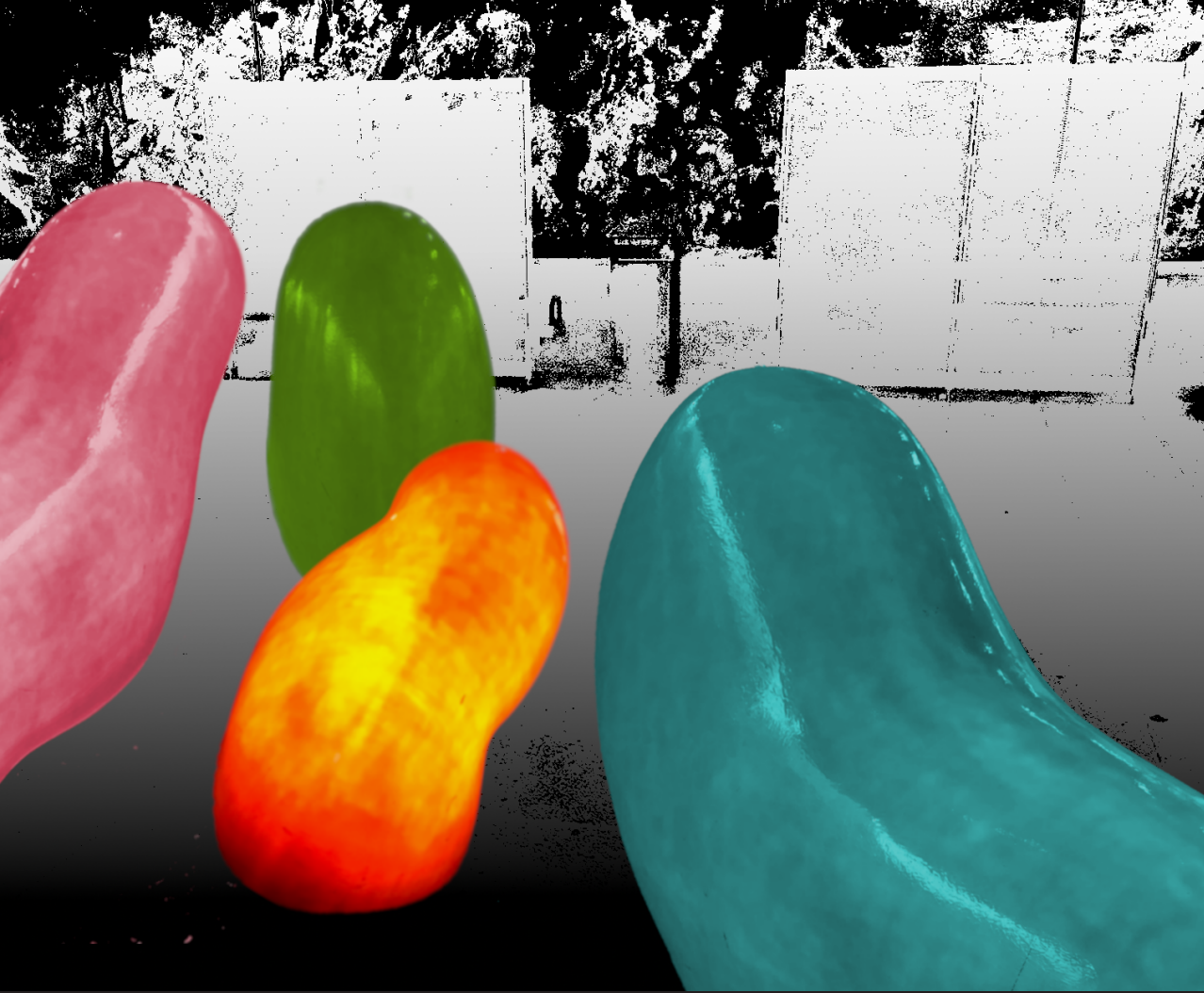


Hantering av hybrida hot

Teoretiska utgångspunkter och val av strategi för Polismyndigheten

Ola Svenonius och Anders Strindberg

FOI-R--4966--SE

Oktober 2020

FOI

Ola Svenonius och Anders Strindberg

Hantering av hybrida hot

Teoretiska utgångspunkter och val av strategi för Polismyndigheten

Titel	Hantering av hybrida hot–Teoretiska utgångspunkter och val av strategi för Polismyndigheten
Title	Countering Hybrid Threats in Law Enforcement – Theoretical Starting Points and Choice of Strategy
Rapportnr/Report no	FOI-R--4966--SE
Månad/Month	Oktober
Utgivningsår/Year	2020
Antal sidor/Pages	46
ISSN	1650-1942
Kund/Customer	Regeringskansliet
Forskningsområde	Krisberedskap och civilt försvar
FoT-område	Inget FoT-område
Projektnr/Project no	A112070
Godkänd av/Approved by	Malek Finn Khan
Ansvarig avdelning	Försvarsanalys

Bild/Cover: Ola Svenonius. ”Diffusa hot #2”, 2020.

Sammanfattning

”Hybrida hot” är ett begrepp som har fått allt större betydelse för svensk säkerhetspolitik och har i studien operationaliserats som statlig antagonistisk subversion under tröskeln för väpnat angrepp.

Rapporten presenterar ett ramverk som Polismyndigheten kan använda i utvecklingsarbetet när det gäller hantering av hybrida hot. Dels diskuteras vilka institutionella system som idag existerar för att hantera hybrida hot; dels presenteras tre strategier som på ett principiellt plan kan bilda utgångspunkter för en framtida strategi för hantering av hybrida hot. Dessa tre strategier är den beskyddande, den bemötande och den störande. Med utgångspunkt i dessa tre strategier diskuterar rapporten olika sätt för Polismyndigheten att förhålla sig till den diffusa hotbild som det som ofta benämns hybrida hot utgör.

Nyckelord: hybrida hot; Polismyndigheten; krisberedskap; civilt försvar; motståndskraft.

Summary

"Hybrid threats" is a term that designates antagonistic subversion by state or proxy actors below the threshold of conventional warfare. It has become increasingly important in Swedish security policy.

This report presents a framework that the Swedish Police Authority can use in the development of a comprehensive strategy for countering hybrid threats. It discusses the institutions that already exists to mitigate such threats, and then presents three ideal typical strategies – in terms of overarching plans of action – for countering hybrid threats. The three strategies are the protective strategy, the bolstering strategy, and the disruptive strategy. Using these strategies as a starting point, the report discusses different ways to counter vague and opaque threats posed by antagonist states.

Keywords: hybrid threats; the Swedish Police Authority; crisis management; civilivan defence; resilience.

Innehållsförteckning

1 Inledning 7
1.1 Problemställning: Polisens arbete med hybrida hot idag . 8
1.2 Syfte, frågeställningar och avgränsningar 9
1.3 Avgränsningar 9
1.4 Tillvägagångssätt 10
1.5 Läsanvisningar 11
2 Hybrida hot: ett nygammalt begrepp 13
2.1 Hybrida hot som begrepp 14
2.2 Hybrida hot är statlig antagonistisk verksamhet 17
2.3 Påverkas polisen av hybrida hot? 18
3 Hantering av hybrida hot 20
3.1 Avskräckning och motståndskraft 20
3.2 Delmoment i hanteringen av hybrida hot 21
3.3 Strategier för hantering av hybrida hot 24
4 Hantering av hybrida hot ur ett institutionellt perspektiv 28
4.1 Hybrida hot och totalförsvaret 28
4.2 Hybrida hot innan höjd beredskap 29
5 Konsekvenser för Polismyndigheten: principer för hantering av hybrida hot 34
5.1 Upptäcka 34
5.2 Höja medvetenheten 36
5.3 Bygga motståndskraft 37
5.4 Institutionaliserad samverkan 39
5.5 Tre strategier för hantering av hybrida hot 41
6 Sammanfattning och diskussion 43
6.1 Vad är hybrida hot, och hur kan de bemötas? 43
6.2 Frågor för diskussion 45

Förord

FOI har fått i uppdrag av Regeringskansliet att i samverkan med Polismyndigheten under perioden 2018–2020 studera detektion och hantering av hybrida hot ur ett polisiärt perspektiv. Under 2018 fokuserade arbetet på nationell särskild händelse Val 2018 i samband med riksdagsvalet den 9 september. Under 2019 breddades arbetet till att fokusera dels på vilka teoretiska konsekvenser hybrida hot har för polisen, dels utreda hur myndigheten idag arbetar med hybrida hot generellt. Den här rapporten utgör en delleverans från projektet och syftar till att ge en teoretisk introduktion till hybrida hot samt presentera verktyg som Polismyndigheten kan använda i utvecklingsarbetet för en framtida strategi för hantering av hybrida hot. Parallellt med rapporten lanserar FOI också en samling exempel på hybrida hot hämtade från verkligheten och en uppsättning hybridhotsscenarier. Tillsammans ger dessa studier en teoretisk och praktisk introduktion till hybrida hot som kan användas både i medvetandehöjande syfte och för planeringsaktiviteter.

Vi i projektgruppen vill rikta ett varmt tack till er alla vid Polismyndigheten som tagit er tid och ställt upp för intervjuer och delat värdefulla tankar och idéer med oss under projektets gång.

Ann-Sofie Stenérus Dover

Projektledare

Juni 2020

1 Inledning

Hybrida hot är ett begrepp som har fått allt större betydelse för svensk säkerhetspolitik de senaste åren. Det betecknar statlig antagonistisk subversion, ofta under tröskeln för väpnat angrepp. Även om fenomenet i sig inte är nytt har det fått förnyad aktualitet i efterdyningarna av Rysslands krigföring i framför allt Ukraina 2014. Det säkerhetspolitiska läget för Sverige har sedan dess försämrats och Säkerhetspolisen (Säpo) noterar i årsboken från 2019 att ”främmande makt agerar allt oftare medvetet under tröskeln för väpnad konflikt.”[1]

Sedan 2014 har totalförsvaret återupptagits. Uppbyggnaden av det nya totalförsvaret innebär ett utvecklingsarbete av svensk försvarsförmåga, både i fråga om det militära och det civila försvaret. Försvarsberedningens rapport *Motståndskraft* och Myndigheten för samhällsskydd och beredskaps (MSB) skrivelse *Så skapar vi motståndskraft* beskriver behovet av att skapa motståndskraftiga civila myndigheter. Frågan kvarstår kring vad detta betyder för varje enskild organisation?[2] Motståndskraft mot vad? Svaren på dessa frågor är komplicerade och kräver stor detaljkunskap om varje enskild organisation, men en del av arbetet innebär att undersöka frågan om hybrida hot närmare.

FOI har nyligen publicerat rapporten ”Strategisk verktygslåda mot hybridhot”[3] som också behandlar hantering av hybrida hot. Strategisk verktygslåda fokuserar på nationell nivå och utgår från Regeringskansliet. Denna rapport utgår ifrån myndighetsnivån, med fokus på Polismyndigheten. Rapporterna kompletterar således varandra.

Polismyndigheten har sedan sammanslagningen 2015 tillsammans med Säpo ansvar för polisär verksamhet i Sverige. Arbetet mot hybrida hot är ännu under utveckling. Nedanstående rapport ämnar stödja detta arbete. Rapporten diskuterar vilken typ av antagonistisk verksamhet som kan riktas mot Sverige, vilka institutioner som kan användas till att hantera dem, samt ger Polismyndigheten verktyg som kan användas när den utformar en strategi för att bemöta statlig antagonism.[4]

---

[1] Säpo, *Säkerhetspolisens årsbok 2019* (Solna: Säkerhetspolisen, 2020), 18.

[2] Försvarsdepartementet, *Motståndskraft. Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025*, Ds 2017:66 (Stockholm: Regeringskansliet, 2017); MSB, *Så skapar vi motståndskraft. Skrivelse med underlag till försvarsbeslutsperioden 2021–2025*, MSB 2020-02262 (Stockholm: Myndigheten för samhällsskydd och beredskap, 2020).

[3] Jessica Appelgren, Sebastian Bay, Johannes Malminen och Erik Zouave, *Strategisk verktygslåda mot hybridhot: Ett ramverk för gemensam problemförståelse*, FOI-R-4816--SE (Stockholm: FOI Totalförsvarets Forskningsinstitut, 2020).

[4] Med *strategi* menas i denna rapport ”övergripande plan”. Se: Svenska Akademien (2020). Sökord: ”strategi”, i: *Svensk ordbok* (tryckår 2009). Tillgänglig på: https://svenska.se/so/?id=51157&pz=7 (hämtad 2020-05-04).

1.1 Problemställning: Polisens arbete med hybrida hot idag

Polisens övergripande funktion i samhället är att värna rättssystem och statsskick. Polismyndigheten styrs av ett antal processer som är tänkta att svara mot polisens uppgifter som de uttrycks i polislagen, till exempel utredning, lagföring och brottsprevention. Polismyndigheten och Säpo är enligt polislagen de myndigheter som har rättsligt mandat att utöva våld mot person och egendom för att kunna bekämpa och förebygga brott, övervaka den allmänna ordningen, samt ge befolkningen skydd i händelse av fara.[5] Dessa mål medför även en lång rad sociala och administrativa aktiviteter – allt från att samverka med kommun och socialtjänst kring ungdomar i utsatta områden till att skydda grundlagsfästa politiska rättigheter under t.ex. en valrörelse.

Polismyndigheten har inte idag något helhetsgrepp för hantering av hybrida hot, men ett utvecklingsarbete pågår vid nationella operativa avdelningens underrättelseenhet (NOA-UND). Hittills har händelser hanterats i isolation såtillvida att inte sakförhållanden pekar på inblandning från till exempel främmande makt.[6] En viktig fråga är hur hybrida hot ska upptäckas. Polisen är en förhållandevis decentraliserad myndighet och det finns ett flertal sätt på vilka information kan förmedlas uppåt i organisationen, till exempel:

- Regionala UND-enheter kan kontakta Säpo direkt.
- NOA-UND:s eget underrättelsearbete på nationell ger upphov till uppslag.
- Ärenden vidarebefordras i organisationen av de regionala och nationella ledningscentralerna till underrättelsefunktioner i respektive polisregion eller NOA-UND.
- Utredande enhet kan vidarebefordra information vid misstanke om främmande makts inblandning.

---

[5] Polislagen (SFS 1984:387) §2 uttrycker att: ”Till Polismyndighetens uppgifter hör att
1. förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten,
2. övervaka den allmänna ordningen och säkerheten och ingripa när störningar har inträffat,
3. utreda och beivra brott som hör under allmänt åtal,
4. lämna allmänheten skydd, upplysningar och annan hjälp, när sådant bistånd lämpligen kan ges av polisen,
5. fullgöra den verksamhet som ankommer på Polismyndigheten enligt särskilda bestämmelser. *Lag (2014:588)*.”

Det är värt att notera att Polislagen även gäller under höjd beredskap. Skillnaden är att vissa uppgifter då tillkommer som annars inte är aktuella, till exempel att bistå Försvarsmakten på olika sätt.

[6] Nedanstående bygger på intervjuer vid Polismyndigheten-NOA som genomförts inom ramen för projektet Detektion och hantering av hybrida hot i polisiär verksamhet under 2019.

Utbytet av underrättelseinformation inom myndigheten och till Säpo har utvärderats av Statskontoret, som beskriver systemet som effektivt. Inom ramen för FOI:s forskning har indikationer uppkommit som antyder att det finns faktorer i verksamheten som ökar risken för att statlig antagonistisk verksamhet som riktas mot Sverige aldrig upptäcks. En sammanhållen strategi för hantering av hybrida hot skulle kunna ta ett helhetsgrepp och styra arbetet på ett systematiskt vis inom organisationen.

1.2 Syfte, frågeställningar och avgränsningar

Med utgångspunkt i ovanstående är syftet med rapporten att ta fram verktyg som Polismyndigheten kan använda i utformningen av en strategi för hantering av hybrida hot. Frågeställningarna som ligger till grund för rapporten är:

Vad är hybrida hot?

Hur kan hybrida hot bemötas?

Hur kan Polismyndigheten resonera i utformningen av en strategi för hantering av hybrida hot?

Svaren på dessa frågor ger Polismyndigheten möjlighet att, ensam eller i samverkan med till exempel Säpo, utforma en strategi för hantering av hybrida hot.

1.3 Avgränsningar

Denna rapport gör en serie avgränsningar. Dessa gäller hybrida hot konceptuellt, frågan om militära aspekter av hybrida hot och fokus på Polismyndigheten. Hybrida hot är ett begrepp som kan beteckna en uppsjö av fenomen. Det finns också ett antal närliggande begrepp som används i det närmaste synonymt med hybrida hot. Exempel på sådana begrepp är gråzon, icke-linjär krigföring och grand strategy. Av resursmässiga skäl kan rapporten inte behandla samtliga av dessa fenomen och begrepp. I kapitel 2 diskuterar vi begreppsanvändningen och operationaliserar hybrida hot i termer av statligt sanktionerad subversiv verksamhet.

Rapporten fokuserar på hybrida hot under fredstid. Därför diskuteras inte konventionella militära maktmedel, till exempel väpnade angrepp. Istället fokuserar rapporten på hybrida hot i en situation där regeringen inte har höjt Sveriges beredskap. Således är inte heller totalförsvaret ett centralt fokus i rapporten. Vi återkommer till detta resonemang i kapitel 4.

Rapporten fokuserar på Sverige. Det betyder att vi inte kommer att diskutera vikten av, till exempel, internationella samarbeten. I framtida arbeten kan internationella faktorer spela en större roll, till exempel i fråga om gemensam strategiutveckling mellan de nordiska länderna eller dylikt.

Till sist fokuserar rapporten på Polismyndigheten. Resonemangen som förs genomgående i rapporten kan vara tillämpliga även på andra myndigheter och/eller organisationer, men här diskuteras övriga aktörer endast i relation till Polismyndigheten.

1.4 Tillvägagångssätt

I rapporten utvecklas ett teoretiskt ramverk som kan användas för att ta fram en strategi för hantering av hybrida hot. Arbetet bygger dels på en litteraturgenomgång, dels på en genomgång av svensk lagstiftning på området och dels på behovsorienterad teoriutveckling. Rapportens tillvägagångssätt beskrivs nedan.

Litteraturgenomgången bestod i att utifrån existerande forskning och teoretisk litteratur inom området ”hybridkrigföring”, ”hybrida hot”, ”gråzon”, ”icke-linjär krigföring” och ”aktiva åtgärder” extrahera delar som har bäring på rapportens frågeställningar. Dessa delar rör dels rent konceptuella frågor (*Vad är hybrida hot?*), dels hur denna typ av hotbild kan omhändertas (*Hur kan hybrida hot bemötas?*). Underlaget till analysen hämtades dels från akademiska databaser, dels från öppna källor på internet. Källorna är framtagna per iterativ behovsbasis.[7] I ett inledande steg identifierades vägledande dokument (i Sverige och utomlands) samt central akademisk litteratur. I steg två granskades dessa, bl.a. i syfte att identifiera centrala begrepp för ytterligare litteratursökningar. I ett nästa steg identifierades och granskades nya källor. I ett slutligt steg analyserades det sammanställda materialets övergripande fokus, mönster och slutsatser.

Litteraturgenomgången resulterade framförallt i en operativ förståelse för vad hybrida hot är, samt de fyra delmoment som i denna rapport utgör stommen till de strategiska överväganden för hantering av hybrida hot som diskuteras i kapitel 5.

I kapitel 4 redovisas och diskuteras existerande institutionella system för hantering av de säkerhetsproblem som hybrida hot utgör. Källorna för detta kapitel består dels av för svensk försvarspolitik centrala dokument,

[7] För denna s.k. ”hermeneutiska ansats” se Boell, Sebastian K. och Dubravka Cecez-Kecmanovic, ”Literature Reviews and the Hermeneutic Circle”. *Australian Academic & Research Libraries*, 2010, 41(2): 129-144.

exempelvis Försvarsberedningens rapport *Motståndskraft*, dels av relevanta lagar och riktlinjer.

I kapitel 5 utvecklas resonemanget om de tre olika strategier som rapporten presenterar. För att skapa dessa strategityper användes ett teoretiskt tankegrepp som kan kallas för *differens-heuristik, vilket redovisas* i kapitel 3.[8] Den kan i korthet summeras så här: Antag att problemet *X* bär ett ändligt antal egenskaper *a,b,c…[n]*. Ställ sedan frågan: *Hur många teoretiska variationer av egenskaperna har X?* För att komma till en slutsats konstruerar analytikern därefter svar på varje egenskap som är så olika som möjligt, utifrån hans eller hennes existerande kunskap. Beroende på hur *X* är konstituerat och vilka parametrar som tas i åtanke kan det röra sig om olika många idealtyper, men av praktiska skäl försöker analytikern att hålla antalet lågt för att skapa enkelhet. Dessa måste vara ömsesidigt uteslutande, annars rör det sig inte om idealtyper. Den enklaste variationen är ett traditionellt motsatsförhållande, men ett större antal idealtyper är möjliga. Differens-heuristikens uppgift är att skapa teoretiska verktyg som kan användas för att leda tänkandet i arbetet med att konstruera en sammanhållen strategi. I detta fall konstruerades tre principiella strategier, som alltså är skapade för att besvara problemet *X* på så olika sätt som möjligt. Strategierna är med andra ord teoretiska verktyg vars uppgift är att hjälpa oss att hantera hybrida hot.

1.5 Läsanvisningar

Rapporten är skriven för tjänstemän vid Polismyndigheten och andra myndigheter med uppdrag att hantera hybrida hot. Den består av fem kapitel, undantaget inledningskapitlet:

Kapitel 2 och 3 utgör rapportens teoretiska del. Kapitel 2 handlar om att beskriva hybrida hot som begrepp, och kapitel 3 hur de kan bemötas utifrån existerande teoretisk kunskap. Dessutom behandlas frågan om hur hybrida hot påverkar Polismyndigheten. Vidare diskuteras i kapitel 3 vad det betyder att ”hantera” hybrida hot. Det finns olika principer som kan ligga till grund för en strategisk hantering av hybrida hot. I slutet av kapitlet definieras tre sådana principer: *beskyddande*, *bemötande* och *störande*. Dessa är centrala för rapportens huvudsakliga utsaga och vidareutvecklas i kapitel 5.

Kapitel 4 diskuterar hur hybrida hot förhåller sig till de institutionella system som redan finns i Sverige, vilket är viktigt att ha med i den vidare

[8] Ansatsen bygger på Max Webers metod kring idealtyper. För utförlig beskrivning av ett liknande förfarande, se: Swedberg, Richard, ”How to Use Max Weber’s Ideal Type in Sociological Analysis:”, *Journal of Classical Sociology*, 2017. https://doi.org/10.1177/1468795X17743643.

diskussionen om hur Polismyndigheten ska hantera sådana hot. De system som diskuteras är säkerhetsskydd, krisberedskap och rättsväsende.

Kapitel 5 vidareutvecklar strategierna från kapitel 3 med utgångspunkt i fyra delmoment som i litteraturen om hybrida hot anses vara av särskild vikt. En läsare som uteslutande är intresserad av olika sätt att bemöta hybrida hot kan med fördel fokusera på detta kapitel.

Kapitel 6 sammanfattar rapportens huvudsakliga utsaga och tar upp ett antal frågor som Polismyndigheten och andra organisationer kan behöva komma att ta ställning till i framtiden.

2 Hybrida hot: ett nygammalt begrepp

När Krim annekterades av Ryssland 2014 började allt fler analysera händelseförloppet i termer av ”hybridkrig”. Begreppet var långt ifrån nytt, men fick snabbt spridning och återfinns idag i alltifrån nyhetsartiklar till Försvarsberedningens rapport *Värnkraft*.[9] Den militära aspekten av hybridkrigföring är dock bara en del av problemet. Hybridkrigföring förutsätter inte nödvändigtvis väpnad konflikt. European Center of Excellence for Countering Hybrid Threats i Helsingfors (Hybrid CoE), en nätverkshub för ett antal europeiska stater och USA, fokuserar därför på *hybrida hot* och *hybrid påverkan* snarare än hybridkrigföring. Oavsett avgränsning är begreppet inte helt oproblematiskt, bland annat på grund av att det är politiskt betingat snarare än analytiskt neutralt.[10]

Inom forskningen har begreppsapparaten kring hybrida hot[11] utvecklats i en mer analytisk riktning, men begreppet är icke desto mindre svårhanterligt. Litteraturen kring hybrida hot, som diskuteras nedan, kommer från den militära domänen och hybridkrig är en sorts ”moderterm” till hybrida hot som beskriver krigföring där konventionella vapen bara är ett medel bland många andra. Blandningen av olika typer av medel, eller metoder, benämns ”hybrid”.

Kapitlet är uppdelat i tre delar: först diskuterar vi hybrida hot i litteraturen rent konceptuellt, för att sedan gå vidare till en operativ definition. Den sista delen behandlar kortfattat hybrida hot utifrån ett polisperspektiv.

[9] Se t.ex. Peter Pomerantsev, ”How Putin is reinventing Warfare”, *Foreign Policy* (5 maj 2014), https://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/, hämtad 2020-05-13; Mark Galeotti, ”(Mis)Understanding Russia’s two ’hybrid wars’”, *Eurozine* (29 november 2018), https://www.eurozine.com/misunderstanding-russias-two-hybrid-wars/, hämtad 2020-05-13. Försvarsberedningen, *Värnkraft – Inriktningen av säkerhetspolitken och utformningen av det militära försvaret 2021-2025, Ds 2019:8* (Stockholm: Regeringskansliet, 2019).

[10] Notera bl.a. NATOs generalsekreterare Jens Stoltenbergs påpekande att “Hybrid is the dark reflection of our comprehensive approach. We use a combination of military and non-military means to stabilize countries. Others use it to destabilize them. Of course, hybrid warfare is nothing new.” Jens Stoltenberg, “Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar”, (25 mars 2015), https://www.nato.int/cps/en/natohq/opinions_118435.htm, hämtad 2020-05-13.

[11] I denna rapport används “hybridhot” och “hybrida hot” synonymt.

2.1 Hybrida hot som begrepp

Hybridkrigföring har illustrerats genom empiriska studier av olika konflikter, t.ex. krigen i Libanon[12] och i Tjetjenien.[13] I dessa kontexter förstås begreppet som en kombination av olika typer av operationer (militära, icke-militära, gerilla, sponsring av terrorister och kriminella, spridande av propaganda och desinformation), ett utsuddande av skiljelinjerna mellan reguljär och icke-reguljär krigföring.[14] Detta utsuddande av skiljelinjer innebär att begreppet har en bredare innebörd än bara den militära. Ur denna synvinkel kan hybridkrig ses som en modern form av vad som ibland kallas ”grand strategy.”[15]

I sina försök att skapa definitioner tvistar forskare och institutioner framförallt om ramverk och ansats – t.ex. huruvida det bästa vore att studera fenomenet med utgångspunkt i hybrida ”verktyg” eller i hybridkrigets faser.[16] Detta är naturligt då, som Europeiska kommissionen påpekar, en definition av hybridhot ”måste vara flexibel eftersom hotet hela tiden förändras.”[17] Även själva begreppet är en diskussionsfråga. Vissa menar att det är mer korrekt att tala om *hybrida hot* än om hybrid krigföring eftersom själva huvudsyftet med verksamheten är ”att uppnå sina mål utan

---

[12] Frank G. Hoffman, *Conflict in the 21st century – the rise of hybrid wars*. “Washington, DC: Potomac Institute for policy Studies, 2007), https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf, hämtad 2020-03-31.

[13] Se t.ex.: Malin Severin, *Tidig förvarning och icke-militära angreppssätt.* FOI-R--4577—SE. (Stockholm: FOI Totalförsvarets forskningsinstitut, 2018); William J. Nemeth, *Future war and Chechnya: A Case for Hybrid Warfare*, DTIC Document (Monterey: Naval Postgraduate School, 2002), http://hdl.handle.net/10945/5865, hämtad 2020-03-31; András Rácz, *Russia's Hybrid Warfare in Ukraine* (Helsinki: The Finnish Institute of International Affairs, 2014), https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf, hämtad 2020-03-31.

[14] James N. Mattis och Frank Hoffman, “Future warfare: The rise of hybrid wars”, *Proceedings Magazine, 2005* 131. nr 11 (November 2005), https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars, hämtad 2020-03-31.

[15] “Grand strategy” har definierats som "the purposeful employment of all instruments of power available to a security community". Se: Colin Gray, *War, Peace and International Relations: An Introduction to Strategic History* (Abingdon & New York: Routledge, 2007), 283.

[16] Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee och Madeline McCue, *Addressing Hybrid Threats* (Stockholm: Försvarshögskolan, 2018), 10, https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf, hämtad 2020-03-31, s. 10; Robert R. Leonhard, Stephen P. Phillips och The Assessing Revolutionary and Insurgent Strategies (ARIS) Team, *Little Green Men: A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014.* (Fort Bragg, NC: United States Army Special Operations Command, 2015), https://www.jhuapl.edu/Content/documents/ARIS_LittleGreenMen.pdf, hämtad 2020-03-31.

[17] Unionens höga representant för utrikes och säkerhetsfrågor, *Gemensamt meddelande till europeiska parlamentet och rådet – Gemensam ram för att motverka hybridhot* (Bryssel: Europeiska kommissionen, 2016), https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52016JC0018&from=EN, hämtad 2020-03-31.

att föra reellt krig" och att "taktiken bygger på att sätta in en rad potentiella instrument *samtidigt*, från hot om krig till propaganda och allt annat däremellan". [18] Andra föredrar uttrycket "hybrid störning" (hybrid interference) som avser i princip samma gränsöverskridande verksamhet.[19] Även Hybrid CoE anammar denna primärt icke-militära ansats när uttrycket "hybrid påverkan" används. I en rapport definieras detta som "medveten påverkan som utövas av en aktör som använder ett flertal metoder för att nå sitt mål".[20] Slutsatsen är att litteraturen inte innehåller någon knivskarp definition men pekar på ett antal karakteristika som kännetecknar hybrida hot.

Enligt denna generella samsyn kombinerar hybrida hot ett flertal verktyg och maktmedel. Måltavlan angrips i syfte att utnyttja sårbarheter och skapa asymmetriska effekter.[21] Dessutom kan verktygskombinationen synkroniseras på ett sätt som gör helheten till ett *attackpaket* som kan eskaleras eller de-eskaleras både i intensitet och i fråga om kombinationen av påverkansmetoder.[22] Hybrida hot innebär tvetydighet och förnekbarhet, vilket kan skapa förvirring i den angripna staten och samhället angående vem som angriper, vad som angrips, eller om det ens rör sig om angrepp över huvud

[18] Treverton et al. (2018), *Addressing Hybrid Threats*, 3. Egen översättning. I original: "to achieve outcomes without actual war" och "the tactic is the *simultaneous* employment of the range of possible instruments, from threats of war to propaganda and everything in between".

[19] Mikael Wigell, *Democratic Deterrence*, *FIIA Working Paper* (Helsinki, Finnish institute of International Affairs, 2019a), 4, https://www.fiia.fi/wp-content/uploads/2019/09/wp110_democratic-deterrence.pdf, hämtad 2020-03-31; Cf. Mikael Wigell, "Hybrid Interference as a Wedge Strategy". *International Affairs* 95, 2 (2019b), https://doi.org/10.1093/ia/iiz043.

[20] Harjanne, Atte, Eetu Muilu, Jekaterina Pääkkönen, och Hanna Smith. "Helsinki in the era of hybrid threats – Hybrid influencing and the city". Publications of the Central Administration 2018:22 (Helsinki: City of Helsinki, 2018), 5. https://www.hybridcoe.fi/wp-content/uploads/2018/08/Helsinki-in-the-era-of-hybrid-threats-%E2%80%93-Hybrid-influencing-and-the-city_ENG.pdf.

[21] Patrick J. Cullen och Erik Reichborn-Kjennerud, *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare* (Multinational Capability Development Campaign, 2017), 8, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf, hämtad 2020-03-31; Severin (2018), *Tidig förvarning och icke-militära angreppssätt*, 17-18; Treverton et al. (2018), *Addressing Hybrid Threats*, 59-62; Appo Cederberg och Pasi Eronen, *How Can Societies Be Defended Against Hybrid Threats?* (Zürich: Centre for Security Policy, 6 november 2015), https://css.ethz.ch/en/services/digital-library/articles/article.html/194510, hämtad 2020-03-31; Nathan P. Freier (red.) *Outplayed: Regaining the Strategic Initiative in the Gray Zone* (Carlisle Barracks, PA: U.S. Army War College, 2016), 5, https://apps.dtic.mil/dtic/tr/fulltext/u2/1013807.pdf (hämtad 2020-03-31); Håkan Gunneriusson och Rain Ottis "Cyberspace from the Hybrid Threat Perspective". *Journal of Information Warfare* 12, nr. 3 (2013), 68f.

[22] Cullen och Reichborn-Kjennerud (2017), 8; Severin (2018), *Tidig förvarning och icke-militära angreppssätt*, 18-19.

taget.[23] Detta kan till exempel ske genom att aktiviteterna utförs av icke-statliga aktörer på uppdrag av en stat. Detta förmodas vara en strategi som koordineras av en statlig aktör för att uppnå ett givet politiskt mål.[24] Hur hög grad av koordination som verkligen står bakom hybrida hot är svårt att säga – även slumpmässiga eller opportunistiska angrepp kan ge upphov till stor förvirring och kan dessutom ofta vara svåra att skilja från ett genomtänkt och koordinerat attackpaket.

I litteraturen är skribenter eniga om att hybrida hot inte följer någon mall utan är framtagna för ett specifikt måls sårbarheter och svagheter.[25] En antagonist kan använda verktygen när ett tillfälle uppstår eller när externa faktorer, t.ex. i form av en internationell ekonomisk kris, gör verktygen mer användbara. Från angriparens sida går det inte att utesluta att myndigheter och departement som inte traditionellt räknas som säkerhets- eller försvarsorganisationer deltar. Det beskrivs ofta att hybrida hot skapar långsamma förskjutningar av styrkeförhållanden, i en sådan takt att varje enskild aktivitet inte ses som en direkt kränkning eller en särskilt allvarlig provokation.[26] Därför behöver de som ska hantera hybrida hot sätta upp gränser för vad de anser är acceptabelt eller inte och när en motåtgärd ska sättas in.[27] De överväganden som lägger grunden till sådana gränser utgör strategiska beslut i hanteringen av hybrida hot.

Som vi har beskrivit ovan är hybrida hot summan av en myriad av aktiviteter som sker i olika domäner med större eller mindre grad av koordination, koppling till geopolitiska strävanden och med olika tidshorisont. Detta är dock för ospecifikt för att fungera som en definition. Nästa avsnitt förtydligar vad vi menar med hybrida hot i denna rapport.

---

[23] Valery Gerasimov "The Gerasimov Model", *Military-Industrial Kurier*, (February 27, 2013), översatt av Robert Coalson, 21 juni 2014. Länk till originalet finns på https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf, hämtad 2020-03-31; Nina Jankowicz, "Avoiding the Band-Aid Effect in Institutional Responses to Disinformation and Hybrid Threats, (Washington, DC: German Marshall Fund of the United States, German Marshall Fund of the United States, 2019), 20, http://www.gmfus.org/publications/avoiding-band-aid-effect-institutional-responses-disinformation-and-hybrid-threats, hämtad 2020-03-31; Freier (2016), *Outplayed: Regaining the Strategic Initiative in the Gray Zone* , 4.

[24] Anton Dengg och Mikael Schurian (red.) *Networked Insecurity – hybrid threats in the 21st century: Schriftenreihe der Landesverteidigungsakademie No. 17* (Wien: Federal Ministry of Defence and Sports, 2016), http://www.bundesheer.at/pdf_pool/publikationen/2016_17_sr__networked_security_dengg_schurian.pdf, hämtad 2020-03-31.

[25] Se tex. Sean Monaghan (red) *Countering Hybrid Warfare* (Multinational Capability Development Campaign, 2019), 21-22, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf, hämtad 2020-03-31; Cederberg och Eronen (2015), *How Can Societies Be Defended Against Hybrid Threats?*, 4.

[26] Robert Haddick, "America has No Answer to China's Salami-Slicing". *War on the Rocks* (6 februari 2014), som citerad i Severin (2018), *Tidig förvarning och icke-militära angreppssätt*, 3.

[27] Monaghan (red) (2019), *Countering Hybrid Warfare*, 21-22.

2.2 Hybrida hot är statlig antagonistisk verksamhet

Hybrida hot är, som vi har sett ovan, ett begrepp som har ett flertal olika betydelser och konnotationer. För att operationalisera detta komplexa begrepp definieras det i denna rapport i linje med dess minsta gemensamma nämnare: *subversiv antagonistisk verksamhet utgående från en statlig eller statligt sanktionerad aktör bestående* av *två eller flera olika maktmedel*. Verksamheten är av subversiv natur och ytterst med militärt eller geopolitiskt inflytande som mål. När en stat påverkas av antagonistisk subversion på ett sätt som skapar problem för centrala institutioner att fungera effektivt, kan staten som helhet anses befinna sig i ett ansträngt eller utsatt läge. Det betyder i sig inte att det är en gråzon mellan krig och fred. Hur stor krigsfara som råder är ytterst en subjektiv bedömning från mottagarsidan. Olika sätt att tolka begreppen hybrida hot kan ge olika resultat i en analys.

I den vardagliga användningen av begreppet hybrida hot, till exempel i politiska sammanhang, finns stora skillnader. Vissa förespråkar en mer strikt tolkning som i den akademiska litteraturen. Här kan vi endast tala om hybrida hot i de fall där faktiska händelser kan attribueras till en och samma främmande makt och där operationer är domänöverskridande. Andra använder hybrida hot mer för att beteckna subversiv verksamhet i allmänhet. Då är det mer löst definierat vad som kan räknas som hybrida hot; koordination och domänöverskridande verksamheter är inte vad som definierar dem. Istället definieras de genom att de är subversiva, det rör sig om mer än vanlig brottslighet. I den förståelsen kan t.ex. gängvåld mycket väl förstås som hybrida hot även om koppling till främmande makt inte har fastställts. Denna skillnad i begreppsanvändning kan antas vara skyldig till en betydande del av den förvirring och skepsis mot begreppen som har funnits, både i Sverige och internationellt.

Hybridkrig, hybrida hots ”moderterm”, är – enligt beskrivningen ovan – krigföring som sker inom flera domäner samtidigt, där effekterna från olika domäner påverkar varandra. Att angripa ett lands infrastruktur samtidigt som en region ockuperas, kriminella gäng stöds med vapen och diplomatiska medel används för att försvaga omvärldens vilja att hjälpa till, skulle kunna utgöra ett exempel på hur hybridkrig kan se ut.

Det finns ett spann från isolerade subversiva handlingar och en ”breddad hotbild”, till en koordinerad verksamhet med utgångspunkt i en strategi. Huruvida koordination föreligger eller inte är emellertid ofta svårt att avgöra (detta är fokus för studier kring tidig förvarning och detektion, men ligger utanför rapportens täckningsområde). Sabotage, cyberspionage, diplomatiska eller ekonomiska påtryckningar – alla syftar till att

underminera en verksamhet eller ett samhälle. Risken är att den som för svepande talar om hybrida hot tappar i trovärdighet om hoten uppfattas som vaga och odefinierade. I vissa fall kan det därför vara bättre att tala om ett ”utsatt läge” eller ”breddat hot” snarare än hybridhot, men detta beror på vilken typ av definition som används.

Kortfattat kan begreppen beskrivas som följer:

- *Hybrida hot* är en strategisk satsning (över kort eller utdragen tid), för att med varierande metoder försvaga måltavlan, minska dennes handlingsutrymme, eller på annat sätt reducera dennes förmåga.[28]
- Ett *breddat hot* från främmande makter(er) är ett sätt att mer förutsättningslöst beskriva den typen av subversion som statliga antagonister kan ägna sig åt utan att det behöver handla om en strategi med ett givet mål i snäv bemärkelse.
- Den mer generella formuleringen *subversiv antagonistisk verksamhet utgående från en statlig eller statligt sanktionerad aktör* kan beskriva enskilda händelser eller planerade strategier och spänner således över både hybrida hot och breddat hot.

Vi applicerar i denna rapport den grundläggande definitionen ”statlig antagonistisk verksamhet” i allmänna termer, vilket inkluderar både aktiviteter relaterade till hybrida hot och andra typer av hot mot svenska myndigheter. Detta för att undvika begreppsförvirring.

2.3 Påverkas polisen av hybrida hot?

Om hybrida hot är svåra att skilja från annan verksamhet, hur påverkar de då Polismyndigheten? Inträffar en brottslig handling måste ju polisen ingripa, oavsett om det är en statlig aktör som står bakom eller inte. Varför ska Polismyndigheten befatta sig med hybrida hot? Dessa är naturliga följdfrågor på diskussionen ovan. Det finns flera aspekter av dessa frågor, och vi nämner de viktigaste nedan.

Polismyndigheten kan vara både måltavla för en antagonist, och en av de aktörer som har ansvar för att hantera effekterna av statlig antagonistisk verksamhet riktad mot andra. Sabotage mot en polisfunktion – till exempel polisflyget – har vissa specifika effekter, medan en utdragen informationspåverkan riktad mot exempelvis Folkhälsomyndigheten har helt andra. I det första fallet kan Polismyndigheten behöva förstärkning från exempelvis Försvarsmakten för att kunna bibehålla flygförmågan, emedan i det senare fallet snarare handlar om utredningsarbete. Vilka typer

[28] Med förmåga åsyftas i denna rapport ”möjlighet att utföra något, som enbart beror av inre egenskaper”. Se: Svenska Akademien (2020). Sökord ”förmåga”, i *Svensk ordbok*. Tillgänglig på: https://svenska.se/so/?sok=f%C3%B6rm%C3%A5ga (hämtad 2020-05-04).

av antagonistiska verksamheter som riktas mot Sverige och/eller Polismyndigheten är utslagsgivande för hanteringen.

Ytterligare en fråga kring hanteringen av hybrida hot är tidsfaktorn. Ett angrepp mot Sverige kan vara lågintensivt och utdraget, eller vara över på ett par dagar. Tidsfaktorn kommer att vara viktig i ett scenario där Sverige utsätts för subversiv verksamhet, också för Polismyndigheten. I många av de intervjuer som projektgruppen har genomfört vid Polismyndigheten beskrivs myndigheten som en i första hand minutoperativ organisation. Ur ett kortsiktigt perspektiv, 24–48 timmar, är det för Polismyndigheten i många fall oviktigt om exempelvis en hotaktör stödjs av främmande makt eller inte.

En lite mer ingående analys visar dock att så inte alltid behöver vara fallet. Även på kort sikt bör rimligtvis frågan om en serie händelser är relaterade till antagonistisk verksamhet från främmande makt påverka Polismyndighetens arbete. Dels behöver poliser generellt ha en medvetenhet om att främmande makt är aktiv och att det föreligger en hotbild. Endast med en sådan medvetenhet kan poliser i yttre tjänst och vakthavande befäl identifiera misstänkta fall och vidarebefordra information uppåt i organisationen. Dels kan frågan huruvida främmande makt står bakom olika typer av brott påverka hur händelser bör hanteras på kort sikt. Måste till exempel beslut om särskild händelse fattas? Om ja – nationellt eller regionalt? Ska Säpo kopplas in i en utredning, eller ta över den? Behöver Polisen samordna sig med andra myndigheter eller regeringskansliet? Det är frågor som inte kan skjutas upp, utan måste behandlas omedelbart.

Ur ett längre perspektiv blir det ännu tydligare att samtliga av polisens funktioner påverkas av huruvida främmande makt understödjer viss brottslig verksamhet eller inte. Givet att underrättelseunderlag föreligger som visar på att främmande makt har påverkat eller provocerat fram en händelse kan detta potentiellt påverka både utredning och lagföring samt brottsprevention på ett grundläggande sätt.

3 Hantering av hybrida hot

I nedanstående kapitel presenteras förslag på verktyg för hur hybrida hot kan hanteras. Det finns tydliga och naturliga skiljelinjer mellan den militärt och civilt fokuserade litteraturen. Denna består framförallt i att den militära litteraturen överlag lägger stor emfas på avskräckningsförmåga. ”Deterrence by punishment” och ”deterrence by denial” är här centrala begrepp.[29] I denna rapport spelar dessa mindre roll eftersom vi fokuserar på Polismyndigheten, som inte har den typ av offensiv förmåga och uppgift som militära organisationer har. I det nedanstående diskuterar vi först idén om ”demokratisk avskräckning”, för att därefter titta på några delmoment i hantering av hybrida hot som lyfts fram i litteraturen. I kapitel 3.3 presenteras tre principiella strategier för hantering av hybrida hot. Dessa utvecklas sedan vidare i kapitel 5.

3.1 Avskräckning och motståndskraft

Det finns i litteraturen en föreställning om att demokratier skulle ha strategiska nackdelar i hanteringen av hybrida hot gentemot auktoritära stater, på grund av politiska fri- och rättigheter. Eftersom det rör sig om en strategi där angriparen utnyttjar det angripna samhällets relativa öppenhet finns omedelbara problem för detektion men även för skydds- och motåtgärder. Treverton menar till exempel att det är svårare för ett öppet demokratiskt samhälle än för en auktoritär angriparstat att ”samordna beslutsprocessen på olika nivåer och att göra det fort”.[30] Sahin, som citeras av Treverton, har påpekat att:

> Demokratier kan inte bedriva hybridkrigföring på samma övergripande och samordnade sätt som deras icke-demokratiska och icke-statliga motparter. Om de gjorde det så skulle de äventyra själva kärnan av det som de försöker försvara.[31]

Detta ses som ett grundläggande problem. En icke-centraliserad statsmakt med starka regelverk och allmän insyn i verksamheten ter sig i detta hänseende relativt tungrodd. I litteraturen diskuteras detta av bland annat Treverton som en asymmetri som kan vara mycket problematisk. Huruvida

[29] Monaghan (red) (2019), *Countering Hybrid Warfare*, 35ff.
[30] Treverton et al. (2018), *Addressing Hybrid Threats*, 79.
[31] Kaan Sahin, *Liberal Democracies and Hybrid War* (Washington, DC: International Institute for Strategic Studies, 2016), som citerad i Treverton et al. (2018), 80.

detta är fallet eller inte är både en empirisk fråga och en fråga om perspektiv. Svaret varierar beroende på vilket fall som studeras.[32]

Det finns dock på liknande sätt idéer om strategiska fördelar hos demokratier. Till skillnad från klassisk avskräckning, där höga kostnader för ett angrepp ska får motståndaren att underlåta ett angrepp, talar litteraturen här om så kallad ”demokratisk avskräckning.”

Demokratisk avskräckning är väsensskilt från traditionell militär avskräckning. [33] Idén är att den demokratiska värdegrundens attraktionskraft tillsammans med motåtgärder som ligger i linje med densamma, ses som kärnan i en ”soft power”-strategi för att hantera hybrida hot.[34] Men det finns en betydande nackdel för mottagarsidan: demokratisk avskräckning måste enligt Wigell utgå från insikten att vissa antagonistiska aktioner helt enkelt inte kan avskräckas. Däremot kan målet anpassa sig så att subversiv verksamhet blir mindre effektiv och därför mer sällan förekommande.[35] Det finns alltså indikationer som tyder på att avskräckning är svårt att uppnå, men att påverkan på samhället kan minimeras genom att utveckla motståndskraft.[36]

Som vi diskuterar i kapitel 3.3 och kapitel 5 finns det inget principiellt som motsäger att aktörer i demokratiska system arbetar med avskräckning. Det är snarare en fråga om *hur* en aktör väljer att angripa problemet. Det som exemplet med demokratisk avskräckning visar är snarare ett nytt sätt att tänka kring hantering av hybrida hot. Nackdelen är möjligen att om demokratiska system avskräcker redan i egenskap av att vara demokratiska, och om fullständig avskräckning är omöjlig så behövs ju inga genomgripande åtgärder. Det blir till slut en fatalistisk idé.

3.2 Delmoment i hanteringen av hybrida hot

Hur bör då samhällen och enskilda aktörer som Polismyndigheten förhålla sig mer konkret till den latenta och diffusa hotbild som hybrida hot utgör? På detta område finns vitt skilda förslag. Vi kommer här att nämna några

[32] Levitsky och Way studerade t.ex. 2010 över 30 auktoritära stater och fann att endast cirka en tredjedel kunde betecknas som effektiva. Se: Steven Levitsky och Lucan A. Way, *Competitive authoritarianism: hybrid regimes after the Cold War*, Problems of international politics (New York: Cambridge University Press, 2010).
[33] Wigell (2019a), *Democratic Deterrence*, 4.
[34] Wigell (2019a), *Democratic Deterrence*, 4-5. Om “soft power” jmfr. Joseph Nye, *The Future of Power*. (London: Hachette, 2011).
[35] Ibid., 10.
[36] Jmfr. Försvarberedningen, *Motståndskraft – Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021-2025, Ds 2017:66* (Stockholm: Regeringskansliet, 2017) som bygger på ett liknande argument.

för att sedan definiera fyra gemensamma delmoment som kommer att utvecklas i kapitel 5.

Treverton et al. menar att alla goda nationella handlingsplaner för att hantera hybrida hot har ett antal gemensamma nämnare. De:

- bygger på en lägesbild som är grundad på högkvalitativa underrättelser som delas mellan samtliga relevanta parter
- utgår från en sårbarhetsanalys
- har särskilt fokus på cyberförsvar
- är kreativa vad gäller samarbeten med den privata sektorn, och
- är institutionellt och samhälleligt samordnade.[37]

Andra har lanserat sina egna strategier. Enligt Multinational Capability Development Campaign (MCDC), en internationell samarbetsgrupp på försvarsområdet som har arbetat med att konceptualisera bemötande av hybrida hot, är det första steget i hanteringen att *identifiera* hotet.[38] MCDC gör här en åtskillnad mellan att *bevaka* och att *upptäcka*. Att bevaka innebär att läsa av sin omgivning, vanligtvis med hjälp av en lista på indikatorer, för att söka efter aktiviteter som troligen eller säkerligen utgör hybridhot. Att upptäcka innebär att uppfatta och korrekt tolka information om tidigare okända verktyg eller mål i ett potentiellt hybridangrepp.[39] Problemet uppstår när den typ av statligt sanktionerad antagonistisk verksamhet som diskuteras här använder nya och därför tidigare okända medel. De upptäcks då inte genom bevakning medelst vare sig mönsteranalys eller indikatorlista. Denna rapport utgår från att okända hot utgör en betydande del av den verksamhet som kan komma att rikta sig mot Sverige. I ett sådant scenario blir ett effektivt och samordnat lägesbildsarbete ett viktigt delmoment i detektionsarbetet.

Cederberg och Eronen menar att ett antal frågeställningar är grundläggande när man planerar motåtgärder. Att förstå sina egna sårbarheter och hur en antagonist kan tänkas utnyttja dessa måste följas av frågor som:

- Är alla nödvändiga samhällssektorer involverade i försvarsåtgärderna och är de tillräckligt förberedda för att agera mot hotet inom sina respektive sektorer?
- Finns en gemensam förståelse av situationen i både fred och kris som kan användas för att leda aktiviteterna i de olika samhälls-sektorerna?

[37] Treverton et al. (2018), *Addressing Hybrid Threats*, 80.
[38] Monaghan (red) (2019), *Countering Hybrid Warfare*, 19.
[39] Ibid., 26.

- Ger underrättelseaktiviteter tidig förvarning, kontinuerlig lägesbild och analys?[40]

Utöver frågan om lägesbilder sätter författarna här fingret på frågan om hot och medvetenhet bland tjänstemän och befolkning. Att de som ska rapportera in incidenter förstår den typ av hotbild som statlig subversion innebär är av stor vikt i hanteringen av hybrida hot.

Likt Försvarsberedningens rapport *Motståndskraft*, där en myndighet med samordningsansvar för totalförsvaret diskuteras utförligt,[41] menar MCDC vidare att det är grundläggande att ”utveckla det institutionella maskineriet” som förväntas upptäcka, avskräcka och besvara hybrida hot.[42] MCDC beskriver de policyval som ligger till grund för motåtgärder och pekar på ett antal nyckelfaktorer. Man betonar bland annat vikten av att synkronisera motåtgärderna mellan aktörer och sektorer i samhället, vilket i sin tur kräver institutionell samordning, även kring lägesbilder.[43] Att möta och besvara hybrida hot är en ”whole-of-government”-aktivitet och ”hellre än att skapa ett nytt institutionellt maskineri bör existerande institutioner, processer och organisationer justeras och förstärkas.”[44] Det finns alltså olika ståndpunkter kring frågan om det är nödvändigt att skapa helt nya funktioner, eller om samordningsfrågan kan lösas inom existerande strukturer.

I litteraturen finns sammanfattningsvis ett antal delmoment som anses vara centrala för hantering av hybrida hot:

- att upptäcka dem
- medvetandegöra de som arbetar vid ansvariga myndigheter
- att bygga motståndskraft
- att skapa institutionella arrangemang där så behövs[45]

Dessa delmoment återkommer i kapitel 5, där vi diskuterar dem i samband med tre strategier för hantering av hybrida hot. Dessa strategier utvecklas nedan i kapitel 3.3.

[40] Cederberg och Eronen (2015), *How Can Societies Be Defended Against Hybrid Threats?*, 7-8.
[41] Försvarsberedningen (2017), 93ff.
[42] Monaghan (red) (2019), *Countering Hybrid Warfare*, 4.
[43] Ibid., 56.
[44] Ibid., 63.
[45] Jämför med Appelgren et al. (2020), som diskuterar frågan utifrån en liknande utgångspunkt.

3.3 Strategier för hantering av hybrida hot

Litteraturen ger oss en övergripande bild av vad subversiv statlig antagonism kan vara och vad som bör ingå i ett bemötande därav. Den beskriver upptäckande, medvetandegörande, motståndskraft och institutionella arrangemang som viktiga delmoment i hantering av hybrida hot. *Vad* som ska hanteras är fastställt på en generell nivå, men *hur* dessa delmoment ska hanteras återstår att diskutera. Det finns rimligtvis olika sätt att skapa motståndskraft, upptäcka subversion, och så vidare. Det är viktigt att reflektera över olika typer av ansatser inför utvecklingen av en strategi för hantering av hybrida hot. I nedanstående avsnitt utvecklar vi ett synsätt på vad det betyder att ”hantera” hybrida hot i tre principiella förhållningssätt.

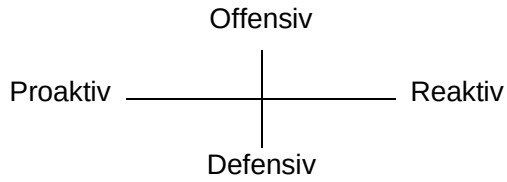
Själva ordet ”hantering” är inte alltid så tydligt, men det är inte en slump att vi på svenska talar om just detta. Ordet ”hantera” är både centralt och insiktsfullt i det svenska sammanhanget: att hantera är att manipulera något, leda det, att skaffa sig svängrum i relation till något.[46] Ett offer för övermäktiga krafter hanterar inte – det försvarar sig, skyddar sig, drar ihop sig. Att ”hantera” innebär att den som utsätts styr aktivt för att avvärja hotet. Det kan till och med handla om att använda sig av *aggression* – långt från en passiv roll som endast håller emot. Med denna förståelse av hantering som utgångspunkt kan vi skapa en bild av olika sätt att bemöta hybrida hot.

3.3.1 Dimensioner för hantering

För att utforska olika sätt för hantering av statlig antagonism är ett första steg att definiera generella dimensioner som beskriver olika typer av svar på de problem som sådana hot utgör.[47] Den första dimensionen skiljer mellan reaktiva och proaktiva åtgärder, där reaktivitet handlar om att skydda först när något händer, och proaktivitet handlar om att agera innan något har hänt. Den andra dimensionen går mellan en defensiv hållning, som handlar om att fokusera ”inåt”, på att säkra de egna skyddsvärdena; och en mer offensiv hållning som syftar till att påverka motståndaren – att agera ”utåt”. Dessa dimensioner är teoretiska, men ger oss ett sätt att tänka kring hur hybrida hot kan bemötas. Om de två dimensionerna ställs i relation till varandra ser vi att de kan kombineras enligt figur 1 nedan.

[46] Resonemanget bygger på Svenska akademiens definition av order hantering. Se: Svenska akademien (2020). Sökbegrepp: ”hantera”, i: *Svenska Akademiens ordbok* (tryckår 1930). www.svenska.se (hämtat 2020-02-17)

[47] Metoden som ligger till grund för följande stycke beskrivs utförligare i inledningskapitlet.



Figur 1. Dimensioner för hantering av hybrida hot.

För Polismyndigheten kan dessa olika dimensioner ge riktning åt olika strategier, i betydelsen *övergripande planer*, i relation till hybrida hot:

- En reaktiv/defensiv inriktning. Detta skulle kunna kallas en *beskyddande strategi*. Målet är att försöka behålla förmågor och skydda samhällsviktig verksamhet när påfrestningar uppstår.
- En proaktiv/defensiv inriktning. Detta skulle kunna kallas för en *bemötande strategi*. Målet är att manövrera självständigt i relation till hotbilden för att på så sätt undvika att påverkas av hybrida hot.
- En proaktiv/offensiv inriktning. Detta skulle kunna kallas en *störande strategi*. Målet är att påverka motståndaren innan denne hinner utföra subversiv verksamhet, till exempel genom att avleda fienden med lockbeten eller vilseleda den med avledningsmanövrar.
- En reaktiv/offensiv inriktning. Detta skulle kunna kallas en *konfrontativ strategi*. Målet är att avskräcka fienden genom att lägga stor vikt vid vedergällning efter att ett angrepp har konstaterats.

Strategierna kan också anses vara inspirerade av olika typer av avskräckning.[48] Den bemötande strategin skulle kunna utgöra grunden för en mer operativ version av det som vi ovan kallade ”demokratisk avskräckning” medan den störande strategin bär likheter med traditionell, bestraffande avskräckningstaktik.[49] Den beskyddande strategin, i denna principiella form, visar snarare frånvaron av avskräckning eftersom den endast reagerar *efter* att något har hänt. Dessa strategier kan användas för att tänka på olika sätt att förhålla sig till de olika delmoment som definierades i kapitel 3.2. Vi återkommer till detta i kapitel 5, där vi diskuterar varje delmoment utifrån de olika strategierna.

[48] Jmfr. Robert Dalsjö, *Fem dimensioner av tröskelförsvar*, FOI-R--4458--SE (Stockholm: FOI Totalförsvarets forskningsinstitut, 2017).

[49] Demokratisk avskräckning skulle kunna uppfattas som en offensiv strategi, men i detta sammanhang klassificeras den som defensiv eftersom den inte agerar ”utåt” utan huvudsakligen fokuserar på inre angelägenheter.

Eftersom civila myndigheter inte har någon förmåga till vedergällning och eftersom konfrontation rimligen är en fråga för en högre politisk nivå kommer den konfrontativa strategin inte att diskuteras vidare i denna rapport.

3.3.2 Strategiernas vägledande frågeställningar

För att förtydliga de olika förhållningssätt som ligger bakom de olika strategierna kan de beskrivas i termer av olika vägledande frågeställningar. Detta är endast ett sätt att illustrera skillnaderna i strategierna – en rad andra frågor till varje strategi är givetvis möjliga.

Svensk krishantering definieras enligt krisberedskapsförordningen (SFS 2015:1052) och MSB:s föreskrifter. Som vi beskriver i kapitel 4 föreskriver dessa att aktörer i krisberedskapssystemet ska fokusera på varje organisations sårbarheter och skyddsvärda verksamheter. [50] Krisberedskapens bärande frågeställningar utifrån dessa dokument är, smått förenklat:

Vilka är en aktörs kritiska skyddsvärden?

Hur kan vi skydda dem?

Ska vi utveckla tänkandet kring strategier för hantering av hybrida hot kan emellertid ytterligare frågor ställas, t.ex:

- Vilka förmågor tappar vi när vi utsätts för åtgärd X, Y eller Z?
- Vilka förmågor måste behållas för att klara av de uppgifter som definieras i respektive myndighets styrande dokument?
- Vilka åtgärder stör antagonisten mest?
- Vilka förmågor behövs för att utföra dem?

Dessa är potentiellt viktiga frågor när det gäller hantering av hybrida hot, beroende på vilken strategi som följs. En beskyddande strategi frågar vilka skyddsvärden och förmågor som är mest centrala. En bemötande strategi frågar vilka förmågor som måste utvecklas. En störande strategi, till sist, frågar hur vi stör (den potentiella) antagonisten på bästa sätt. Andra eller ytterligare frågor är givetvis också möjliga, men dessa kan ses som exempel på hur strategierna är tänkta att utformas. Tabell 1 sorterar in de olika frågorna till varje strategi.

[50] MSB, *Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser*, MSBFS 2016:7 (Stockholm: Myndigheten för samhällsskydd och beredskap, 2016).

Tabell 1. Frågor för olika typer av strategier

Strategityp – Centrala frågor		
Beskyddande	*Bemötande*	*Störande*
Vilka skyddsvärden är mest sårbara?	Hur maximeras en organisations motståndskraft?	Vilka åtgärder stör antagonisten mest?
Vilka förmågor måste behållas för att klara av uppgifter enl. lag?	Vilka förmågor ska utvecklas för att nå dit?	Vilka förmågor behövs för att utföra dem?

Beskyddande, bemötande och störande utgör alltså tre principer som kan användas i kombination, var för sig och på olika nivåer. I kapitel 5 utvecklas diskussionen kring dessa frågeställningar och vad de betyder i praktiken, med särskilt fokus på Polismyndigheten. Kapitlet innehåller en diskussion om hur dessa strategier kan kopplas till de olika delmoment för hantering av hybrida hot som definierades i kapitel 3.2: upptäckande, medvetandehöjande, organisatorisk motståndskraft och institutionell samverkan. Innan dess beskriver vi de system som redan idag existerar i Sverige för hantering av situationer utanför det normala.

4 Hantering av hybrida hot ur ett institutionellt perspektiv

I kapitel 3 definierades dels skilda delmoment i hanteringen av hybrida hot med utgångspunkt i existerande litteratur. Dels definierades tre strategier som i kapitel 5 används för att beskriva hur de olika delmomenten kan utföras på olika sätt. Emellertid är det viktigt att först upprätta en bild av existerande institutionella system i Sverige som är tänkta att hantera situationer utöver det normala under fredstid.

Hybrida hot är en på många sätt relevant företeelse, om än i varierande grad för olika aktörer och institutioner. Regeringen har på strategisk nivå det övergripande ansvaret för svensk försvarspolitik. En nationell strategi skiljer sig emellertid från en enskild myndighets strategi – ur nationellt försvarsperspektiv utgör Polismyndighetens hantering i det närmaste en taktisk fråga. Det är inte heller nödvändigt att en svensk defensiv försvarsstrategi, till exempel, måste motsvaras av en defensiv hantering av hybrida hot inom Polismyndigheten.

En myndighet har således möjlighet att själv internt utforma en egen strategi för hantering av hybrida hot, särskilt innan subversiv antagonistisk verksamhet har hunnit bli en fråga för Sveriges internationella relationer. Hur olika myndigheter hanterar frågor om krisberedskap, säkerhetsskydd och hybrida hot skiljer sig därför också avsevärt. En översikt som nyligen genomfördes vid FOI visar dock att en stor andel av de svenska aktörerna inte ens har ett aktivt risk- och sårbarhetsarbete för krisberedskap.[51] I fråga om planering för hybrida hot är det därför rimligt att anta att andelen är än mindre. I detta kapitel diskuteras betydelsen av hybrida hot, dels under höjd beredskap, dels i fredstid. Vi fokuserar framförallt på frågan om hybrida hot i fredstid för civila myndigheter generellt, och Polismyndigheten specifikt.

4.1 Hybrida hot och totalförsvaret

Totalförsvaret består av det civila och det militära försvaret. För båda delarna är hybrida hot ytterst relevanta. Totalförsvaret är enligt lag (1992:1403) om totalförsvar och höjd beredskap den verksamhet som behövs för att förbereda Sverige för krig. Vid krig aktiveras lagstiftning i Sverige som omdefinierar bl.a. Försvarsmaktens och Polismyndigheternas rollfördelning och ansvar. Polisen ska under höjd beredskap utföra de

[51] Lovisa Mickelsson, *Uppföljning av risk- och sårbarhetsanalyser – Resultatredovisning från en enkätundersökning genomförd 2019*, FOI-R--4803--SE (Stockholm: FOI Totalförsvarets Forskningsinstitut, 2020).

uppgifter som organisationen har i fredstid, men även stödja totalförsvaret på olika sätt. För närvarande pågår omfattande planeringsverksamhet som påverkar samtliga bevakningsansvariga myndigheter. Polismyndighetens planering på området civilt försvar rör i viss utsträckning frågan om hybrida hot.[52]

I en situation där totalförsvaret har aktiverats kommer substantiella hot redan att ha riktats mot Sverige. Säkerhetsläget kommer att ha försämrats väsentligt från det som råder under fredstid. Bland annat kommer attribuering av den eller de aktörer som hoten utgår från med all sannolikhet att ha skett innan beslut fattas om höjd beredskap. Också de hybrida hotens överraskningseffekt kommer att vara dämpad eftersom samhället i en sådan situation förväntar sig antagonistisk verksamhet från en eller flera aktör(er). Totalförsvaret står således inför en komplicerad, men sannolikt något tydligare problembild än den som denna rapport behandlar. Hur totalförsvaret ska hantera hybrida hot, utöver de aspekter som sammanfaller med krisberedskapsplanering, faller således utanför denna rapports ram.[53]

Nedan fortsätter vi med en diskussion om hybrida hot för svenska myndigheter under fredstid.

4.2 Hybrida hot innan höjd beredskap

Hybrida hot är utformade för att riktas mot mål redan under fredstid och för att innebära en belastning för måltavlan som begränsar dennes handlings- eller försvarsförmåga. Antagonistisk verksamhet kan på mer eller mindre systematiskt vis riktas mot Sverige utan att detta innebär en tydlig krigshandling eller ens är primärt riktat mot Sverige.

Det svenska samhället är emellertid inte oförberett på denna typ av situation. I Sverige existerar olika institutionella system[54] med uppgift att hantera påfrestande tillstånd inom riket i fredstid. Beroende på vilken typ av verksamhet som antagonisten utför kan det röra sig om synbarligen

[52] Eftersom planeringen sker med utgångspunkt i krisberedskapen diskuterar vi detta i nästa avsnitt.

[53] Emellertid konstaterar Johansson et al. (2017, 58). att: ”Gränsen mellan när fredstida antagonistiskt våld ska tolkas som en aggression som gör att det är påkallat att införa höjd beredskap eller beteckna det som krig är dock otydlig. Det innebär inte heller att det självklart finns en naturlig gräns mellan det som civilt försvar respektive fredstida krisberedskap ska hantera.”

[54] Ett *institutionellt system* är en uppsättning regler, konventioner, fysiska objekt och handlingsmönster som styr människors beteende inom ett givet område, såväl som den eller de aktörer som utövar tillsyn över reglernas efterlevnad. Jmfr. Levis definition av ”institution”, återgiven av Rothstein ”Political Institutions: An Overview”, i *A New Handbook of Political Science*, red. Robert E. Goodin och Hans-Dieter Klingemann (Oxford: Oxford University Press, 1996), 145.

orelaterade saker som angrepp mot företagshälsovård, transportsystem eller smittskydd. För Polismyndighetens vidkommande, bedöms *säkerhetsskyddet, krisberedskapen* och *rättsväsendet* vara de mest relevanta institutionella systemen:

- Säkerhetsskyddet består av regler för skydd av säkerhetskänslig verksamhet.
- Krisberedskapen är utformad för att hantera naturkatastrofer, olyckor eller andra händelser som påverkar medborgares liv och hälsa. Det överlappar i viss utsträckning med det civila försvaret, både organisatoriskt och planeringsmässigt.
- Rättsväsendet, där Polismyndigheten ingår, är utformat att upprätthålla lag och ordning.

Dessa system är utformade för att förhindra och hantera avvikelser i samhället av den typ som hybrida hot kan komma att innebära. När vi senare i rapporten diskuterar olika sätt att hantera hybrida hot är det därför viktigt att ha med sig en förståelse för dessa systems grundläggande drag och uppgifter. Nedan diskuteras därför relationen mellan hybrida hot och dessa tre institutioner. Varje del presenterar först de olika systemens allmänna drag, för att sedan beskriva betydelsen för Polismyndigheten.

4.2.1 Säkerhetsskydd

Säkerhetsskyddet definieras i säkerhetsskyddslagen (SFS 2018:585) och säkerhetsskyddsförordningen (SFS 2018:658). Dessa specificeras ytterligare av Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2) och MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6). Säkerhetsskydd består av en uppsättning regler och föreskrifter som syftar till att skydda säkerhetskänslig verksamhet och är uppdelat på de tre delarna:

- informationssäkerhet
- fysisk säkerhet
- personalsäkerhet.

Kravet är att samtliga myndigheter ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Tillsynsmyndigheter är Säkerhetspolisen och Försvarsmakten (gällande de aktörer som faller under deras respektive område).

Säkerhetsskyddet är en förhållandevis ”smal” institution i det hänseendet att ansvarsområdet såväl som antalet lagar och förordningar är begränsat. Det operativa ansvaret ligger därutöver på varje enskild aktör som omfattas av lagstiftningen.

Säkerhetsskyddets första krav är att alla myndigheter ska utföra en säkerhetsskyddsanalys där skyddsvärd information och annan skyddsvärd verksamhet identifieras (SFS 2018:658 2. Kap. §1). Dessutom ska organisationen vidta åtgärder för att säkra de aspekter av verksamheten som bedöms vara särskilt känsliga ur säkerhetssynpunkt. Säkerhetsskyddslagstiftningen som trädde i kraft 2019 ställer höga krav på organisationers förmåga att upptäcka, försvåra och hantera skadlig inverkan.

I fredstid är säkerhetsskyddet i allra högsta grad relevant för hantering av hybrida hot. Påverkan mot personal, fysiska objekt och informationssystem bedöms kunna vara centrala mål för en antagonist. Säkerhetsskydd syftar ytterst till att skapa motståndskraft mot subversiv verksamhet, såsom sabotage, informationsintrång, hot mot enskilda osv. Säkerhetsskyddet föreskriver dessutom att aktörerna identifierar och rapporterar händelser till tillsynsmyndigheterna,[55] som på det viset får insikt i de typer av antagonistiska verksamheter som pågår i Sverige. De åtgärder som ingår i säkerhetsskyddets tre huvudområden (se ovan) utgör således det primära skyddet på organisationsnivå för säkerhetskänslig verksamhet mot hybrida hot.

För Polismyndigheten betyder det att säkerhetsskyddet har potential att avlasta polisen, eftersom det syftar till att skapa en bättre riskhantering hos samtliga myndigheter och därmed reducera antalet incidenter. I den mån som angrepp uppdagas kan ett effektivt säkerhetsskydd också ge upphov till informationsdelning från civila myndigheter till polisen och Säpo, vilket ökar chansen att skapa en rättvisande lägesbild.

4.2.2 Krisberedskapssystemet

Svenska myndigheters agerande under samhällsstörning eller kris regleras av krisberedskapsförordningen.[56] Förordningen definierar krisberedskap som den verksamhet som syftar till att förebygga, motstå och hantera krissituationer (§4). De krav som krisberedskapslagstiftningen ställer på svenska myndigheter är i första hand att i så stor utsträckning som möjligt upprätthålla ”förmågan till verksamhet” (§8), vilket särskilt gäller samhällsviktiga funktioner och oförutsedda händelser. Myndigheter ska alltså kunna fungera som normalt, även vid stora påfrestningar. Vidare ska myndigheter dela lägesbilder med MSB och Försvarsmakten om så krävs

[55] Dessa är Säkerhetspolisen och Försvarsmakten.

[56] Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Utöver denna finns en rad andra lagar och förordningar av relevans för krisberedskapen. Se: MSB ”Gemensamma grunder för samverkan och ledning vid samhällsstörningar”, 4:e uppl., MSB777 (Stockholm: Myndigheten för samhällsskydd och beredskap, 2018), 27.

(§14), och i vissa fall ”omgående kunna upprätta en ledningsfunktion” (§12) för att hantera krissituationer.

För att åstadkomma detta ska myndigheter analysera sina respektive verksamhetsområden och upprätta en risk- och sårbarhetsanalys (RSA) (§8). Likt säkerhetsskyddsanalysen är RSA ett sätt att identifiera vilka delar av verksamheten som riskerar att bli särskilt utsatta. Polismyndighetens RSA, till exempel, samlar en mängd information om verksamheten. Detta arbete är till del synkroniserat med säkerhetsskyddet, men inte helt.[57] I polisens RSA ingår centrala externa uppgifter, som civilt försvar och skydd av samhällsviktig verksamhet. För närvarande pågår ett arbete på Polismyndigheten med kontinuitetshantering med utgångspunkt i polisens RSA, som är tänkt att stärka myndighetens motståndskraft och säkra tillgången till resurser och personal även under stora påfrestningar.[58]

Utöver säkerhetsskyddet är krisberedskapen ytterligare ett lager av förberedelser för det oväntade, som syftar till att bygga motståndskraft mot påfrestningar. Eftersom hybrida hot bygger på antagonistens anpassningsförmåga och utnyttjande av en motståndares svagheter, kan sårbarheter som inte har aktualiserats i tidigare RSA exploateras. Krisberedskapsplaneringen står därmed inför mycket höga krav på egen anpassningsförmåga, intern styrning och tillgång till rätt resurser.

Polismyndigheten är en del av krisberedskapssystemet och har enligt krisberedskapsförordningen (SFS 2015:1052, bilaga) ett särskilt ansvar för områdena ”farliga ämnen” samt ”skydd, undsättning och vård”.

Polismyndigheten kan emellertid också utsättas för påverkansoperationer. I en situation där Sverige är utsatt för ett breddat eller hybridt hot, i linje med diskussionen i kapitel 2, ska polisen fortsatt kunna utföra sina uppgifter såsom de definieras i polislagen (SFS 1984:387). För att uppskatta hur Polismyndigheten kan påverkas av hybrida hot är det rimligt att först se till de sårbarheter som präglar organisationen. Det finns inga sårbarheter som är specifika för hybrida hot. Vilka delar av organisationen som påverkas beror i stor utsträckning på vilka typer av subversiv verksamhet som riktas mot Sverige. Således kan en initial utgångspunkt för hantering av hybrida hot vara att fokusera på att stärka motståndskraften i den befintliga organisationen och täppa igen kända säkerhetsluckor.

[57] Vissa aspekter går utöver säkerhetsskyddet, till exempel frågor kring CBRNE och farliga ämnen (Intervju Krisberedskapsgruppen, Polismyndigheten-NOA, 2019-05-10).

[58] Polismyndigheten, *Polisens arbete inom krisberedskap* (Polismyndigheten: Stockholm, 2019) Polismyndighetens webbplats: https://polisen.se/om-polisen/polisens-arbete/polisens-krisberedskapsarbete/polisens-arbete-inom-krisberedskap/ (hämtat 2020-02-17)

4.2.3 Rättsväsendet

Rättsväsendets mål är att upprätthålla den enskildes rättssäkerhet och rättstrygghet.[59] Det består av bland andra Sveriges domstolar, Polismyndigheten, Säkerhetspolisen, Åklagarmyndigheten och Kriminalvården. Dessa myndigheter ansvarar gemensamt för rättssäkerhet och rättstrygghet i Sverige. För diskussionen om hybrida hot generellt, och denna rapport i synnerhet, är rättsväsendet centralt.

En antagonists syfte med att utsätta sin motståndare för hybrida hot är att försämra dennes försvarsförmåga, uthållighet, eller sammanhållning under tröskeln för krigsutbrott. I Sverige har detta uppfattats i termer av att verksamheten inte ska resultera i att regeringen utlyser höjd beredskap.[60] Detta utesluter till exempel inte att hybrida hot i en betydande utsträckning handlar om brottslig verksamhet, särskilt i de fall där underrättelseunderlag föreligger som pekar på att händelserna ingår i en systematisk strategi från en främmande makt. Svensk lag definierar de flesta former av statlig antagonistisk verksamhet som brottsliga såtillvida de inte faller under grundläggande politiska rättigheter enligt Regeringsformen. Sålunda är till exempel sabotage, spioneri, dataintrång, påverkan på samhällsviktig verksamhet och dokumentation av skyddsobjekt straffbara under svensk lag. Endast när det gäller utövandet av politiska rättigheter, till exempel i informationsmiljön eller tillstånd för allmänna sammankomster, tolereras subversion i viss utsträckning. Rättsväsendet har således en övergripande funktion i hanteringen av hybrida hot, även om den subversiva verksamheten sker inom ramen för andra delar av samhället. Detta är anledningen till att polisen i vissa fall talar om ”blåzon” istället för det mer generella begreppet ”gråzon”; Polisen tillsammans med de övriga rättsvårdande myndigheterna är helt enkelt de aktörer som har uppdraget att hantera hybrida hot under en initial fas.

Polisen är ofta den första delen i rättskedjan och för sedan vidare underrättelser och utredningsmaterial till de andra rättsvårdande myndigheterna. Det är dock viktigt att behålla ett övergripande perspektiv, dels genom att förstå Polismyndighetens roll i relation till regeringskansliet, Försvarsmakten och MSB, men även till de myndigheter som tillhör rättsväsendet.

[59] Regeringskansliet, *Det svenska rättsväsendet* (Stockholm: Regeringskansliet, 2015), 5.
[60] Jmfr. Freddy Jönsson Hanberg (red.), *Totalförsvarsstudien. Förstudie* (Stockholm: Totalförvarsstiftelsen, 2016).

5 Konsekvenser för Polismyndigheten: principer för hantering av hybrida hot

I det ovanstående har rapporten först efter en litteraturgenomgång operationaliserat begreppet hybrida hot som subversiv antagonistisk verksamhet utgående från en statlig eller statligt sanktionerad aktör. Tre institutionella system i Sverige identifierades som är tänkta att hantera sådana samhälleliga hot – säkerhetsskydd, krisberedskap och rättsväsende. I det nedanstående utgår vi från motståndskraft som avskräckande princip för myndigheter utan offensiv förmåga. Vi diskuterar de fyra delmoment för hantering av hybrida hot som identifierades i kapitel 3.2: upptäcka, höja medvetenheten, organisatorisk motståndskraft och samverkan. Dessa aktiviteter kan betyda olika saker beroende på vilka strategier som kopplas till dem. För att vidare mejsla ut strategiska vägval för hantering av hybrida hot kopplas de till de tre strategier som presenterades i kapitel 3.3.

5.1 Upptäcka

Ett första steg i någon form av förhållande till hybrida hot är att upptäcka deras existens. I vissa fall överrumplas måltavlan av en antagonist, vilket var fallet med den ryska annekteringen av Krim 2014. I andra fall, motsvarande Sveriges situation idag, finns medvetenheten om de hot som riktas mot svenska intressen bland säkerhetsexperter, tjänstemän inom regeringskansliet, Polismyndigheten och Säpo, såväl som hos politiska beslutsfattare. Upptäckande-aspekten av en strategisk hantering av hybrida hot fokuserar på att dessa grupper ska nås av så tillförlitliga och användbara lägesbilder som möjligt. Frågan som de bör ställa sig är:

> *Hur vet vi om Sverige eller enskilda myndigheter utsätts för statlig antagonistisk verksamhet?*

Som vi diskuterade i kapitel 2 är strategin bakom hybrida hot i första hand att hålla konfliktnivån låg nog för att undvika repressalier från måltavlan. Krigsutbrott undviks så lång det är möjligt. Temperaturen i vattnet ska höjas gradvis så att grodan inte märker att den snart inte har något annat val än att kokas eller hoppa ut ur bägaren. Hybrida hot ska i många fall inte upptäckas alls, i andra fall är själva syftet att antagonistisk verksamhet ska märkas, men inte med säkerhet kunna attribueras.[61] Rör det sig om väl

[61] Rory Cormac och Richard J. Aldrich, ”Grey Is the New Black: Covert Action and Implausible Deniability”, *International Affairs* 94, nr 3 (01 maj 2018): 477–94, https://doi.org/10.1093/ia/iiy067.

utförd subversiv verksamhet kommer detta att innebära en stor utmaning för måltavlan.

För att avskräcka en motståndare kan en organisation gå strategiskt tillväga, också i fråga om upptäckande. Den kan använda en viss princip i analysen av tillgänglig eller inhämtning av ny information. I kapitel tre diskuterades tre olika strategiska principer, eller strategityper: beskyddande, bemötande och störande. Vi kan nu applicera dessa på problemet kring detektion:

En *beskyddande* strategi fokuserar på att bevara det som redan finns. Således riktas informationssökningen, om en aktör vill skapa sig en bild av säkerhetsläget, mot den egna verksamheten. Är min personal utsatt för utpressning eller hot? Förekommer skadegörelse eller dataintrång i min organisations system? Aktören som följer denna strategi har inte – eller vill inte skaffa sig – förmågan att se utanför den egna verksamheten. Aktören kan inte verka uppsökande, utan endast bekräfta när något händer och rapportera detta uppåt i hierarkin till närmast ansvariga tillsynsmyndighet.

En *bemötande* strategi för att upptäcka huruvida hybrida hot riktas mot den egna verksamheten är mer aktiv. Här utvecklar aktören den beskyddande ansatsen och tar i större utsträckning saken i egna händer. Det kan handla om att identifiera hotaktörer och aktivt hålla dem under uppsikt, eller att begära information från externa källor som på ett eller annat sätt beskriver deras verksamhet. En aktiv informationsinhämtning från Polismyndighetens sida kan även skapa nya samverkansformer med andra aktörer som har liknande intressen. Till sist kan en aktör välja att skapa helt nya informationskällor anpassade för dennes syften.

En *störande* strategi för upptäckande av hybrida hot bygger vidare på den bemötande. En mer offensiv hållning till upptäckande innebär dock att taktiken förändras. Den störande aktören kan lägga ut beten, till exempel i form av servrar med enkla lösenord för att undersöka hur lång tid det tar innan ett intrång kan konstateras. Aktören kan offentliggöra dimridåer, till exempel i form av felaktig information, för att vilseleda en antagonist och få denne att röja sina intentioner. Den störande aktören kan till sist snabbt sprida eller offentliggöra information om antagonistens handlande och på så sätt skapa medvetenhet om aktuell hotbild, eller skämma ut motparten.

Dessa tre riktningar kan antas av små och stora organisationer och kräver inte alltid omfattande resurser. Det är framförallt en fråga om hur aktören själv vill agera, samt vilket risktagande som anses vara acceptabelt. För Polismyndigheten kan en störande strategi i vissa fall vara olaglig, men i andra fall ett möjligt val. Det är också möjligt att agera aktivt på olika sätt, tex. kan Polismyndigheten välja att fokusera på enskilda ”aktiva” åtgärder på taktisk nivå men att agera mer defensivt på en mer övergripande,

strategisk nivå. I dagsläget är det svårt att uppskatta vilken eller vilka strategier myndigheten följer, eftersom det inte finns någon uttalad strategi på detta område.

5.2 Höja medvetenheten

Att höja medvetenheten hos en befolkning, de anställda på Polismyndigheten, eller en specifik grupp är nästa delmoment. Höjd medvetenhet kan öka människors benägenhet att rapportera in incidenter som annars skulle ha gått dem förbi. Det ger i bästa fall en hög vaksamhet och underlättar upptäckande (i värsta fall skapas dock onödig rädsla hos målgruppen). En antagonistisk aktör som är medveten om att måltavlans befolkning är vaksam kommer att behöva lägga mer resurser på att dölja eller maskera subversiva verksamheter än annars, vilket höjer kostnaden för att utöva hybrida hot.

Åtgärder som höjer medvetenheten om hybrida hot handlar om kommunikation. Kommunikationsarbete är komplicerat på grund av svårigheten att kontrollera hur ett budskap tolkas och sprids – detta än mer i de sociala mediernas tidsålder. Informationsinsatser bör således utföras parallellt med en riskanalys där eventuella negativa aspekter vägs in innan arbetet påbörjas.

På liknande sätt som upptäckandeaspekten kan flera olika ansatser särskiljas:

En *beskyddande* strategi skapar generell information som finns tillgänglig för den eller de som söker upp den. Den beskyddande aktören försöker inte marknadsföra information till människor utan anser sig ha fullföljt sin informationsplikt i samband med att ett material *i princip* görs tillgängligt. Det är så att säga en passiv inställning till kommunikationsarbete, där det räcker att informationen existerar så att människor kan tillgå den om behovet skulle uppstå. Ett exempel är MSB:s internetportal krisinformation.se.

En *bemötande* strategi, bygger på den beskyddande men arbetar mer uppsökande. I samband med hybrida hot finns det en risk för att drabbas av informationsoperationer, till exempel liknande de som förekom i samband prisutdelningen av Tucholskypriset till Gui Minhai 2019.[62] En aktivt bemötande aktör publicerar inte bara sin version av ett narrativ, utan försöker att sprida den och skapa ett ifrågasättande av antagonistens status. Aktivt kommunikationsarbete analyserar och segmenterar målgruppen för att nå ut med sitt budskap, till skillnad från den mer passiva strategin som

[62] Anders Johansson, ”Kina fördömer kulturminister Amanda Linds prisutdelning”, *Aftonbladet*, 16 november 2019, https://www.aftonbladet.se/a/9ve265.

endast publicerar sin version. Till sist försöker den aktiva kommunikatören driva på samhällsdebatten och förskjuta tolkningsramen i det samhälleliga samtalet till en för aktören gynnsam inriktning.

Den *störande* strategin, till sist, arbetar likt den bemötande aktören aktivt med kommunikationsarbete, men försöker därutöver störa antagonisten genom att själv genomföra informationsoperationer. Det kan också handla om att snabbt offentliggöra information som ställer antagonisten i dålig dager eller att särskilt tydligt påvisa hotbilden. Den störande aktören behöver vara försiktig och inte passera gränsen för vad som är lagligt, eller vad som uppfattas som oetiskt, till exempel att köpa följare till inlägg på sociala medier.[63] Inte alla aktörer kan anta en störande strategi, eftersom den på sätt och vis liknar det *modus operandi* som vanligtvis associeras med statliga antagonister.

Polismyndigheten har på grund av sin roll i samhället hittills intagit en passiv, beskyddande ställning. Exempel på detta är frågan om NMR skulle få demonstrationstillstånd i Visby under Almedalsveckan och under valrörelsen 2018. I flera fall har Polismyndighetens opartiskhet ifrågasatts i medierapporteringen kring fallen.[64] Det är svårt att se att polisen skulle kunna inta en störande hållning, men det är inte omöjligt att myndigheten skull kunna arbeta mer aktivt med att bemöta fientlig propaganda i det fall att en statlig antagonist försöker skapa osäkerhet kring polisen och ifrågasätta polisens legitimitet.

5.3 Bygga motståndskraft

Försvarsberedningens rapport *Motståndskraft* utgår ifrån att ett hållbart samhälle som motstår påverkan är den bästa avskräckningen för en fiende eftersom det höjer kostnaden för att åstadkomma ett givet mål.[65] Rent principiellt kan vi föreställa oss två extremscenarier:

I ett positivt idealfall skulle det svenska samhället, när det utsätts för subversiv verksamhet, fortsätta att fungera precis som vanligt. Alla

[63] Det uppdagades under valkampanjen i Österrike 2018 att de österrikiska Socialdemokraterna hade köpt följare och likes, och även engagerat sig i negativ marknadsföring av motståndarsidan. Följden blev en skandal och stor förlust i valet. Se: Philip Oltermann. ”Negative Campaign Sites Scandal Shakes up Austrian Election Race”. *The Guardian*, 05 oktober 2017. http://www.theguardian.com/world/2017/oct/05/negative-campaign-sites-scandal-shakes-up-austrian-election-race.

[64] Se: Holmqvist, Tobias, ”Nazistiska NMR får tala i Almedalen”. *SVT Nyheter*. 30 maj 2018. https://www.svt.se/nyheter/lokalt/ost/nmr-far-halla-torgmote-i-almedalen (hämtad 2019-03-04); ”Kritiken mot polisen växer efter NMR:s närvaro i Almedalen”. 2018. *DN.SE*. 12 juli 2018. https://www.dn.se/nyheter/sverige/kritiken-mot-polisen-vaxer-efter-nmrs-narvaro-i-almedalen/ (hämtad 2019-03-04).

[65] Försvarsdepartementet, *Motståndskraft. Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025*. Ds 2017:66 (Stockholm: Regeringskansliet, 2017).

avvikelser skulle hanteras i linjeverksamheten på samma sätt som alltid. I detta fall skulle delar av samhället möjligtvis påverkas negativt av varje enskild attack, men inte i den grad att dess institutioner upphörde att fungera eller att samhällsviktig verksamhet påverkades nämnvärt. Samhället skulle vara motståndskraftigt. En angripare skulle inte ha substantiella fördelar med att upprätthålla subversionen då måltavlan inte lät sig påverkas av den. Detta skulle även bli svårare och innebära högre kostnader för angriparen i takt med att rättsväsendet lagförde gärningspersonerna, och således med allt högre säkerhet kunde attribuera vem som stod bakom subversionen. I detta fall skulle motståndskraften i sig utgöra en avskräckande faktor, eller driva konfliktnivån uppåt och på så sätt exponera den antagonistiska partens verkliga intentioner.

I den motsatta situationen – där Sverige har en mycket *dålig* motståndskraft – kommer varje påverkansförsök att resultera i stor effekt både på det svenska samhället och på svensk försvarsförmåga. Till och med de enklaste attacker, påverkansförsök och den ringaste subversion ger stor utdelning för motståndaren. Denne inser snabbt att konventionella angrepp, ett av de tydligare maktmedlen, inte är nödvändigt och att Sverige är manipulerbart. Detta sätter svensk utrikes- och säkerhetspolitik under stor press och svensk autonomi är låg.

Det är inte den här rapportens syfte att uppskatta svensk förmåga och bestämma var på skalan mellan dessa två poler som samhället står. Snarare kan de tjäna som tankefigurer i hur en myndighet eller annan organisation skulle vilja utforma arbetet för att stärka motståndskraften. Återigen tar vi hjälp av de tre strategityperna:

En *beskyddande* strategi sätter fokus på skyddsvärden och samhällsviktig verksamhet, enligt krisberedskapsförordningen. Utöver detta skapar organisationen ett fungerande säkerhetsskydd som, likt delmomentet ”upptäckande” ovan, fungerar som ett incidentrapporteringssystem samtidigt som det skyddar personer, information och fysiska objekt mot påverkan. Organisationen planerar för kontinuitetshantering för att säkra fortsatt effektivitet även under svåra påfrestningar. Kort sagt, en myndighet som följer den beskyddande strategin följer svensk lag – de övriga bryter den inte, men gör mer än vad som är tvingande.

Den *bemötande* strategin utför samma analys och inför liknande åtgärder, men med långt större resursallokering. Medan många myndigheter bara knappt kan säkra en godtagbar nivå av motståndskraft, går den bemötande aktören längre och lägger mer omfattande resurser i säkerhetsskydd, kontinuitetsplanering och planering för civilt försvar. Systemets resurser överkompenseras och lägger stor energi på att visa det genom övningar och dylikt. Idén är att avskräcka motståndaren från att ens försöka angripa en så motståndskraftig organisation; att få antagonisten att ändra strategi medelst en sorts ”show of force.” Priset är högt i termer av de resurser som måste tas från andra delar av verksamheten.

Den *störande* strategin sätter fokus på hoten snarare än skyddsvärdena. Med det menas inte att aktören själv ska angripa antagonisten. Detta är ett annat sätt att tänka kring motståndskraft i termer av offensiv förmåga snarare än skademinimering och återhämtning. En grundläggande faktor för Polismyndigheten är en offensiv hållning i fråga om lagföring av brott, där hotaktörers verksamhet störs genom övervakning och penibel lagföring med målet att göra det svårt att verka i Sverige.[66] Den störande aktören satsar på att den tuffa hållning som antagonisten möter ska avskräcka denne från att utföra handlingar och omvärdera situationen. Om detta inte går ska antagonisten ändå störas i den grad att dennes operationer blir mindre verkningsfulla. Den störande strategin lämnar bakgården fri genom att sätta in de flesta resurser på att hålla fienden ute, ”på framsidan”. Som alla strategier har den nackdelar, till exempel att de svenska rättsvårdande myndigheterna i samband med arbetet riskerar att offentliggöra underrättelseinformation i samband med lagföringen.

I Polismyndighetens fall kan det handla om särskilt intensivt utrednings- och lagföringsarbete riktat mot hotaktörer för att göra det svårt för dem att verka i Sverige. De flesta myndigheter har inte egen möjlighet att agera offensivt genom lagföring, men i Polismyndighetens fall torde det möjligt i viss utsträckning, givet rätt underrättelseunderlag.

5.4 Institutionaliserad samverkan

Det sista delmomentet i hanteringen av hybrida hot är samverkan, eller institutionella aspekter. Vi väljer att kalla det institutionaliserad samverkan. Som vi har beskrivit tidigare finns ett antal system i Sverige som är utformade för att hantera avvikelser. I kapitel 4 diskuterade vi totalförsvaret, krisberedskapen, säkerhetsskyddet och rättsväsendet som de huvudsakliga system som den svenska staten har till sitt förfogande när den ska hantera subversiva angrepp från statliga antagonister. Säkerhetsskyddet och krisberedskapen är centrala för att bygga motståndskraft; totalförsvaret och krisberedskapen ställer i sin tur höga krav på samverkan mellan myndigheter. Rättsväsendet och säkerhetsskyddet kan bemöta hybrida hot i fredstid, medan totalförsvaret ytterst syftar till att försvara landet mot ett väpnat angrepp. Således både överlappar och kompletterar de fyra institutionerna varandra. Institutionaliserad samverkan handlar här om hur aktörer väljer att nyttja de möjligheter som finns, eller att skapa nya sätt att samverka. De tre strategierna föreskriver även här olika förhållningssätt:

Den *beskyddade* strategin deltar i de forum som redan har etablerats. Det anses inte behövas ytterligare samverkansformer, särskilt eftersom

[66] En jämförelse kan här göras med NSH Rimfrost när det gäller det grova våldet.

resurserna är knappa och planeringsarbetet redan är ansträngt. Exempelvis nyttjas de samverkansforum som krisberedskapslagstiftningen beskriver för bevakningsansvariga myndigheter. Kontakter mellan myndigheter sker reaktivt, på uppdrag från regeringskansliet eller för att lösa konkreta uppgifter. På sätt och vis är den beskyddande strategin i detta avseende minimalistisk: Den förordar inga särskilda åtgärder som inte motiveras av ett specifikt behov.

Den *bemötande* strategin däremot, intar en mer aktiv hållning. Om inte existerande samverkansformer fungerar tillräckligt bra försöker aktören skapa nya som är bättre anpassade för att hantera hybrida hot. Aktören försöker i samverkan med andra och på egen hand påverka lagstiftaren för att lätta på regelverket eller att instruera myndigheterna att satsa på nya samverkansformer, samt på lagstiftning som gör det enklare att bemöta de antagonistiska verksamheter som identifieras. Exempelvis skulle lagar om etableringsformer för utländska investerare eller upphandling kunna utformas (möjligtvis på europeisk nivå) för att försvåra för fienden att verka i Sverige. Den bemötande aktören tar också fram nya ledningsmetoder och -principer speciellt anpassade för hantering av hybrida hot, som inbegriper samverkan som en väsentlig del i arbetet.

Den *störande* strategin kan endast beskrivas utifrån ett samhällsövergripande perspektiv eftersom den institutionaliserar samverkan i samtliga delaspekter av hantering av hybrida hot. Ett hybridcentrum, eller motsvarande enhet inom regeringskansliet, etableras på högsta ort som inkluderar samtliga för frågan viktiga aktörer.[67] Samordningen är så omfattande som möjligt, och utformas för att försvåra för främmande makts att agera i Sverige. Går strategin i en mer konfrontativ riktning kan staten antyda att minsta tecken på aggression kan resultera i storskaliga motåtgärder. Exempelvis annonseras att totalförsvarets resurser kommer att kunna användas även innan regeringen har fattat beslut om höjd beredskap, om situationen kräver detta.

Den störande strategin är även den mest resurskrävande och kräver bred samverkan mellan regering, myndigheter och civilsamhälle.[68] De gränsdragningar som nämndes i kapitel 2 är tänkta att tydliggöra vilken typ av subversion eller påverkan som samhället inte kommer att tolerera. Regeringen söker här också aktivt efter pålitliga internationella allianser som ytterligare förstärker bilden av ett samhälle som är väl förberett för såväl subversion som krig.

[67] Jmfr. diskussionen som förs i Försvarsberedningens rapport *Motståndskraft* (2017), s. 93ff.
[68] Risken finns även att välfungerande delar av existerande arbete omintetgörs när nya lösningar prioriteras.

5.5 Tre strategier för hantering av hybrida hot

Utifrån underlaget som har presenterats i denna rapport har tre principiella strategier presenterats. Det ska betonas att strategierna inte är reella förslag på hur Polismyndigheten eller andra svenska myndigheter bör förhålla sig till hybrida hot. Snarare visar de ytterligheter som kan tjäna som tankekonstruktioner när en organisation arbetar med att ta fram ett förhållningssätt i relation till hybrida hot. Varje strategi för hantering av hybrida hot kan innehålla element från två eller alla tre strategier. I flera fall finns exempel på hur myndigheter i andra länder har hanterat hybrida hot som tangerar åtgärderna som beskrivs ovan. I vissa fall, som i fallet med den bemötande strategins agerande när det gäller att skapa motståndskraft, är resonemangen rent teoretiska. Det är emellertid fruktbart att arbeta med idealtyper när nya riktlinjer och principdokument ska tas fram. Det visar hur en idé kan se ut om den förs till sin logiska slutpunkt, vilket är viktigt att visualisera i samband med strategiskt arbete. Hur en strategi används när den väl är fastlagd beror på hur den tolkas av de som ska omsätta den i verklighet. Om åtgärderna eller inriktningen inte har operationaliserats väl kan resultaten skilja sig markant från det som var tänkt.

Diskussionen summeras översiktligt i tabell 2 på nästa sida.

Tabell 2. Typer av hantering av hybrida hot

	Strategityp		
Delmoment	*BESKYDDANDE*	*BEMÖTANDE*	*STÖRANDE*
Centrala frågor	Vilka skyddsvärden är mest sårbara? Vilka förmågor måste behållas för att klara av uppgifter enl. lag?	Hur maximeras en organisations motståndskraft? Vilka förmågor ska utvecklas för att nå dit?	Vilka åtgärder stör fienden mest? Vilka förmågor behövs för att ta fram dem?
Upptäcka	Ej uppsökande; hitta tecken i existerande källor; rapportera incidenter uppåt	Uppsökande; skapa nya informationskällor; informationsutbyte horisontellt	Skapa nya källor; lägga ut beten och dimridåer; snabbt offentliggöra information
Höja medvetenhets-nivån	Ta fram information reaktivt till de som söker den; produkter finns tillgängliga men marknadsförs inte	Aktivt uppsökande i informationsförmedlingen; analys av målgrupper; pådriva samhällsdebatt	Tydligt påvisa hotbilden och snabbt offentliggöra känd antagonistisk verksamhet
Bygga motståndskraft	Kontinuitetshantering, fokus på skyddsvärden och samhällsviktig verksamhet	Demonstration av hållbarhet genom övningar (*show of force*); överkompensera systemens resurser	Fokus på hoten snarare än skyddsvärden; offensiv lagföring mot hotaktörer
Institutionaliserad samverkan	Bygga samarbeten mellan aktörer i existerande system	Skapa nya institutionella lösningar för samverka; ändra lagstiftning för att försvåra för fienden; nya ledningsmetoder med samverkansfunktion	Inrätta hybridcentrum på högsta politiska nivå med bred kompetens; samordna samtliga åtgärder; aktivera totalförsvaret i fredstid

6 Sammanfattning och diskussion

Hybrida hot utgör en särskild sorts utmaning för Polismyndigheten på grund av deras otydliga karaktär, oförutsägbarhet, mångfald i metoder för påverkan, med mera. Hybrida hot kan både liknas vid ett spöke och en bläckfisk med många från varandra oberoende armar. Hur ska ett samhälle skydda sig mot ett sådant hot?

Hanteringen av hybrida hot under fredstid är intimt kopplad till informationsunderlag. Givet rätt information kan de institutioner som beskrevs i kapitel 4 kopplas samman med varandra. Då kan en serie bilbränder klassificeras som anlagda, ett dataintrång som del av en större antagonistisk attack, och ett uppklippt staket vid ett skyddsobjekt i Stockholms södra skärgård som sabotage. I den stund då information presenteras som tyder på att en antagonistisk statlig aktör ligger bakom en händelse förändras således mycket. Krisberedskapen hanterar inte bara en olycka eller en serie händelser, utan ett antagonistiskt hot. Värderingen av vilken information som är skyddsvärd ställs i ny dager. Underrättelseinformation utgör således de ”glasögon” med vilka vi analyserar verkligheten.

Polismyndigheten har idag ingen övergripande strategi gällande hybrida hot, men ett utvecklingsarbete pågår som berör detta. Rapporten presenterar verktyg som Polismyndigheten kan använda i detta arbete. Nedan sammanfattas rapportens huvudsakliga utsaga och ett antal frågor som Polismyndigheten och andra organisationer kan behöva komma att ta ställning till i utvecklingsarbetet tas upp för diskussion.

6.1 Vad är hybrida hot, och hur kan de bemötas?

Inledningsvis konstaterar rapporten att Polismyndigheten idag arbetar på *case-by-case*-basis gällande hybrida hot, och att det kan leda till att fall av statlig antagonistisk verksamhet i Sverige aldrig upptäcks. Detta är rapportens utgångspunkt. Rapportens andra och tredje kapitel behandlar hur begreppet hybrida hot har använts i forskarvärlden. Olika sätt att använda begreppet diskuteras. Vi argumenterar för att det är viktigt med stringens i begreppsanvändningen eftersom hybrida hot inte primärt är ett analytiskt begrepp, utan ett politiskt. Vi operationaliserar begreppet till *subversiv antagonistisk verksamhet utgående från en statlig eller statligt*

sanktionerad aktör. Denna verksamhet sker inte i isolation, utan i flera domäner eller på flera sätt samtidigt.

Litteraturen om hybrida hot innehåller en rad rekommendationer i fråga om på vilka områden som motåtgärder bör inriktas. Det handlar för det första om att upptäcka antagonistisk verksamhet tidigt. För detta anses det krävas effektiva informationskanaler inom varje organisation, och samlade lägesbilder på olika områden. För att detta ska ske behövs, för det andra, en hög grad av medvetenhet, både om de egna sårbarheterna, men även om hotbilden. För det tredje rekommenderar forskare att såväl civila som militära aktörer måste kunna hantera påfrestningar, till exempel i form av en cyberattack eller omfattande personalbortfall, utan att detta reducerar förmågan[69] att uppfylla de uppgifter som åläggs dem, bland annat genom lag. Till sist accentueras institutionella lösningar som överbryggar avståndet mellan samhällets olika aktörer, som kan koordinera ett samlat svar på antagonistisk verksamhet. Dessa fyra delmoment – upptäckande, medvetandegörande, motståndskraft och institutionella arrangemang – beskrivs således som centrala beståndsdelar i hanteringen av hybrida hot. I rapporten tar vi fasta på dessa punkter och använder dem som utgångspunkt i diskussionen av de tre strategier som utgör rapportens primära resultat.

Rent institutionellt har Sverige, som visades i kapitel 4, viss beredskap för att hantera den typ av statlig antagonistisk verksamhet som hybrida hot innebär. Samtliga myndigheter har idag krav ställda på sig att verka för ett effektivt säkerhetsskydd, och i förekommande fall att planera för kris och krig. Problemet är att myndigheter endast i viss utsträckning kan planera för hantering av hybrida hot, eftersom det inte är klart vilken typ av påverkan de ska planera för. I många fall kan existerande institutioner säkerligen vara tillräckliga för att neutralisera de hot som riktas mot landet. I andra fall inte. Hur myndigheter i allmänhet, och Polismyndigheten i synnerhet, ska resonera för att uppnå de delmoment som nämndes i stycket ovan, är fortfarande en öppen fråga. Strategierna som diskuteras i den här rapporten kan tjäna som verktyg för att öppna upp en diskussion om olika sätt att hantera hybrida hot.

I kapitel 3 och 5 utformas tre principiella inriktningar för hantering av hybrida hot. De motsvarar olika strategier, nämligen den *beskyddande, bemötande* och den *störande.*[70]

- I den *beskyddande strategin* försöker Polismyndigheten behålla förmågor och skydda samhällsviktig verksamhet när påfrestningar uppstår.

[69] Med ”förmåga” menas kapaciteten att uträtta något.
[70] En fjärde strategi – den *konfrontativa* – nämns också, men diskuteras inte vidare på grund av rättsliga och politiska aspekter, vilka skulle göra det omöjligt för en myndighet att följa den.

- Den *bemötande strategin* manövrerar Polismyndigheten självständigt och proaktivt i relation till hotbilden för att på så sätt undvika att påverkas av hybrida hot.
- I den *störande strategin* påverkar Polismyndigheten motståndaren innan denne hinner utföra subversiv verksamhet, till exempel genom att avleda fienden med lockbeten eller vilseleda den med avledningsmanövrar.

Dessa tre strategier är tänkta att tjäna som verktyg för att hjälpa den strategiska planeringen att tänka på nya sätt i arbetet mot hybrida hot. Redan etablerade lösningar är säkerligen tillräckliga för viss hantering av hybrida hot, men kan behöva infogas i ett bredare strategiskt tänkande. De vägval som sedan träffas kan innehålla aspekter av samtliga tre strategier, eller ytterligare varianter som inte diskuterats i denna rapport.

6.2 Frågor för diskussion

Hantering av ett så diffust problem som hybrida hot är förknippad med svåra etiska, politiska och ekonomiska avvägningar. Det är inte säkert att ett visst strategival i efterhand visar sig vara det optimala. Okonventionella strategival kan göra aktörer utanför Sverige förbryllade och utrymmet för feltolkningar är potentiellt stort. Stora ekonomiska och politiska värden, bland annat i termer av prioriteringar av resurser, står på spel. För den enskilda myndigheten handlar det om resurser som idag används till andra ändamål i en redan pressad organisation. För Sverige som land handlar det om att svara på antagonistiska hot på ett överlagt och tydligt sätt. Det är till exempel möjligt att en störande strategi skulle kunna vara politiskt känslig både i Sverige och för svenska internationella relationer. Såväl den beskyddande som den bemötande strategin har dessutom både för- och nackdelar som bör övervägas noga innan ett vägval görs.

Eftersom arbetet med en strategi för hantering av hybrida hot med nödvändighet kommer att ske med ett mått av osäkerhet kring det faktiska utfallet är det viktigt att inkludera en viss ödmjukhet i utvecklingsarbetet. Rent konkret kan det innebära att strategin behöver utvärderas särskilt noga och att en mekanism för detta måste planeras in redan från början. Det är också viktigt att eventuell ny kunskap kontinuerligt kan påverka strategins utformning. Till exempel skulle framtida forskning kunna utöka idealtyperna med nya alternativ, som då bör vägas in i utvecklingsarbetet. Det är därför en god idé att inkludera ett utvärderingsperspektiv i ett tidigt skede av arbetet för hantering av hybrida hot.

Med utgångspunkt i de tre strategier som presenterats ovan ställer sig ett antal frågor. Olika strategier ger olika svar på dessa. Listan som följer är

inte uttömmande, och kan säkerligen göras lång. Här följer endast några exempel:

- Ska myndigheter i allmänhet, eller bara de rättsvårdande myndigheterna, omprioritera sina resurser för att bättre kunna motstå påverkan från främmande makt?
- Behövs en särskild organisation med samordningsansvar och/eller planering för hantering av hybrida hot?
- Behöver Polismyndigheten tilldelas ett särskilt uppdrag av regeringen på detta område?
- Behövs ny lagstiftning på något område för att Polismyndigheten ska kunna hantera hybrida hot? Vilka av strategierna som diskuterats ovan kräver det, och vilka kräver det inte?
- Hur stor vikt ska detta problem tillskrivas i relation till andra uppgifter?
- I vilken mån bör Polismyndigheten betrakta organisationen i sig som hotad?
- Vad är en tillräcklig nivå av medvetenhet om hybrida hot? Hur ska medvetandegörande åtgärder utvärderas?
- Blir en mer motståndskraftig polisorganisation också en *bättre* sådan, eller kommer myndigheten att tappa förmåga på vissa områden beroende på vilken strategi som väljs?

Vi kommer inte att kunna besvara dessa frågor här, men anser att det är viktiga aspekter att väga in i utvecklingsarbetet för hantering av hybrida hot.

ISSN 1650-1942

www.foi.se