



Försvvarshögskolan

Självständigt arbete (30 hp)

Författare		Program/Kurs
Johan Dahlman		HOP SA 2026
Handledare		Antal ord: 9999
Arash Heydarian Pashakhanlou		Kurskod
		2UK045
<h3>Svensk cyberavskräckning inom Nato?</h3> <p><i>En inramningsanalys av de militärstrategiska implikationerna</i></p>		
<p>ABSTRACT: This thesis investigates how Sweden and Nato frame the cyber domain and what implications these frames can have for the strategic manoeuvre of Sweden as a new member. The study applies van Hulst and Yanows dynamic framing theory to an analysis of key policy papers and doctrines of Sweden and Nato. The analysis shows that Swedish frames are characterized by normative stability and societal resilience while Nato, on a higher level, frames the cyber domain as a military strategic tool for operations. These differences create a tension between normative prudence and operational freedom of action. The thesis argues that this difference is structural rather than temporary and demonstrates how strategic culture illuminates small-state alliance behaviour and shapes the opportunities for Swedish cyber deterrence within Nato. These findings contribute to the understanding of strategic planning within Nato's cyber defence.</p>		
<p>Nyckelord: Militärstrategi, Framinganalys, Sverige, Nato, Cyberdomänen</p>		

Innehåll

1	INLEDNING OCH PROBLEM.....	3
1.1	SYFTE.....	4
1.2	FORSKNINGSÖVERSIKT – CYBERDOMÄNEN, NATO OCH SVERIGE.....	4
1.2.1	<i>Forskningslucka och vetenskapligt bidrag</i>	7
1.3	DISPOSITION.....	7
2	TEORI OCH METOD.....	8
2.1	INRAMNING SOM TEORI.....	8
2.1.1	<i>Dynamisk inramning</i>	9
2.2	INRAMNING SOM METOD.....	9
2.2.1	<i>Meningsskapande</i>	10
2.2.2	<i>Välja, namnge och kategorisera</i>	10
2.2.3	<i>Berättande</i>	10
2.2.4	<i>Operationalisering</i>	11
2.3	VAL AV FALL OCH KÄLLMATERIAL.....	12
2.3.1	<i>Källmaterial</i>	12
2.4	METODOLOGISK REFLEXIVITET.....	13
2.4.1	<i>Etiska överväganden och självreflexivitet</i>	14
3	ANALYS.....	15
3.1	SVENSK INRAMNING.....	15
3.1.1	<i>Meningsskapande</i>	15
3.1.2	<i>Välja, namnge och kategorisera</i>	16
3.1.3	<i>Berättande</i>	18
3.2	NATOS INRAMNING.....	19
3.2.1	<i>Meningsskapande</i>	19
3.2.2	<i>Välja, namnge och kategorisera</i>	21
3.2.3	<i>Berättande</i>	22
3.3	RESULTAT AV ANALYS – RAMAR I RELATION.....	23
4	AVSLUTNING.....	24
4.1	DISKUSSION.....	24
4.2	SLUTSATSER.....	26
4.3	METODOLOGISK REFLEKTION.....	26
4.4	UPPSATSENS INOM- OCH UTOMVETENSKAPLIGA BIDRAG.....	27
4.5	FÖRSLAG FÖR VIDARE FORSKNING.....	28
5	REFERENSER.....	29

1 Inledning och problem

Cyberdomänens växande betydelse som arena för staters säkerhet, försvar och krigshandlingar sätter internationella relationer i ny kontext. En ökad militarisering i kombination med cyberkriminalitet gör att länder tvingas sätta upp strategier för att hantera den ständigt ökande hotbilden (Oluyemi 2024). Sveriges positionspapper för appliceringen av internationell rätt i cyberdomänen (Regeringskansliet 2022) är Sveriges officiella ställningstagande när det gäller synen på cyberdomänen. Här lyfter Sverige fram det folkrättsliga perspektivet vilande på *Tallinnmanualen* (Schmitt & NATO Cooperative Cyber Defence Centre of Excellence 2017) och FN-stadgan och därmed Sveriges internationella positionering med ett meningsskapande om regelbaserad ordning och normativ stabilitet.

Natos cyberstrategi, däremot, betonar vikten av militär förmåga som ett medel för den kollektiva säkerheten. Även om Nato liksom Sverige är noggranna med att poängtera rättsstatsprinciper när det kommer till cyberdomänen så handlar det strategiska ställningstagandet i Nato mer om en allomfattande ansats med multidoräna operationer som strategiska medel och operativa verktyg vilket ger en potentiell spänning mellan en defensiv förhållning och en strategiskt offensiv sådan. Genom att djupare analysera hur Sverige och Nato beskriver problemen med cyberdomänen och lösningarna på problemen kan denna spänning studeras.

Då Sverige betonar en regelbaserad ordning och normstyrd stabilitet i sin syn på cyberdomänen och Nato i ökande grad framhåller militär förmåga och operativ integration skapar dessa förhållningssätt både ett inom- och utomvetenskapligt problem. De två perspektiven bygger på olika antaganden om hot, ansvar och strategiska mål. När Sverige nu har blivit medlem i Nato uppstår en oklarhet kring hur dessa ramar förhåller sig till varandra och vad den skillnaden innebär för Sveriges strategiska handlingsutrymme. Genom en analys av hur respektive aktör ramar in cyberdomänen ger det en ökad förståelse för hur det svenska bidraget kan se ut i relation till handlingsutrymmet. Cyberdomänen är därför inte enbart en fråga om internationell rätt eller säkerhetspolitik, utan berör den militära professionens praktiska handlingsutrymme. För krigsvetenskapen aktualiseras frågor om hur cyberdomänen påverkar möjligheten att skapa operativa effekter i multidoränaoperationer.

1.1 Syfte

Syftet med uppsatsen är att undersöka hur Sverige och Nato ramar in cyberdomänen. Genom en dynamisk framinganalys av Sveriges respektive Natos cyberstrategi kan samspelet eller konflikten mellan en regelbaserad normbundenhet och militärstrategisk anpassningsförmåga problematiseras. För att nå syftet har nedan forskningsfråga formulerats:

Hur ramar Sverige och Nato in cyberdomänen på strategisk nivå och vilka militärstrategiska implikationer följer av dessa skillnader?

1.2 Forskningsöversikt – Cyberdomänen, Nato och Sverige

Forskningsöversikten tar sin utgångspunkt i cyber som en plats för militära operationer och de utmaningar och möjligheter som följer med det. Vidare görs en forskningsöverblick över svensk syn på cyberdomänen och Natos följt av en jämförelse dem emellan som leder fram till forskningsluckan och uppsatsens bidrag till forskningsläget.

Det finns forskning kring begreppet cyber och dess framväxt där en del hävdar att de framväxande hoten som uppstått beror på att det från början inte fanns en säkerhetsdimension när internet designades och således inga tankar om den senare utvecklingen mot en militär domän (Libicki 2009:3; Robinson et al. 2015; Whyte & Mazanec 2019:11). Detta är motsägelsefullt då internet kan sägas ha ”fötts” ur den amerikanska militärens forskningscentra (ARPA) som en del av grundforskningen under kalla kriget. Det fanns dock ingen tanke då om att denna domän senare skulle militariseras (Russell 2001). Forskning visar kritik till hur utarbetandet av militärstrategier med cyberelement fungerar i praktiken. Ett exempel är avskräckning med cyber som medel.

En del forskning hävdar att oförutsägbarheten som finns inbyggd i vapnets karaktär gör att avskräckning inte kan uppnås på samma sätt som exempelvis med kärnvapen (Libicki 2009) medan annan forskning hävdar att en cyberattack som militärt vapen, åtminstone hitintills, inte kan uppnå en sådan effekt att det skulle få så stora politiska konsekvenser att det skulle aktivera ett kollektivt försvar likt Natos artikel fem (Lindsay 2013; Fitton 2016; Buchanan 2021). Debatten rymmer också en skepsis mot cybervapnets förmåga att i en strategi kunna utgöra ett tvångsmedel då det oftast handlar om att degradera tekniska system som senare går att återställa

(Lindsay & Gartzke 2019) samtidigt som det finns stora osäkerheter om det aktuella vapnet har tillräcklig förmåga att slå mot ett fientligt nätverk och få den avsedda effekten (Brandon et al. 2018:4). Det finns även en diskussion om relevansen i att utveckla en cyberstrategi. Strategin bör i sådana fall acceptera cyberdomänen ungefär som en marin strategi måste acceptera marindomänen, det vill säga i terrängen och miljön så finns det inte bara militär maktövning utan även viktig civil trafik, regler och att en generell aktörshänsyn behöver tas (Hoffman 2019).

När det kommer till det regelbaserade internationella systemet, den svenska normativa hållningen, och cyberdomänen finns det mycket forskning. För att öka förståelsen för tolkning av normer på området tillsatte Nato CCD COE (Nato Cooperative Cyber Defence Center of Excellence) en oberoende internationell grupp med akademiska jurister som tillsammans utvecklade *Tallinnmanualen*. Det är viktigt att påpeka att manualen är expertgruppens syn, inte CCDCOE eller Natos syn. Det är heller inte medlemsländernas syn. Medlemsländerna väljer själva hur de använder manualen (Schmitt & NATO Cooperative Cyber Defence Centre of Excellence 2017). Flera forskare poängterar domänens omognad, att det finns för få prejudikat, och kan ibland vara oense om den regelbaserade tolkningen. Forskningen är till exempel oense om den amerikansk-israeliska cyberattacken mot Irans urananrikningsanläggningar, även kallad STUXNET, skall ses som en våldshandling eller inte (Ramírez & García-Segura 2017:252; Dörmann u.å.).

Natos syn på cyberdomänen har utvecklats mycket de senaste åren. Vid toppmötet i Wales 2014 beslutades att FN-stadgan även gäller för cyber och att det kollektiva försvaret även omfattar denna domän (Nordatlantiska rådet 2014). Två år senare erkände Nato cyberdomänen som en egen domän likt övriga domäner, en plats där alliansen behöver försvaras, och där den nya domänen måste integreras i den operativa planeringen precis som vilken domän som helst (Nordatlantiska rådet 2016). Den nyare hållningen passar väl in i en mer offensiv ram som USA är en varm anhängare av då landet ogärna vill sätta upp regler som skapar ett ofördelaktigt läge gentemot konkurrerande stormakter (Singer 2014:186) och i praktiken innebärande att amerikansk militär närvaro måste finnas i motståndarens virtuella terräng (Nakasone 2019). Detta utgör ett exempel på den mer expansiva synen på cyberdomänen. I kontrast till Nakasone menar Jeppe T Jacobsen (2021) att Nato bör ta en mer defensiv roll i cyberdomänen då det finns en inbyggd ovilja från medlemsstaterna att dela underrättelser och cyberverktyg vilket krävs

för en offensiv förmåga. Marios Efthymiopoulos (2019) menar istället att Nato behöver ta ett ledarskap i utvecklingen av cyberförsvaret genom att kombinera militär strategi med marknadsdriven innovation. Här finns en intressant spänning mellan en unilateral offensiv dominans, kollektiv normförankrad försiktighet och innovationsbaserad expansion, tre konkurrerande logiker för hur Nato bör agera i den nya framväxande operationsmiljön som nu även Sverige är en del av.

Forskningsläget avseende cyberdomänen och Sverige handlar ofta om cybersäkerhet och totalförsvaret och mindre om defensiva och offensiva cyberoperationer även om det exempelvis finns forskning kring cyber som strategiskt instrument. Gazmend Huskaj och Esmiralda Moradian (2018) argumenterar för att Sveriges cyberstrategi, särskilt inom området cyberavskräckning, präglas av en återhållsam och delvis outvecklad attityd. Författarna identifierar bland annat avsaknaden av en tydlig doktrin för vedergällning, oklara beslutsvägar och en begränsad trovärdighet i Sveriges cyberförsvarshållning. I forskning flera år senare finns också empiriskt stöd för en fortsatt avsaknad av statlig styrning på området (Andreasson et al. 2024) där det bygger på enskilda medarbetares skicklighet eller djupare förståelse hos myndighetschefer snarare än ett systematiskt statligt ansvar. Forskning visar också på ett svenskt totalförsvaret som saknar motståndskraft mot hybrida hot i den digitala sektorn som ligger under tröskelvärdet för ett väpnat angrepp (Berg & Pettersson 2022) vilket i förlängningen kan skapa utmaningar för den holistiska cyberavskräckningen i Nato. Det finns också nyare forskning som visar på en framväxande diskussion i Sverige om att utveckla offensiva cyberförmågor som kan stödja ledningskrigföring och operationskonst, inte bara IT-säkerhet (Huskaj & Axelsson 2023).

I denna uppsats kommer definitionen av cyberdomänen utgå från Natodoktrin, fritt översatt, och lyder:

Den globala domän som består av alla sammankopplade kommunikationer, informationsteknologi och andra elektroniska system, nätverk och ingående data. Detta inkluderar det som är separerat eller oberoende som processar, lagrar eller transiterar data (Nato 2020).

1.2.1 Forskningslucka och vetenskapligt bidrag

Även om Nato fortfarande lyfter fram vikten av regelupplevnad och förutsägbarhet när det gäller cyberdomänen så finns det här en tydlig förskjutning mot mer militarisering och operativ förmåga som sätter den svenska positioneringen i en mer återhållsam ram. Sveriges Natointräde är så nytt att det kan vara svårt att idag veta vilken roll Sverige kommer att ta i alliansen. Även om alliansinträdet i sig självt är en omfattande strategisk omsvängning som saknar motstycke i modern tid (Westberg 2023:13) så kan det finnas militärstrategiska hinder för Sverige att anta den mer expansiva synen med offensiva operationer i cyberdomänen. Här finns en forskningslucka avseende hur Sveriges strategiska positionering i cyberdomänen förstås och analyseras i relation till Natos utvecklade syn på cyberavskräckning, särskilt mot bakgrund av strategisk kultur samt utrikes- och säkerhetspolitisk orientering. Denna forskningslucka adresseras genom denna uppsats i en dynamisk framinganalys av relevanta strategiska policydokument från Sverige och Nato vilket gör den här studien unik i sitt slag.

1.3 Disposition

Efter denna inledning följer ett kapitel som omfattar uppsatsens teoretiska ram och metod som utgår från van Hulst och Yanows teoribildning. Sen följer ett analyskapitel som omfattar analys av den insamlade empirin och en jämförelse mellan hur Sverige respektive Nato ramar in problem och lösningar samt de framtagna dynamiska ramarna för respektive aktör. Slutligen kommer ett kapitel som hanterar uppsatsens diskussion, slutsatser, förslag för vidare forskning och innebörd för professionen.

2 Teori och metod

Detta kapitel presenterar uppsatsens teoretiska ramverk och metod. Studien utgår från *framing* som analytisk ansats, vilken i fortsättningen benämns inramning och används synonymt med det engelska begreppet. Den teoretiska utgångspunkten hämtas från van Hulst och Yanows syn på inramning som en dynamisk och kontextuell process av meningsskapande (van Hulst & Yanow 2016). Kapitlet redogör översiktligt för teorins ursprung och vidareutveckling följt av en metodologisk operationalisering anpassad för analys av svenska och Nato-relaterade policy- och doktrindokument. Avslutningsvis presenteras det empiriska materialet samt en metodologisk och forskningsetisk reflektion.

2.1 Inramning som teori

Ursprunget i teorin grundas i Erving Goffmans idéer om att knyta ihop ett brett spektrum av till synes osammanhängande aktiviteter till ett och samma ramverk (Jerolmack et al. 2024). Goffman (1974, p. 310) ger själv ett exempel från *San Fransisco Chronicle* om hur verkligheten beror på inramningen:

”...this guy is lying face down on Powell St., with traffic backed up for blocks. A little old lady climbs down from a stalled cabled car and begins giving him artificial respiration – whereupon he swivels his head and says: “Look lady, I don’t know what game you are playing, but I’m trying to fix this cable!”

Exemplet ovan visar enligt Goffman på ett ”ramfel” genom att en person bygger upp ett scenario med hjälp av information som kan tolkas på olika sätt men missar delar av kontexten. Han menar att det är ett exempel på hur tvetydig verkligheten kan vara och att det inte går att få någon ordning på informationen utan att sätta den inom en ram (Miller & Sardais 2013).

Robert M Entman ger vidare en övergripande beskrivning av inramning som ett sätt att analysera text och att välja ut de delar som är den upplevda verkligheten med utgångspunkt i att texten inte är neutral utan att den försöker rama in ett problem och sen också hitta lösningen på problemet. Tyngdpunkten ligger här på vad som framträder i texten och vad som väljs ut (Entman 1993). Den teoretiska modellen har utvecklats ytterligare och använts inom olika

forskningsfält, exempelvis statsvetenskap och organisationsteori (Schön & Rein 1994; Klemsdal & Clegg 2022). Benford och Snows definition av inramningar utgår mer från att i tolkningen göra en kodning av objekt, situationer, erfarenheter och sekvenser (Benford & Snow u.å.) medan exempelvis William Gamson argumenterar för att ramarna inte bara är den aggregerade koden av individuella viljor och uppfattningar utan resultatet av en förhandling som lett fram till en enad syn (Nikolayenko 2019; Gamson u.å.:111). I det teoretiska ramverket som används för denna studie finns tydliga spår av både Schön och Rein och Goffman men också från exempelvis Benford & Snow (van Hulst & Yanow 2016).

2.1.1 Dynamisk inramning

Schön och Rein har utvecklat inramningsteorin i en riktning som gör den mer anpassad för studier av politik och policyprocesser. De vill överbrygga klyftan mellan teori och praktik genom att utmana beslutsfattare att reflektera över genom vilken ram ett grundantagande kommer ifrån, exempelvis i fråga om vård eller kriminalitet. Genom att medvetandegöra de olika ramarna istället för att söka en objektiv sanning så menar de att politiska kontroverser kan förstås och hanteras bättre (Schön & Rein 1994). van Hulst och Yanow har utvecklat Schön och Reins teori ytterligare. Istället för att se ramarna som objekt och något aktörer har så betonar de istället ramarna som en interaktion, process och meningsskapande i stunden (van Hulst & Yanow 2016:93). Då både Benford och Snow och Schön och Rein har en mer statisk syn på ramar så lämpar sig van Hulst och Yanows teori bättre för att tolka dynamiska policydokument genom ett tydligare fokus på processen (van Hulst & Yanow 2016:104). Genom denna teoretiska modell kan dynamiken mellan den svenska återhållsamma hållningen kring cyberdomänen och den mer expansiva i Nato förstås och gör denna teori lämplig för denna studie.

2.2 Inramning som metod

van Hulst och Janows modell för analys utgår från tre distinkta handlingar (van Hulst & Yanow 2016:97). De direktöversätts till *meningsskapande*, *välja/namnge/kategorisera* och *berättande*. Dessa tre kategorier syftar till att rama in potentiellt dynamiska karaktärer på politiska handlingar. I denna uppsats avser det även att rama in militärstrategiska val som bygger på politiska inramningar vilket återspeglas i valet av källmaterialet. Nedan följer en mer utförlig beskrivning av kategorierna.

2.2.1 Meningsskapande

Meningsskapande är en process som utgår från att aktörer konstruerar en mening i en kontext som de själva är en del av. I en värld av osäkerheter återkommer oftast aktörer, implicit eller explicit, tillbaka till Erving Goffmans grundfråga ”*What is it that’s going on here?*” (Goffman 1974:8; van Hulst & Yanow 2016:97). Genom att aktörer kan omsätta en problematisk situation till en problembeskrivning kan de skapa mening av en situation som till en början ser helt meningslös ut (Schön 1983:40). Genom att använda erfarenheter, förväntningar och värderingar i formuleringen av problemet kan en situation förstås och en modell för handling tas fram. Handlingar är intersubjektiva men samtidigt ofta utan en medveten reflektion vilket i sig kan skapa politiska kontroverser som kan bli svårhanterliga då de utgår från en egen förståelse av världen snarare än instrumentella värden (van Hulst & Yanow 2016:97).

2.2.2 Välja, namnge och kategorisera

Genom att tillskriva något någonting, att *namnge* det, så skapas ett perspektiv. Detta perspektiv ger automatiskt ett *val*. Valet innebär att någonting hamnar i strålkastarljuset och något annat utelämnas. Detta fenomen är typiskt för politiska handlingar och beslutsfattare generellt (van Hulst & Yanow 2016:99). Genom att tillskriva problemet en benämning så kan det göra problemet mer begripligt. Oftast används metaforer för att göra det enklare för mottagare i samma socio-politiska område och kultur att förstå problemet på samma sätt. Genom att *kategorisera* och redogöra för ”det här” och ”inte det där” så kan dikotomier skapas. Kategorierna kan vara explicita eller underförstådda. Dessa tre handlingar tillsammans fungerar som tre centrala inramningsverktyg och möjliggör handlingsalternativ för beslutsfattare (van Hulst & Yanow 2016:99).

2.2.3 Berättande

Denna kategori handlar om att binda ihop meningsskapande och namngivna kategorier till en sammanhängande berättelse. Genom att sätta mening till en situation dras kategorin mer till att skapa ett narrativ snarare än att beskriva en logisk följd av argument för ett visst ställningstagande (van Hulst & Yanow 2016:100). Genom berättelserna som består av namn, kategorier och metaforer kan en aktör förklara för en lyssnare eller läsare vad det är ”som har hänt” (Schön & Rein 1994). På det sättet skapar berättelsen en begriplig helhet genom att skildra situationens början, dess utveckling från något normalt till något problematiskt och slutligen genom att antyda lösningar eller ett möjligt slut (van Hulst & Yanow 2016:100).

2.2.4 Operationalisering

Den teoretiska modellen framtagen av van Hulst och Yanow utgör ramverket och operationaliseras enligt design i bild 1. Både teori och metod lämpar sig väl för att tolka policydokument från Sverige och Nato rörande cyberdomänen och kommer att rama in likheter och skillnader. Då analysen är processtyrd kommer iterationer främst att göras här men påverkar alla kapitel i uppsatsen.

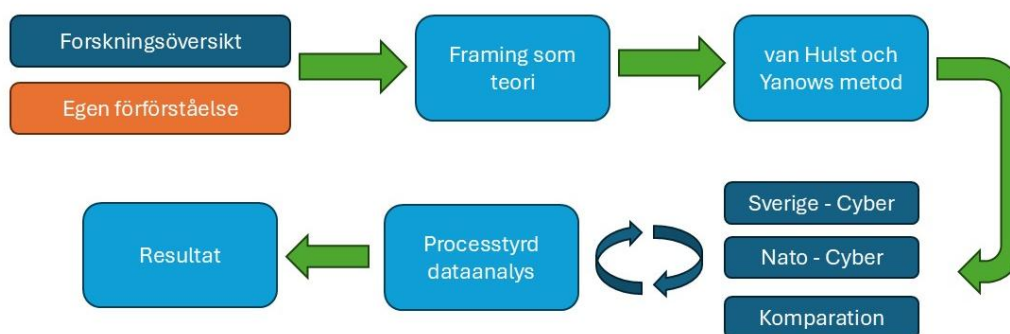


Bild 1. Operationalisering av teori, metod och verktyg för analys. Författarens bild.

För att omsätta van Hulst och Yanows teori till ett analysverktyg behöver processbeskrivningen av kategorierna översättas till relevanta frågeställningar utgående från uppsatsens problembeskrivning i kapitel ett. Operationaliseringen följer teorins fokus på process och politiska förståelse för hur policyvärldar skapas genom att gå från frågan *VAD?* till *HUR?* Dessa frågeställningar framgår av tabellen nedan:

Analysverktyg			
Kategorier	Processbeskrivning	Analytiskt fokus	Frågor till källmaterialet
<i>Meningsskapande</i>	Aktörer tolkar en situation genom att försöka förstå <i>vad som pågår</i> och <i>vad som är problemet</i> baserat på erfarenheter och värderingar (van Hulst & Yanow 2016:97).	Problemdefinition Osäkerheter Ansvar Normer Handlingsutrymme	Hur beskrivs problemen i cyberdomänen och hur framställs den centrala utmaningen?
<i>Välja, namnge och kategorisera</i>	Aktörer beslutar <i>vad</i> som ska uppmärksammas, ger detta <i>namn</i> (ofta med metaforer) och <i>kategoriserar</i> dem för att	Begrepp Metaforer Dikotomier Ansvarsfördelning Makt	Vilka aspekter av cyberdomänen lyfts fram eller tonas ner?

	forma hur världen framstår (van Hulst & Yanow 2016:99).		Hur namnges hot, aktörer och förmågor och hur kategoriseras de?
<i>Berättande</i>	De namngivna enheterna och kategorierna binds ihop till en berättelse (narrativ) som förklarar hur situationen ser ut och hur lösningen ser ut (van Hulst & Yanow 2016:100).	Narrativ logik Vägval Lösningar Möjliga framtider	Hur beskrivs domänens berättelse – från problem till lösning? Vilka strategiska handlingsalternativ finns tillgängliga?

Tabell 1. Metodologiskt verktyg baserad på inramningsteorin (van Hulst & Yanow 2016).

2.3 Val av fall och källmaterial

Val av fall utgörs av Sverige och Nato. Det kan i någon mening verka märkligt att jämföra en nationalstat och en militärallians som denna nationalstat ingår i. Det är dock relevant för studien att titta på Sverige som aktör och Nato som aktör även om Nato som aktör är en kompromiss av 32 länder och Sverige som aktör är ett resultat av en politisk förhandling som omfattar mer än militärstrategi och försvars- och säkerhetspolitik. Representationen är en ögonblicksbild vid ett givet tillfälle, tidsstämpeln för respektive dokument. Den viktigaste strategiska skillnaden för Sverige i denna period är Natomedlemskapet och för Sverige och Nato det försämrade säkerhetspolitiska läget med den fullständiga ryska invasionen av Ukraina 2022. Empirin kan här skilja sig åt vilket kan försvåra analysen men det kan också vara en styrka att se hur den strategiska övergången ramar in.

2.3.1 Källmaterial

Urvalet av källmaterial är målstyrt och utgör typiska fall som syftar till att exemplifiera ett perspektiv som är av intresse (Bryman 2021:497). Empirin utgörs av primärkällor som är fastställda av Sveriges regering, Försvarsmakten och Nato vilket stärker materialets äkthet och samtidighet (Esaiasson et al. 2024:138). När det gäller oberoende och tendens så förväntas dokumenten innehålla både narrativ och en säkerhetspolitisk och militärstrategisk dimension som både riktar sig inåt och utåt. Skärningspunkten militärstrategi, säkerhetsstrategi och försvarsplanering i förhållande till cyberdomänen behöver här stå i fokus och inte cybersäkerhet i allmänhet eller samhällets allmänna resiliens inom cyberområdet.

För svensk del utgörs urvalet av två policydokument från Regeringskansliet (Regeringskansliet 2022; 2024) samt en doktrin. Syftet med urvalet av de två policydokumenten utgår från den

officiella svenska synen på cyberdomänen som för uppsatsens skrivande är aktuell (Regeringskansliet 2022) samt den senaste totalförsvarspropositionen som beskriver hur det militära förmågebyggandet skall fortsätta i nästa försvarsbeslutsperiod. Det tredje svenska dokumentet utgörs av Militärstrategisk doktrin (Försvarmakten 2022). Syftet med valet av detta dokument är att det är det svenska huvuddokumentet doktrinärt och rör sig i gränslandet mellan att omsätta en politisk vilja till hur det militära maktmedlet skall stödja denna.

Vad gäller Nato så kommer också två policydokument samt en doktrin att studeras. Det första policydokumentet är ”*Nato Strategic Concept*” (Nato 2022) som togs fram som ett resultat efter ett kraftigt försämrat säkerhetsläge i Europa sen Rysslands fullskaliga invasion av Ukraina. Syftet med valet av detta dokument är att det ramar in det övergripande problemet för Nato och hur Nato avser lösa detta. Det andra policydokumentet är ”*Cyber Defence*” vilket är Natos generella beskrivning av cyberdomänen och hur den behöver hanteras (Nato 2024). Detta dokument är från 2024 och är således mer aktuellt. Det tredje Natodokumentet för analys är Natos doktrin för cyberoperationer (Nato 2020). Även om den inte är en huvuddoktrin så beskriver den hur Nato avser lösa den operativa verksamheten i cyberdomänen.

Sammanfattningsvis är policydokument från Regeringskansliet och Nordatlantiska rådet (NAC) i kombination med svensk- och Natodoktrin en empiri som både är institutionellt auktoritativa och representerar aktörernas officiella meningsskapande i cyberdomänen.

2.4 Metodologisk reflexivitet

I en tolkande inramningsanalys står inte forskaren utanför forskningsobjektet och observerar. I stället är de analytiska val som görs, empiri och komparationer en del av kunskapsproduktionen. Synen på verkligheten är en konstruktion eller rekonstruktion snarare än en avbild (Davidsson & Patel 2019:40). I den meningen handlar inte reflexivitet om att eliminera subjektivitet utan mer om att synliggöra hur forskaren förhåller sig till och rör sig mellan forskningsläge, teori, metod och empiri.

I en inramningsanalys är intertextualitet också central eftersom policydokument skapar mening genom att anknyta till andra texter, normer och tidigare positioner. Det handlar inte enbart om att identifiera vedertagna fraser som återanvänds utan mer om att identifiera meningsskapande

(Schwartz-Shea & Yanow 2012:86). Särskilt i cyberdomänen, där rättsliga och militära normer ännu inte är stabila, fungerar referenser till tidigare dokument som ett sätt att rama in legitimitet. Reflexiviteten här handlar om att medvetet uppmärksamma hur dokumenten hämtar auktoritet från andra texter och hur detta påverkar tolkningen av dessa.

Den avslutande metodologiska reflektionen handlar om inramning som teori och metod. Det finns kritik mot metoden som hävdar att den är inkonsekvent, vag och där operationalisering ofta blir för spretig (Entman 1993; Scheufele 1999). En kritik består i att analysen av ramar ofta stannar vid själva ramen i stället för att analysera dynamiken i meningsskapandet, alltså att analysverktyget blir för statiskt. Björnehed och Eriksson (2018) visar på att inramning får störst analytisk kraft när den är dynamisk och fokus riktas mot processerna där ramarna skapas. I denna uppsats används inramning på just detta sätt, som ett verktyg för att analysera meningsskapande i rörelse, snarare än ett statiskt kodningsschema. Metodvalet ska på det sättet stödja den vetenskapsfilosofiska grunden om att det finns ett problem som behöver förstås djupare, inte genom att sätta upp variabler, utan att genom att låta kunskapen själv komma ut ur det studerade fältet (Schwartz-Shea & Yanow 2012:18).

2.4.1 Etiska överväganden och självreflexivitet

Uppsatsen är professionsnära vilket innebär att forskaren intar en form av ”insiderposition” i relation till forskningsfältet. Eftersom forskningsobjektet tillika är forskarens egna arbetsområde är det särskilt viktigt med integritet, reflexivitet och medvetenhet kring den ”dubbla rollen” och makten över den egna forskningen (Drake & Heath 2010; Bryman 2021:191). Förförståelsen inom området kommer också att påverka tolkning av texter, val av empiri och ansättning av teori mot metodologiska verktyg. Personliga erfarenheter kan på det sättet samtidigt vara en styrka men också skapa kognitiva fallgropar som forskaren inte själv tänker på (Drake & Heath 2010). För att hantera denna risk har empirival till del utgjorts av dokument som forskaren inte är helt inläst på vilket ”stör” den egna förförståelsen. En annan åtgärd för att minska risken för att tillskriva empirin egna ramar är att analysen görs utan kodning vilket ökar trovärdigheten men ställer samtidigt högre krav på transparens genom att kontinuerligt väva samman empiri och teori. Metodansatsen skiljer sig här från exempelvis tematisk analys som i högre grad är instrumentell och kodningsbaserad. Inga personuppgifter har hanterats i denna uppsats.

3 Analys

Analysen är uppdelad i tre steg. Det första är en inramningsanalys av empirin kring Sverige. Det andra rör empirin kring Nato och det sista steget är en sammanfattande jämförelse. Varje inramningsanalys inleds med en kort sammanfattning vilket utgör den dynamiska ramen enligt van Hulst och Yanows teori.

3.1 Svensk inramning

Sammanfattningsvis framträder en dynamisk inramning av cyberdomänen där hotet är reellt men manifesterat genom hybrida hot och gråzonsaktiviteter. Även om cyber erkänns som ett militärt medel i den väpnade striden så handlar mycket om att öka resiliensen i det uppkopplade samhället mot de hot som finns i alla konfliktnivåer. Inramningen betonar internationell rätt, statligt ansvar och normativ stabilitet som grund för ordning i en domän som präglas av osäkerheter. Cyberoperationer erkänns som ett militärt verktyg men ramas i huvudsak in som ett sätt att skydda nationell suveränitet snarare än som ett självständigt militärstrategiskt verktyg.

3.1.1 Meningsskapande

Inom den första underkategorin från analysmodellen ställs en analytisk fråga:

Hur beskrivs problemen i cyberdomänen och hur framställs den centrala utmaningen?

Problembeskrivningen utgår från ett framväxande hot från stater eller statsunderstödda aktörer. Dessa utgörs framförallt av Ryssland men även Kina och Iran tas upp (Regeringskansliet 2024:15). Detta utgör fonden för beskrivningen av cyberdomänen där nya hot växer fram som behöver hanteras med nya metoder. En del av problemformuleringen utgår från efterdyningar av digitaliseringen som skapar nya sårbarheter för samhällsviktig verksamhet (Försvarmakten 2022:32; Regeringskansliet 2024:17). Tillsammans utgör denna meningsskapande beskrivning en modell av hur världen kan förstås och hur aktörer kan nyttja den till sin egen fördel (van Hulst & Yanow 2016:98).

Sverige poängterar att cyberdomänen behöver regleras i en internationell kontext. I den svenska positioneringen framgår exempelvis hur cyberangrepp både kan utgöra en våldshandling men också väpnat angrepp om det uppnår en tillräcklig effekt enligt vad som i internationell rätt kan hävdas som ett väpnat angrepp (Regeringskansliet 2022:4). Den svenska hållningen beskriver också de specifika riskerna som finns med cyberoperationer och det som benämns kollateral

skada. Detta lyfts fram genom det faktum att infrastrukturen i cyberrymden ofta delas mellan militära och civila entiteter (Regeringskansliet 2022:7). Det här skulle kunna vara ett exempel på det ”normativa språnget” som Schön och Rein beskriver (van Hulst & Yanow 2016:98). Genom att tydliggöra vad Sverige anser är ett övertramp mot ett lands suveränitet skapar det en norm i en tidigare oreglerad och kaosartad värld, att gå från hur ett förhållande *är* till hur det *borde vara*. Här beskrivs en grundkonflikt mellan demokratiska stater som vill upprätthålla den regelbaserade ordningen och revisionistiska stater som anser sig ha rätt till egna intressesfärer (Regeringskansliet 2024:16).

Kriget i Ukraina sätter prägeln på hur Sverige skapar mening i cyberdomänen. Här beskrivs hur den förödelse och de påfrestningar som kriget innebär för Ukraina skulle kunna innebära för Sverige och dess allierade (Regeringskansliet 2024:12). Cyberdomänen tas särskilt upp, liksom långräckviddig bekämpning och drönare, som en ny företeelse på krigsskådeplatsen som framtidens totalförsvaret behöver kunna hantera (Regeringskansliet 2024:13). Här inramas cyberdomänen främst i en kontext av cybersäkerhet, totalförsvaret och samhällsresiliens. Det kan delvis förstås genom att ryska icke-militära och hybrida resurser kan verka mot Sverige och dess närområde parallellt med det pågående kriget i Ukraina, denna hotbild finns både kognitivt, geografiskt och tidsmässigt närmare men det förstås även genom rapporter från Myndigheten för samhällsskydd och beredskap som visar på sårbarheter i samhällsviktiga funktioner (Regeringskansliet 2024:148).

3.1.2 Välja, namnge och kategorisera

Inom denna underkategori ställs enligt analysmodellen två frågor enligt nedan:

Vilka aspekter av cyberdomänen lyfts fram eller tonas ner?

Hur namnges hot, aktörer och förmågor och hur kategoriseras de?

När det gäller **aspekter** av cyberdomänen så ramas dessa in i de tre dokumenten på ett tydligt sätt. Cyber utgör ofta ett prefix i begrepp som används för att beskriva fenomen med allt från cyberattacker till cybersäkerhet, cyberrymden och cyberdomänen. Cyberdomänen beskrivs exempelvis omfatta allt från elektroniska kommunikationstjänster, styr- och reglersystem, digitala informationssystem till den data som lagras och hanteras i dessa system (Försvarsmakten 2022:55). Det empiriska materialet visar också konsekvent på hur Sverige beskriver cyber i termer av hybridhot, säkerhet, påverkan och sårbarhet (Försvarsmakten 2022:32; Regeringskansliet 2022:2; 2024:146) snarare än krigföring eller maktutövning. På det

viset ramas cyberdomänen in som ett problemområde snarare än ett strategiskt verktyg. Genom denna namngivning och kategorisering väljs cyber som självständig militärstrategisk domän bort till förmån för en förståelse av cyber som ett mer samhälleligt problemområde. Här skapas en logisk grund att senare kunna agera inom (van Hulst & Yanow 2016:99).

När det kommer till den andra analytiska frågan, att namnge *hot*, *aktörer* och *förmågor*, finns här en bred generell beskrivning men också intressanta iakttagelser. Även om cyberoperationer beskrivs som en naturlig del av krigföringen likt andra stridskrafter och domäner finns ingen utförligare beskrivning av hur dessa kan utgöra en del av alliansens offensiva verktygslåda eller som en nationell självständig stridskraft likt armén. Cyberoperationer beskrivs istället som ett verktyg för att skapa handlingsfrihet åt nationen och ytterst dess suveränitet (Regeringskansliet 2024:150). Statliga och privata aktörers brister när det gäller att upprätta cybersäkerhet i en teknikutveckling som går med raska steg lyfts fram som en allvarlig sårbarhet (Regeringskansliet 2024:148). Det skulle i sig kunna vara ett intressant utvecklingsområde för Sverige, att bidra både till Nato och inte minst EU som lyfts fram som en viktig aktör för att hantera växande utmaningar mot hybridkrig och cyberhot (Regeringskansliet 2024:35, 149). Genom att beskriva cyberoperationer främst som ett hot mot samhället och staten utgör denna inramning också nyckeln för vad som ligger i det politiskt legitima handlingsutrymmet.

I de svenska dokumenten finns tydliga *kategorier* och samtidigt en del tvetydigheter. Empirin beskriver tydligt vilket *ansvar* som åligger stater både när det gäller relationer till andra stater men även statens ansvar att hantera cyberrelaterade aktiviteter som sker på det egna territoriet riktat mot andra stater (Regeringskansliet 2022:2). I korta drag kan man säga att det ansvar som åligger stater i den fysiska världen också gäller för den digitala världen. I hotbeskrivning finns en växande oro för stater som lägger avsevärda resurser på att bygga upp offensiva förmågor inom cyberdomänen för att kunna genomföra cyberattacker (Försvarsmakten 2022:29). Här återfinns en tudelning mellan demokratier som försöker upprätthålla en regelbaserad världsordning och auktoritära stater som utnyttjar svagheter i det öppna samhället till sin egen fördel. I beskrivningen finns cyberaktiviteter som en del av hybrida hot eller hybridkrigföring som behöver hanteras inom ramen för ett starkt, resilient totalförsvar som klarar av att stå emot cyberangrepp mot samhällsviktig verksamhet (Regeringskansliet 2024:18).

En intressant iakttagelse i totalförsvarspropositionen är att cyberdomänen är upptaget som ett eget kapitel och inte beskrivs under kapitlet ”Militärt försvar” (Regeringskansliet 2024:4). Det visar å ena sidan på att regeringen ser mer holistiskt på cyber som fenomen men också att regeringen i första hand ser cyberdomänen som en del av hybridhotet som behöver hanteras med ökad cybersäkerhet snarare än en del av det militära försvaret. Detta visar sammantaget hur svensk policy namnger, kategoriserar samt väljer bort delar av cyberdomänen och det som ramas än handlar främst om skydd, resiliens och upprätthållande av normer snarare än militär maktutövning.

3.1.3 Berättande

Inom denna underkategori ställs också två frågor:

Hur beskrivs domänens berättelse – från problem till lösning?

Vilka strategiska handlingsalternativ finns tillgängliga?

Berättelsen är inte bara ett sätt att rama in problemet och lösningen på detta utan även hur framträdande fenomen binds ihop för att skapa en helhet. Denna helhet blir ofta en stereotypisk skildring av ett fenomen eller en situation och saknar ofta precision (van Hulst & Yanow 2016:101). I den svenska berättelsen om att gå från problem till lösning i cyberdomänen finns en korrelation mellan normativ stabilitet i mellanstatliga relationer och hur stater bör bete sig när det kommer till regelupplevning i cyberdomänen. Här menar regeringen att genom att skapa en bättre förståelse för hur denna regelupplevning tillämpas så kan en säkrare, stabilare, mer tillgänglig och fredligare cybermiljö skapas (Regeringskansliet 2022). Upprätthållandet av den regelbaserade världsordningen är central för Sverige (Försvarsmakten 2022:35; Regeringskansliet 2024:21) och blir naturligt också en del av narrativet kring cyberdomänen.

Det hybrida hotet eller hybridkrigföring, där cyberangrepp är en del, beskrivs som en utmärkande del av vår tid. Här berättas hur den tekniska utvecklingen i samhället har skapat nya sårbarheter och angreppspunkter som ställer högre krav på ett skydd och försvar mot aktörer som kan utnyttja detta (Regeringskansliet 2024:19). En beskrivning finns också om vad en eskalering inom ramen för en hybridaktivitet kan syfta till, både ytterst ett väpnat angrepp men också genom att tillskansa sig egna fördelar inom ramen för en egen nationell strategi (Försvarsmakten 2022:31). Genom denna inramning av cyber som en del av en ny framväxande hotmiljö är det också logiskt att cybersäkerhet och cyberförsvar kopplas ihop som ”ömsesidigt förstärkande verksamheter” (Regeringskansliet 2024:146). Genom denna beskrivning så finns

det goda politiska argument för att stärka den allmänna cybersäkerheten i samhället och cyberförsvaret för att kunna möta en ny typ av hotbild som kommer med det nya digitala samhället. På liknande sätt beskrivs cyberförmågorna i Försvarsmakten som en förutsättning för att stridskrafterna uppnå krigföringsförmåga (Försvarsmakten 2022:56). Detta blir en verklighetsbeskrivning som är trovärdig och skapar möjligheter att agera inom (van Hulst & Yanow 2016:101).

I analyssteget *strategiska handlingsalternativ* kan man ur materialet hitta en del vägval. Genom definitioner av defensiva och offensiva cyberoperationer som utgår från att antingen att försvara egna system eller att förvägra motståndaren att använda sina system för angrepp mot Sverige finns här en tydlig defensiv karaktär i berättelsen. Genom att bygga dessa förmågor skall en ökad tröskeleffekt och avskräckning kunna uppnås både nationellt och om som en del av Natos kollektiva försvar (Regeringskansliet 2024:151). Här finns en indikation på vilka strategiska valmöjligheter som finns för Sverige. EU och Nato beskrivs som de viktigaste samarbetsorganisationerna när det kommer till cyberförsvaret. De svenska nationella intressena skall vara vägledande samtidigt som onödig duplicering av strukturer och resurser skall undvikas (Regeringskansliet 2024:151). Här kan man se en svensk vilja att verka mer resurseffektiv.

3.2 Natos inramning

Den dynamiska inramningen av cyberdomänen i Nato beskrivs i källmaterialet som en kognitiv och pragmatisk resa där starten är en slutsats om att informationen i ledningsstödsystemen behöver skyddas mot logiska angrepp från antagonister. Från denna syn på cyber har utvecklingen gått genom upprättandet av CCDCOE i Tallinn, framtagande av dokument som stöd för tolkning av vad som kan anses utgöra en våldshandling eller väpnat angrepp, till att vara en integrerad del av den operativa militära verksamheten. I Natos inramning finns också en hotbedömning som gör att man ser cyber som en strategisk nödvändighet då brister i cybersäkerheten hos ett enskilt medlemsland kan påverka handlingsfriheten för hela alliansen i operationsmiljön. Genom att göra cybereffekter till ett möjligt handlingsalternativ i den operativa planeringen ges också defensiva och offensiva cyberoperationer legitimitet.

3.2.1 Meningsskapande

Hur beskrivs problemen i cyberdomänen och hur framställs den centrala utmaningen?

De utmaningar som Nato står inför när det kommer till cyberdomänen är del av en större utmaning med en värld som är mer oförutsägbar där internationella normer ifrågasätts. Genom hybridaktiviteter, där cyberdomänen är framträdande, kan statliga och icke-statliga aktörer destabilisera alliansen genom att utnyttja sårbarheter i samhällsviktiga funktioner och militära system (Nato 2020:1; 2022:3; 2024:3). Även om de senaste åren har varit explosionsartade så finns det en längre historik i formuleringar kring cyber som begrepp. Cyberdomänen har en framväxt i Nato från det att begreppet kom upp på den politiska agendan 2002 i termer av att skydda och försvara digital information till att 2024 innehålla flera olika centra både för cyberförsvar men också samordning av defensiv och offensiv cyberstrid i en egen militär domän (Nato 2024:10). Denna utveckling ger en logik bakom definieringen av denna nya domän som inte bara handlar om att bli konfronterad med en ny verklighet utan också agera, att skapa mening i den (van Hulst & Yanow 2016:98).

Sårbarheterna som uppkommer på grund av det moderna samhället lyfts fram. Här beskrivs en ökande grad av sårbarhet mot nationer som är mer beroende av en fungerande cybermiljö och samtidigt ett system- av systemtänkande där en bristande cybersäkerhet hos ett medlemslands ledningsstödsystem kan bli en akilleshäla för alliansen som helhet (Nato 2020:62). Här indikerar analysen utmaningar för Nato som kan uppstå då alliansen behöver ägna mer tid och resurser åt att skapa samhällelig resiliens mot cyberattacker då nationernas väpnade styrkor i olika grad är beroende av dessa funktioner för att kunna utveckla effekter i alla domäner.

Den framväxande cyberdomänen och den allmänt låga kunskapsnivån kring hur den skall hanteras lyfts fram. Genom att säga att cyberförsvar handlar lika mycket om teknik som det handlar om människor (Nato 2024:5) sätter Nato tonen för att mer resurser behöver sättas för utbildning, träning och övning. Domänens omogenhet tar sig också uttryck i en tydlig centralisering av beslut kring när cybereffekter får användas. Cybereffekterna styrs på samma sätt som andra förmågor genom att nordatlantiska rådet godkänner operationsplaner med ingående insatsregler men effekterna som sådana finns inte på den operativa nivån utan samordnas vid det strategiska högkvarteret och det som benämns som ”*Cyber Operations Center*” (Nato 2020:11). Här kan ett dilemma uppstå då Nato också lyfter fram risker med att cyberoperationer kan leda till kollaterala effekter utanför operationsområdet samtidigt som man är rädd för att lämna hela spelplanen åt antagonisterna. Med denna inramning så måste cyberdomänen försvaras.

Detta meningsskapande ger förståelse av cyberdomänen som en strategisk nödvändighet i Natos kollektiva försvar där integration, resiliens och handlingsfrihet prioriteras framför återhållsamhet och en mer konservativ syn på militär maktutövning.

3.2.2 Välja, namnge och kategorisera

Vilka aspekter av cyberdomänen lyfts fram eller tonas ner?

Hur namnges hot, aktörer och förmågor och hur kategoriseras de?

I aktörsbeskrivningen lyfter Nato upp ett antal viktigare **aktörer** i cyberdomänen. I den strategiska beskrivningen om Nato och dess syften lyfts medlemsländernas relation byggd på individuell frihet, mänskliga rättigheter och demokrati vilande på den internationella regelbaserade ordningen som en grundsats. Här lyfts exempelvis FN-stadgan och det Nordatlantiska fördraget upp. I den strategiska hotmiljön så beskrivs hoten som globala och teknologiskt sammanbundna med de tydligaste antagonisterna i Ryssland, Kina och den globala terrorismen. Kina lyfts särskilt fram som en aktör i cyberdomänen främst när det handlar om industrisektorn, teknologi, kritisk infrastruktur och strategiska produkter (Nato 2022:5).

När det kommer till **aspekter** som **lyfts fram** och **tonas ner** ser Nato cyberdomänen som en del av informationsmiljön och därmed en ram som försvårar urskiljning av den strategiska, operativa och taktiska nivån från varandra. Av den anledningen krävs koordinering och synkronisering av de effekter som får påverkan i informationsmiljön genom hela konfliktskalan (Nato 2020:1). Hotaktörerna i cyberdomänen beskrivs som statliga och icke-statliga aktörer, kriminella och insiders där statliga aktörer är de som främst utgör ett hot mot alliansen. Genom att vissa stater har utvecklat avancerade förmågor att verka i cyberdomänen genom offensiva och defensiva cyberoperationer (Nato 2020:6) så finns det en tydlig logik för Nato att bygga upp ett försvar mot detta. Genom detta logiska resonemang och sortering (van Hulst & Yanow 2016:99) så blir det lättare att argumentera för hur det konceptuella ramverket för cyberförsvaret skall utformas. Detta är Natos sätt att ordna världen, inte spegla den.

Nato definierar viktiga begrepp doktrinärt. Genom denna inramning så blir det väldigt tydligt vad som väljs ut och vad som inte väljs ut samt hur kategoriseringen ger en tyngdpunkt åt militära operationer och hur dessa skall lyckas. De begrepp som definieras är direktöversatt *cyberrymden (cyberdomänen), cyberoperationer, defensiva cyberoperationer, offensiva*

cyberoperationer, cybersäkerhet och uppdragsförsäkringen (Nato 2020:4). Här finns tydliga vägval vad cyber i Nato handlar om, antingen att skapa effekter i cyberdomänen för att kunna påverka en motståndare eller att skapa en gynnsam utgångspunkt för egna förband att bibehålla en krigföringsförmåga och därigenom fortsatt kunna genomföra militära operationer.

Sammanfattningsvis innebär denna namngivning och kategorisering att cyberdomänen i Nato ramas in som ett militärstrategiskt verktyg för kollektiv handlingsfrihet, där militära operationer, säkerhet och kontroll prioriteras.

3.2.3 Berättande

Hur beskrivs domänens berättelse – från problem till lösning?

Vilka strategiska handlingsalternativ finns tillgängliga?

I det strategiska konceptet, **berättelsen**, lyfter Nato fram att den nationella och kollektiva resiliensen är kritisk för genomförandet av grundläggande uppgifter och understryker ansträngningarna att skydda medlemsländernas samhälle och värderingar. Vidare beskriver Nato visionärt att målet är att leva i en värld där suveränitet, territoriell integritet, mänskliga rättigheter och internationell rätt respekteras. Här finns ingen plats för aggressioner, tvångsmedel och subversion (Nato 2022:2). För att lyckas uppnå denna målsättning krävs en grundlagd militär förmåga som bygger på avskräckning och försvar. Dessa element bygger på en lämplig kombination av nukleära, konventionella och missilförsvarskapaciteter kompletterade av förmågor inom rymd och cyber (Nato 2022:6). Genom denna inramning finns det en tydlig beskrivning av hur cyberdomänen skall bidra till alliansens yttersta målsättningar genom att utgöra en del av det kollektiva försvaret och avskräckningen.

Ovan beskrivning är grunden för de **strategiska handlingsalternativen** som Nato har och återspeglas i omsättningen till militära operationer. Den operativa förmågan i cyberdomänen syftar till handlingsfrihet i domänen och på det sättet göra militära operationer mer resilienta mot cyberhot. Ett nära informationsutbyte inom alliansen i alla konfliktnivåer skapar en bättre situationsförståelse som kan uppnå detta (Nato 2024:4). Förutom att de egna operationerna skall kunna bli mer resilienta skall också motståndaren påverkas genom offensiva attacker i cyberdomänen. Genom att använda cybereffekter som en del i operationsplaneringen skall dessa ingå i operationsplaner tillsammans med alla andra effekter och på så sätt skapa synergier i striden. Genom att slå mot alla delar av cyberdomänen, där motståndaren har en svag eller

oförsvarad punkt, så kan krigföringsförmågan hos motståndaren påverkas (Nato 2020:8). Här visar Nato tydligt på hur de olika delarna binds ihop till ett sammanhang genom att sätta cybereffekter i samma planerings- och beslutsprocesser som alla andra effekter i övriga domäner. Det blir ett mönster som är sammanhängande (van Hulst & Yanow 2016:100).

Det sammanhängande mönstret ovan får en törn av specifika cyberutmaningar. I beskrivningen finns det risker i cyberdomänen som de militära cheferna behöver vara väl insatta i när det handlar om operationsplanering och genomförande av operationer. Här beskrivs i synnerhet risken för att en cyberoperation får konsekvenser utanför operationsområdet samt risken för att en cyberoperation kan leda till en oväntad eskalering av den pågående konflikten (Nato 2020:25). Här uppstår ett dilemma i berättandet och logiken kring cybereffekter där beslut kring dessa ligger i det strategiska högkvarteret och inte på den operativa nivån (Nato 2020:11) vilket i sammanhanget kan försvåra en effektintegrering i en multidomän operation.

3.3 Resultat av analys – ramar i relation

Det här kapitlet har analyserat hur Sverige, respektive Nato, ramar in cyberdomänen. Analysen visar att även om det finns en gemensam normativ grund, präglas de två aktörernas meningsskapande av delvis olika strategiska logiker. Den svenska logiken bygger i huvudsak på att det moderna samhällets tekniska nivå och den nya hotbilden som har växt fram kräver ett robust cyberförsvar där cybersäkerhet utgör den viktigaste komponenten. Nato lyfter också fram denna aspekt men här finns i mycket högre utsträckning cyber som ett militärt medel för att nå militärstrategiska mål.

Sverige vill bidra konstruktivt och solidariskt i Natos cyberförsvar. För Sverige är det viktigt att Nato fortsätter att utveckla cyberförmågor som både är avskräckande och kan användas i ett kollektivt försvar (Regeringskansliet 2024:151). Sammantaget visar analysen att Sveriges inramning betonar ansvar och normativ stabilitet, men att empirin i begränsad utsträckning explicit kopplar cyberförmågor till ett sammanhängande narrativ kring avskräckning.

4 Avslutning

Avslutningskapitlet inleds med en diskussion kring analysens resultat och en återkoppling till syftet med uppsatsen. Därefter följer slutsatserna av denna diskussion och ett kapitel om uppsatsen bidrag till vetenskapen samt professionen. Slutligen följer förslag för vidare forskning.

4.1 Diskussion

Syftet med denna uppsats har varit att undersöka hur Sverige och Nato ramar in cyberdomänen och vilka militärstrategiska implikationer dessa skillnader medför.

Sverige är en ny spelare i Nato och trots ett strategiskt närmande till alliansen under många år så finns det delar av anpassningen som kan ta längre tid och till del kanske aldrig bli fullständig. Edström och Westberg (2022) visar att nya Nato-medlemmar i praktiken sällan omformulerar externa värderingar utan snarare filtrerar den externa organisationens krav genom nationella hotuppfattningar och strategisk kultur. Sett i detta ljus framstår Sveriges normativa inramning av cyberdomänen inte som ett problem, utan som ett uttryck för ett välkänt småstatsmönster inom alliansen. Argumenten kring småstaters vilja att normalisera och uttrycka vikten av en regelbaserad världsordning i cyberdomänen stärks av att det flesta nordiska länder har tagit fram liknande dokument som Sverige som beskriver den egna synen på cyberdomänen och regelbaserad ordning.

van Hulst och Yanow beskriver den berättande inramningsprocessen som en förhandling som bygger på att övertyga kollektivet om hur olika ageranden kan lösa problemen (van Hulst & Yanow 2016:101). Här finns det för Sverige och Nato olika kollektiv. För Sverige är det viktigt att övertyga aktörer i totalförsvaret, exempelvis myndigheter och samhällsviktiga funktioner i näringslivet, att cyberförsvaret börjar med en robust cybersäkerhet och att alla behöver ta ansvar inom sitt eget verksamhetsområde för att lösa detta. Nato behöver övertyga ett mycket större kollektiv men behöver samtidigt bara fokusera på en del av maktinstrumentet i sin säkerhetsstrategi vilket å ena sidan ger en bredare syn att hantera terrorism och säkerhet i medelhavet och samtidigt vara avskräckande mot stormakter men å andra sidan kan fokus ligga på att utveckla militära förmågor.

Undersökningen visar att svensk strategisk kultur skulle kunna stå i vägen för en djupare alliansintegration med offensiva cyberoperationer som strategiska medel. Martin Zapfe (Zapfe 2016) visar hur den tyska strategiska kulturen sätter gränser för doktrinär implementering inom Nato. Trots att man utförde operationer i Afghanistan enligt Natos operativa doktriner så ville man inte acceptera doktrinutvecklingen i Tyskland. På ett liknande sätt visar denna studie hur Sveriges inramning av cyberdomänen präglad av normativ stabilitet, operativ återhållsamhet och samhällsresiliens kan begränsa ett fullt accepterande av offensiva cyberoperationer som ett legitimt alliansverktyg. Samtidigt finns det en debatt i Sverige om offensiva cyberoperationer som visar en pågående problematisering av den traditionellt defensiva inramningen. Cybersäkerhetsexperter som Gazmend Huskaj (Huskaj 2025) argumenterar för att en offensiv cyberstrategi behövs för avskräckning och för att skydda samhället mot destabiliserande attacker, samt att Sveriges strategi behöver utvecklas i denna riktning. I förhållande till Zapfes kulturella analys ovan illustrerar detta hur strategisk kultur inte är statisk, utan kan vara föremål för debatt, omförhandling och potentiell förändring även i frågor som rör offensiva förmågor. Sveriges Natointräde i sig kan här ses som ett exempel på strategisk omförhandling.

En ytterligare dimension av skillnaden mellan Sveriges och Natos inramningar av cyberdomänen rör frågor om samhällseliga och etiska implikationer. Cyberoperationer, särskilt offensiva sådana, skiljer sig från många andra militära medel genom sin inneboende osäkerhet och sin täta koppling till civila infrastrukturer. Eftersom militära och civila system i cyberdomänen ofta är tekniskt sammanlänkade finns en påtaglig risk för kollaterala effekter som kan slå mot samhällsviktiga funktioner även utanför det avsedda operationsområdet. Denna osäkerhet påverkar hur risk kan och bör accepteras i militärstrategisk planering. En högre riskaptit i användningen av offensiva cyberoperationer kan visserligen öka handlingsfriheten i ett militärt perspektiv, men samtidigt öka risken för oavsiktlig eskalation, svårkontrollerade spridningseffekter och påverkan på egna eller allierade system. I dagens uppkopplade samhälle kan sådana effekter i praktiken få konsekvenser som går långt utanför operationsområdet och beröra samhällselig stabilitet och legitimitet. Mot denna bakgrund kan Sveriges betoning på normativ återhållsamhet, rättslig förankring och samhällselig resiliens förstås inte enbart som ett uttryck för strategisk försiktighet, utan också som en etiskt stark hållning i en domän där gränserna mellan militärt och civilt är särskilt svårdragna. Samtidigt aktualiserar Natos mer operativa inramning ett behov av tydlig politisk styrning,

ansvarsutkrävande och riskmedvetenhet för att säkerställa att användningen av cybereffekter inte underminerar de värden och samhällsfunktioner som alliansen ytterst syftar till att skydda.

4.2 Slutsatser

Sveriges inramning av cyberdomänen präglas av normativ stabilitet, rättslig återhållsamhet och ett starkt fokus på samhällelig resiliens där effekter i cyberdomänen främst syftar till att säkra militära system, samhällsviktiga funktioner samt göra samhället motståndskraftigt.

Natos inramning betonar cyber som ett militärstrategiskt verktyg integrerat i multidoromänoperationer, med både defensiva och offensiva cybereffekter. Dessa effekter samordnas vid det militärstrategiska högkvarteret men nyttjas av operativa chefer i operationsplaner precis som effekter i andra domäner.

De militärstrategiska implikationerna innebär att Sveriges handlingsutrymme i Nato präglas av spänningen mellan normativ återhållsamhet och operativ integration. Denna skillnad förstås genom en svensk återhållsam strategisk kultur, som visserligen kan omförhandlas, men just nu begränsar viljan till hög operativ risktagning med potentiell kollateral skada i ett oförutsägbart cyberkrig.

Denna spänning bör också förstås som strukturell snarare än tillfällig och är förenlig med ett småstatsperspektiv inom alliansen. Samtidigt påbörjades en strategisk-kulturell resa i Sverige genom Natointrädet som kan påverka synen på alliansledda offensiva cyberoperationer i framtiden.

4.3 Metodologisk reflektion

Ur ett vetenskapsteoretiskt perspektiv har valet av dynamisk inramningsanalys haft avgörande betydelse för vilka resultat som kunnat genereras i studien. Genom att analysera hur cyberdomänen görs meningsfull i policy- och doktrindokument har fokus kunnat riktas mot de underliggande antaganden, normer och narrativ som formar strategiskt handlingsutrymme snarare än mot faktiska beslut eller operativa utfall. Detta har möjliggjort en förståelse av strategi som en process av meningsskapande snarare än som en linjär relation mellan mål, medel och metod.

Detta metodval innebar samtidigt också tydliga begränsningar. Studien kan inte fastställa kausala samband mellan inramningar och konkret militärt agerande, ej heller fånga hur dessa ramar förhandlas i praktiken inom politiska eller militära beslutsprocesser. Analysen är vidare begränsad till officiella dokument och speglar därmed institutionellt sanktionerade positioner snarare än informella tolkningar eller operativ praktik. I efterhand framstår dessa begränsningar som en konsekvens av studiens tolkande ansats, där ambitionen varit att fördjupa förståelsen av hur strategiska problem definieras, snarare än att förklara hur de löses.

Sammantaget visar studien hur val av teori och metod inte enbart är ett tekniskt forskningsbeslut utan i sig formar vilken typ av kunskap som produceras. Just eftersom studien har syftat till att förstå hur Sverige respektive Nato ramar in cyberdomänen framstår en dynamisk inramningsanalys som särskilt ändamålsenlig. Inramningsanalysen har här möjliggjort en problematisering av cyberdomänen och därigenom bidragit till en djupare förståelse av de villkor under vilka svensk cyberavskräckning inom Nato kan tänkas utformas.

4.4 Uppsatsens inom- och utomvetenskapliga bidrag

Uppsatsens inomvetenskapliga bidrag tar utgångspunkt i den identifierade forskningsluckan i första kapitlet. Här kan uppsatsen bidra med en fördjupad förståelse av hur Sverige ramar in cyberdomänen i relation till Nato. En central del i detta bidrag utgår från att visa hur cyberdomänen fungerar som en spegel för djupare skillnader i strategisk kultur, där valet av problemformulering och ansvarsfördelning i praktiken avgör vilka militära handlingsalternativ som framstår som legitima.

I relation till befintlig forskning om cyberavskräckning och Natos cyberförmågor positionerar sig denna uppsats inom ett tolkande och strategiskt kulturperspektiv. Snarare än att analysera hur cyberförmågor utvecklas eller implementeras fokuserar studien på hur cyberdomänen görs strategiskt meningsfull och därmed politiskt och militärt användbar. Här handlar mycket om vad Försvarmakten och Sverige, i alliansperspektivet, kan bidra med när det kommer till att utveckla förmågor inom cyberdomänen som bidrar till alliansens avskräckning och försvar. För högre svenska officerare innebär det en tydligare bild av hur inramningen av problemet och lösningarna på detsamma skiljer sig åt hos de båda aktörerna vilket är en viktig utgångspunkt i

formandet av strategiska medel för att uppnå militära och politiska mål. Här finns det fortsättningsvis möjligheter för Sverige att justera sin problemdefinition och prioritering när det handlar om att lyfta fram aspekter för att lösa problemet. Ett ytterligare bidrag rör förmågeutveckling där Sverige, som ett tekniskt välutvecklat land med en stark försvarsindustri, har potential att bidra till såväl Nato som EU inom forskning, innovation och teknologisk utveckling kopplad till cyberdomänen.

4.5 Förslag för vidare forskning

Denna studie har fokuserat på hur cyberdomänen ramas in på strategisk och policynivå i Sverige och Nato. Genom detta angreppssätt har vissa aspekter av cyberavskräckning och strategiskt handlingsutrymme kunnat belysas, medan andra nödvändigtvis hamnat utanför studiens räckvidd. Dessa begränsningar pekar samtidigt ut flera relevanta och logiska spår för vidare forskning. En kvalitativ djupdykning som exempelvis tittar på hur Finland eller Norge ramar in cyberdomänen skulle här kunna vara intressant. Finland har militärstrategiskt gjort en liknande resa som Sverige med en lång tid av alliansfrihet till att nyligen blivit alliansmedlemmar vilket gör landet särskilt intressant. Norge skulle motsatt vara intressant att titta på då många likheter med Sverige och Finland finns men här finns i stället en lång period av Natomedlemskap och gemensam militärstrategi.

Eftersom denna studie analyserar inramningar i officiella dokument, men inte praktiskt beslutsfattande vore ett naturligt nästa steg att titta på hur synen på cyberdomänen har utvecklats globalt och parallellt i Sverige. Det skulle kunna ge en tydligare bild av vart vi är på väg i termer av militärstrategiska effekter för att nå politiska mål.

Sammantaget visar dessa forskningsspår att cyberdomänen inte enbart är en teknisk eller militär fråga, utan ett strategiskt och politiskt problem där inramning, legitimitet och handlingsutrymme fortsätter att vara centrala analytiska utgångspunkter.

Generativ AI (Chat-GPT) har använts som stöd för att förbättra läsbarheten och som bollplank under arbetets gång. Författaren har slutligen skrivit all text och tar fullt ansvar för den.

5 Referenser

- Andreasson, A., Artman, H., Brynielsson, J. & Franke, U. (2024). Cybersecurity work at Swedish administrative authorities: taking action or waiting for approval. *Cognition, Technology & Work*, 26 (4), 709–731. <https://doi.org/10.1007/s10111-024-00779-1>
- Benford, R.D. & Snow, D.A. (u.å.). Framing Processes and Social Movements: An Overview and Assessment.
- Berg, E. & Pettersson, U. (2022). Resilience and Resistance in the Digital Age: Revisiting the Threshold Effect in Total Defence. https://doi.org/10.57767/JOBS_2022_0015
- Björnehed, E. & Erikson, J. (2018). Making the most of the frame: developing the analytical potential of frame analysis. *Policy Studies*, 39 (2), 109–126. <https://doi.org/10.1080/01442872.2018.1434874>
- Brandon, V., Jensen, B.M. & Maness, B.C. (2018). *Cyber strategy: the evolving character of power and coercion*. Oxford university press.
- Bryman, A. (2021). *Samhällsvetenskapliga metoder*. Liber.
- Buchanan, B. (2021). Cyberwar Redux. I: *The Oxford handbook of cyber security*. (Oxford handbooks online Political Science). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780198800682.001.0001>
- Davidsson, B. & Patel, R. (2019). *Forskningsmetodikens grunder*. Studentlitteratur AB.
- Drake, P. & Heath, L. (2010). Thinking about ethical considerations. *Practitioner research at doctoral level*, 1, 12
- Dörmann, K. (u.å.). Applicability of the Additional Protocols to Computer Network Attacks.
- Edström, H. & Westberg, J. (2022). *Military Strategies of the New European Allies: A Comparative Study*. 1. uppl. Routledge. <https://doi.org/10.4324/9781003298052>
- Efthymiopoulos, M.P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*, 8 (1), 12. <https://doi.org/10.1186/s13731-019-0105-z>
- Entman, R.M. (1993). Framing: Toward Clarification of a Fractured Paradigm. *Journal of Communication*, 43 (4), 51–58. <https://doi.org/10.1111/j.1460-2466.1993.tb01304.x>
- Esaiasson, P., Gilljam, M., Oscarsson, H., Sundell, A., Towns, A. & Wängnerud, L. (2024). *Metodpraktikan*. Norstedts Juridik AB.
- Fitton, O. (2016). Cyber Operations and Gray Zones: Challenges for NATO. *Connections: The Quarterly Journal*, 15 (2), 109–119. <https://doi.org/10.11610/Connections.15.2.08>
- Försvarsmakten (2022). Militärstrategisk Doktrin. Försvarsmakten, FMLOG.

- Gamson, W.A. (u.å.). *Talking Politics*. Cambridge University Press.
https://books.google.com/books/about/Talking_Politics.html?hl=sv&id=mQGrGC5W6wkC [2025-11-27]
- Goffman, E. (1974). *Frame analysis: an essay on the organization of experience*. 1. Northeastern Univ. Press ed., reprint. Northeastern Univ. Press.
- Hoffman, W. (2019). Is Cyber Strategy Possible? *The Washington Quarterly*, 42 (1), 131–152. <https://doi.org/10.1080/0163660X.2019.1593665>
- van Hulst, M. & Yanow, D. (2016). From Policy “Frames” to “Framing”: Theorizing a More Dynamic, Political Approach. *The American Review of Public Administration*, 46 (1), 92–112. <https://doi.org/10.1177/0275074014533142>
- Huskaj, G. (2025). *Sverige måste svara offensivt på cyberhot. Forskning & Framsteg*. [Debattartikel]. www.fof.se [2026-01-20]
- Huskaj, G. & Axelsson, S. (2023). A Whole-of-Society Approach to Organise for Offensive Cyberspace Operations: The Case of the Smart State Sweden. *European Conference on Cyber Warfare and Security*, 22 (1), 592–602.
<https://doi.org/10.34190/eccws.22.1.1188>
- Huskaj, H. & Moradian, E. (2018). *Proceedings of the 13th International Conference on Cyber Warfare and Security: ICCWS 2018 : hosted by National Defense University, Washington DC, USA : 8-9 March 2018*. Academic Conferences and Publishing International Limited.
- Jacobsen, J.T. (2021). Cyber offense in NATO: challenges and opportunities. *International Affairs*, 97 (3), 703–720. <https://doi.org/10.1093/ia/iiab010>
- Jerolmack, C., Westberry, A. & Teo, B. (2024). Frame Analysis and Animal Studies: Erving Goffman’s Overlooked Thesis on Animal Metacommunication and Mind. *Symbolic Interaction*, 47 (4), 578–597. <https://doi.org/10.1002/symb.715>
- Klemsdal, L. & Clegg, S. (2022). Defining the work situation in organization theory: bringing Goffman back in. *Culture and Organization*, 28 (6), 471–484.
<https://doi.org/10.1080/14759551.2022.2090563>
- Libicki, M.C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation. (RAND Corporation monograph series)
- Lindsay, J.R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22 (3), 365–404. <https://doi.org/10.1080/09636412.2013.816122>

- Lindsay, J.R. & Gartzke, E. (red.) (2019). *Cross-domain deterrence: strategy in an era of complexity*. Oxford University Press. (Oxford scholarship online Political Science).
<https://doi.org/10.1093/oso/9780190908645.001.0001>
- Miller, D. & Sardais, C. (2013). How our Frames Direct Us: A Poker Experiment.
Organization Studies, 34 (9), 1381–1405. <https://doi.org/10.1177/0170840612470231>
- Nakasone, P.M. (2019). A Cyber Force for Persistent Operations. *Joint Force Quarterly*, 92 (1)
- Nato (2020). Allied Joint Doctrine for Cyberspace Operations. NATO Standardization Office (NSO).
- Nato (2022). Nato Strategic Concept 2022
- Nato (2024). Cyber Defence. <https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence> [2025-12-03]
- Nikolayenko, O. (2019). Framing and counter-framing a Peace March in Russia: the use of Twitter during a hybrid war. *Social Movement Studies*, 18 (5), 602–621.
<https://doi.org/10.1080/14742837.2019.1599852>
- Nordatlantiska rådet (2014). Wales Summit Declaration. Pressmeddelande 2014 (120).
https://www.nato.int/cps/en/natohq/official_texts_112964.htm [2025-10-16]
- Nordatlantiska rådet (2016). Warsaw Summit Declaration. Pressmeddelande 2016 (100).
https://www.nato.int/cps/en/natohq/official_texts_133169.htm [2025-10-16]
- Oluyemi, A. (2024). Militarization of Cyberspace and its Implications on National/International Security. *International Journal of Social Science Research and Review*, 7 (7), 1–16. <https://doi.org/10.47814/ijssrr.v7i7.2192>
- Ramírez, J.M. & García-Segura, L.A. (red.) (2017). *Cyberspace: Risks and Benefits for Society, Security and Development*. Springer International Publishing.
<https://doi.org/10.1007/978-3-319-54975-0>
- Regeringskansliet (2022). Swedens position paper on the application of international law in cyberspace. Positionspapper. [2025-09-11]
- Regeringskansliet (2024). Svensk totalförsvarsproposition 2025-2030. Regeringens proposition 2024/25:34.
- Robinson, M., Jones, K. & Janicke, H. (2015). Cyber warfare: Issues and challenges.
Computers & Security, 49, 70–94. <https://doi.org/10.1016/j.cose.2014.11.007>
- Russell, A.L. (2001). Ideological and Policy Origins of the Internet, 1957-1969. arXiv.
<https://doi.org/10.48550/ARXIV.CS/0109056>

- Scheufele, D. (1999). Framing as a Theory of Media Effects. *Journal of Communication*,
- Schmitt, M.N. & NATO Cooperative Cyber Defence Centre of Excellence (red.) (2017).
Tallinn manual 2.0 on the international law applicable to cyber operations. Second
edition. Cambridge University Press.
- Schwartz-Shea, P. & Yanow, D. (2012). *Interpretive research design: concepts and
processes*. Routledge. (Routledge series on interpretive methods)
- Schön, D.A. (1983). *The reflective practitioner: how professionals think in action*. Basic
Books.
- Schön, D.A. & Rein, M. (1994). *Frame reflection: toward the resolution of intractable policy
controversies*. Basic Books.
- Singer, P.W. (2014). *Cybersecurity and cyberwar: what everyone needs to know*. Friedman,
A. (red.) (Friedman, A., red.). Oxford University Press, USA. (What everyone needs
to know)
- Westberg, J. (2023). *Svenska Säkerhetsstrategier*. Studentlitteratur AB. (Från
neutralitetspolitik till ansökan om Natomedlemskap)
- Whyte, C. & Mazanec, B.M. (2019). *Understanding cyber warfare: politics, policy and
strategy*. Routledge, Taylor & Francis Group.
- Zapfe, M. (2016). Strategic Culture Shaping Allied Integration: The Bundeswehr and Joint
Operational Doctrine. *Journal of Strategic Studies*, 39 (2), 246–260.
<https://doi.org/10.1080/01402390.2015.1115044>