



Självständigt arbete, Påbyggnadskurs Krigsvetenskap (15 HP)

Författare: Victor Bredberg Holm	Årskull: 22-25
Lärosäte: FHS	
Handledare: Peter Thunholm	
Antal ord: 11745	
Hybridhoten mot Sverige	
<u>Abstract</u>	
<p>Hybrid warfare is an ever-growing threat to Sweden's national security. Hybrid warfare is the act of operating in the so-called grey zone between peace and open conflict. In Sweden, recent incidents have been reported that could be categorized as possible hybrid attacks. The problem with hybrid warfare is founded in the difficulty of detecting, attributing, and responding to hybrid attacks, as they often involve deniability, and non-military means that complicate traditional defense strategies.</p>	
<p>The purpose of this study is to investigate how hybrid warfare is conducted against Sweden today, using a theory-consuming approach and creating a theoretical framework based of Hoffman's concept of hybrid warfare, Weissman's Hybridity Blizzard Model, and Suchkov's New Generation Warfare. Through a qualitative analysis of empirical cases of suspected hybrid attacks, the study seeks to understand the methods used, their effects on Swedish society, and the challenge that hybrid warfare poses to Swedish national security.</p>	
<p>The results of this study show that hybrid threats against Sweden are multifaceted, combining methods like sabotage, cyber influence, and psychological operations. These actions possible aim is to destabilize Swedish society, reduce trust in democratic institutions, and weaken the country's resilience. The study concludes that hybrid warfare represents a persistent and evolving challenge that demands an enhanced capability to identify, classify, and manage hybrid threats within Swedish defense and security policy.</p>	
<u>Nyckelord:</u> Hybridkrigföring, Sverige, Säkerhetshot, Teorikonsumerande, Hoffman, Suchkov, Weissman	

1 Innehållsförteckning

1	INNEHÅLLSFÖRTECKNING	2
2	INLEDNING/PROBLEMFÖRMLERING	4
3	FORSKNINGSÖVERSIKT	5
3.1	FORSKNING OM RYSK HYBRIDKRIGFÖRING OCH DESS UTVECKLING	5
3.2	FORSKNING KRING FÖRNEKBARHET OCH SYNSÅTT	7
3.3	SAMMANFATTNING FORSKNINGSÖVERSIKT.....	8
4	SYFTE OCH FRÅGESTÄLLNING	9
5	AVGRÄNSNINGAR	9
6	TEORI	10
6.1	FRANK HOFFMAN	10
6.1.1	<i>Fourth Generation Warfare</i>	10
6.1.2	<i>Compound Wars</i>	11
6.1.3	<i>Unrestricted Warfare</i>	11
6.1.4	<i>Sammanfattning och centrala begrepp</i>	12
6.2	WEISSMAN, MIKAEL	14
6.3	MAXIM A. SUCHKOV	16
6.4	SAMMANFATTNING OCH SYFTET MED TEORIN I DENNA STUDIE	17
7	METOD	18
7.1	FORSKNINGSDESIGN	18
7.2	OPERATIONALISERING	19
8	MATERIAL	20
9	KÄLLKRITIK	21
9.1	SÄKERHETSPOLISEN.....	21
9.2	MUST/FÖRSVARSMAKTEN	21
9.3	FOI/MPF/MSB.....	21
9.4	SVT	21
9.5	FRIVÄRLD	21
10	FORSKNINGSETIK	22
11	ANALYS	23
11.1	TYPFALL 1: OMBUD/SPECIALFÖRBAND.....	23
11.1.1	<i>Analysfrågor typfall 1</i>	24
11.2	TYPFALL 2: INFORMATIONSKRIGFÖRING/PÅVERKANSKAMPANJER	26
11.2.1	<i>Analysfrågor typfall 2</i>	27
11.3	TYPFALL 3: STÖRNING AV INFRASTRUKTUR.....	28
11.3.1	<i>Analysfrågor typfall 3</i>	29
11.4	TYPFALL 4: INFILTRERING/CYBERATTACKER	31
11.4.1	<i>Spioneri/infiltrering</i>	31
11.4.2	<i>Cyberattacker</i>	31
11.4.3	<i>Analysfrågor typfall 4</i>	32
11.5	SAMMANFATTNING ANALYS	33
12	SLUTSATSER	34
13	DISKUSSION	35
13.1	RESULTATETS BETYDELSE FÖR OFFICERSYRKET	36
14	VIDARE FORSKNING	37
15	KÄLLFÖRTECKNING	38

2 Inledning/Problemformulering

Hybridkrigföring handlar i korthet om att försvaga eller skada ett samhälle genom förnekbart agerande som inte går att reagera på mot någon identifierbar motståndare. I Sverige har dessa former av attacker blivit alltmer framträdande och aktuella med händelser som exempelvis kabelbrott¹ och GPS-störningar.²

Denna studie är ett fall av hur modern hybridkrigföring utförs, och kan således ur ett större perspektiv ses som en del i att förstå den gråzonsproblematik som finns inom det moderna slagfältet, där fientliga aktörer påverkar andra aktörer utan att inleda en formell konflikt.

Eftersom ett av de syften som finns med hybridkrigföring är förnekbarhet kommer denna uppsats undersöka huruvida misstänkta attacker inom ramen för hybridkrigföring bedrivs mot Sverige i nutid genom att analysera konkreta fall av säkerhetshotande verksamhet som misstänks vara hybridkrigföring.

Genom att skapa ett teoretiskt ramverk som definierar hybridkrigföring, dess påverkan och metoder och kvalitativt analysera fall av misstänkta hybridattacker mot Sverige kan uppsatsen skapa en större förståelse för effekten av hybridkrigföring. Genom detta bidrar även uppsatsen till en förståelse för hur dessa misstänkta attacker samt andra fall av säkerhetshotande verksamhet manifesteras i svensk kontext, för att i förlängningen bidra med hur detta påverkar Sveriges säkerhetspolitiska trygghet.

Hybridkrigföring är ett väletablerat begrepp inom krigsvetenskap, men det saknas studier som applicerar teoretiska ramverk för hybridkrigföring och analyserar svenska misstänkta fall. Detta skapar en forskningslucka kring hur hybridkrigföring bedrivs i svensk kontext och hur det påverkar vår säkerhetspolitik.

Denna studie är således ett fall av att problematisera hur hybridkrigföring utförs och mer precist mot Sverige i modern tid. Detta för att ge en tydligare bild av det säkerhetsläge vi befinner oss i och vad det faktiskt innebär mer konkret för Sverige som suverän stat.

¹ J. Granlund, O. Jönsson. 60 Hybridattacker mot Europa - spåren pekar mot Ryssland. *SVT*. (12/3 2025) <https://www.svt.se/nyheter/inrikes/60-hybridattacker-mot-europa-sporen-pekare-mot-ryssland> (Hämtad 13 mar. - 25)

² S. Ritzén. Sverige drabbat av stor GPS-störning. *SVT*. (3/1 2024) <https://www.svt.se/nyheter/inrikes/sverige-drabbat-i-storsta-gps-sabotaget-i-ostersjon> (Hämtad 13 mar. -25)

3 Forskningsöversikt

Forskningsöversikten ämnar behandla rysk hybridkrigföring och hur utvecklingen kring hybridkrigföring sett ut. Vidare ämnar forskningsöversikten se till begreppet förnekbarhet, samt hur hybridkrigföring påverkat det svenska synsättet på konflikter.

3.1 Forskning om rysk hybridkrigföring och dess utveckling

Mattson beskriver hur rysk krigföring diskuteras inom rysk nutida militärteori genom att analysera och studera ryska källor och västerländska tolkning av moderna ryska krigsföringsdiskussioner mellan 1980 och 2014.³ Mattson diskuterar bland annat Ryssland och Generalmajor Alexander Vladimirovs syn på det moderna kriget, där det gått från en tydlig distinktion mellan fred och krig till ett mer permanent tillstånd av krig som en naturlig del av en stats förefintlighet. Detta innebär att det inte längre bara är rena militära enheter som strider med varandra, utan hela stater och befolkningar.⁴

Vidare diskuterar Mattson hur Vladimirov och Ryssland resonerar kring tre tydliga delar i den permanenta krigföringen. De menar att det skiftat från krig om territorium till krig om existens, där man inte längre vill förintä eller förstöra utan i stället vill utmatta den fiendliga statens politiska, ekonomiska och kulturella inflytande över sitt eget land. Således handlar det inte längre om rent militära angrepp, utan att strategiskt uppnå organiserat kaos genom metoder så som politik, ekonomi eller kultur. Därmed är syftet att påverka motståndaren och skapa en intern kollaps, genom propaganda, specialoperationer och irreguljära styrkor.⁵

Slutligen menar Mattson att Vladimirov och Ryssland ser en total krigföring med varierande intensitet och fokus. Krig genomförs enligt Vladimirov och Ryssland inom en motståndares territoriella gränser, med omtumlande och avledande operationer till dess att det är strategiskt och operationellt fördelaktigt att genomföra en attack.⁶

Denna artikel bidrar med att förstå hur ryska militärteoretiker beskriver modern krigföring, genom att kombinera konventionella och okonventionella metoder, som exempelvis informationskrigföring, specialförbandsoperationer och psykologiska operationer.

Oscar Jonsson⁷ beskriver det ryska perspektivet på gråzon och hur Ryssland förstår sig på den nutida krigföringen. Jonsson exemplifierar detta genom att titta på hur Ryssland i Ukraina och andra länder använt sig av metoder som i väst beskrivs som hybridkrigföring.

När Ryssland invaderade och erövrade Krimhalvön gjorde de detta utan något större motstånd samtidigt som de skapade uppror i östra delen av Ukraina. Jonsson menar att detta påvisar en hög grad av koordination mellan Rysslands militära och icke-militära medel och metoder. Jonsson lyfter särskilt fram Rysslands agerande inom informationsarenan där ryska soldater tog kontrollen över både TV och Radio inom deras operationsområde samt genomförde koordinerade kampanjer via sociala medier.⁸

³ P. A. Mattson. Russian military thinking – A new generation of warfare. *Journal on Baltic Security*. Vol 1. Issue 1. (2015). S. 61.

⁴ Ibid, 66.

⁵ Ibid

⁶ Ibid, 67.

⁷ O. Jonsson. *The russian understanding of war – Blurring the lines between war and peace*. (Georgetown University Press, 2019).

⁸ Ibid, 44.

Vidare beskriver Jonsson hur Ryssland påverkade det amerikanska valet 2016 genom att genomföra en påverkansoperation. Där användes en kombination av desinformationspåverkansmetoder i sociala samt traditionella medier. Vidare gjordes även intrång i databaser som används för valet samt hackerattacker som genomfördes för att läcka e-post från demokraterna.⁹

Ett annat exempel som Jonsson lyfter är hur Ryssland nyttjade hybridkrigföring när de lyckades kontrollera informationsarenan under invasionen av Georgien 2008. Jonsson menar att Ryssland redan innan invasionen samlade journalister från statlig media i Sydossetien för att kunna rapportera enligt det synsätt som ryska staten ville förmedla. Vidare beskriver Jonsson hur Ryssland gjorde så att Georgien inte kunde kommunicera med sina invånare genom att genomföra hybridattacker mot deras infrastruktur. Dessutom kapade ryska styrkor georgiska undervattenskablar för internet och telefoni.¹⁰

Jonsson menar att denna typ av informationskrigföring blivit en central del i hybridkrigföringen samt den offensiva strategin för Ryssland mot väst och NATO. Detta har genomförts genom bland annat ryskt statskontrollerade TV-kanaler i länder som Storbritannien och USA men också med trollfabriker som haft syftet att exempelvis underminera och förtrycka protester mot Ryssland, både nationellt och internationellt.¹¹

Jonssons bok ger oss en förståelse för hur viktigt det är med icke-militära medel och informationskrigföring för Ryssland. Således är det rimligt att anta att detta även nu genomförs mot Sverige inom ramen för hybridkrigföring.

Dansarie har studerat den tekniska utvecklingen i relation till moderna konflikter genom att titta på teknikens påverkan på utformningen av framtidens slagfält.¹² Detta ger en teknisk bakgrund till problematiken och förklarar varför hybridkrigföring ökat i takt med den teknologiska utvecklingen. Vidare diskuterar Dansarie riskerna med samhällets digitalisering, och hur det finns risker med att förlita sig allt för mycket på modern teknik. Författaren diskuterar cyberkrigföring och exemplifierar detta genom cyberoperationen som spred programmet NotPetya. Programmet spred sig inom ett ukrainskt bokföringsprogram och raderade samtlig information på datorerna programmet påverkade. Dansarie menar att syftet med programmet var att slå mot ukrainskt näringsliv. Programmet beräknas ha kostat Ukraina över 10 miljarder dollar i skador. Ett flertal länder har anklagat Ryssland för att ligga bakom cyberoperationen.¹³

Artikeln bidrar till att förstå hur teknikutvecklingen har gett antagonister fler verktyg att arbeta med och ger oss en förståelse för cyberhoten som en del av hybridkrigföringen. Artikeln belyser och exemplifierar även problematiken med förnekbarhetsprincipen inom hybridkrigföring med programmet NotPetya och Rysslands inblandning.

⁹ O. Jonsson. *The russian understanding of war – Blurring the lines between war and peace*. (Georgetown University Press, 2019). S. 44.

¹⁰ Ibid, 116.

¹¹ Ibid, 156.

¹² M. Dansarie. Teknisk utveckling och Hybridkrigföring. *Kungliga krigsvetenskapsakademin*. Bilaga 3, (2020). S. 162.

¹³ Ibid, 163–164.

3.2 Forskning kring förnekbarhet och synsätt

Vidare tittar Gunneriussons artikel *Hybrid warfare and deniability as understood by the military* på hur kärnbegreppet inom hybridkrigföring **förnekbarhet** spelar in i hybridkrigföring och hur synsättet på det divergerar mellan officerare och politiska individer inom Natostrukturen. Gunneriussons artikel fokuserar på hybridkrigföring med fokus på förnekbarhet det vill säga att dölja eller förneka inblandning. Han menar att det är en viktig del i Rysslands nutida krigföring.¹⁴ Han argumenterar för att ryska och kinesiska hybridstrategier systematiskt underminerar västerländska länder genom svårdefinierade metoder, vilket gör det svårt att bemöta dessa politiskt eller militärt.¹⁵

Studien bygger på en undersökning med NATO-officerare och visar att det finns en skillnad mellan hur militära och politiska personer uppfattar (eller väljer att se på) hybridkrigföring.¹⁶ Resultatet av artikeln belyser en splittring inom västvärlden mellan den militära och den politiska sfären när det gäller tolkningen av det ryska och kinesiska agerandet. Detta grundar sig i att politiker undviker konfrontation av rädsla för att destabilisera det globala ekonomiska systemet medan officerarna inte kan bortse från verkligheten och kräver objektivitet i Ryssland och Kinas agerande.¹⁷

Detta är relevant för forskningen som denna uppsats genomför då det bidrar till att förstå hur olika aktörer tolkar hybridhotet mot Sverige, både nationellt och i vår allians NATO och vilka utmaningar det skapar för försvaret och samhället i stort.

För att tydligare förstå hur Sveriges säkerhetsstrategi ändrats på grund av hybridkrigföring kan vi se till Ljungkvists artikel *The Military-Strategic Rationality of Hybrid Warfare: Everyday Total Defence under Strategic Non-Peace in the Case of Sweden*. Ljungkvists artikel undersöker på vilket sätt hybridkrigföring påverkar Sveriges totalförsvar och hur Sveriges strategiska synsätt har förändrats i ett gråzonsläge.¹⁸ Studien visar att Sveriges försvarspolitiska doktrin successivt har gått från det att det bara handlar om kris eller krig inom ramen för en väpnad konflikt till ett decentraliserat totalförsvar som används dagligen. En viktig aspekt är att det civila samhället i allt högre grad förväntas delta i att identifiera och motverka hybridkrigföring.¹⁹

Artikeln gör en analys av hur hybridkrigföringen har format strategiska val och därmed kan den bidra till en miljö eller kontext för min analys av hybridkrigföringens påverkan och tillvägagångssätt gentemot Sverige.

¹⁴ H. Gunneriusson. Hybrid warfare and deniability as understood by the military. *Polish Political Science Yearbook*. 48: 2 (2019). S. 268.

¹⁵ Ibid, 283-284.

¹⁶ Ibid, 268.

¹⁷ Ibid, 283.

¹⁸ K. Ljungkvist. The Military-Strategic Rationality of Hybrid Warfare: Everyday Total Defence under Strategic Non-Peace in the Case of Sweden. *European Journal of International Security*. 9 (2024). S. 533.

¹⁹ Ibid, 551.

3.3 Sammanfattning forskningsöversikt

För att summera den tidigare forskningen bidrar samtlig litteratur till förståelsen för hybridkrigföring och dess uppträdande samt metoder från ett ryskt perspektiv. Den tidigare forskningen diskuterar även begreppet förnekbarhet samt påverkan som hybridkrigföring har haft på den svenska säkerhetsstrategin men saknar en systematisk, kvalitativ analys av empiriska fall av hybridangrepp mot Sverige med direkt koppling till effekt, vilket är det författaren vill undersöka i denna studie.

4 Syfte och frågeställning

Denna uppsats syftar till att ur ett större perspektiv bidra till forskningen om hur hybridkrigföring bedrivs. Mer specifikt kommer uppsatsen genom en teorikonsumerande studie förklara hybridkrigföring och hur denna form av krigföring misstänks bedrivs mot Sverige i nutid. Genom Hoffmans teori om hybridkrigföring, Weissmans Hybridity Blizzard Model och Suchkovs NGW kan studien etablera ett teoretiskt ramverk för att sedan applicera detta ramverk på fall av misstänkt säkerhetshotande verksamhet i Sverige och Sveriges territoriella närhet som skett inom närtid. Genom dessa analyser syftar studien till en djupare förståelse och hur hybridkrigföring manifesteras i svensk kontext.

Uppsatsen kommer dessutom att belysa vad hybridkrigföringens effekt är på det svenska samhället och individer inom detta samhälle. Forskningsfrågan har bearbetats till *”Vilka metoder av hybridkrigföring kan identifieras mot Sverige i nutid och hur kan dess effekt förklaras genom ett teoretiskt ramverk av moderna hybridkrigföringsteorier?”*

5 Avgränsningar

Frågeställningen och uppsatsen avgränsas till efter 2014 och händelser inom Sveriges ekonomiska zon. Detta inkluderar även luftrummet samt på och under havsytan. Anledningen till att uppsatsen begränsas till efter 2014 är för att det är då Ryssland påbörjade sin invasion av Ukraina vilket skapade en förändring i det världspolitiska säkerhetsläget och således gjort att hybridkrigföringen troligen ökat och att den fått mer medial uppmärksamhet.

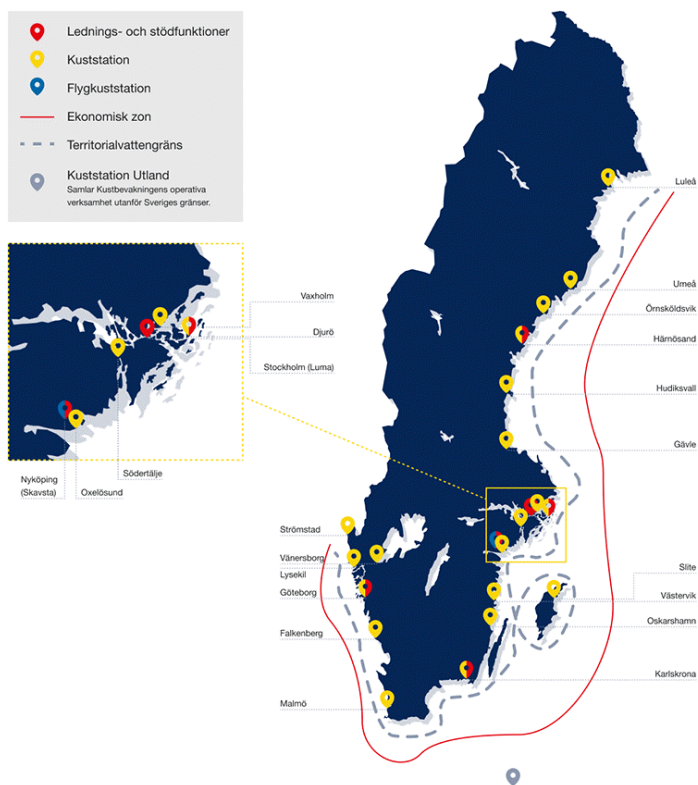


Bild 1 Den ekonomiska zonen symboliseras av den röda linjen på denna karta.²⁰

²⁰ Kustbevakningen. *Sveriges territorialhav och ekonomiska zon*. (u.å.). <https://www.kustbevakningen.se/bilder-och-fakta/sveriges-territorialhav-och-ekonomiska-zon/> (Hämtad 13 mar. -25)

6 Teori

För att skapa ett teoretiskt ramverk kommer uppsatsen använda Frank Hoffmans teori om hybridkrigföring²¹ för att ge grund för förståelse kring vad hybridkrigföring är, vad det innebär samt vilka delar det innehåller. Tillsammans med Hybridity Blizzard model från Weissman²², där Weissman klassificerar hybridangrepp och beskriver hur dessa är sammanflätande och metoder utifrån rysk NGW (NEW GENERATION WARFARE) genom Suchkovs artikel²³ vill denna uppsats skapa ett teoretiskt ramverk för att kunna analysera den misstänkta hybridhotsverksamheten som sker mot Sverige.

Studien kommer dels att använda Hoffmans teori om hybridkrigföring med anledning av att den teorin är den första och mest etablerade inom västvärlden för att beskriva hybridkrigföring som fenomen. Sedan kommer författaren komplettera Hoffmans teori med Weissmans Hybridity Blizzard Model för att fånga en mer modern aspekt med mer fokus på klassificering av själva utförandet av hybridkrigföring och med fokus på simultana attacker. Slutligen kommer författaren komplettera båda dessa teorier med de metoder som Suchkov beskriver som nyckelparametrar i NGW. Detta kommer att skapa det teoretiska ramverk som möjliggör analysering av empirin, det vill säga fall av misstänkt hybridkrigföring mot Sverige.

6.1 Frank Hoffman

Den första teorin som uppsatsen kommer att nyttja för att skapa en grundläggande förståelse för hybridkrigföring är Frank Hoffmans teori om Hybridkrigföring. Den syftar främst i denna studie till att vara begreppsförklarande. Teorin är deskriptiv och ger en konceptualisering av hur moderna slag utkämpas. Teorin är i grunden baserad på tre andra koncept om krigföring, ”4GW” (Fourth generation warfare), ”Compound wars” och ”Unrestricted warfare.”²⁴ Hoffman menar att alla dessa teorier bidrar till förståelsen av hybridhot och hybridkrigföring, men är bristfälliga på olika vis vilket gör dem otillräckliga för en fullständig förståelse, då de inte belyser alla aspekter av modern hybridkrigföring, vilket hans teori ämnar göra.²⁵

6.1.1 Fourth Generation Warfare

Hoffman förklarar att fjärde generationens krigföring (4GW) grundar sig i det paradigmskifte som skedde 1648 i och med att nationer fick en tydligare struktur i världsordningen. 4GW förutspådde genom detta på ett korrekt sätt framtidens krigföring. Detta enligt Hoffman innebär att 4GW belyser den utsuddade gränsen mellan fred och krig samt kombattanter och icke-kombattanter. Hoffman menar att grunden för detta krigföringskoncept är att försvaga en suverän stat på ett organisatoriskt sätt för att ickestatliga aktörer ska kunna utmana legitimiteten av staten. 4GW använder en rad konventionella och icke konventionella metoder

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

²² M. Weissman. m.fl. *Hybrid Warfare – Security And Symmetric Conflict in International Relations*. (I.B TAURIS Bloomsbury Publishing, 2021).

²³ M. A. Suchkov. *Whose hybrid warfare? How ‘the hybrid warfare’ concept shapes Russian discourse, military, and political practice, Small wars & Insurgencies*, (Routledge, 2021).

²⁴ F. Hoffman. *Conflict in the 21st Century: The Rise of Hybrid Wars*. (Potomac Institute for Policy Studies, 2007). S. 17-18.

²⁵ Ibid, 40.

så som terrorism och information för att underminera viljan av den suveräna staten, för att således skapa en intern social kollaps.²⁶

4GW har dock fått kritik för att bland annat vara baserad på dålig historisk dokumentation och att den saknar logisk följdriktighet. Detta är något som Hoffman noterat och sammanfattar 4GW som att den döljer mer än vad den visar för någon som försöker förstå sig på krigföringsidén. Han menar dock att den fortfarande är relevant för att kunna bidra till förståelsen om den moderna krigföringen.²⁷

6.1.2 Compound Wars

Vidare diskuterar Hoffman konceptet som benämns som Compound Wars, detta kommer att förkortas som CW vidare i denna uppsats.

Hoffman beskriver CW som ett koncept där det sker signifikant koordination och samspel mellan reguljära och irreguljära styrkor i en konflikt. Det sker en form av kraftmultiplicering när förmågan av olika former av styrkor nyttjas. Han menar att detta utnyttjas genom att de irreguljära styrkorna slår mot motståndarens svaga områden, vilket tvingar motståndaren att fördela sina styrkor. Detta leder till att den reguljära styrkan möjliggörs till att genomföra avgörande offensiva operationer. Hoffman exemplifierar denna strategiska synergieffekt med Vietnamkriget, där de Viet Cong som nyttjade irreguljära taktiker stred sida vid sida med den traditionellt kapabla Nordvietnamesiska armén. Denna tvetydiga blandning av konventionella och icke-konventionella metoder var någonting som förvirrade och förargade amerikanska försvarsplanerare länge.²⁸

Hoffman menar att denna teori erbjuder en förståelse för synergier mellan reguljära och irreguljära styrkor samt kombinationen av dessa på strategisk nivå, men saknar komplexiteten på en operativ och taktisk nivå. Eftersom teorin är baserad på två operationellt olika styrkor fångar inte modellen sammansmältningen av fred och krig som identifierats i modernare slag.²⁹

6.1.3 Unrestricted Warfare

Hoffman menar även att konceptet Unrestricted Warfare bidrar till teorin om hybridkrigföring. Unrestricted Warfare kommer vidare att benämnas som UW i denna uppsats.

Hoffman beskriver UW som en kinesisk krigföringsteori som handlar om krig utan gränser. Teorin identifierade tidigt implikationerna som den alltmer globaliserade världen medgav, således kunde även krig bli mer globaliserade och moderniserade med enheter och effekter utanför det traditionella militäriska synsättet. Konceptet bidrog med förståelsen av att kombinera organisationstyper och domän som nationen besitter. Detta inkluderar bland annat informationskrigföring, ekonomisk krigföring och handelskrigföring. Hoffman menar att idén om att krigföring sträckte sig förbi det enbart militära var något nytt när detta koncept blev till.³⁰

²⁶ F. Hoffman. *Conflict in the 21st Century: The Rise of Hybrid Wars*. (Potomac Institute for Policy Studies, 2007). S.17-18.

²⁷ Ibid, 20.

²⁸ Ibid, 20-21.

²⁹ Ibid, 21-22.

³⁰ Ibid, 22-24.

Vidare beskriver Hoffman hur det finns tre grundpelare eller centrala begrepp som UW bygger på. Den första är **Omni-directionality** vilket innebär att en befälhavare måste se till ett slagfält utan förutfattade meningar, och utformningen av planeringen och utförandet måste nyttja samtliga resurser som är frigjorda. Befälhavaren ska inte heller göra distinktioner för vad som är en del av slagfältet eller inte. Samtliga traditionella domäner (Luft, Sjö, Mark, Rymd) såväl som politik, ekonomi, kultur eller moral kan vara en del av slagfältet.³¹ Den andra är **Synchrony** vilket innebär att befälhavare möjliggör en strategisk seger tidigare, genom att agera i flertal av tidigare nämnda domäner samtidigt, i stället för att se det som enskilda slag där resultatet läggs samman.³² Den sista principen är **Asymmetry** vilket handlar om att uppträda asymmetriskt mot sin motståndare.³³

Efter att Hoffman beskrivit dessa tre koncept för bidragandet av förståelsen för hybridkrigföring belyser han även att han hämtat inspiration för sin teori i den amerikanska försvarsplaneringen från 2005. Där menar Hoffman att deras klassificering av olika typer av hot, det vill säga traditionella, irreguljära, katastrofala och störande kan bidra till förståelsen för moderna hot och hybridhot. Han menar dock att dessa inte bör särskiljas, utan att en kombination av dessa är vad som är hybridhot. Hoffman kritiserar dessutom denna försvarsplanering i att den kan förklara och bidra med förståelse på en strategisk nivå, men inte på en operationell nivå.³⁴

6.1.4 Sammanfattning och centrala begrepp

Hoffman har skapat en ny teori där han tagit delar av de tidigare nämnda koncepten och idéerna, då dessa saknat någon eller några aspekter av den moderna krigföringen. Med detta har han skapat en mer övergripande och allomfattande teori som ger en grundläggande förståelse för vad hybridkrigföring faktiskt är och vad det syftar till, samt hur denna typ av krigföring utvecklats med tiden.

De centrala och väsentliga begreppen för att förstå hybridkrigföring för denna studie är³⁵:

Hybridkrigföring vilket beskrivs som ett krigföringssätt där aktörer kombinerar konventionella, irreguljära, terroristliknande och kriminella metoder för att uppnå sina strategiska och politiska målsättningar. Hybridkrigföring kännetecknas av att man kombinerar flera olika former av krigföring.³⁶ Hybridkrigföring som begrepp kommer att hjälpa min studie eftersom det definierar vad det faktiskt innebär och därmed kan hjälpa mig undersöka det i relation till Sverige.

Konvergens bygger på att olika typer av krigföring och/eller aktörer (statliga och icke-statliga) arbetar tillsammans och således förstärker varandra.³⁷ Detta kan innebära att militära styrkor och irreguljära grupper samarbetar eller att konventionella metoder kombineras med okonventionella metoder så som cyberattacker och informationskrigföring.

³¹ F. Hoffman. *Conflict in the 21st Century: The Rise of Hybrid Wars*. (Potomac Institute for Policy Studies, 2007). S. 22-24.

³² Ibid

³³ Ibid

³⁴ Ibid, 25-27.

³⁵ Ibid

³⁶ Ibid, 14.

³⁷ Ibid, 28.

Konvergens kan hjälpa min studie att analysera hur olika typer av hot samverkar mot Sverige, genom att se exempelvis hur kriminella nätverk samarbetar med andra statliga aktörer eller hur desinformation påverkar synsättet på Sverige.

Multimodalitet vilket innebär att hybridkrigföring använder flera stridsmetoder samtidigt. Exempelvis kan en aktör genomföra konventionella militära operationer samtidigt som den bedriver desinformation och ekonomisk påverkan.³⁸ Genom att studera multimodaliteten kan det underlätta för att kategorisera och identifiera vilka typer av hybridhot som riktas mot Sverige.

Adaptivitet innebär att aktörer som nyttjar sig av hybridkrigföring anpassar sig och nyttjar fiendens svagheter för att maximera sin egen verkan.³⁹ Adaptivitet kan hjälpa oss att förstå hur en aktör anpassar sina metoder för att påverka det säkerhetspolitiska läget i Sverige.

Denna teori ger studien en grund för att analysera fall av hybridkrigföring mot Sverige samt dess påverkan på svensk säkerhetspolitik. En annan anledning till att författaren valt denna teori som en del i ramverket är för att teorin är den första och mest etablerade inom västvärlden för att beskriva hybridkrigföring som fenomen.

³⁸ F. Hoffman. *Conflict in the 21st Century: The Rise of Hybrid Wars*. (Potomac Institute for Policy Studies, 2007). S. 29.

³⁹ *Ibid*, 10.

6.2 Weissman, Mikael

Weissmans bok ger ett helhetsperspektiv på den forskning som finns om hybridkrigföring och diskuterar bland annat hybridkrigföring ur perspektiv från NATO, USA och EU. Vidare diskuterar boken verktyg och konceptualisering kring hybridhot och hybridkrigföring genom exempelvis informations- och cyberdomänen samt multilaterala underrättelsesamarbeten. Slutligen ger boken olika exempel och fall av hybridkrigföring samt bidrar med en modell om kombinerade hybridattacker.⁴⁰

Syftet med att inkludera denna bok i uppsatsen är för att nyttja modellen om hybridattacker för att förstå hur hybridhot har en sammankoppling och integration mellan attackerande stat, försvarande stat och långsiktiga samt kortsiktiga målsättningar och ageranden. Detta kommer att bidra med att klassificera misstänkta hybridhot.

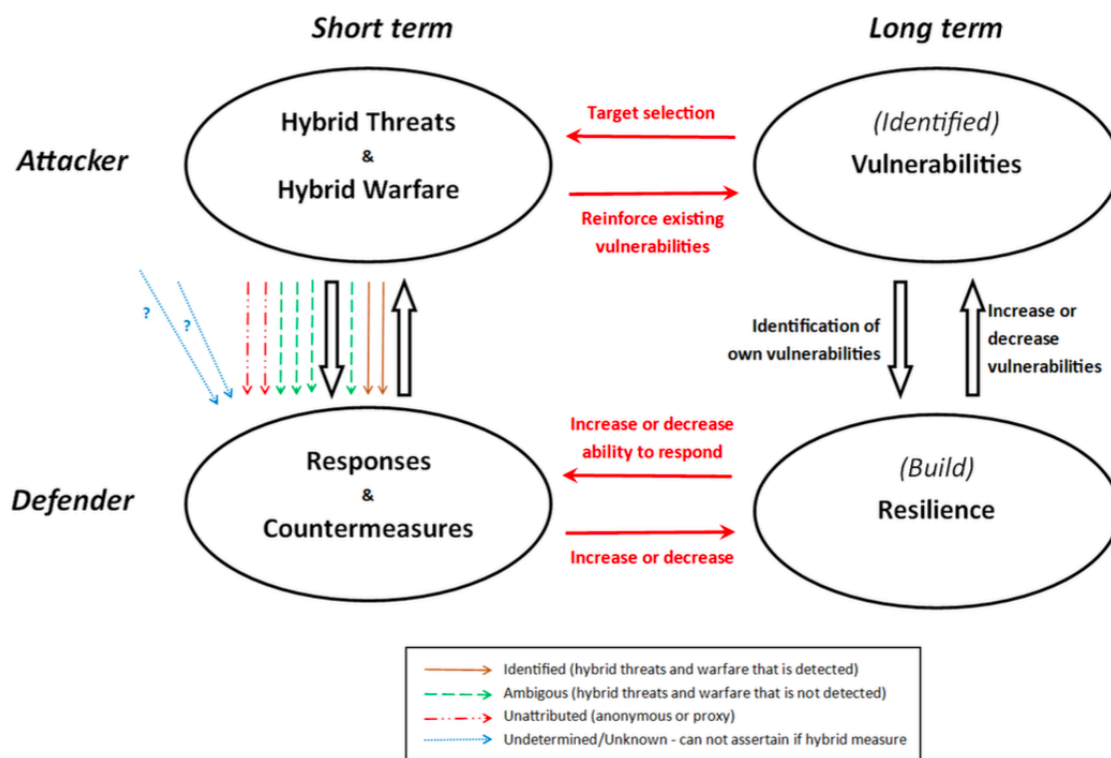


Bild 1 Illustration av Hybridity Blizzard Model⁴¹

Modellen **Hybridity Blizzard model** består av fyra grundpelare vilket är den offensiva och defensiva staten ur ett långsiktigt och kortsiktigt perspektiv. Vidare tittar modellen på hur dessa parter interagerar med varandra under tid och rum, likt ett ekosystem. Därefter ser modellen till relationen mellan de långsiktiga och kortsiktiga perspektiven och mellan både offensiva och defensiva sidan. Slutligen visar modellen pilar för olika klassificeringar av hybridhot.⁴²

⁴⁰ M. Weissman. m.fl. *Hybrid Warfare – Security And Symmetric Conflict in International Relations*. (I.B TAURIS Bloomsbury Publishing, 2021).

⁴¹ Ibid, 268.

⁴² Ibid, 266-272.

Modellen liknar hybridkrigföring med en snöstorm. Detta eftersom de som är utsatta för hybridhot och hybridkrigföring förblindat blir attackerade från alla möjliga vinklar hela tiden med flera mindre attacker. Dessa kan i sin tur inte urskiljas från varandra och gör det omöjligt att lokalisera den attackerande parten vilket gör det svårt att besvara attackerna.⁴³

Enligt författarna är det som gör hybridkrigföring så komplext och svårt det faktum att hoten är tvetydliga och anonymiserade från en aktör. Dessutom finns risken att man som mottagande part hittar falska attacker som rent av kan vara en slump i stället för ett faktiskt hybridangrepp. Hybridkrigföring handlar i stort om vilseledning och förnekbarhet, där källan till angrepp ofta är dold eller anonymiserad.⁴⁴

Denna uppsats kommer endast att fokusera på det kortsiktiga perspektivet (Short term) från en motståndare (attacker) mot Sverige (defender), men det som gör att modellen bidrar till arbetet är klassificeringen av hybridhot.

Modellen klassificerar hybridangrepp efter fyra kategorier. Identified – Identifierat, Ambiguous – Svårförståligt, Unattributed – Otillskrivet, Undetermined – Obestämt.⁴⁵

Identifierat innebär att man identifierat med säkerhet att det är ett hybridangrepp samt vem som ligger bakom attacken.⁴⁶

Svårförståligt innebär att man inte identifierat överhuvudtaget att det sker ett hybridangrepp eller någon annan form av hybridkrigföring.⁴⁷

Otillskrivet innebär att man förstår att det sker ett hybridangrepp men att hybridattacken i sig är anonym eller dold med hjälp av olika ombud, vilket gör det svårt att avgöra vem eller vad som ligger bakom angreppet.⁴⁸

Obestämt innebär att händelser eller observerade aktioner mot en stat kan vara tvetydliga eller obestämda. Det kan vara svårt att avgöra om det som den försvarande staten upplever är en form av hybridangrepp eller om det är något annat form av hot. Detta exemplifieras i boken med bland annat banksystem och el-infrastruktur. Problem som påverkar banksystem eller tillfälliga avbrott i el-infrastrukturen kan vara en manifestation av hybridkrigföring likväl som det bara kan vara en tillfällig bugg i systemet.⁴⁹

Eftersom denna uppsats kommer att titta på misstänkta hybridangrepp mot Sverige är både det författarna kallar ”Unattributed” samt ”Undetermined” särskilt viktiga förstå.

⁴³ M. Weissman, m.fl. *Hybrid Warfare – Security And Symmetric Conflict in International Relations*. (I.B TAURIS Bloomsbury Publishing, 2021). S. 268.

⁴⁴ Ibid, 269.

⁴⁵ Ibid

⁴⁶ Ibid

⁴⁷ Ibid

⁴⁸ Ibid

⁴⁹ Ibid

6.3 Maxim A. Suchkov

I denna studie kommer den slutliga delen i det teoretiska ramverket bestå av Suchkovs beskrivande av metoder utifrån den ryska hybridkrigföringsteorin NGW (New Generation Warfare.)

För att vidare förstå hur Rysslands syn, metoder och medel beskrivs gällande hybridkrigföring beskrivs detta i Suchkovs artikel.⁵⁰ Denna artikel kommer användas i uppsatsen för att återkoppla till de metoder som beskrivs samt användas i analysen för att konkretisera studiens typfall av säkerhetshot mot Sverige.

Denna artikel skriven av Suchkov tillhörande Moskvas institut för internationella relationer (Mgimo-Universitet) beskriver den ryska synen på både österländsk och västerländsk hybridkrigföring och dess påverkan på det ryska politiska och militära utövandet.⁵¹

Artikeln argumenterar för att Ryssland ser hybridkrigföring på ett väsentligt annorlunda sätt än vad väst gör och att det främst är någonting som Ryssland blir utsatta för hellre än att det används av dem själva. Författaren beskriver bland annat att allt från kriget i Ukraina till Covid-19-vaccin eller Eurovision ses av Ryssland på ett sätt som att västvärlden bedriver hybridkrigföring mot dem.⁵²

Vidare diskuterar författaren hur den ryska idén om hybridkrigföring utvecklats till konceptet ”New Generation Warfare.” Suchkov beskriver NGW som något som fokuserar på hur Ryssland engagerar sig proaktivt utomlands, medan hybridkrigföring för ryssar mer handlar om att försvara sig mot västerländska destabiliseringsförsök. Hybridkrigföringen har därför blivit ett sätt för rysk säkerhetsstrategi att legitimera inrikes- och utrikespolitiska åtgärder och insatser.⁵³

Suchkov diskuterar fem nyckelparametrar som kommer att nyttjas i analysen för denna uppsats för att beskriva tillvägagångssättet med NGW, vilket är⁵⁴:

Politiskt Tryck vilket innehåller metoder så som informationskrigföring, desinformationskampanjer, användande av inflytelserika ombud.

Indirekt inflytande (cyberattacker, störning av infrastruktur, användandet av ombud.)

Militärt ingripande (användandet av specialförband i olika områden och miljöer, organisering av milisgrupper, infiltrering.)

Utmattning (Aggressiv patrullering av luftrummet, förflyttning av taktiska kärnvapen, flyttandet av större militära enheter.)

Manipulerande av avtal (Användandet av vapenvila-avtal för att skapa oenighet mellan stridande parter, manipulering av energitransporter.)⁵⁵

⁵⁰ M. A. Suchkov. *Whose hybrid warfare? How ‘the hybrid warfare’ concept shapes Russian discourse, military, and political practice, Small wars & Insurgencies*, (Routledge, 2021).

⁵¹ Ibid, 415.

⁵² Ibid, 416.

⁵³ Ibid, 416-422.

⁵⁴ Ibid, 426-427.

⁵⁵ Ibid

Slutligen belyser Suchkov det faktum att hybridkrigföring som begrepp har förlorat sitt värde. Författaren menar att västerländska och ryska säkerhetsexperter har använt begreppet så mycket att det riskerar att förlora sin betydelse. Han menar att det i väst ses som ett verktyg av Ryssland, medan Ryssland ser det som en taktik som används mot dem.⁵⁶

6.4 Sammanfattning och syftet med teorin i denna studie

Hoffmans teori beskriver hybridkrigföring som en kombination av konventionella och okonventionella metoder, där statliga och icke-statliga aktörer använder både militära och icke-militära angreppsformer för att destabilisera en motståndare.

The Hybridity Blizzard Model fokuserar på hur hybridkrigföring fungerar i praktiken, där attacker sker simultant och är svåra att identifiera. Modellen används för att klassificera hybridhot mot Sverige.

Suchkovs NGW ger en tydlig indelning i metoder som används i den moderna hybridkrigföringen.

För att sammanfatta vad respektive teori bidrar med i ramverket ger Hoffmans teori en grundläggande förståelse av hybridkrigföring som fenomen, medan The Hybridity Blizzard Model klassificerar dessa angreppsformer och NGW från Suchkov förklarar metoder och verktyg utifrån den ryska hybridkrigföringen.

⁵⁶ M. A. Suchkov. *Whose hybrid warfare? How 'the hybrid warfare' concept shapes Russian discourse, military, and political practice, Small wars & Insurgencies*, (Routledge, 2021). S. 416-422.

7 Metod

7.1 Forskningsdesign

Denna studie genomförs med en kvalitativ forskningsansats och är en teorikonsumerande fallstudie där fallet är möjlig hybridkrigföring mot Sverige. Syftet med att genomföra en teorikonsumerande studie är inte att generalisera, utan snarare att få en djupare förståelse för hur misstänkt hybridkrigföring manifesteras mot Sverige eftersom fallet står i centrum.⁵⁷

En traditionell fallstudie innebär att kontexten för studien är en och samma.⁵⁸ Denna studie syftar därmed inte till att jämföra två olika fall, utan att bättre förstå fallet misstänkt hybridkrigföring mot Sverige.

Teorin som appliceras på fallet är baserat på ett teoretiskt ramverk. Ramverket består av en kombination av tre olika teorier om hybridkrigföring.

Uppsatsen ämnar göra en teoretisk grundad analys av hybrida hot mot Sverige. Metodologiskt kommer detta genomföras genom en kvalitativ textanalys. Detta innebär att författaren tar fram det centrala innehållet av empirin genom att noggrant läsa och analysera textens delar, helhet och kontext.⁵⁹

Kvalitativ textanalys är lämpligt metodologiskt för denna uppsats eftersom det innebär att det genomförs mer komplexa tolkningar för en djupare förståelse av händelserna.⁶⁰ En djup förståelse för händelseförloppen är en förutsättning för denna uppsats.

⁵⁷ P. Esaiasson. M.fl. *Metodpraktikan*. Femte Upplagan. (Wolters Kluwer, 2015). S. 41-42.

⁵⁸ Ibid, 108-109.

⁵⁹ Ibid, 211.

⁶⁰ K. Boréus. G. Bergström. *Textens mening och makt*. Fjärde Upplagan. (Studentlitteratur, 2018). S. 50-51.

7.2 Operationalisering

Förståelsen för det teoretiska ramverket har syftat att ge en grund för läsarens förståelse av analysen samt stärka validiteten eftersom ramverkets komponenter beskrivs. Vidare har sex analysfrågor utifrån frågeställningen och det teoretiska ramverket operationaliserats fram. Dessa analysfrågor kommer utgöra grunden för analysen. Respektive analysfrågas syfte och användning kommer även presenteras här.

Dessa fall analyseras utifrån följande analysfrågor:

1. Vilka hybrida angreppsmetoder kan identifieras enligt Suchkovs NGW?

Denna fråga syftar till att förstå vilken specifik metod som används vid respektive fall av möjliga hybridangrepp utifrån de parametrar som Suchkov beskriver i sin teori. Detta bidrar till en förståelse för hur hybridangreppet anknyter till en bredare hybridstrategi, snarare än endast den isolerade händelsen. Dessa parametrar och metoder kommer också utgöra grunden ur analysens uppdelning.

Politiskt Tryck vilket innehåller metoder så som informationskrigföring, desinformationskampanjer, användande av inflytelserika ombud.

Indirekt inflytande (cyberattacker, störning av infrastruktur, användandet av ombud.)

Militärt ingripande (användandet av specialförband i olika områden av miljöer, organisering av milisgrupper, infiltrering.)

Utmattning (Aggressiv patrullering av luftrummet, förflyttning av taktiska kärnvapen, flyttandet av större militära enheter)

Manipulerande av avtal (Användandet av vapenvila-avtal för att skapa oenighet mellan stridande parter, manipulering av energitransporter)⁶¹

2. Vad är det för typ av attack enligt The Hybridity Blizzard Model?

Denna fråga nyttjas för att tydliggöra skillnaden mellan identifierat, svårförståeligt, otillskrivet eller obestämt. Denna skillnad är viktig då den inte bara belyser hybridattacker utifrån metod, utan också utifrån hur pass identifierbara eller tolkningsbara de är för den utsatta parten. Det är alltså inte enbart attackens innehåll som är avgörande, utan även hur attacken uppfattas eller om den upptäcks överhuvudtaget.

3. Vilka centrala begrepp kan utifrån Hoffmans teori om hybridkrigföring appliceras på fallet?

Denna fråga används för att undersöka till vilken utsträckning de observerade fallen av misstänkta hybridangrepp knyter an till Hoffmans centrala begrepp för hybridkrigföring och för att förstå hur det sammanvägda resultatet av flera attacker och metoder kan destabilisera den påverkade staten. De centrala begreppen är enligt tidigare Hybridkrigföring, Konvergens, Multimodalitet samt Adaptivitet.

⁶¹ M. A. Suchkov. *Whose hybrid warfare? How 'the hybrid warfare' concept shapes Russian discourse, military, and political practice, Small wars & Insurgencies*, (Routledge, 2021). S. 416.

4. Vad i dessa angreppsmetoder pekar mot främmande makts påverkan?

Denna fråga syftar till att utifrån det teoretiska ramverket finna någon form av koppling till vilken aktör som genomfört det misstänkta angreppet. Detta görs genom att se till den strategiska eller politiska vinningen som angreppet medför samt tillvägagångssättet för angreppet.

5. Vilka av de identifierade metoderna är särskilt svåra att attribuera och hur påverkar det möjligheten till respons?

Denna fråga syftar till att skapa en förståelse för vilka typer av angrepp som är svårast för den påverkade staten att tillskriva en aktör samt reagera på genom klassificeringen som gjorts genom The Hybridity Blizzard Model.

6. Vilken typ av påverkan eller effekt kan observeras i det svenska samhället till följd av dessa angrepp?

Denna fråga syftar till att utläsa effekten på Sverige, dess samhälle samt dess invånare utifrån de misstänkta hybridangreppen. Detta kommer att bidra till uppsatsens förståelse för konsekvenserna som angreppet medför.

8 Material

Författaren har funnit en rad rapporter, böcker och artiklar som behandlar fallet misstänkt hybridkrigföring gentemot Sverige och kan bidra till studien. Som empiri kommer uppsatsen att använda en kombination av källor för att utifrån Suchkovs beskrivna metoder skapa typfall.

Uppsatsen kommer specifikt nyttja 12 artiklar från SVT (Sveriges television), två rapporter från FOI (Totalförsvarets forskningsinstitut), en rapport från MPF (Myndigheten för psykologiskt försvar), en handbok från MSB (Myndigheten för samhällsskydd och beredskap) samt fyra av SÄPOs (Säkerhetspolisens) årsrapporter (2020, 2021, 2022 samt 2024–2025) som empiri. I samtliga av dessa källor diskuteras misstänka fall av hybridattacker.

9 Källkritik

För att tydliggöra relevansen och trovärdigheten för det empiriska material som nyttjas i denna uppsats kommer författaren att granska materialet enligt Ädel-OST-principerna, äkthet, oberoende, samtidighet, tendens.⁶² Eftersom majoriteten av materialet kommer från samma källor kommer respektive källa endast granskas en gång.

9.1 Säkerhetspolisen

Denna källa bidrar med beskrivningar av upplevda säkerhetshot mot Sverige. Då de publiceras av en statlig myndighet kan denna källa ha en viss intern tendens för att legitimera sin verksamhet vilket gör att dess oberoende minskar. Rapporterna är på årsbasis vilket betyder att de är mycket samtida i relation till mina avgränsningar.

Dessa rapporter är officiella publikationer från en svensk myndighet vilket stärker källans äkthet. Rapporterna är offentligt publicerade på SÄPO:s hemsida vilket innebär att källans identitet och ursprung är identifierbara.

9.2 MUST/Försvarmakten

Denna källa är likt SÄPO aktuell, äkta och baserade på underrättelser men kan ha en viss tendens för att beskriva och påvisa verksamhetens relevans. Denna publikation är publicerad på Försvarmaktens hemsida och således är källans ursprung identifierbar.

Detta gäller även de artiklar som publicerats och går att läsa på Försvarmaktens sida.

9.3 FOI/MPF/MSB

FOI som källa är äkta och erbjuder forskningsrapporter som finansieras av Försvarmakten. MPF är en statlig myndighet som är ansvariga för Sveriges psykologiska försvar. MPF är således en statlig och äkta källa som bland annat erbjuder definitioner och rapporter om påverkanskampanjer. Rapporterna som används i denna uppsats är offentliga och går att komma åt via FOI:s och/eller MPF:s hemsida vilket gör källorna identifierbara. MPF används som källa i denna uppsats, både med självständiga rapporter samt de rapporter som är skrivna i samarbete med FOI.

9.4 SVT

Nyhetsartiklarna från SVT är särskilt starka gällande samtidighet och äkthet. I enlighet med dess uppdrag som Public-Service-aktör är SVT även oberoende och har låg tendens. Detta gör källan mycket användbar i att få en objektiv bild av hur hybridangrepp presenteras i svensk media och offentlighet.

9.5 Frivärld

Denna källa påvisar äkthet genom att den bygger på externa källor såsom NATO och nationella underrättelse- och säkerhetstjänster. Rapporten är publicerad 2024 vilket innebär att

⁶² P. Esaiasson. M.fl. *Metodpraktikan*. Femte Upplagan. (Wolters Kluwer, 2015). S. 290-299.

den uppfyller kraven för samtidighet då innehållet också diskuterar fall från de närmaste åren. Rapporten en dock en viss tendens att förstärka hotbilden av rysk hybridkrigföring. Organisationen Frivärld är politiskt oberoende och har en rad etablerade forskare knutna till sig.

Sammanfattningsvis bedöms samtliga källor som äkta med god samtidighet. Källorna kan vara något tendensiösa.

10 Forskningsetik

Eftersom författaren till detta arbete är verksam inom Försvarmakten finns en risk för viss förförståelse eller partiskhet i tolkningen av hot mot Sverige. För att hantera detta har författaren strävat efter att hålla analysen nära det teoretiska ramverket och vara transparent i vilka tolkningar som gjorts utifrån det material som använts.

Denna uppsats bygger uteslutande på öppet och allmänt tillgängligt material. Källorna som använts är kontrollerbara och kommer från exempelvis Säkerhetspolisen, Försvarmakten och etablerade nyhetskanaler som SVT.

Författaren bedömer att uppsatsen inte har någon direkt påverkan på samhället i stort, men kan bidra till vidare forskning inom ämnet hybridkrigföring, särskilt ur ett svensk-statligt perspektiv. Studien kan vara relevant för framtida forskning om hybridhot mot mindre stater.

Målet har varit att redovisa resultaten av forskningen på ett transparent och tydligt sätt. Eventuella begränsningar i materialet, såsom svårigheter att säkert tillskriva angrepp en viss aktör, har redovisats öppet.

11 Analys

Det analyserade materialet är mycket omfattande och en mängd möjliga och sannolika hybrida angrepp av olika typer har identifierats. För att göra presentationen av empirin översiktlig har den delats upp i fyra olika huvuddelar beroende på angreppstyp, så kallade typfall. Typfallen kan i enlighet med hybridkrigföringens komplexa natur antingen vara ett faktiskt påvisat hybridangrepp eller en olyckshändelse som liknat ett hybridangrepp. Därefter analysera dessa typfall genom det teoretiska ramverk som skapats och givit grunden för analysfrågorna. Analysen är strukturerad av Suchkovs metoder, dels för att det ska bli lättare och följa, dels för att tydliggöra variationen i att en nyckelparameter kan ha flertalet metoder. Inom varje fall används de teoretiska indikatorerna/frågorna som analysverktyg i enlighet med det operationaliserade ramverket.

11.1 Typfall 1: Ombud/specialförband

Den 17:e november 2024 påverkades en undervattenskabel som förbinder Sverige och Litauen. Kabeln förstördes cirka 5 mil från Gotland, det vill säga inom svensk ekonomisk zon (SEZ). Den 18:e november 2024 påverkades en kabel som förbinder Tyskland med Finland. Denna kabel ligger också inom SEZ. Den 26:e Januari 2025 påverkades en undervattenskabel mellan Lettland och Gotland. Kabeln gick av inom SEZ. Den 21:a februari 2025 skadades ytterligare en kabel utanför Gotland.⁶³

Den 3:e mars 2025 drabbades en ytvattentäkt på Gotland av ett misstänkt sabotage. Sabotaget innebar att pumpar som pumpade upp vatten från ytvattentäkten slutade fungera och således fick inte Gotland tillgång till det vatten som krävs för att tillverka dricksvatten till öborna. Det var någon som brutit sig in i ett elskåp och stängt av pumparna.⁶⁴

Natten mellan den 2–3 april 2025 påverkades en kopplingsstation i Emmaboda. Det var någon som brutit sig in i stationen och slitit loss en kabel som försörjer 100-tals hushåll med ström.⁶⁵

En telestation i Växjö påverkades i december 2024 genom att någon tagit sig in genom ett taggtrådsstaket för att sedan klippa av kablar. Detta resulterade i att telefonförbindelser inom området bröts fullständigt.⁶⁶

Den 15:e maj 2016 klockan 22:30 inkommer rapporter om att radio- och tv-masten öster om Borås rasat, vilket kan ha påverkat upp till 188 000 personer. Enligt uppgifter har masten rasat med anledning av att någon eller några lossat muttrar till de vajrar som håller masten uppe. Detta kräver både förkunskaper och specialverktyg enligt experter.⁶⁷

⁶³ E. Lindvall. Detta vet vi: Kabelbrotten i Östersjön. *SVT*. (21/2 2025) <https://www.svt.se/nyheter/inrikes/detta-vet-vi-kabelbrotten-i-ostersjon> (Hämtad 16 apr. -25)

⁶⁴ P. Widegren. Utredning om misstänkt vattensabotage på Gotland läggs ned. *SVT*. (14/4 2025) <https://www.svt.se/nyheter/lokalt/ost/utredning-om-misstankt-vattensabotage-pa-gotland-laggs-ned> (Hämtad 16 apr. -25)

⁶⁵ E. Nielsen. Sabotage mot kopplingsstation i Emmaboda – hundratals blev utan ström. *SVT*. (3/4 2025) <https://www.svt.se/nyheter/lokalt/smaland/sabotage-mot-kraftstation-i-emmaboda> (Hämtad 16 apr. -25)

⁶⁶ TT. Misstänkt sabotage mot telestation i Växjö. *SVT*. (3/12 2024) <https://www.svt.se/nyheter/lokalt/smaland/misstankt-sabotage-mot-telestation-i-vaxjo> (Hämtad 16 apr. -25)

⁶⁷ F. Renman. L Sandborg. Sabotage mot master – detta har hänt. *SVT*. (20/5 2016) <https://www.svt.se/nyheter/lokalt/vast/haglareadmasten-rasade-detta-har-hant> (Hämtad 16 apr. -25)

I slutet av september 2022 blev det en läcka på gasledningarna Nord Stream 1 och 2. Säkerhetspolisen ansvarar för utredningen då det rör sig om allvarliga brott som kan vara riktade mot svenska intressen och det inte går att utesluta att främmande makt är inblandade i detonationerna. Säpos undersökningar har bekräftat att det rör sig om grovt sabotage då man funnit spår av sprängämnen.⁶⁸

Dessa fall exemplifierar det som enligt svensk lag rubriceras som sabotage och är således en del av vad som kommer analyseras i denna uppsats för att tydliggöra hybridkrigföring.

11.1.1 Analysfrågor typfall 1

Vilka hybrida angreppsmetoder kan identifieras enligt Suchkovs NGW?

Enligt Suchkovs NGW klassificeras sabotage som både indirekt inflytande och militärt ingripande, då vi kan anta att alla redovisade händelser ovan om avsiktliga, antingen genomfördes av specialunderättelseförband eller ombud.

Vad är det för typ av attack enligt The Hybridity Blizzard Model?

Enligt The Hybridity Blizzard Model är fallen med sabotagen och undervattenskablarna otillskrivna med anledning av att det är tydligt att en icke-identifierbar aktör har påverkat händelserna. Dock är det inte klargjort om skadorna på undervattenskablarna är medvetet gjorda av ett ombud från exempelvis Ryssland eller om det bara är en olyckshändelse, vilket gör att det hade kunnat klassificeras som obestämt enligt modellen också.

Vid de andra sabotagen som beskrivs är det dock tydligt att aktören avsiktligt erlagt skador på objekten men eftersom det inte framkommit vem eller vilka som gjort detta, gör det sabotagen otillskrivna.

Vilka centrala begrepp kan utifrån Hoffmans teori om hybridkrigföring appliceras på fallet?

Samtliga sabotageangrepp ovan går i enlighet med de centrala begreppen hybridkrigföring och konvergens ur Hoffmans teori. Dessa angrepp kan ses som hybrida då de kombinerar kriminella metoder så som att bryta sig in i elskåp för att stänga av pumpar med irreguljära metoder så som att kapa undervattenskablar och spränga undervattensledningar för att nå strategiska målsättningar. Vidare kan vi även se konvergens i detta typfall, då icke-statliga aktörer som inhemska kriminella ligger i Sverige kan ha genomfört vissa av dessa angrepp för en annan stats intresse, exempelvis Ryssland.

Vad i dessa angreppsmetoder pekar mot främmande makts påverkan?

⁶⁸ Säkerhetspolisen. *Årsredovisning 2022*. (2023). S. 49.

I fallen med undervattenskablarna vet vi att främmande makt varit inblandad tack vare utredningarna⁶⁹, dock råder det i nuläget fortfarande en viss osäkerhet kring om det var avsiktlig skadegörelse eller inte. I de andra sabotagefallen är det oklart vilken aktör som ligger bakom sabotagen. Något som pekar på främmande makt kan varit inblandade är det faktum att experter menar att det krävts speciell utrustning och träning vid sabotaget i Borås vilket tyder på en kvalificerad aktör som exempelvis specialunderättelseförband. Vidare pekar även sabotagen på gasledningarna på att en kvalificerad aktör genomfört dessa då det användes sprängmedel och skedde på ett sådant djup att det kräver speciell utrustning och träning.

Vilka av de identifierade metoderna är särskilt svåra att attribuera och hur påverkar det möjligheten till respons?

Många sabotageangrepp är fall som anses svåra att attribuera eftersom de använder indirekt inflytande, det vill säga användandet av någon form av ombud för att genomföra attackerna. Användandet av ombud innebär att dessa oftast måste tas på bar gärning och således är svåra att koppla till någon motståndare. Metoden militärt ingripande alltså användningen av specialförband är också svårt eftersom dessa är speciellt tränade för att infiltrera och genomföra sabotage utan att upptäckas.

Vilken typ av påverkan eller effekt kan observeras i det svenska samhället till följd av dessa angrepp?

Effekten av sabotageangrepp i det svenska samhället är märkbar både på kollektiv och individuell nivå. De samhällsliga konsekvenserna har exempelvis i fallen ovan inkluderat strömavbrott i flera bostadsområden eller som på Gotland, påverkan på dricksvattnet, vilket i sin tur skapar stora kostnader och praktiska utmaningar. Dessa angrepp kan skapa både en fysisk påverkan av individer i samhället genom inte ha tillgång till vatten att dricka eller elektricitet för att värma sig samtidigt som det kan uppstå en viss psykologisk stress och oro av det faktum att en fientlig aktör, oavsett inhemsk eller någon från annan stat, kan påverka denna samhällsviktiga infrastruktur. Konsekvenserna av Nord Stream är främst politiskt då ledningarna var avstängda men händelsen stärker bilden att påverkan av infrastruktur kan användas och bör ses som ett verktyg i hybridkrigföring.

⁶⁹ E. Lindvall. Detta vet vi: Kabelbrotten i Östersjön. *SVT*. (21/2 2025) <https://www.svt.se/nyheter/inrikes/detta-vet-vi-kabelbrotten-i-ostersjon> (Hämtad 16 apr. -25)

11.2 Typfall 2: Informationskrigföring/Påverkanskampanjer

Myndigheten För Psykologiskt Försvar (MPF) ”MPF definierar påverkanskampanjer som en från främmande makt koordinerad verksamhet som innefattar vilseledande eller oriktig information eller annat för ändamålet särskilt anpassat agerande.”⁷⁰

MPF hävdar att syftet med en påverkanskampanj är att bland annat påverka opinioner av hela eller delar av svenska befolkningen samt beslutsfattare så att Sverige och dess intressen kan komma att påverkas på ett betydande sätt. Det kan också innebära att man påverkar ett annat lands syn på Sverige för att påverka Sverige eller dess intressen.⁷¹

Ett exempel på detta är under valet 2022 då det skapades diskussioner om valfusk på sociala medier, särskilt på Twitter (numera X). Under valkvällen börjar flera konton sprida påståenden om att valresultatet manipulerats, bland annat genom användning av hashtaggen #valfusk. Enligt författarna till rapporten så retweetade många av dessa konton på bestämda tider, vilket skulle kunna tyda på att det var botkonton. Ett av de mest spridda inläggen publiceras av ett konto som utgav sig för att tillhöra en ”högutbildad, rysslandsvän...”⁷² och kommunpolitiker, detta konto visade sig senare vara falskt. Kontot försökte aktivt styra uppmärksamheten mot valfusk genom att retweeta 146 tweets på en mycket kort tid, där samtliga handlade om valfusk, i ett skede då diskussionen annars var på väg att avta. Denna händelse kan ses som ett exempel på riktad informationspåverkan med syfte att underminera förtroendet för Sveriges valsystem.⁷³

Vidare beskriver MPF någonting som kallas för LVU-kampanjen. Det var i början av 2022 som en stor informations- och påverkanskampanj som fokuserade på svenska socialtjänsten och Lagen om bestämmelser av vård av unga (LVU) uppmärksammades. Påverkanskampanjen påstod att socialtjänsten kidnappar barn och då med särskilt fokus på barn med utländskt påbrå som var muslimer. Ett flertal inhemska aktörer demonstrerade både på internet och i verkligheten, vilket gav fenomenet internationell uppmärksamhet. Genom denna påverkanskampanj skapades hat mot Sverige och det uppmanades internationellt till bland annat våld och terrorattentat gentemot Sverige.⁷⁴

I samband med koranbränningarna i Sverige 2023 hackade en iransk cyberaktör ett svenskt företag som kunde skicka ut massmeddelanden. Genom attacken skickade den iranska cyberaktören ut sms till flera tusen personer i Sverige där man uppmanade att lämna information om vilka som utfört koranbränningar. Påverkanskampanjens syfte var att stärka den iranska regimen genom att insinuera att Sverige var islamfientligt och skapa splittring inom Sverige.⁷⁵

⁷⁰ MPF. *Ordlista*. (u.å.). <https://mpf.se/hjalpmedel/ordlista> (Hämtad 16 apr. -25)

⁷¹ MPF. *Ordlista*. (u.å.). <https://mpf.se/hjalpmedel/ordlista> (Hämtad 16 apr. -25)

⁷² O. Svenonius, S. Olsson, M. Michélsen Forsgren, E. Dungen och M Jarlsbo. *Sa någon valfusk? Informationsmiljön på sociala medier i samband med valrörelsen 2022*. (FOI-R--5429--SE. Stockholm: Totalförsvarets forskningsinstitut. 2023). S.47.

⁷³ *Ibid*, 47-48.

⁷⁴ M. Ranstorp, L. Ahlerup. *LVU-kampanjen*. (Försvarshögskolan, MPF, 2023). S.4.

⁷⁵ Säkerhetspolisen. *Årsredovisning 2024/2025*. (2025). S. 37.

11.2.1 Analysfrågor typfall 2

Vilka hybrida angreppsmetoder kan identifieras enligt Suchkovs NGW?

Enligt Suchkov NGW kategoriseras metoderna informationskrigföring och desinformationskampanjer vilket exemplifieras ovan som politiskt tryck.

Vad är det för typ av attack enligt The Hybridity Blizzard Model?

Enligt analysen av Blizzard model är dessa attacker identifierade, otillskrivna och svårförståeliga. I fallet med massmeddelandena (det vill säga iranska cyberangreppet) är det identifierat eftersom vi vet med säkerhet att det rörde sig om ett hybridangrepp och vilka som genomförde hybridangreppet. I fallet med LVU-kampanjen vet vi att det är en typ av hybridangrepp men inte vilka som initierat angreppet, särskilt eftersom det var en debatt som pågick under en längre tid. Detta innebär att LVU-kampanjen var otillskriven. I fallet med den förfalskade kommunpolitikern är det svårförståeligt i och med att det inte var självklart att det rörde sig om en informationskampanj från början och det förfalskade kontot inte gick att spåra till en avsändare.

Vilka centrala begrepp kan utifrån Hoffmans teori om hybridkrigföring appliceras på fallet?

Dessa angrepp kan förstås enligt de centrala begreppen konvergens och adaptivitet enligt Hoffmans teori. Begreppet konvergens är relevant eftersom både statliga och icke-statliga aktörer var inblandade i LVU-kampanjen. Begreppet adaptivitet är relevant på både LVU-kampanjen och det iranska cyberangreppet, eftersom fienden anpassade sig utifrån en svaghet som upptäckts i det svenska samhället. För att förtydliga detta hävdar författaren att antagonisten vid LVU-kampanjen påverkade och förstärkte någonting som redan ansågs som ett problem och genom denna förstärkning gav detta problem internationell uppmärksamhet. På samma sätt så såg troligen Iran en splittring i Sverige vid cyberangreppet och valde att genomföra en påverkanskampanj för att förstärka detta.

Vad i dessa angreppsmetoder pekar mot främmande makts påverkan?

I fallet med den iranska cyberaktören har det påvisats att Iran var inblandade i påverkansoperationen.⁷⁶ Vid LVU-kampanjen kan den plötsliga spridningen tyda på att det fanns en påverkan från främmande makt. Vid fallet med den förfalskade kommunpolitikern tyder faktumet att han uppgav sig vara rysslandsvän att det kan ha funnits en koppling till Ryssland.

Vilka av de identifierade metoderna är särskilt svåra att attribuera och hur påverkar det möjligheten till respons?

Samtliga påverkanskampanjer är svåra att spåra och hänföra till en motståndare. Generellt är det svårt att respondera på en påverkanskampanj när den redan fått spridning. Troligen är det lättaste av dessa exemplifierade fall att besvara den iranska cyberattacken som är identifierad, eftersom det då går att förklara varför och hur något hänt, samt vilken aktör som ligger bakom detta. Detta innebär också att man kan tydliggöra motståndarens motiv.

⁷⁶ Säkerhetspolisen. *Årsredovisning 2024/2025*. (2025). S. 37.

Vilken typ av påverkan eller effekt kan observeras i det svenska samhället till följd av dessa angrepp?

Effekten av dessa angrepp är tydlig. Dessa angrepp skapar splittring i det svenska samhället och påverkar den nationella och internationella bilden av Sverige negativt. Genom att underminera valsystemet minskar förtroendet för staten och genom att framställa Sverige som islamfientligt ökar risken för våld- och terroristangrepp, vilket i sin förlängning gör Sverige mer osäkert.

11.3 Typfall 3: Störning av infrastruktur

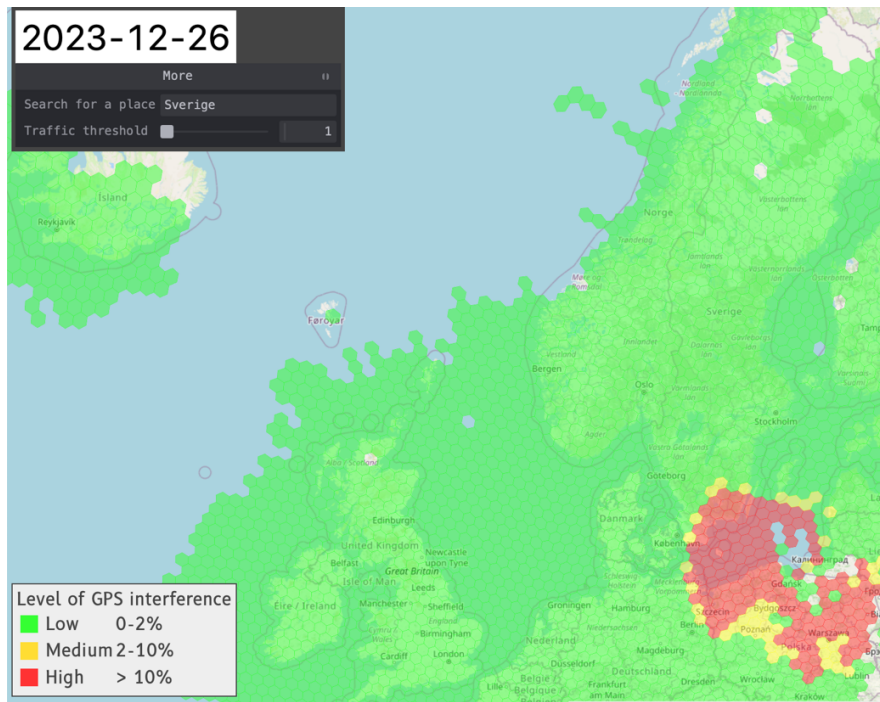


Bild 2 Visar GPS-störningen över Sverige den 26 december 2023⁷⁷

GNSS (Global Navigation Satellite Systems) är någonting som används hela tiden, både på den civila sidan och militärt. Dessa system som exempelvis GPS, Galileo eller GLONASS används för att bestämma position, hastighet och/eller tid.⁷⁸

I juni 2022 rapporterade Kustbevakningen och Sjöfartsverket om störningar på GPS-signalen i Stockholms skärgård.⁷⁹

Även under julhelgen 2023 utsattes Sverige för stora GPS-störningar. Under denna störning slogs delar av satellitnavigeringen för både fartyg och flygplan ut. I samband med störningen uppger ryska utrikesministeriet att deras förband för elektronisk krigföring har övat med målsättningen att hejda motståndarens navigerings- och kommunikationssystem.⁸⁰

⁷⁷ J. Wiseman. *GPSJAM*. (u.å.). <https://gpsjam.org/?lat=62.01934&lon=15.31820&z=3.5&date=2023-12-26> (Hämtad 16 apr. -25)

⁷⁸ FOI. *Om GNSS*. (2021). <https://www.foi.se/kurser/gnss--satellitnavigeringssystem/om-gnss.html> (Hämtad 16 apr. -25)

⁷⁹ MSB. *Handbok i kommunal krisberedskap 4. Riskkatalog*. (2022). <https://rib.msb.se/filer/pdf/30061.pdf> (Hämtad 16 apr. -25)

⁸⁰ S. Ritzén. Sverige drabbat av stor GPS-störning. *SVT*. (3/1 2024) <https://www.svt.se/nyheter/inrikes/sverige-drabbat-i-storsta-gps-sabotaget-i-ostersjon> (Hämtad 13 mar. -25)

Även under 2025 har det pågått störningar av GPS-system i Östersjöområdet. Störningarna sträcker sig även över Gotland. Det som påverkas mest är den flygtrafik som går över östersjön. Många piloter måste använda andra typer av navigeringssystem under flygturer i området.⁸¹

FOI uppger att dessa störningar inte har någon annan förklaring än medveten påverkan.⁸²

11.3.1 Analysfrågor typfall 3

Vilka hybrida angreppsmetoder kan identifieras enligt Suchkovs NGW?

Enligt Suchkovs NGW ingår störning av infrastruktur i indirekt inflytande. Eftersom denna störning genomförs genom elektronisk krigföring med trupp kan det också ses som en form av militärt ingripande. Det kan också ses som utmattning då Ryssland flyttat större militära enheter för att uppnå rätt effekt av störningen.

Vad är det för typ av attack enligt The Hybridity Blizzard Model?

Enligt Hybridity Model är dessa angrepp identifierade eftersom det är känt att det är Ryssland som genomför dessa störningar och en definierbar metod för hybridangrepp.

Vilka centrala begrepp kan utifrån Hoffmans teori om hybridkrigföring appliceras på fallet?

GPS-störningarna definieras definitivt som hybridkrigföring enligt Hoffmans teori eftersom Ryssland genom en irreguljär metod med konventionella trupper påverkar Sverige utan att gå över tröskeln som innebär ett väpnat angrepp.

Vad i dessa angreppsmetoder pekar mot främmande makts påverkan?

I dessa angrepp är det tydligt att det finns en främmande makts påverkan eftersom de största störningarna varit i samband med stora ryska övningar. Dessutom uppger FOI att dessa störningar inte kan förklaras på något annat sätt än att det är medvetna.⁸³

Vilka av de identifierade metoderna är särskilt svåra att attribuera och hur påverkar det möjligheten till respons?

Dessa attacker är lätta att upptäcka och identifiera men svåra att besvara. Det kräver att man använder alternativa metoder i stället för de traditionella satellitnavigeringssystemen. Detta

⁸¹ P. Widegren. Störningar i GPS-system allt vanligare – påverkar flyg över Östersjön. *SVT*. (21/1 2025) <https://www.svt.se/nyheter/lokalt/ost/storningar-i-gps-system-allt-vanligare-paverkar-flyg-over-ostersjon> (Hämtad 16 apr. -25)

⁸² K. Airaksinen. Gps-bortfall i luften: En ny vardag för Europas piloter. *SVT*. (4/5 2024) <https://www.svt.se/nyheter/inrikes/gps-bortfall-i-luften-en-ny-vardag-for-europas-piloter> (Hämtad 21 apr. -25)

⁸³ Ibid

går inte att besvara eftersom det inte räknas som ett väpnat angrepp och hamnar i en form av gråzon för vad som är okej att genomföra eller inte.

Vilken typ av påverkan eller effekt kan observeras i det svenska samhället till följd av dessa angrepp?

Attackerna påverkar framför allt navigeringen för flygplan och båtar i Östersjön samt södra delarna av Sverige inklusive Gotland. Angreppen har inte en allt för stor påverkan eftersom det finns alternativa navigeringsmetoder, men orsakar en del problem för transporterna i de drabbade områdena. Om längden och intensiteten av dessa angrepp skulle öka finns det dock en ökad risk att det skulle kunna påverka andra system också eftersom många system till exempel använder satelliter för att bestämma tid.

11.4 Typfall 4: Infiltrering/Cyberattacker

11.4.1 Spioneri/infiltrering

Den 22:a juni 2020 döms en man för grov obehörig befattning med hemlig uppgift av stor betydelse. Han misstänkts bland annat för att ha dokumenterat och fotograferat skyddsobjekt på olika platser i Sverige och spridit del av detta.⁸⁴

Den 5:e februari 2021 åtalas en man för att olovligen spridit hemliga och känsliga uppgifter om ett stort antal försvarsanläggningar. Även en annan man åtalas 23:e februari 2021 för grov obehörig befattning med hemlig handling där han misstänkts att olovligen spridit hemliga och känsliga uppgifter om elva försvarsanläggningar.⁸⁵

En man döms för spioneri hösten 2021. Denna person var en högutbildad forskare som arbetade som konsult inom fordonsindustrin. Personen började kort efter han träffat en rysk underrättelseofficer spionera åt Ryssland. Enligt Säpo kan informationen mannen lämnat ut leda till omfattande men för Sverige både militärt och ekonomiskt, på kort och lång sikt.⁸⁶

Detta är bara några exempel på de fall av underrättelseinhämtning och spioneri som skett mot Sverige i närtid.

11.4.2 Cyberattacker

Den 13-14:e februari 2024 upplevde ett flertal av Sveriges samhällsaktörer teknikproblem, bland annat SVT, 1177, Polismyndigheten, Transportstyrelsen och SL blev påverkade. En grupp kallad ”Anonymous Sudan” tog på sig attackerna och sa på sociala medieplattformen Telegram att de hade utfört en mycket stor cyberattack mot svenska sjukvårdsinfrastrukturen.⁸⁷

Detsamma skedde under 2023 när bland annat Vattenfall, Kivra, SAS och SOS Alarms hemsidor blev påverkade. Även då påstod sig Anonymous Sudan ligga bakom attackerna. Säkerhetsexperter menar att det kan ha varit ryska staten som låg bakom attackerna och sedan låtsas varit Sudan som attackerat Sverige.⁸⁸

Anledningen till att många säkerhetsexperter tror att Ryssland är inblandade är på grund av den strategiska vinning de tros ha fått av dessa attacker. Erdoğan hade tidigare uttryckt att Sverige inte var välkommet in i NATO av Turkiet på grund av koranbränningarna. Detta var det som Anonymous Sudan rättfärdigade sina attacker med. Vidare krävs det relativt stora resurser för att angripa flera sidor samtidigt, vilket pekar på en större aktör. Dessutom skapas en rädsla i befolkningen att våra system är gripbara, vilket hade kunnat försvaga det svenska samhället.⁸⁹

⁸⁴ Säkerhetspolisen. *Årsredovisning 2020*. (2021). S. 17.

⁸⁵ Säkerhetspolisen. *Årsredovisning 2021*. (2022). S. 74.

⁸⁶ Säkerhetspolisen. *Årsredovisning 2021*. (2022). S. 20-23.

⁸⁷ H. Ekberg Skog. Teknikstrul hos flera samhällsaktörer. *SVT*. (19/2 2024)

<https://www.svt.se/nyheter/inrikes/tekniska-storningar-pa-flera-hall> (Hämtad 16 apr. -25)

⁸⁸ I. Wahlund. Efter hotet om hackerattack – flera sajter drabbade av problem. *SVT*. (19/2 2023)

<https://www.svt.se/nyheter/inrikes/efter-hotet-om-hackerattack-flera-webbsajter-nere> (Hämtad 17 apr. -25)

⁸⁹ M. Grill Pettersson. It-attackerna mot Sverige – här är kontot som tar på sig ansvaret. *SVT*. (14/2 2023)

<https://www.svt.se/nyheter/inrikes/en-rad-it-attacker-mot-sverige-har-ar-kontot-som-tar-pa-sig-ansvaret> (Hämtad 18 apr. -25)

11.4.3 Analysfrågor typfall 4

Vilka hybrida angreppsmetoder kan identifieras enligt Suchkovs NGW?

Enligt Suchkovs nyckelparametrar ingår cyberattacker i indirekt inflytande av en annan stat. Underrättelseinhämtning skulle kunna klassificeras som militärt ingripande då detta inkluderar metoden infiltrering.

Vad är det för typ av attack enligt The Hybridity Blizzard Model?

Cyberattackerna ovan är otillskrivna enligt Hybridity model eftersom det tydligt framkommit att det skett ett hybridangrepp men användandet av en proxygrupp (Anonymous Sudan) gör det svårt att peka på vilket exakt aktör som ligger bakom attacken. Det kan vara proxygruppen själva men likväl kan det i stället vara någon annan aktör som försöker överföra ansvaret på Anonymous Sudan. Exemplet av underrättelseinhämtningen ovan är något mer komplicerade då de både kan klassificeras som identifierade och otillskrivna angrepp. Detta eftersom man i ett av fallen omhändertagit spionen samt fastställt åt vilket land denna man spionerat för (Ryssland). Detta gör exemplet identifierat. I de andra spionfallen vet man inte vilka som fått tillgång till informationen som inhämtats och spridits, således kan dessa spioner liknas med ett ombud. Därmed blir de spionfallen otillskrivna.

Vilka centrala begrepp kan utifrån Hoffmans teori om hybridkrigföring appliceras på fallet?

Utifrån Hoffmans teori blir begreppen hybridkrigföring, konvergens och adaptivitet aktuella. Hybridkrigföring som begrepp blir aktuellt då fienden kombinerar kriminella och irreguljära metoder för att nå politiska målsättningar genom att genomföra dataintrång och spioneri. Konvergens blir aktuellt eftersom en statlig aktör samarbetar med en icke-statlig aktör vid både underrättelseinhämtning och cyberattackerna. Adaptivitet blir aktuellt eftersom en den möjliga fiendliga aktören anpassat sig genom att nyttja sig av Anonymous Sudan som berättigade sina cyberangrepp med koranbränningarna. För att förtydliga ses detta som adaptivt då även Turkiet hävdade koranbränningarna som anledning till att Sverige inte skulle ingå som medlem i NATO. Den fiendliga aktören använde således en svaghet (koranbränningarna) för att maximera sin verkan (att Sverige inte skulle få ingå i försvarsalliansen NATO.)

Vad i dessa angreppsmetoder pekar mot främmande makts påverkan?

Mannen som dömdes för spionage spionerade åt Ryssland och hade kontakt med en rysk underrättelseofficer, vilket är något som framkommer i årsredovisningen.⁹⁰ Därmed finns det en tydlig inblandning av främmande makt.

Vid de övriga spionerifallen är det mer betydelsefullt att undersöka vilka fiendliga aktörer som hade kunnat få nytta av informationen som spridits. Genom att se till länders intressen finns det ett flertal länder som skulle se vinning i att förvärva denna typ av information om Sveriges försvarsanläggningar.

⁹⁰ Säkerhetspolisen. *Årsredovisning 2021*. (2022). S. 74

Främmande makt tros även varit inblandat vid cyberangreppet eftersom säkerhetsexperter menar att Ryssland hade en strategisk vinning i dessa attacker. Dessutom krävs stora resurser för att genomföra parallella cyberangrepp, vilket tyder på en större och mer kapabel aktör än en hackergrupp.

Vilka av de identifierade metoderna är särskilt svåra att attribuera och hur påverkar det möjligheten till respons?

Cyberangrepp är svåra att reagera på eftersom man endast kan förbättra sin egen cybersäkerhet. Det är dessutom svårt att förstå vem som ligger bakom attackerna eftersom hackare oftast "gömmar" sina spår. Vid spionfall och underrättelseinhämtning kan Sverige reagera genom rättsliga processer. Detta kan innebära konsekvenser som fängelse för själva spionen eller utvisning för den ryske underrättelseofficieren.

Vilken typ av påverkan eller effekt kan observeras i det svenska samhället till följd av dessa angrepp?

Underrättelseinhämtning påverkar samhället och Sverige genom att den inhämtade informationen kan hamna hos en fientlig aktör vilket kan leda till omfattande men ekonomiskt och militärt. Det kan innebära att de exempelvis får tillgång till ny teknik eller får reda på var en militäranläggning finns eller vilka sårbarheter anläggningen har. Vid cyberattackerna kan det skapas en rädsla i att våra hemsidor inte är säkra eller att vi är gripbara via cyberangrepp. Dessutom finns risken att mer omfattande cyberangrepp kan påverka mer vitala nätverkssystem men även vital infrastruktur.

11.5 Sammanfattning analys

Sammanfattningsvis har denna analys identifierat 20 misstänkta hybridangrepp mot Sverige mellan åren 2016 och 2025. Dessa misstänkta angrepp har nyttjat metoder som sabotage (9st), cyberattacker (2st), störning av infrastruktur (3st), underrättelseinhämtning (3st) och påverkansoperationer (3st). De misstänkta angreppen har varit otillskrivna, obestämda, identifierade eller svårförståeliga. Trots att majoriteten av angreppen varit antingen otillskrivna, svårförståeliga eller obestämda tyder analysen på att många av händelserna har haft en inblandning av främmande makt. Aktörer bakom de misstänkta angreppen har använt adaptivitet och konvergens för att uppnå det som Hoffman definierar som hybridkrigföring.

12 Slutsatser

Syftet med denna undersökning var att identifiera och analysera möjliga hybridangrepp mot Sverige med hjälp av ett teoretiskt ramverk.

Frågeställningen *”Vilka metoder av hybridkrigföring kan identifieras mot Sverige i nutid och hur kan dess effekt förklaras genom ett teoretiskt ramverk av moderna hybridkrigföringsteorier?”* kan besvaras med att hybridkrigföring mot Sverige ger uttryck genom lågintensiva, varierade angrepp som riktas mot både fysisk infrastruktur, samhällets psykologiska motståndskraft och förtroendet för den svenska statsapparaten. Angreppen karakteriseras av låg spårbarhet och hög komplexitet och bör förstås som medvetna strategiska och politiska handlingar som syftar att destabilisera, försvaga och påverka Sveriges säkerhetspolitiska läge utan att gå över tröskeln till ett väpnat angrepp.

Analysen påvisar att samtliga typfall har tydliga drag av hybridkrigföring enligt Hoffmans definition och att flera av de metoder som används beskrivs av Suchkovs NGW. Vidare påvisar analysen att många av dessa överlappar och förstärker varandra vilket är någonting som Weissman beskriver i *The Hybridity Blizzard Model*. Det är också återkommande att dessa angrepp är otillskrivna enligt *Hybridity Blizzard Model* vilket försvårar möjligheten till respons, eftersom man inte vet vem som genomfört angreppet. Dock går det att utläsa att flera av fallen troligen haft inblandning av främmande makt, främst Ryssland men också Iran. Detta är särskilt framträdande i fallen med GNSS-störningar och påverkanskampanjer. Kombinationen av låg spårbarhet, fysisk påverkan på samhällskritisk infrastruktur och psykisk påverkan på samhället i stort gör att dessa angrepp utgör ett reellt hot mot svensk säkerhet.

Sammanfattningsvis framhäver undersökningen att Sverige sannolikt är utsatt för en rad hybrida angreppsmetoder vars effekt hotar såväl fysisk infrastruktur som psykologisk motståndskraft i samhället. Metoderna syftar till att underminera Sveriges ledning och samhälle och skapa strategiska fördelar utan att överträda tröskeln för väpnad konflikt. Denna studie tydliggör därmed behovet av en ökad förmåga att identifiera, klassificera och hantera hybridhot i svensk försvars- och säkerhetspolitik.

13 Diskussion

Uppsatsen har fokuserat på att problematisera hur hybridkrigföring utförs mot Sverige i modern tid genom att undersöka vilka metoder som används, hur dessa kan förstås genom teorier om hybridkrigföring samt vilken effekt dessa har på samhället. Undersökningen har visat att hybridmetoder används mot Sverige men att dessa är svåra att attribuera, vilket bekräftar den tidigare forskningen om hybridkrigföringens komplexitet. Precis som Gunneriusson⁹¹ beskriver i sin forskning är förnekbarhet tydligt tonsättande i hybridhot. Undersökningen har likt Ljungkvist⁹² dragit slutsatser om att det blir allt viktigare för civilsamhället att bidra med identifieringen och motverkandet av hybridhot och genom detta skapa en form av kollektiv motståndskraft. Mattson⁹³ beskrev i sin artikel att denna form av krigföring syftar till att utmatta motståndaren genom att uppnå organiserat kaos. Detta är en slutsats som också går att dra utifrån denna undersöknings resultat kring den effekt som de misstänkta hybridangreppen tros ha haft på samhället.

Uppsatsen har bidragit till forskningen genom att tillämpa ett teoretiskt ramverk på fallet Sverige. Mycket av den tidigare litteraturen kring hybridkrigföring har varit rent teoretisk eller fokuserat på andra delar av världen. Genom att använda Hoffmans teori, Hybridity Blizzard Model och Suchkovs NGW har uppsatsen visat hur olika angreppsmetoder samverkar i praktiken och svårigheten i att bemöta dessa. Uppsatsen synliggör behovet av att anpassa svensk försvarsförmåga och strategi till att både klara av lågintensiva hybridangrepp med stor strategisk verkan likväl som fullskaliga väpnade angrepp.

De teorier som använts i denna uppsats har varit effektiva för att identifiera, klassificera och förklara dessa angrepp. Hoffmans teori har varit centralt för att förstå hur hybridkrigföring kombinerar reguljära och irreguljära metoder och har bidragit till en grundläggande förståelse om vad hybridkrigföring är, medan The Hybridity Blizzard Model har möjliggjort en nyanserad klassificering av hybridhotens (o)synlighet, komplexitet och samverkan. Suchkovs modell har konkretiserat medel och metoderna samt gett en tydlig ram för att identifiera deras möjliga tillämpning mot Sverige.

Valet att fokusera på typfall innebar att analysen blev djupare, men något selektiv. Det kan inte uteslutas att andra angrepp eller metoder också varit relevanta att undersöka vilket innebär att resultatet inte är fullt generaliserbart, men eftersom studien är teorikonsumerande var inte det heller syftet. De teorier och det teoretiska ramverk som skapats har varit kärnfullt för att synliggöra angreppen och skapa en förståelse för dessa. Materialet har bestått av öppna källor som exempelvis rapporter från SÄPO, FOI, MUST och MPF samt artiklar från SVT vilket innebär att viss information kan ha undanhållits av sekretessskäl. Fördelen med detta är dock att källorna är fullt spårbara, vilket har bidragit till undersökningens validitet.

Avgränsningarna i denna uppsats möjliggjorde djupare analyser av respektive händelse. Det fanns dock relativt lite information om misstänkta hybridangrepp mellan 2014–2016, därav hade avgränsningarna tidsmässigt kunnat avsmalnas mer. Samtidigt finns det en poäng med att inte bara undersöka Sverige, utan bredda perspektivet av undersökningen till hela Norden. Detta för att kunna generalisera mer och kunna öka uppsatsens tillämpbarhet på en större

⁹¹ H. Gunneriusson. Hybrid warfare and deniability as understood by the military. *Polish Political Science Yearbook*. 48: 2 (2019).

⁹² K. Ljungkvist. The Military-Strategic Rationality of Hybrid Warfare: Everyday Total Defence under Strategic Non-Peace in the Case of Sweden. *European Journal of International Security*. 9 (2024).

⁹³ P. A. Mattson. Russian military thinking – A new generation of warfare. *Journal on Baltic Security*. Vol 1. Issue 1. (2015).

geografisk kontext, samtidigt som man hade kunnat se mönster och dra lärdomar från de andra länderna i och med de nordiska försvarssamarbeten som pågått under en längre tid.

13.1 Resultatets betydelse för officersyrket

Att förstå hybridkrigföringens medel, metoder och effekter är centralt för en officer i en tid där hybridkrigföring blivit en del av den nya normalbilden. Som officer i Försvarsmakten måste det finnas en vilja att identifiera, klassificera och bestämma var dessa hot kommer ifrån och vilken effekt det har på vår verksamhet, samhället i stort och de individer som ingår i samhället. Resultatet av denna uppsats visar på behovet av att anpassa vår yrkesutövning för att klara komplexiteten som hybridkrigföringen medför. Vidare krävs det att dagens officerare fortsätter vara innovativa och bidrar med förmågor, taktiker och strategier för att identifiera, fastställa och motverka angrepp som faller inom ramen för hybridkrigföring.

14 Vidare forskning

För att bygga vidare på denna studie hade det varit intressant att bibehålla det teoretiska ramverket men utöka det geografiska området och genomföra en jämförande studie mellan de nordiska länderna Sverige, Finland, Danmark och Norge mot de baltiska länderna Estland, Lettland och Litauen för att skapa en mer nyanserad bild av regionala variationer i hybridhot. Genom detta skulle forskningen kunna bidra till en förståelse för hur hybridkrigföring påverkar Östersjöregionen som helhet.

15 Källförteckning

- Airaksinen, K. Gps-bortfall i luften: En ny vardag för Europas piloter. *SVT*. (4/5 2024) <https://www.svt.se/nyheter/inrikes/gps-bortfall-i-luften-en-ny-vardag-for-europas-piloter> (Hämtad 21 apr. -25)
- Boréus, K. Bergström, G. *Textens mening och makt*. Fjärde Upplagan. (Studentlitteratur, 2018).
- Dansarie, M. Teknisk utveckling och Hybridkrigföring. *Kungliga krigsvetenskapsakademien*. Bilaga 3, (2020).
- Ekberg Skog, H. Teknikstrul hos flera samhällsaktörer. *SVT*. (19/2 2024) <https://www.svt.se/nyheter/inrikes/tekniska-storningar-pa-flera-hall> (Hämtad 16 apr. -25)
- Esaiasson M.fl (2015). *Metodpraktikan*. Wolters Kluwer, Femte upplagan.
- FOI. *Om GNSS*. (2021) <https://www.foi.se/kurser/gnss---satellitnavigeringssystem/om-gnss.html> (Hämtad 16 apr. -25)
- Granlund, J. Jönsson, O. 60 Hybridattacker mot Europa - spåren pekar mot Ryssland. *SVT*. (12/3 2025) <https://www.svt.se/nyheter/inrikes/60-hybridattacker-mot-europa-sporen-pekar-mot-ryssland> (Hämtad 13 mar. -25)
- Grill Pettersson, M. It-attackerna mot Sverige – här är kontot som tar på sig ansvaret. *SVT*. (14/2 2023) <https://www.svt.se/nyheter/inrikes/en-rad-it-attacker-mot-sverige-har-ar-kontot-som-tar-pa-sig-ansvaret> (Hämtad 18 apr. -25)
- Gunneriusson, H. Hybrid warfare and deniability as understood by the military. *Polish Political Science Yearbook*. 48: 2 (2019).
- Hoffman, F. *Conflict in the 21st Century: The Rise of Hybrid Wars*. (Potomac Institute for Policy Studies, 2007).
- Jonsson, O. *The russian understanding of war – Blurring the lines between war and peace*. (Georgetown University Press, 2019).
- Kustbevakningen. *Sveriges territorialhav och ekonomiska zon*. (u.å.). <https://www.kustbevakningen.se/bilder-och-fakta/sveriges-territorialhav-och-ekonomiska-zon/> (Hämtad 13 mar. -25)
- Lindvall, E. Detta vet vi: Kabelbrotten i Östersjön. *SVT*. (21/2 2025) <https://www.svt.se/nyheter/inrikes/detta-vet-vi-kabelbrotten-i-ostersjon> (Hämtad 16 apr. -25)
- Ljungkvist, K. The Military-Strategic Rationality of Hybrid Warfare: Everyday Total Defence under Strategic Non-Peace in the Case of Sweden. *European Journal of International Security*. 9. (2024).
- Mattson, P. A. Russian military thinking – A new generation of warfare. *Journal on Baltic Security*. Vol 1. Issue 1. (2015).

Suchkov, M. A. *Whose hybrid warfare? How 'the hybrid warfare' concept shapes Russian discourse, military, and political practice, Small wars & Insurgencies*, (Routledge, 2021).

MPF. *Ordlista*.(u.å.). <https://mpf.se/hjalpmedel/ordlista> (Hämtad 16 apr. -25)

MSB. *Handbok i kommunal krisberedskap 4. Riskkatalog*. (2022).

<https://rib.msb.se/filer/pdf/30061.pdf> (Hämtad 16 apr. -25)

Nielsen, E. Sabotage mot kopplingsstation i Emmaboda – hundratals blev utan ström. *SVT*. (3/4 2025). <https://www.svt.se/nyheter/lokalt/smaland/sabotage-mot-kraftstation-i-emmaboda> (Hämtad 16 apr. -25)

Ranstorp, M. Ahlerup, L. *LVU-kampanjen*. (Försvarshögskolan, MPF, 2023).

Renman, F. Sandborg, L. Sabotage mot master – detta har hänt. *SVT*. (20/5 2016) <https://www.svt.se/nyheter/lokalt/vast/haglareadmasten-rasade-detta-har-hant> (Hämtad 16 apr. -25)

Ritzén, S. Sverige drabbat av stor GPS-störning. *SVT*. (3/1 2024) <https://www.svt.se/nyheter/inrikes/sverige-drabbat-i-storsta-gps-sabotaget-i-ostersjon> (Hämtad 13 mar. -25)

Säkerhetspolisen. *Årsredovisning 2020*. (2021).

Säkerhetspolisen. *Årsredovisning 2021*. (2022).

Säkerhetspolisen. *Årsredovisning 2022*. (2023).

Säkerhetspolisen. *Årsredovisning 2024/2025*. (2025).

Svenonius, O. Olsson, S. Michélsen Forsgren, M. Dungel, E. och Jarlsbo, M. *Sa någon valfusk? Informationsmiljön på sociala medier i samband med valrörelsen 2022*. (FOI-R--5429--SE. Stockholm: Totalförsvarets forskningsinstitut, 2023).

TT. Misstänkt sabotage mot telestation i Växjö. *SVT*. (3/12 2024) <https://www.svt.se/nyheter/lokalt/smaland/misstankt-sabotage-mot-telestation-i-vaxjo> (Hämtad 16 apr. -25)

Wahlund, I. Efter hotet om hackerattack – flera sajter drabbade av problem. *SVT*. (19/2 2023) <https://www.svt.se/nyheter/inrikes/efter-hotet-om-hackerattack-flera-webbsajter-nere> (Hämtad 17 apr. -25)

Weissman, M. m.fl. *Hybrid Warfare – Security And Symmetric Conflict in International Relations*. (I.B TAURIS Bloomsbury Publishing, 2021).

Widegren, P. Störningar i GPS-system allt vanligare – påverkar flyg över Östersjön. *SVT*. (21/1 2025) <https://www.svt.se/nyheter/lokalt/ost/storningar-i-gps-system-allt-vanligare-paverkar-flyg-over-ostersjon> (Hämtad 16 apr. -25)

Widegren, P. Utredning om misstänkt vattensabotage på Gotland läggs ned. *SVT*. (14/4 2025)
<https://www.svt.se/nyheter/lokalt/ost/utredning-om-misstankt-vattensabotage-pa-gotland-laggs-ned> (Hämtad 16 apr. -25)

Wiseman, J. *GPSJAM*. (u.å.).
<https://gpsjam.org/?lat=62.01934&lon=15.31820&z=3.5&date=2023-12-26> (Hämtad 16 apr. -25)