågående kris till följd av Covid-19-pandemin har påvisat att regeringen har goda möjligheter att på relativt kort tid styra myndigheter med regeringsbeslut, såväl som att anpassa lagstiftning och tilldela extra ekonomiska resurser med hjälp av en ändringsbudget.[120] Ett omfattande hybridangrepp skulle kunna ställa motsvarande krav på en sammanhållen krishantering på regeringsnivå, dock med ett betydligt större fokus på de utrikespolitiska dimensionerna för att möjliggöra ett multilateralt bemötande.

Eftersom regeringen ansvarar för utrikes- och säkerhetspolitiken, kommer arbetet med att genomföra motåtgärder för att motverka ett hybridangrepp att behöva ledas och samordnas av regeringen. Detta ställer stora krav på ett nära och omfattande nationellt samarbete för att detektera, analysera och motverka hybridangrepp. Utrikesdepartementets förmåga att företräda Sverige och samordna de internationella kontakterna kommer att vara avgörande för att säkerställa ett multilateralt bemötande.

3.5 Förmågor

För att motverka hybridhot och möta hybridangrepp krävs ett antal specifika förmågor. Det förslag till förmågor som föreslås nedan utgår från de rekommendationer som EU,[121] MCDC[122], Hybrid CoE[123] och StratCom CoE[124] utvecklat. De är indelade i motståndskraft och motåtgärder.

Motståndskraft skapas genom att reducera egna sårbarheter och genom förmåga att reducera konsekvenserna av ett hybridangrepp.

Motåtgärder handlar om att påverka antagonistens vilja och förmåga att genomföra ett hybridangrepp.

Förmågan att skapa motståndskraft och förmågan att vidta motåtgärder går hand i hand. Syftet med både motståndskraft och motåtgärder är inledningsvis att förebygga sårbarheter och avskräcka den som hotar (före), för att därefter säkerställa effektiv hantering av angreppet (under och efter).

3.5.1 Motståndskraft

Motståndskraft[125] är proaktivt förberedande åtgärder[126] mot hybridhot, vilka inte är vedergällande eller bestraffande i sig. Förebyggande åtgärder bygger förmågor som är grundläggande för fortsatt bemötande av hybridhoten. Centrala delkomponenter för att bygga motståndskraft är medvetenhet, detektion och attribution.[127] Därtill tillkommer ett antal föreslagna förmågor som kommunikativ beredskap, förstärkt erfarenhetshantering och en nationell förstärkningsresurs som troligen kan bidra till att stärka svensk motståndskraft mot hybridhot.

3.5.1.1 Medvetenhet

Medvetenhet är nödvändig för snabb och effektiv planering och behandlas ofta som en funktion av utbyten mellan aktörer som har relevant information och kan använda informationen för att bemöta hoten; det vill säga mellan multinationella organisationer, stater, myndigheter och privat sektor.[128] Medvetenhet innefattar även kunskap om vilka motåtgärder som kan detektera och minimera konsekvenserna av hybridhot, och är därför en viktig del av arbetet med att välja lämpliga strategier och åtgärder för att motverka hybridhot.[129]

Mycket kan komma att vara otydligt vid ett hybridangrepp och komplett eller tillförlitlig information kommer troligen att saknas. [130] Sverige kan därför behöva utveckla förmågan att agera handlingskraftigt även i ett osäkert läge, för att kunna ta initiativet och självständigt sätta agendan för händelseutvecklingen.

Förmåga att agera handlingskraftigt även i ett osäkert läge kräver medvetenhet om hotet, planering, utbildning, och övning. Denna förmåga kan förstärkas med ytterligare övningsverksamhet.[131] För att förstärka den nationella övningsverksamheten för att öka förmågan att möta hybridhot skulle ett antal nationella scenarier för hybridhot kunna utvecklas. Sådana scenarier kan möjliggöra både en tydligare kravställning gentemot enskilda myndigheter och en sammanhängande gemensam problemformulering och planering.

3.5.1.2 Detektion

Hybridhot utmanar vår förmåga att upptäcka antagonistisk verksamhet riktad mot Sverige. Utvecklad och anpassad underrättelseförmåga som klarar av att upptäcka hybridangrepp mot såväl kritiska sårbarheter som samhället i stort är sannolikt väsentlig för vår förmåga att hantera hybridhot.[132] Att detektera hybridangrepp är inte enbart en fråga om att generera kunskap om att ett angrepp pågår och vem som är ansvarig för angreppet, utan även att sammanställa information som kan användas för att övertyga och samordna interna och externa aktörer.[133]

Detektion syftar till att säkerställa tidig förvarning om hybridangrepp och bygga underlag för beslut om motåtgärder.[134] Eftersom hybridangrepp är en sammansättning av olika maktmedel som riktar sig mot olika sårbarheter och manifesteras genom olika typer av maktutövning, behövs olika sensorer, förmågor och resurser för att detektera angrepp. Därför kräver effektiv detektion formaliserade samarbeten, utbyte av information samt mandat och resurser för att producera nationella analyser och bedömningar.[135]

Att upptäcka angrepp handlar exempelvis om att identifiera mönster och sammanställa indikatorer.[136] Arbetet med att upptäcka angrepp kan vara beroende av en god förmåga till tidig varning och lägesbild.[137] Tidig förvarning handlar om att detektera tidskritisk information om motståndares styrkor, förmågor, aktiviteter, normalbeteenden och avvikelser i syfte att förvarna om antagonistiska avsikter.[138] Lägesbilder är ett övergripande beslutsunderlag som beskriver den kännedom berörda aktörer, exempelvis myndigheter, innehar om hybridhot eller hybridangrepp vid en viss tidpunkt.[139]

3.5.1.3 Attribution

Attribution[140] handlar om att koppla påståenden, handlingar och händelser till specifika stater, organisationer eller individer. Attribution kan vara både teknisk och politisk.[141] Offentlig attribution kan i vissa fall vara nödvändig för att mobilisera nationella eller internationella resurser för att möta ett hybridangrepp.[142] Eftersom hybridangrepp kan vara utformade för att undvika detektion, kan det vara svårt att uppnå tillräcklig kunskap om särskilda fall som möjliggör tillförlitlig attribution.[143]

Attribution har visat sig vara särskilt svårt vid exempelvis cyberangrepp och digital påverkan.[144] Samtidigt attribuerar både sociala mediebolag[145] och grupper av undersökande journalister[146] framgångsrikt olika typer av hybridangrepp. Det kan i vissa fall också finnas en risk för falsk eller felaktig attribution, vilket riskerar att undergräva förtroendet för en stat och försvåra motverkandet av hybridhot. Samtidigt visar ett antal exempel, såsom Skripal-fallet, på att framgångsrik attribution kan skapa nationell och internationell enighet. Attribution kan även bidra till att bygga ökad motståndskraft genom att öka medvetenheten hos beslutsfattare och allmänhet.[147]

3.5.1.4 Strategisk kommunikation

En betydande del av den svenska strategin för hybrida hot kommer troligen behöva bygga på vår förmåga att påverka antagonisten och att säkra intern och extern sammanhållning. För att framgångsrikt påverka olika målgrupper behöver Sverige ha en god förmåga att målgruppsanpassa och förmedla kommunikationen.

I händelse av hybridangrepp kan Sverige dessutom behöva en förstärkt förmåga att ta emot ett stort antal journalister, inklusive logistik, tillträde och stöd för att förstå och tolka den svenska kontexten. Utrikesdepartementet (UD) stödjer idag utländska journalister inom ramen för UD:s internationella presscenter, men troligtvis kan behov av ytterligare resurser tillkomma i händelse av ett omfattande angrepp. Sådana resurser kan på förväg behöva säkerställas i dialog med andra aktörer i samhället.

3.5.1.5 Erfarenhetshantering

Eftersom hybridhot konstant utvecklas, ändras och anpassas så finns det god anledning att säkerställa att det finns en godtagbar förmåga för att kontinuerligt och systematiskt följa och analysera lärdomar från andra länder, vad de vidtar för skyddsåtgärder och hur de agerar när de utsätts för hybridangrepp.[148]

Det finns därför anledning att ytterligare studera hur Sverige kan utveckla en förberedd och övad förmåga att analysera genomförda hybridangrepp för att långsiktigt hantera effekterna av angrepp och därmed minimera dess negativa konsekvenser.[149]

3.5.1.6 Nationell förstärkningsresurs

Under och efter ett hybridangrepp kommer det att vara viktig att kunna identifiera och kommunicera att det sker, eller har skett, ett hybridangrepp. Trovärdig och effektiv attribution kräver att flera aktörer är involverade, inkluderat privata företag, nyhetsmedia, forskningsinstitut och akademin. Det kan medföra ett behov av att bygga upp en förstärkningsorganisation av såväl statlig som privat analysförmåga som snabbt kan mobiliseras för att bidra med identifikation, attribution och kommunikation. Regeringen kan även behöva styra och prioritera tillgängliga statliga utredningsresurser för att kunna möta ett snabbt händelseförlopp. För effektiv krishantering kan en sådan struktur behöva upprättas och övas regelbundet.

En nationell förstärkningsresurs skulle även kunna nyttja multinationella samarbeten, ramverk och resurser.[150] Det finns flera exempel på sådana samarbeten. Inom EU bidrar bland annat EU Hybrid Fusion Cell, EU:s underrättelseanalyscentrum (EU INTCEN), EU:s snabbvarningssystem för desinformationskampanjer (Rapid Alert System), East Stratcom Taskforce, EU:s Computer Emergency Response Team (CERT-EU) och Critical Infrastructure Information and Warning Network (CIWIN) med analyser och delar information om indikatorer för tidig varning.[151] Nato:s gemensamma underrättelse- och säkerhetsavdelning (Joint Intelligence and Security Division) etablerades bland annat för att öka alliansens förmåga att förstå och analysera hybridhot.[152]

3.5.2 Motåtgärder

Att påverka en angripares vilja handlar om att påverka angriparen genom att antingen påvisa att den angripna staten kan motstå tänkbara angrepp på ett sätt som blockerar en angripares möjligheter att nå framgång med ett angrepp (*deterrence by denial*) eller genom att påvisa att den angripne har förmåga att bestraffa ett angrepp på ett sätt som förändrar en motståndares kostnadskalkyl (*deterrence by punishment*).[153]

Att påverka en angripares förmåga innebär offensiv verksamhet som riktar in sig på att reducera angriparens möjlighet att genomföra hybridangrepp. Det kan exempelvis handla om att utvisa underrättelsepersonal, att identifiera och avbryta säkerhetshotande verksamhet eller att motverka antagonistens utnyttjande av tekniska plattformar.

För att kunna påverka en angripare behöver den som angrips ha en god uppfattning om antagonistens förutsättningar, styrkor och svagheter. I detta ingår bland annat en förståelse för antagonistens historia, kultur, strategiska tänkande och kostnadskalkyl. Det som gör ont för oss eller skadar vårt sätt att leva behöver inte vara detsamma som gör ont för angriparen. Samtidigt är det nödvändigt att ha god kännedom om effekterna av svarsåtgärderna i det egna samhället.[154]

Effektiva motåtgärder behöver dessutom kunna mätas eller utvärderas för att avgöra om avskräckning faktiskt uppnås, vilket medför att motåtgärder kan förstås som en process med stegvis utvärdering tills dess att angriparens vilja och förmåga ändrats.[155]

3.6 Verktyg

I denna rapport väljer vi att kategorisera de verktyg som används för att möta hybridhot efter MPECI.[156] Militära-, politiska- (även diplomatiska), ekonomiska-, civila- (även legala och underrättelsebaserade) och informationsverktyg.

Hybridhot är samordnande och kräver ofta ett samordnat bemötande. Det medför att flera kategorier av verktyg kan behöva användas gemensamt för att uppnå de effekter och mål vi strävar efter. Kombinationsmöjligheterna för den angripnes svarsåtgärder är i princip oändliga. Gemensamt för alla verktyg för att möta hybridhot är att de måste skräddarsys utifrån varje enskilt fall och de mål som ska uppnås på kort och lång sikt.

I detta kapitel redovisas ett urval av specifika verktyg inom ett antal kategorier. Ytterligare kategorier och specifika verktyg kan komma att behöva utvecklas för att motverka ett specifikt hybridangrepp, utifrån dess unika förutsättningar och mål.

3.6.1 Militära verktyg

Militära verktyg syftar ofta till att påverka motståndarens vilja och förmåga att angripa Sverige med militära medel. Styrkeuppvisningar och faktisk uppbyggnad av militär förmåga kan syfta till att övertyga motståndaren att Sverige har vilja och förmåga att nyttja militära verktyg i sådan utsträckning att angriparens kostnadskalkyl för ett angrepp förändras.

Med vår definition (se avsnitt 2.6) av hybridhot och hybridangrepp som medel i fred, är det militära verktyget mindre framträdande. För den som använder begreppet hybridkrig som utgångspunkt, kommer det militära instrumentet däremot att vara centralt.

I fred har Försvarsmakten en viktig roll när det gäller såväl att försvara territoriet mot kränkningar som att bistå krisberedskapen med resurser för att hantera extraordinära händelser.

I en del resonemang om hanteringen av hybrida hot lyfts möjligheten till s.k. ”force projection” upp, det vill säga att med militära styrkedemonstrationer såsom övningar och omflyttning av förband påvisa kapacitet och intention att vid behov använda militärt våld.

Militära verktyg kan således användas för såväl motståndskraft som motåtgärder. Det kan handla om allt från att värna svenskt territorium med våld till att bygga en avskräckande militär förmåga.

Exempel på militära verktyg:

- Militära övningar
- Militär styrkeuppbyggnad
- Defensiv militär verksamhet.

3.6.2 Politiska verktyg

Eftersom hybridhot och hybridangrepp syftar till att påverka staters politiska beslutsfattande spelar den politiska nivån en central roll för att motverkan hybridhot.

Politiska verktyg inkluderar styrning och prioritering av statens resurser, samt exempelvis utvisning av diplomater, införande av reserestriktioner och diplomati. Diplomati innehåller i sig ett stort antal specialverktyg, däribland strategisk kommunikation, folkrättsliga bedömningar, utpekande av främmande makt och internationellt samarbete. Fler av de diplomatiska verktygen handlar om att samordna och möjliggöra andra verktyg i den övergripande strategiska verktygslådan.[157]

Exempel på politiska verktyg:

- Politisk signalering
- Nationell prioritering, styrning och samordning
- Diplomati
- Gemensamma aktioner med andra stater och organisationer
- Politisk utpekning av antagonister.

Med utgångspunkt i svenska förvaltningsprinciper har den politiska nivån (huvudsakligen riksdag, regering och Regeringskansliet) nedanstående ansvarsområden.

Före ett hybridangrepp ansvarar den politiska nivån för att prioritera, styra och samordna svensk motståndskraft mot hybridangrepp. Ansvaret innefattar resurstilldelning, övning och utvärdering av svensk förmåga att motstå och motverka ett angrepp. Ett särskilt ansvar tillfaller den politiska nivån för att tillse att det finns internationella samarbeten för informationsutbyte och hantering av hybridangrepp.

Under ett hybridangrepp ansvarar den politiska nivån för strategisk kommunikation, operativ samordning, nationell sammanhållning, diplomati och internationell samordning, samt eventuell offentligt utpekande av angriparen.

Efter ett hybridangrepp ansvarar den politiska nivån för att tilldela och prioritera resurser för att säkerställa återställning. Långsiktigt ansvarar den politiska nivån

för att utvärdera och tillvarata erfarenheter från angreppet, samt att stärka förmågan inför framtida angrepp.

Offentlig diplomati samt intern- och extern kommunikation är viktiga verktyg för att säkra egen och extern sammanhållning likväl som för att bemöta antagonistens informationspåverkan. Förmåga att genomföra effektiv offensiv kommunikation kan också verka avskräckande om den angripne kan uppvisa betydande förmåga att attribuera och skapa politiska kostnader för antagonisten.

3.6.3 Ekonomiska verktyg

Ekonomiska verktyg förknippas ofta med sanktioner och handelsrestriktioner gentemot länder, organisationer eller individer. Ekonomiska verktyg kan även vara ekonomiskt bistånd eller reduktion av ekonomiska barriärer för att påverka olika målgrupper. Inom kategorin ekonomiska verktyg ryms även en rad direkta och indirekta finansiella verktyg, såsom att frysa ekonomiska tillgångar eller förhindra in- eller utlåning från finansiella institutioner.[158]

Exempel på ekonomiska verktyg:

- Ekonomiska sanktioner
- Ekonomiskt bistånd
- Handelshinder och handelslättnader
- Finansiella hinder och regleringar
- Frysning av ekonomiska tillgångar.

Ekonomiska verktyg används ofta som en bestraffande, eller möjligt bestraffande, åtgärd gentemot stater eller individer som är centrala för genomförande av ett hybridangrepp. Ekonomiska verktyg kan även användas som belöning för att uppmuntra ett specifikt beteende eller förebyggande för att påverka antagonistens förmåga till hybridhot, exempelvis genom att identifiera och stoppa finansiella överföringar till grupper verksamma i Sverige.

3.6.4 Civila verktyg

Civila verktyg används ibland som ett samlingsbegrepp för allt från rättsprocesser till underrättelseverksamhet. Här räknas såväl polisiära resurser, som åtal, offentliga utredningar, underrättelseinhämtning och lagstiftning in.[159]

Exempel på civila verktyg:

- Underrättelseinhämtning
- Polisiära resurser
- Rättsprocesser
- Offentliga utredningar
- Lagstiftning.

I en rättsstat som Sverige är rättsprocesser av sin natur oberoende från den verkställande och lagstiftande makten och den politiska nivån kan inte använda rättsprocesser som verktyg för att nå statens målsättningar. Däremot är det ett politiskt ansvar att tillse att rättsväsendet har tillräckliga resurser och att det finns väl fungerande lagar på plats. Rättsväsendets förmåga är viktig för att bygga motståndskraft mot hybridangrepp. Underrättelseinhämtning är i sin tur ofta avgörande för att kunna detektera och attribuera ett hybridangrepp.

3.6.5 Informationsverktyg

Informationsverktyg innefattar reglering, kontroll och användning av informationsmiljön. Utifrån ett defensivt perspektiv kan information användas för att möta informationspåverkan. Cyberförsvar och cyberangrepp som verkansmedel i informationsmiljön faller också inom denna verktygskategori. [160]

Exempel på informationsverktyg:

- Cyberförsvar
- Psykologiskt försvar
- Reglering av informationsmiljön.

Förmågan att skydda sig mot cyberangrepp är en central komponent för att bygga motståndskraft mot hybridhot – samtidigt kan en offensiv cyberförmåga verka avskräckande för en antagonist. Det är dock viktigt att notera att en offensiv cyberförmåga även kan användas för att hindra eller störa antagonistens förmåga att genomföra hybridangrepp. Digital attribution har dessutom visat sig vara en viktig komponent för att kunna peka ut ansvariga aktörer.[161]

Åtgärder inom ramen för psykologiskt försvar är också viktiga verktyg inom informationsdomänen. Det kan handla om att säkerställa befolkningens försvarsvilja i fred, att saklig information snabbt och effektivt kan förmedlas även under störda förhållanden, samt att myndigheter kan identifiera, analysera och möta informationspåverkan. Psykologiskt försvar innefattar även åtgärder för att stödja oberoende media och genomföra satsningar för att stärka forskning och utbildning.[162]

Reglering av informationsmiljön för att motverka manipulation av sociala medieplattformar fortsätter vara en viktig komponent för att bygga motståndskraft mot informationspåverkan och hybridangrepp.[163]

4 Scenario med hybridhot

Detta kapitel redogör för ett möjligt scenario med hybridangrepp mot Sverige och vårt närområde. Scenariot syftar till att konkretisera den teoretiska diskussionen om hybridhot och vårt föreslagna ramverk för en strategisk verktygslåda för att motverka hybridhot. Det är viktigt att påtala att ett möjligt scenario inte säger något om sannolikheten för att ett scenario ska utspela sig just på det sättet.[164]

Scenariot bygger på ”Typfall 5: Utdragen och eskalerande gråzonsproblematik”[165] som FOI, på MSB:s uppdrag, tagit fram för planeringen av civilt försvar. Typfallet har anpassats för att avgränsas till vår föreslagna beskrivning av hybridangrepp, vilket medför att scenariot formulerats som ett förlopp utan eskalation mot en konfliktsituation där nästa steg kan förväntas vara ett väpnat angrepp. Hanteringen sker därmed inom ramen för regelverket avseende krishantering. Scenariot utspelar sig alltså inte i ett förstadium till krig. Syftet med antagonistens handlande i detta scenario är att lamslå svenskt beslutsfattande, att isolera Sverige internationellt och att förändra EU:s politik gentemot antagonisten.

4.1 Ett fiktivt scenario

Den senaste tiden har Sveriges relation till främmande makt försämrats markant. För att förändra den politiska inriktningen använder främmande makt hybridangrepp mot ett antal länder inom EU. Konsekvenserna av främmande makts agerande är att Sverige, tillsammans med de andra särskilt utsatta länderna, blir allt mer isolerade och det allmänna stödet för Sverige inom Europa och EU minskar.

Den säkerhetspolitiska situationen i närområdet är ansträngd och det har skett en rad dolda angrepp såsom cyberangrepp och sabotage mot samhällsfunktioner i såväl Sverige som i Finland.

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 begränsad men bland allmänheten sprider sig ändå viss oro.

Spridandet av desinformation, som ibland oreflekterat sprids vidare i svenska traditionella medier, förmedlar en skev bild av Sverige. Den svenska allmänheten utsätts för informationspåverkan i frågor som berör ordning och trygghet, migration och integration, krisberedskap och försvar, samt utrikes- och säkerhetspolitik.

Informationspåverkan, som i första hand utnyttjar Sveriges öppna informationsinfrastruktur i form av sociala medier och bloggar, liksom indirekt TV, radio och

tidningar, får negativ påverkan på allmänhetens förtroende för myndigheter och politiker.

Främmande makts underrättelseverksamhet i Sverige och i grannländerna ökar. Det gör även en allt mer konfrontativ diplomatisk retorik i kombination med spridning av desinformation via främmande makts statskontrollerade medier. Eftersom Sveriges grannländer också är drabbade förstärks problemen ytterligare av gränsöverskridande effekter. Den upplevda otryggheten leder till indirekta effekter såsom ordningsstörningar och ökad belastning på räddningstjänst.

När den ansträngda situationen pågått i ungefär ett halvår blir främmande makts diplomatiska utspel allt mer aggressiva. Angreppen intensifieras för att förhindra en gemensam hållning, i synnerhet inom EU. Denna påverkan sker bland annat via diplomatiska utspel, hot om indragna energileveranser och subversiv verksamhet. Sverige och de nordisk-baltiska grannländerna vill gemensamt med EU peka ut en statsaktör som ansvarig och vidta sanktionsåtgärder, men EU är politiskt splittrat.

Påfrestningen på samhället 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 informationspåverkan via såväl främmande makts statskontrollerade medier som via internationella sociala medier.

Den svenska krisberedskapen prövas tidvis hårt; lokala sabotage utförs regelbundet. Vissa försök till påtryckningar mot olika beslutsfattare genomförs via epost, brev och hembesök. Här drabbas inte bara myndighetspersoner utan även nyckelpersonal inom privat samhällsviktig verksamhet. Samtidigt ökar främmande makts militära övningsverksamhet och förflyttning av militära förband i närområdet, liksom omfattande kränkningar av svenskt luft- och sjöterritorium.

4.2 Fiktiv hantering av scenariot

Vårt förslag till möjlig hantering är fiktivt och naturligtvis spekulation, då liknande händelseförlopp inte inträffat i Sverige tidigare. Förslaget bygger på vår tolkning och förståelse av befintliga lagar, ramverk och principer samt på hur dessa skulle kunna användas för att hantera ett mer omfattande hybridangrepp.

Media, försvarsbloggare och säkerhetspolitiska experter har under en längre tid rapporterat öppet om den försämrade säkerhetspolitiska situationen i närområdet. Underrättelsemyndigheterna har under en tid i såväl öppna som hemlig rapporter analyserat det försämrade säkerhetspolitiska läget och Säkerhetspolisen har tillsatt en särskild kommendering för att följa händelseutvecklingen.

De inledande sabotagen och IT-angreppen plockas snabbt upp av media och ett flertal experter börjar tidigt spekulera i om det finns ett samband. Misstankarna

riktas mot främmande makt, men det saknas konkreta bevis. I den inledande fasen hanteras störningarna av enskilda myndigheter, men det blir snart tydligt att det finns ett behov av såväl samordning som en gemensam lägesbild.

MSB begär in information från alla berörda aktörer för att påbörja arbetet med att upprätta en gemensam lägesbild. När situationen försämras går MSB upp i särskild organisation för att stärka beredskapen och tilldela ytterligare resurser till lägesbildsproduktion, stöd till samverkan samt förmedling och prioritering av stödresurser.

Flera av de värst drabbade myndigheterna går upp i stabsläge för att kunna prioritera resurser och se till att den dagliga hanteringen av störningarna fungerar relativt friktionsfritt.

Omfattande informationspåverkan gör att bilden av händelseförloppet blir svårkontrollerad. Myndigheterna lägger därför mycket resurser på att bemöta felaktig information med korrekt information. Det blir dock allt mer uppenbart att det rör sig om informationspåverkan från resursstarka grupper. Trots betydande samverkan med de sociala medieplattformarna, går det inledningsvis inte att bringa klarhet i vem som kan ligga bakom verksamheten.

Lokala medier och ett internationellt nätverk för grävande journalistik lyckas till slut påvisa att observerad informationspåverkan är koordinerad från främmande makt. Flera lokala aktörer är involverade, men troligtvis har de själva inte förstått vem som har finansierat och understött deras verksamhet.

Trycket ökar på sociala medieplattformar att tillgängliggöra information som möjliggör kartläggning av främmande makts informationspåverkan. Säkerhetspolisen påbörjar en förundersökning för att utröna om lokala aktörer tagit emot ersättning från främmande makt för att påverka opinionen i Sverige.

Med hjälp av underrättelseinformation från underrättelsemyndigheterna, gemensam lägesbild från MSB, information från andra stater och analys av öppna källor så framgår det tydligt för Regeringskansliets kansli för krishantering vilken främmande makt det är som ligger bakom hybridangreppen.

Inrikesministern sammankallar gruppen för strategisk samordning och krishanteringsrådet för att samordna informationen till och från myndigheterna. Regeringen fattar en rad regeringsbeslut för att ge uppdrag till ett antal berörda myndigheter att prioritera frågan och stödja andra myndigheter. Extra resurser fördelas till de mest berörda myndigheterna. Regeringen beslutar även att flera myndigheter får en utökad anslagskredit för att kortsiktigt kunna hantera de pågående påfrestningarna. En ändringsbudget förbereds för att vid behov kunna tillföra myndigheterna ytterligare medel.

Regeringen förbereder även en diplomatisk offensiv för att säkerställa stöd från EU:s övriga medlemsstater. En grupp myndigheter får till uppgift att tillhandahålla

löpande och fördjupande information och material till Utrikesdepartementet och Svenska institutet. Ett antal svenska PR-byråer direktupphandlas för att stödja regeringens arbete och diplomatiska offensiv.

För att understryka allvaret i situationen, samt för att säkerställa stöd från andra medlemsstater, åberopar Sverige solidaritetsklausulen (artikel 222 i EUF-fördraget) för att hantera den kris som uppstått pga. främmande makts hybrid-angrepp.

Tack vare ett omfattande arbete lyckas Sverige vända opinionen i unionen och EU närmar sig beslut om sanktioner och handelshinder mot främmande makt. Främmande makt utsätts för allt större intern press då befolkningen börjar ifrågasätta den egna regeringens handlande på grund av den stora mängd information som publiceras internationell och som tydliggör främmande makts involvering – och skuld – i den pågående händelseutvecklingen.

För en långsiktigt avskräckande effekt, koordineras samtidigt en unionsgemensam utvisning av främmande makts diplomater och för ett stort antal individer med koppling till främmande makts regering införs också en stegvis frysning av tillgångar samt inreseförbud. För att tydliggöra att detta är en aktion mot främmande makts regering – och inte mot främmande makts befolkning – införs visumlättnader för främmande makts befolkning och ett omfattande program för utbytesstudier i Europa initieras.

Främmande makt trappar ner sina hybridangrepp när det blir uppenbart att an-greppen inte når önskad framgång – samtidigt som det blir tydligt för främmande makt att konsekvenserna av fortsatt agerande är betydande, såväl internt som externt.

5 Vägen framåt

Vårt fiktiva scenario slutar med framgång för Sverige.

Framgång kräver både motståndskraftiga myndigheter som kan hantera angrepp självständigt, såväl som förmåga att agera samordnat med alla till buds stående medel i verktygslådan.

Den svenska modellen med självständiga och oberoende myndigheter har vissa fördelar för att motverka hybridhot. Den bidrar troligen till att skapa motståndskraft genom att säkerställa att centrala offentliga funktioner har mandat att motverka ett hybridangrepp oberoende av politiskt beslutsfattande.

Samtidigt kräver en långsiktig och intensifierad hantering av ett hybridangrepp ett förberett och övat politiskt beslutsfattande. Regeringen kan komma att behöva ta ett betydande ansvar för att motverka hybridangrepp genom att styra myndigheter, upphandla resurser, genomföra kraftfull extern kommunikation och samverkan och, i ett synnerligen allvarligt läge, besluta om höjd beredskap och att aktivera fullmaktslagar. Detta måste övas och prövas regelbundet för att Sverige ska vara redo om ett storskaligt hybridangrepp sker.

Arbetet med att motverka hybridhot kommer troligen att kräva anpassning och omställning – inte minst då hybridhot utmanar vår syn på traditionella hot, inklusive inre respektive yttre hot, och kopplar ihop utrikes- och säkerhetspolitiken med nationell krishantering och rättsväsendet. Hybridhot medför att lokala frågor får utrikespolitiska konsekvenser, samtidigt som effektiv nationell, regional och lokal hantering i allt större utsträckning beror på internationella samarbeten för att effektivt detektera, analysera och motverka hybridangrepp.

En av de utmaningar som identifierats är att olika myndigheter och aktörer i Sverige använder sig av olika begrepp och definitioner för att beskriva vad som i huvudsak är samma problem. Det är inte självklart att detta i sig är något som underminerar förutsättningarna för att möta hybrida hot. Däremot bedömer vi att det bör övervägas att tydligare definiera Sveriges övergripande prioriteringar för att fortsatt inrikta utvecklingsarbetet. En nationell strategi skulle kunna skapa långsiktiga förutsättningar och bidra till att höja medvetenheten och öka kunskapen i hela samhället om dessa utmaningar. En nationell strategi bör även bidra till att ytterligare definiera begrepp, roller och ansvar för regering, myndigheter, regioner och kommuner.

Den här rapporten har föreslagit att det bör utvecklas en gemensam nationell definition för hybridhot, en svensk strategisk verktygslåda för att motverka hybridhot och en nationell strategi för arbetet med att motverka hybridhot. Vår förhoppning är att detta förslag till ramverk för en strategisk verktygslåda för att möta hybridhot kan bidra till denna utveckling.

6 Slutnoter

[1] Försvarsberedningen, “Värnkraft: Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025” (Stockholm: Försvarsdepartementet, 2019).

[2] Försvarsberedningen, “Försvaret av Sverige: Starkare försvar för en osäker tid ” (Stockholm: Försvarsdepartementet, 2014); Försvarsberedningen, “Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025” (Stockholm: Försvarsdepartementet, 2017); Försvarsberedningen, “Värnkraft: Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025” (Stockholm: Försvarsdepartementet, 2019).

[3] Robert Larsson, “Det kaukasiska lackmustestet : konsekvenser och lärdomar av det rysk-georgiska kriget i augusti 2008”, FOI-R--2563--SE, (Stockholm: FOI, 2008); Försvarsberedningen, “Säkerhet i samverkan” (Stockholm: Försvarsdepartementet, 2007).

[4] Försvarsberedningen, “Värnkraft: Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025” (Stockholm: Försvarsdepartementet, 2019).

[5] Försvarsberedningen, “Försvaret av Sverige: Starkare försvar för en osäker tid ” (Stockholm: Försvarsdepartementet, 2014); Försvarsberedningen, “Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025” (Stockholm: Försvarsdepartementet, 2017); Försvarsberedningen, “Värnkraft: Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025” (Stockholm: Försvarsdepartementet, 2019).

[6] Försvarsberedningen, “Värnkraft: Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025” (Stockholm: Försvarsdepartementet, 2019), 66.

[7] Europeiska kommissionen and Europeiska utrikestjänsten, “Gemensamt Meddelande till Europaparlamentet Och Rådet: Gemensam Ram För Att Motverka Hybridhot” (Bryssel, 2016), https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX%3A52016JC0018.

[8] NATO, “NATO’s Response to Hybrid Threats,” NATO, besökt 24 mars, 2020, http://www.nato.int/cps/en/natohq/topics_156338.htm.

[9] Ben Heap, “Hybrid Threats: A Strategic Communications Perspective” (Riga: NATO StratCom COE, 2019), https://stratcomcoe.org/hybrid-threats-strategic-communications-perspective.

[10] “Hybrid Threats,”Hybrid CoE, besökt 24 mars 2020, https://www.hybridcoe.fi/hybrid-threats/.

[11] Regeringen, “Prop. 2014/15:109. Försvarspolitisk inriktning – Sveriges försvar 2016–2020” (Stockholm: Försvarsdepartementet, 2015), 11.

[12] Regeringen, “Prop. 2014/15:109. Försvarspolitisk inriktning – Sveriges försvar 2016–2020” (Stockholm: Försvarsdepartementet, 2015), 40.

[13] Försvarsberedningen, “Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025” (Stockholm: Försvarsdepartementet, 2017).

[14] Försvarsberedningen, “Värnkraft: Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025” (Stockholm: Försvarsdepartementet, 2019).

[15] Försvarsberedningen, "Värnkraft: Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025" (Stockholm: Försvarsdepartementet, 2019), 66.

[16] Försvarsberedningen, "Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025" (Stockholm: Försvarsdepartementet, 2017), 67.

[17] Försvarsmakten, "Militärstrategisk doktrin – MSD 16" (Stockholm: Försvarsmakten, 2016).

[18] Försvarsmakten, "Militärstrategisk doktrin – MSD 16" (Stockholm: Försvarsmakten, 2016), 36.

[19] Försvarsmakten and Myndigheten för Samhällsskydd och Beredskap, "Sverige kommer att möta utmaningarna: Gemensamma grunder (grundsyn) för en sammanhängande planering för totalförsvaret " (Stockholm: Försvarsmakten, 2016), 3f.

[20] Säkerhetspolisen, "Säkerhetspolisens årsbok 2018" (Stockholm: Säkerhetspolisen, 2019), 25.

[21] Militära underrättelse- och säkerhetstjänsten, "Must: Årsöversikt 2019" (Stockholm: Försvarsmakten, 2020).

[22] Militära underrättelse- och säkerhetstjänsten, "Must: Årsöversikt 2019" (Stockholm: Försvarsmakten, 2020).

[23] Säkerhetspolisen, "Säkerhetspolisens årsbok 2019" (Stockholm: Säkerhetspolisen, 2020), 28.

[24] Säkerhetspolisen, "Säkerhetspolisens årsbok 2019" (Stockholm: Säkerhetspolisen, 2020), 20 och 23.

[25] Myndigheten för Samhällsskydd och beredskap, "Handbok möta informationspåverkan" (Stockholm: MSB, 2018), 7, 11.

[26] Sveriges ständiga representation vid Europeiska unionen, "EU:s försvarsministrar diskuterar hybridhot," Åtkomstdatum 28 april 2020, https://www.regeringen.se/artiklar/2016/04/eus-forsvarsministrar-diskuterar-hybridhot/.

[27] Försvarsdepartementet, " Anförande Krigsvetenskapsakademien," Åtkomstdatum 28 april 2020, https://www.regeringen.se/tal/2014/12/anforande-krigsvetenskapsakademien/.

[28] Regeringen, "Sveriges säkerhet i en ny värld," Åtkomstdatum 28 april 2020, https://www.regeringen.se/tal/2018/01/sveriges-sakerhet-i-en-ny-varld/.

[29] Statsrådsberedningen and Försvarsdepartementet, "Nationell säkerhetsstrategi" (Stockholm: Regeringskansliet, 2017), https://www.regeringen.se/informationsmaterial/2017/01/nationell-sakerhetsstrategi/; Justitiedepartementet, "En ny myndighet för psykologiskt försvar," åtkomstdatum 27 april 2020, https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2018/08/dir.-201880/

[30] Svenska akademin, "hybrid | SAOL | svenska.se," SAOL, besökt 24 mars 2020, https://svenska.se/saol/.

[31] Se t.ex. Matthew Rojansky och Michael Kofman, "A Closer Look at Russia's 'Hybrid War' " (Washington DC: Wilson Center, 2015), https://www.wilsoncenter.org/publication/kennan-cable-no7-closer-look-russias-hybrid-war.

[32] Se t.ex. Atte Harjanne et al., "Helsingfors i Hybridhotens Tid" (Helsingfors: Helsingfors stad, 2018), 5, https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridiraportti_sve_020818_netti.pdf.

[33] Dr. Patrick J. Cullen and Erik Reichborn-Kjennerud, “MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare” (Multinational Capability Development Campaign, 2017), 9.

[34] Säkerhetspolisen, “Säkerhetspolisens årsbok 2019” (Stockholm: Säkerhetspolisen, 2020), 20 och 23.

[35] Dr. Patrick J. Cullen and Erik Reichborn-Kjennerud, “MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare” (Multinational Capability Development Campaign, 2017), 9.

[36] Dr. Patrick J. Cullen and Erik Reichborn-Kjennerud, “MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare” (Multinational Capability Development Campaign, 2017), 13.

[37] Se exempelvis Europeiska kommissionen och Europeiska utrikestjänsten, “Gemensamt Meddelande till Europaparlamentet och Rådet: Gemensam Ram För Att Motverka Hybridhot” (Bryssel, 2016), 2, https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX%3A52016JC0018; Dr. Patrick J. Cullen and Erik Reichborn-Kjennerud, “MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare” (Multinational Capability Development Campaign, 2017), 12.

[38] Europeiska kommissionen och Europeiska utrikestjänsten, “Gemensamt Meddelande till Europaparlamentet och Rådet: Gemensam Ram För Att Motverka Hybridhot” (Bryssel, 2016), 2, https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX%3A52016JC0018; Dr. Patrick J. Cullen and Erik Reichborn-Kjennerud, “MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare” (Multinational Capability Development Campaign, 2017), 24.

[39] James Pamment et al., “Countering Information Influence Activities : The State of the Art” (Stockholm: MSB, 2018).

[40] Försvarsberedningen, “Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025” (Stockholm: Försvarsdepartementet, 2017), 67.

[41] James Pamment and Alicia Wanless, “How Do You Define a Problem Like Influence?,” *Journal of Information Warfare* 18, no. 3 (2019): 11–14.

[42] Se t.ex. Axel Hagelstam, “Cooperating to Counter Hybrid Threats,” NATO Review, November 23, 2018, https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html.

[43] “Redogörelse: Regeringen svarar på nya hot genom att stärka myndigheternas funktionsförmåga”, Sisäministeriö, besökt 24 mars 2020, https://intermin.fi/sv/artikeln/-/asset_publisher/selonteko-hallitus-vastaa-uusiin-uhkiin-vahvistamalla-viranomaisten-toimintakykya.

[44] Europeiska kommissionen and Europeiska utrikestjänsten, “Gemensamt Meddelande till Europaparlamentet Och Rådet: Gemensam Ram För Att Motverka Hybridhot” (Bryssel, 2016), 2, https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX%3A52016JC0018.

[45] Nationalencyklopedin, “Hot - Uppslagsverk - Ne. Se,” besökt 24 mars 2020, https://www.ne.se/uppslagsverk/ordbok/svensk/hot-(1).

[46] Försvarsmakten, “Handbok För Försvarsmaktens Säkerhetstjänst, Hotbedömning” (Stockholm: Försvarsmakten, 2006), 10f.

[47] Försvarsmakten, “Handbok För Försvarsmaktens Säkerhetstjänst, Hotbedömning” (Stockholm: Försvarsmakten, 2006), 10f.

[48] Försvarsmakten, “Handbok För Försvarsmaktens Säkerhetstjänst, Hotbedömning” (Stockholm: Försvarsmakten, 2006), 10f.

[49] Försvarsmakten, "Handbok För Försvarsmaktens Säkerhetstjänst, Hotbedömning" (Stockholm: Försvarsmakten, 2006), 10f.

[50] SFS 1974:152. Regeringsformen. Stockholm: Justitiedepartementet, 15 kap. 14 §.

[51] En rad fullmaktslagar blir tillämpliga och vissa av bestämmelserna i 22 kap. brottsbalken om landsförräderi m.m. blir tillämpliga. En del författningar upphör också att gälla, såsom t.ex. IKFN-förordningen och tillträdesförordningen.

[52] Se exempelvis SOU 1972:15 s. 216 och prop. 1973:90 s. 446 f.

[53] Europeiska kommissionen och Europeiska utrikestjänsten, "Gemensamt Meddelande till Europaparlamentet och Rådet: Gemensam Ram För Att Motverka Hybridhot" (Bryssel, 2016), https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX%3A52016JC0018.

[54] General Secretariat of the Council, "Complementary Efforts to Enhance Resilience and Counter Hybrid Threats - Council Conclusions (10 December 2019)" (Bryssel: Council of the European Union, 2019), https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf.

[55] UK Ministry of Defence, "Countering Hybrid Warfare Project", besökt 1 mars 2020, https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare.

[56] Försvarsdepartementet, "Ett Användbart Försvar" (Stockholm: Försvarsdepartementet, 2008), 14.

[57] Statsrådsberedningen and Försvarsdepartementet, "Nationell säkerhetsstrategi" (Stockholm: Regeringskansliet, 2017), 1, https://www.regeringen.se/informationsmaterial/2017/01/nationell-sakerhetsstrategi/; MSB, "Gemensamma Grunder För Samverkan Och Ledning Vid Samhällsstörningar" (Stockholm: MSB, 2018), 15, https://www.msb.se/sv/publikationer/gemensamma-grunder-for-samverkan-och-ledning-vid-samhallsstorningar/.

[58] Försvarsdepartementet, "Ett Användbart Försvar" (Stockholm: Försvarsdepartementet, 2008), 14ff.

[59] SFS 2015:1052. Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och respektive myndighetsinstruktion. Stockholm: Justitiedepartementet.

[60] Finansdepartmentet, "Budgetpropositionen För 2020" (Stockholm: Finansdepartementet, 2019), 6:72.

[61] SFS 2015:1052. Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och respektive myndighetsinstruktion. Stockholm: Justitiedepartementet.

[62] Finansdepartmentet, "Budgetpropositionen För 2020" (Stockholm: Finansdepartementet, 2019), 6:72.

[63] The Multinational Capability Development Campaign (MCDC) är ett multinationellt projekt för att studera gemensamma utmaningar. Sverige är en deltagande partner i MCDC. Ytterligare information finns här: https://wss.apan.org/public/MCDCpub/default.aspx

[64] Statsrådsberedningen and Försvarsdepartementet, "Nationell säkerhetsstrategi" (Stockholm: Regeringskansliet, 2017), 1, https://www.regeringen.se/informationsmaterial/2017/01/nationell-sakerhetsstrategi/.

[65] Regeringen, "Utrikesdeklarationen 2020", Regeringskansliet, 12 februari 2020, https://www.regeringen.se/tal/2020/02/utrikesdeklarationen-2020/.

[66] Dr. Patrick J. Cullen and Erik Reichborn-Kjennerud, “MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare” (Multinational Capability Development Campaign, 2017).

[67] Europeiska kommissionen and Europeiska utrikestjänsten, “Gemensamt Meddelande till Europaparlamentet Och Rådet: Gemensam Ram För Att Motverka Hybridhot” (Bryssel, 2016), https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX%3A52016JC0018.

[68] Ben Heap, “Hybrid Threats: A Strategic Communications Perspective” (Riga: NATO StratCom COE, 2019), https://stratcomcoe.org/hybrid-threats-strategic-communications-perspective.

[69] Ben Heap, “Hybrid Threats: A Strategic Communications Perspective” (Riga: NATO StratCom COE, 2019), https://stratcomcoe.org/hybrid-threats-strategic-communications-perspective.

[70] SFS 1974:152. Regeringsformen. Stockholm: Justitiedepartementet, 1 kap. 1 §.

[71] Regeringen, “Utrikesdeklarationen 2020”, Regeringskansliet, 12 februari 2020, https://www.regeringen.se/tal/2020/02/utrikesdeklarationen-2020/.

[72] General Secretariat of the Council, “Complementary Efforts to Enhance Resilience and Counter Hybrid Threats - Council Conclusions (10 December 2019)” (Bryssel: Council of the European Union, 2019), https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf.

[73] Förenta Nationerna, “Förenta Nationernas Stadga”, 1945, https://fn.se/wp-content/uploads/2016/07/FN-stadgan.pdf.

[74] Sean Monaghan and Dr Njord Wegge, “MCDC Countering Hybrid Warfare: Conceptual Foundations and Implications for Defence Forces” (Multinational Capability Development Campaign, 2019), 6; Heine Sørensen and Dorthe Bach Nyemann, “Going Beyond Resilience: A Revitalized Approach to Countering Hybrid Threats” (Hybrid CoE, 2018), 4, https://www.hybridcoe.fi/wp-content/uploads/2019/01/Strategic-analysis-Sorensen-Nyeman-11-2018.pdf.

[75] Council of Europe, “Resolution 2217 (2018) - Legal Challenges Related to Hybrid War and Human Rights Obligations,” 10 §, besökt 10 mars 2020, http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?fileid=24762.

[76] NATO, “Bi-SC Input to a New Capstone Concept for the Military Contribution to Countering Hybrid Threats” (Bryssel: SHAPE, 2010); Europeiska kommissionen and Europeiska utrikestjänsten, “Gemensamt Meddelande till Europaparlamentet Och Rådet: Gemensam Ram För Att Motverka Hybridhot” (Bryssel, 2016), https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX%3A52016JC0018.

[77] Regeringen, “Utrikesdeklarationen 2020”, Regeringskansliet, 12 februari 2020, https://www.regeringen.se/tal/2020/02/utrikesdeklarationen-2020/.

[78] “Fördraget Om Europeiska Unionens Funktionssätt ” (Bryssel: Europeiska unionens officiella tidning, 2012), https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX%3AC2012%2F326%2F01.

[79] General Secretariat of the Council, “Complementary Efforts to Enhance Resilience and Counter Hybrid Threats - Council Conclusions (10 December 2019)” (Bryssel: Council of the European Union, 2019), https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf.

[80] Europeiska kommissionen and Europeiska utrikestjänsten, “Gemensamt Meddelande till Europaparlamentet Och Rådet: Gemensam Ram För Att Motverka Hybridhot” (Bryssel, 2016), https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX%3A52016JC0018.

[81] Regeringen, “Utrikesdeklarationen 2020”, Regeringskansliet, 12 februari 2020, https://www.regeringen.se/tal/2020/02/utrikesdeklarationen-2020/.

[82] Regeringen, “Utrikesdeklarationen 2020”, Regeringskansliet, 12 februari 2020, https://www.regeringen.se/tal/2020/02/utrikesdeklarationen-2020/.

[83] General Secretariat of the Council, “Complementary Efforts to Enhance Resilience and Counter Hybrid Threats - Council Conclusions (10 December 2019)” (Bryssel: Council of the European Union, 2019), https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf.

[84] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, “MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare” (Multinational Capability Development Campaign, 2019).

[85] Gregory F. Treverton et al., “Addressing Hybrid Threats” (Helsingfors: Swedish Defence University och Hybrid CoE, 2018; Vytautas Keršanskas, “DETERRENCE: Proposing a More Strategic Approach to Countering Hybrid Threats ” (Helsingfors: Hybrid CoE, 2020), https://www.hybridcoe.fi/wp-content/uploads/2020/03/Deterrence.pdf.

[86] Ben Heap, “Hybrid Threats: A Strategic Communications Perspective” (Riga: NATO StratCom COE, 2019), https://stratcomcoe.org/hybrid-threats-strategic-communications-perspective.

[87] Dr. Patrick J. Cullen and Erik Reichborn-Kjennerud, “MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare” (Multinational Capability Development Campaign, 2017); Ben Heap, “Hybrid Threats: A Strategic Communications Perspective” (Riga: NATO StratCom COE, 2019), https://stratcomcoe.org/hybrid-threats-strategic-communications-perspective.

[88] Ben Heap, “Hybrid Threats: A Strategic Communications Perspective” (Riga: NATO StratCom COE, 2019), https://stratcomcoe.org/hybrid-threats-strategic-communications-perspective.

[89] Ben Heap, “Hybrid Threats: A Strategic Communications Perspective” (Riga: NATO StratCom COE, 2019), https://stratcomcoe.org/hybrid-threats-strategic-communications-perspective.

[90] Sebastian Bay, Michael Batrla, och Henrik Twetman, “Camouflage for the Digital Domain” (Riga: NATO StratCom CoE, n.d.), https://www.stratcomcoe.org/camouflage-digital-domain.

[91] Sebastian Bay och Nora Biteniece, “The Current Digital Arena and Its Risks to Serving Military Personnel” (Riga: NATO StratCom CoE, 2018), https://www.stratcomcoe.org/current-digital-arena-and-its-risks-serving-military-personnel.

[92] Justitiedepartementet, “Samhällets Krisberedskap - Stärkt Samverkan För Ökad Säkerhet” (Stockholm: Justitiedepartementet, 2009), https://www.regeringen.se/rattsliga-dokument/skrivelse/2010/04/skr.-200910124/.

[93] Justitiedepartementet, “Samhällets Krisberedskap - Stärkt Samverkan För Ökad Säkerhet” (Stockholm: Justitiedepartementet, 2009), https://www.regeringen.se/rattsliga-dokument/skrivelse/2010/04/skr.-200910124/.

[94] Justitiedepartementet, “Samhällets Krisberedskap - Stärkt Samverkan För Ökad Säkerhet” (Stockholm: Justitiedepartementet, 2009), https://www.regeringen.se/rattsliga-dokument/skrivelse/2010/04/skr.-200910124/.

[95] SFS 2006:544. Lag om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap. Stockholm: Justitiedepartementet, 2 kap. 7 §.

[96] SFS 2017:868. Förordning med länsstyrelseinstruktion. Stockholm: Justitiedepartementet, 2 kap. 7 § Förordning (2017:868) med länsstyrelseinstruktion, 2-7 §, SFS 2017:870. Förordning om länsstyrelsernas krisberedskap och uppgifter vid höjd beredskap. Stockholm: Justitiedepartementet, 2-4 §.

[97] Finansdepartementet, "Budgetpropositionen För 2012: Förslag till Statens Budget För 2012, Finansplan Och Skattefrågor " (Stockholm: Finansdepartementet), 2011), 75.; Justitiedepartementet, "Stärkt Krisberedskap - För Säkerhets Skull" (Stockholm: Justitiedepartementet, 2007), 13f.

[98] SFS 2015:1052. Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och respektive myndighetsinstruktion. Stockholm: Justitiedepartementet.

[99] SFS 2015:1052. Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och respektive myndighetsinstruktion. Stockholm: Justitiedepartementet.

[100] SFS 2008:1002. Förordning med instruktion för Myndigheten för samhällsskydd och beredskap. Stockholm: Justitiedepartementet.

[101] SFS 2015:1052. Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och respektive myndighetsinstruktion. Stockholm: Justitiedepartementet, 1, 5, 10, 13, 15 §§.

[102] Försvarsdepartementet, "Näringslivets Roll Inom Totalförsvaret" (Stockholm: Försvarsdepartementet, 2019), https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2019/12/sou-201951/., Jenny Ingemarsdotter et al., "Näringslivets Roll i Totalförsvaret – Centrala Frågor Och Vägar Framåt", FOI-R--4649--SE, (Stockholm: FOI, 2018).

[103] Regeringskansliet, "Rättsväsendet," Åtkomstdatum 27 April 2020, https://www.regeringen.se/regeringens-politik/rattsvasendet/.

[104] Jmfr. Gregory F. Treverton et al., "Addressing Hybrid Threats" (Stockholm: Swedish Defence University, 2018).

[105] SFS 1984:387. Polislag. Stockholm: Justitiedepartementet, 3 §.

[106] Se Polislag (1984:387). Vid terrorismbekämpning kan polisen, enligt lag (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning, begära stöd av Försvarsmakten. Försvarsmakten kan även ge stöd till civila aktörer enligt förordning (2002:375) om Försvarsmaktens stöd till civil verksamhet.

[107] Polisen, " Hemställan om ökat samarbete med Försvarsmakten," Åtkomstdatum 27 April 2020, https://polisen.se/aktuellt/nyheter/2020/januari/hemstallan-om-okat-samarbete-med-forsvarsmakten//.

[108] Försvarsmakten, " Försvarsmaktens Strategiska Inriktning 2015" (Stockholm: Försvarsmakten, 2016), 3ff.

[109] SFS 2007:1266. Förordning med instruktion för Försvarsmakten. Stockholm: Försvarsdepartementet, 3 §.

[110] 15 kap. 13 § 2 st. uttrycker regeringens rätt att ge Försvarsmakten detta uppdrag, vilket har gjorts genom förordning (1982:756) om Försvarsmaktens ingripanden vid kränkningar av Sveriges territorium under fred och neutralitet m.m. (IKFN-förordning).

[111] Försvarsberedningen, "Värnkraft: Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025" (Stockholm: Försvarsdepartementet, 2019), 118.

[112] SFS 1992:1403. Lag om totalförsvar och höjd beredskap. Stockholm: Försvarsdepartementet.

[113] Se t.ex. förfogandelag (1978:262), ransoneringslag (1978:268) och lag (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.

[114] SFS 2015:1052. Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och respektive myndighetsinstruktion. Stockholm: Justitiedepartementet, 17-18 §§.

[115] SFS 2015:1053. Förordning om totalförsvar och höjd beredskap. Stockholm: Försvarsdepartementet, 4 §.

[116] SFS 1992:1403. Lag om totalförsvar och höjd beredskap. Stockholm: Försvarsdepartementet, 1 §.

[117] Myndigheten för Samhällsskydd och Beredskap, "Underlag inför nästa försvarspolitiska inriktningsbeslut " (Stockholm: Myndigheten för Samhällsskydd och Beredskap, 2018), 25.

[118] Se exempelvis KU (1973:20), "*Konstitutionsutskottets betänkande med anledning av granskning av statsrådens ämbetsutövning och regeringsärendenas handläggning*, s. 16-17 och KU (1977/78:35), *Konstitutionsutskottets betänkande 1977/78:35 med anledning av granskning av statsrådens tjänsteutövning och regeringsärendenas handläggning*, s. 15.

[119] SOU 2008:61, *Krisberedskapen i grundlagen - Översyn och internationell utblick*, Stockholm: Fritzes.

[120] Regeringen, "Regeringens beslut och initiativ med anledning av nya coronaviruset," 28 februari 2020, https://www.regeringen.se/regeringens-politik/regeringens-arbete-med-anledning-av-nya-coronaviruset/regeringens-beslut-och-initiativ-med-anledning-av-nya-coronaviruset/.

[121] General Secretariat of the Council, "Complementary Efforts to Enhance Resilience and Counter Hybrid Threats - Council Conclusions (10 December 2019)" (Bryssel: Council of the European Union, 2019), https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf.

[122] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare" (Multinational Capability Development Campaign, 2019).

[123] Gregory F. Treverton et al., "Addressing Hybrid Threats" (Helsingfors: Swedish Defence University och Hybrid CoE, 2018; Vytautas Keršanskas, "DETERRENCE: Proposing a More Strategic Approach to Countering Hybrid Threats " (Helsingfors: Hybrid CoE, 2020), https://www.hybridcoe.fi/wp-content/uploads/2020/03/Deterrence.pdf.

[124] Ben Heap, "Hybrid Threats: A Strategic Communications Perspective" (Riga: NATO StratCom COE, 2019), https://stratcomcoe.org/hybrid-threats-strategic-communications-perspective.

[125] Benämns oftast som "resilience" på engelska och ibland som "resiliens" på svenska.

[126] Igor Linkov, Lada Roslycky, and Benjamin D. Trump, eds., *Resilience of Hybrid Threats: Security and Integrity for the Digital World*, Nato Science for Peace and Security Series - d: Information and Communication Security 55 (Washington: IOS Press, 2019); General Secretariat of the Council, "Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats - Establishment and Adoption of Its Terms of Reference" (Bryssel: Council of the European Union, 2019).

[127] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare" (Multinational Capability Development Campaign, 2019).

[128] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare" (Multinational Capability Development Campaign, 2019), 30; Europeiska kommissionen och Europeiska utrikestjänsten, "Gemensamt Meddelande till Europaparlamentet och Rådet: Gemensam Ram För Att Motverka Hybridhot" (Bryssel, 2016), 4, https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX%3A52016JC0018.

[129] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare" (Multinational Capability Development Campaign, 2019), 19.

[130] NATO, "Brussels Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels, 11-12 July 2018," NATO, besökt 24 mars 2020, 13 §, http://www.nato.int/cps/en/natohq/official_texts_156624.htm.

[131] Ben Heap, "Hybrid Threats: A Strategic Communications Perspective" (Riga: NATO StratCom COE, 2019), https://stratcomcoe.org/hybrid-threats-strategic-communications-perspective.

[132] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare" (Multinational Capability Development Campaign, 2019), 25ff.

[133] Ben Heap, "Hybrid Threats: A Strategic Communications Perspective" (Riga: NATO StratCom COE, 2019), https://stratcomcoe.org/hybrid-threats-strategic-communications-perspective.

[134] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare" (Multinational Capability Development Campaign, 2019), 25-27.

[135] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare" (Multinational Capability Development Campaign, 2019).

[136] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare" (Multinational Capability Development Campaign, 2019), 26-27.

[137] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare" (Multinational Capability Development Campaign, 2019), 64-65.

[138] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare" (Multinational Capability Development Campaign, 2019), 25.

[139] Ödlund Ann, "Informationsdelning och Lägesbild", FOI Memo 6588, (Stockholm: FOI, 2018), 3f.

[140] NATO, "Brussels Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels, 11-12 July 2018," NATO, 20 §, accessed March 24, 2020, http://www.nato.int/cps/en/natohq/official_texts_156624.htm.

[141] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare" (Multinational Capability Development Campaign, 2019), 41.

[142] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare" (Multinational Capability Development Campaign, 2019), 76; Sean Monaghan. (2019). Sean Monaghan and Dr Njord Wegge, "MCDC Countering Hybrid Warfare: Conceptual Foundations and Implications for Defence Forces" (Multinational Capability Development Campaign, 2019), 6.

[143] Sean Monaghan and Dr Njord Wegge, “MCDC Countering Hybrid Warfare: Conceptual Foundations and Implications for Defence Forces” (Multinational Capability Development Campaign, 2019), 6; Heine Sørensen and Dorthe Bach Nyemann, “Going Beyond Resilience: A Revitalized Approach to Countering Hybrid Threats” (Hybrid CoE, 2018), 4, https://www.hybridcoe.fi/wp-content/uploads/2019/01/Strategic-analysis-Sorensen-Nyeman-11-2018.pdf.

[144] European Council on Foreign Relations. ”Protecting Europe against hybrid threats | European Council on Foreign Relations”. Åtkomstdatum 18 mars 2020. https://www.ecfr.eu/publications/summary/protecting_europe_against_hybrid_threats.

[145] Facebook. ”Coordinated Inauthentic Behavior Explained - About Facebook”. Åtkomstdatum 18 mars 2020. https://about.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/.

[146] Bellingcat. ”bellingcat - MH17 Archives - bellingcat”. Åtkomstdatum 18 mars 2020. https://www.bellingcat.com/tag/mh17/.

[147] European Council on Foreign Relations. ”Protecting Europe against hybrid threats | European Council on Foreign Relations”. Åtkomstdatum 18 mars 2020. https://www.ecfr.eu/publications/summary/protecting_europe_against_hybrid_threats.

[148] Ben Heap, “Hybrid Threats: A Strategic Communications Perspective” (Riga: NATO StratCom COE, 2019), https://stratcomcoe.org/hybrid-threats-strategic-communications-perspective.

[149] James Pamment et al., “Countering Information Influence Activities : The State of the Art” (Stockholm: MSB, 2018).

[150] Dr. Patrick J. Cullen and Erik Reichborn-Kjennerud, “MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare” (Multinational Capability Development Campaign, 2017), 11.

[151] General Secretariat of the Council, “Complementary Efforts to Enhance Resilience and Counter Hybrid Threats - Council Conclusions (10 December 2019)” (Bryssel: Council of the European Union, 2019), https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf; General Secretariat of the Council, “Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats - Establishment and Adoption of Its Terms of Reference” (Bryssel: Council of the European Union, 2019); High representative of the union for foreign and affairs and security policy, “JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats” (The European Commission, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0016&from=GA.

[152] NATO, “NATO’s Response to Hybrid Threats,” NATO, besökt 24 mars 2020, http://www.nato.int/cps/en/natohq/topics_156338.htm.

[153] Robert Dalsjö, “Fem Dimensioner Av Tröskelförsvar”, FOI-R--4458--SE, (Stockholm: FOI, 2017); Lawrence Freedman, *Deterrence* (Cambridge, UK ; Malden, MA: Polity Press, 2004).

[154] Ben Heap, “Hybrid Threats: A Strategic Communications Perspective” (Riga: NATO StratCom COE, 2019), https://stratcomcoe.org/hybrid-threats-strategic-communications-perspective.

[155] Ben Heap, “Hybrid Threats: A Strategic Communications Perspective” (Riga: NATO StratCom COE, 2019), https://stratcomcoe.org/hybrid-threats-strategic-communications-perspective; Vytautas Keršanskas, “DETERRENCE: Proposing a More Strategic Approach to Countering Hybrid Threats ” (Helsingfors: Hybrid CoE, 2020), https://www.hybridcoe.fi/wp-content/uploads/2020/03/Deterrence.pdf.

[156] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, “MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare” (Multinational Capability Development Campaign, 2019), 13, 58.

[157] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, “MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare” (Multinational Capability Development Campaign, 2019), 58.

[158] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, “MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare” (Multinational Capability Development Campaign, 2019), 58.

[159] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, “MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare” (Multinational Capability Development Campaign, 2019), 58.

[160] Sean Monaghan, Dr Patrick Cullen, and Dr Njord Wegge, “MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare” (Multinational Capability Development Campaign, 2019), 58.

[161] European Council on Foreign Relations. ”Protecting Europe against hybrid threats | European Council on Foreign Relations”. Åtkomstdatum 18 mars 2020. https://www.ecfr.eu/publications/summary/protecting_europe_against_hybrid_threats.

[162] Justitiedepartementet, “En ny myndighet för psykologiskt försvar,” åtkomstdatum 27 april 2020, https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2018/08/dir.-201880/

[163] The European Commission, “A Europe That Protects: The EU Steps up Action against Disinformation,” åtkomstdatum 27 april 2020, https://ec.europa.eu/commission/presscorner/home/en.

[164] För vidare läsning om scenariometodik, se t.ex. Daniel K Jonsson, “Att Använda Scenarier i Planering För Civilt Försvar ”, FOI-R--4434--SE, (Stockholm: Kista, 2017).

[165] Daniel K Jonsson, “Typfall 5: Utdragen och eskalerande gråzonsproblematik”, FOI Memo 6338, (Stockholm: FOI, 2018).

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se