



Självständigt arbete (30 hp)

Författare	Program/kurs
Christelle Elm	HOP SA KrV 2025–26
Handledare	Antalet ord
Peter Bovet Emanuel	9984 (+ bilagor 902)
	Kurskod
	2UK045
<p>Från föreställning till förmåga: Hur sociotekniska föreställningar formar utvecklingen av svensk militär cyberförmåga</p> <p>From Imaginaries to Capability: How Sociotechnical Imaginaries Shape the Development of Swedish Military Cyber Capability</p>	
<p>Abstract:</p> <p>This study examines how sociotechnical imaginaries expressed in Swedish governing documents between 2017 and 2025 shape the development of cyber as a domain of warfare. Drawing on Jasanoff and Kim’s framework of sociotechnical imaginaries, the study analyses how imaginaries take shape, become embedded, encounter resistance and are extended in relation to major security policy shifts, particularly Russia’s invasion of Ukraine in 2022.</p> <p>The analysis shows that military capability development is a process in which capability is conceptually and institutionally shaped through the interaction of imaginaries, organisation and technology.</p>	

HOP SA

Change following major security shifts is selective: strategic framings are revised comprehensively, while more fundamental understandings of cyber as a domain display greater stability. Institutionalisation through governing documents enables capability development but also constrains what can be re-imagined.

The study also contributes an analytical model that shows how sociotechnical imaginaries shape the conditions under which military capability becomes thinkable, legitimate and actionable.

Nyckelord:

Cyberdomän, cyberförsvar, cyber som krigföringsdomän, militär förmågeutveckling, sociotekniska föreställningar

Innehållsförteckning

1. Inledning.....	5
1.1. Bakgrund och problemformulering.....	5
1.2. Syfte och forskningsfråga.....	6
1.3. Begreppsanvändning.....	6
1.4. Forskningsöversikt.....	6
1.5. Forskningslucka.....	9
1.6. Vetenskapligt bidrag.....	9
1.7. Studiens disposition.....	10
2. Teori.....	11
2.1. Sociotekniska föreställningar.....	11
2.2. Teoretisk reflektion.....	12
3. Metod.....	13
3.1. Metodansats.....	13
3.2. Forskningsdesign.....	13
3.3. Empiri och urval.....	14
3.4. Analysmetod.....	15
3.5. Genomförande och kodning.....	15
3.6. Forskningsetiska överväganden.....	16
4. Analys och resultat.....	17
4.1. Temaöversikt.....	17
4.2. Tema 1 – STF om egna sårbarheter och extern hotbild.....	17
4.3. Tema 2 – STF om cyberdomänen som militärt maktmedel.....	20
4.4. Tema 3 – STF om stärkt militär cyberförmåga.....	23
4.5. Sammanfattning och syntes.....	26
5. Avslutning.....	29
5.1. Resultatdiskussion.....	29
5.2. Metoddiskussion.....	32

HOP SA

5.3.	Slutsatser	33
5.4.	Teoretiskt bidrag och implikationer	35
5.5.	Praktiska, samhälleliga och etiska implikationer	37
5.6.	Studiens styrkor och begränsningar	37
5.7.	Framtida forskning	38
5.8.	Redovisning av generativ AI i skrivprocessen	39
6.	Litteraturförteckning	40
	Bilaga 1 – Dokumentöversikt	43
	Bilaga 2 – Kodningsindikatorer	44
	Bilaga 3 – Kodningsexempel tematisk analys	45

HOP SA

1. Inledning

1.1. Bakgrund och problemformulering

Under de senaste decennierna har cyberdomänen kommit att betraktas som en naturlig del av modern krigföring. Samtidigt har utvecklingen av domänen präglats av både höga förväntningar och betydande osäkerhet kring domänens militära roll och effekt. Fortfarande saknas en samlad syn på hur cyberdomänen ska definieras och användas (Robinson et al. 2015:74). Detta medför att politiska och militära beslut om cyberdomänen fattas under osäkerhet. Oenigheten kring cyberdomänens användning och effekt skapar därav utrymme för att föreställningar med osäker empirisk grund får stor betydelse för vilken förmåga som faktiskt utvecklas.

Forskning om framväxande områden visar att de inte enbart formas av teknisk utveckling eller organisatoriska strukturer, utan även av aktörers föreställningar om hur området bör förstås och utvecklas. Jasanoff och Kim (2009:120; 2015a:4) benämner dessa som sociotekniska föreställningar (STF), vilka utgör kollektiva visioner om önskvärda framtider som styr politiska val samt institutionell och teknisk utveckling. Genom sådana föreställningar formas inte bara tekniska lösningar utan även normerande bilder av organisatoriska strukturer och inriktning av förmågan.

Militär cyberförmåga utgör ett tydligt exempel på denna dynamik. Föreställningar om cyberdomänens framtida roll formades långt innan tekniken möjliggjorde operativa tillämpningar. Redan i början av 1980-talet beskrev Gibson (1984) i romanen, *Neuromancer* en dystopisk värld där människa och teknik smält samman till ett globalt nätverk benämnt ”cyberspace”. Succesivt har föreställningar om domänen fått militärt och politiskt genomslag och cyberdomänen beskrivs idag som en fullvärdig krigföringsdomän av många försvarsmakter (Smeets 2022:1; Kerttunen 2023:21).

Samtidigt har Rysslands fullskaliga invasion av Ukraina 2022 utmanat tidigare antaganden om cyberoperationers roll i modern krigföring (Kerr 2023). Det aktualiserar frågor om domänens strategiska betydelse, operativa användning och organisatoriska utformning.

Mot denna bakgrund är det särskilt relevant att studera hur svenska politiska och militära aktörers STF om cyberdomänen formas, stabiliseras och omformas i relation till säkerhetspolitiska förändringar samt hur dessa påverkar utvecklingen av svensk militär

HOP SA

cyberförmåga. För detta ändamål används Jasanoffs (2015b:3–15) ramverk om STF vilken möjliggör analys av STF:s uppkomst, institutionalisering, motstånd och utvidgning.

1.2. Syfte och forskningsfråga

Mot bakgrund av den begreppsliga osäkerhet som präglar cyberdomänen syftar studien till att fördjupa förståelsen för hur STF formuleras i svenska styrande dokument, hur de förändras över tid och hur de påverkar utvecklingen av svensk militär cyberförmåga.

Studiens forskningsfråga formuleras därför enligt följande:

Hur formar sociotekniska föreställningar, uttryckta i svenska styrande dokument mellan 2017–2025, utvecklingen av svensk militär cyberförmåga?

Ovan forskningsfråga har brutits ned i tre delfrågor:

1. Vilka centrala STF om cyberdomänen uttrycks i dokumenten och hur legitimeras dessa?
2. Hur påverkas dessa föreställningar av omvälvande säkerhetspolitiska förändringar såsom Rysslands invasion av Ukraina 2022?
3. Hur påverkar STF förutsättningarna för militär förmågeutveckling?

1.3. Begreppsanvändning

I studien används begreppet *cyberdomän* genomgående och avser militär cyberförmåga eller cyberdomänen som krigföringsdomän, om inget annat anges. *Militär förmågeutveckling* förstås som en socioteknisk process där teknik, organisatoriska strukturer, kompetens, metoder och styrande dokument samutvecklas i syfte att möjliggöra militär verkan i cyberdomänen.

1.4. Forskningsöversikt

Utifrån studiens fokus på STF och militär förmågeutveckling inriktas forskningsöversikten på fyra sammanhängande forskningsfält: cyberdomänen som krigföringsförmåga, föreställningar och STF, militär förmågeutveckling samt doktrin och doktrinutveckling.

1.4.1. Cyberdomänen som krigföringsdomän

Forskning om cyberdomänen har under en lång tid präglats av oenighet kring domänens roll och funktion i krigföring. Forskningssamhället har diskuterat huruvida cyberförmågan innebär

HOP SA

en revolution eller om dess betydelse i den moderna krigföringen är överdriven (Gartzke 2013:42; Limnell & Rid 2014:166–168; Boeke & Broeders 2018:74).

Även bland de forskare som betraktar cyberdomänen som militärt relevant, råder oenighet om dess huvudsakliga funktion – som ett medel för att skapa militära effekter eller som en resurs för underrättelseinhämtning (Boeke & Broeders 2018:74; Libicki 2021:114, 244; Smeets 2022:5). Vidare råder även oenighet kring huruvida cyberförmåga bör förstås som ett strategiskt maktmedel eller integrerad krigföringsdomän tillsammans med övriga domäner (Finlay 2018:357; Libicki 2021:112–114; Smeets 2022:3).

Dunn Caverty (2013) visar samtidigt på att cyberdomänen konstrueras genom visioner och narrativ snarare än genom etablerad operativ erfarenhet. I detta sammanhang argumenterar Hayden (2016:4) för att den politiska och militära ledningens bristande kunskap och förståelse om området bidrar till svårigheter att implementera cyberdomänen i den militära förmågepaletten. Sammantaget pekar tidigare forskning på att cyberdomänens roll formas under förhållanden präglade av osäkerhet, konkurrerande tolkningar och svag empirisk förankring.

1.4.2. Föreställningar och STF

Begreppet *föreställningar* används inom flera forskningsfält såsom samhällsvetenskap, krigsvetenskap och Science and Technology Studies (STS). Trots skillnader i hur begreppet definieras förenas forskningsfälten genom utgångspunkten att föreställningar utgör den kollektiva uppfattningen om ett fenomen, samt att föreställningar formar hur samhällen och organisationer förstår nutid och framtid (Jasanoff & Kim 2013:190; Ní Mhurchú & Shindo 2016:1; Ördén 2024:609; Zehfuss & Vaughan-Williams 2024:3; Hendriks et al. 2025:2).

STF är det forskningsfält som är mest utvecklat och Jasanoff och Kim (2009; 2015) utvecklade ramverket i syfte att möjliggöra studier kring hur kollektiva bilder om framtid, teknik och samhälle formas samt hur de stabiliseras och institutionaliseras i offentliga dokument.

Tidigare studier använder STF för att analysera föreställningar kring säkerhetspolitik och framväxande förmågor såsom AI samt energiomställning (Jasanoff & Kim 2013; Malmio 2023; Sartori & Bocca 2023; Ølgaard 2025). Såvitt känt har tidigare forskning inte explicit analyserat hur STF om militär cyberförmåga påverkar områdets utveckling i relation till säkerhetspolitiska förändringar.

HOP SA

1.4.3. Förmågeutveckling

Liwång et al. (2023:406–407) beskriver forskningen om militär förmågeutveckling som omfattande men präglad av divergerande kunskapstraditioner. En inriktning betonar teknikens centrala roll medan andra betonar hur förmåga formas i samproduktion mellan teknik och samhälle. Inom denna tradition har sociotekniska perspektiv utvecklats där förmåga förstås som ett resultat av samspelet mellan tekniska, organisatoriska och normativa faktorer (Mumford 2006; Baxter & Sommerville 2011).

Dessa forskningsfält har även kompletterats med studier som belyser kognitiva dimensioner av militär förmågeutveckling. Modig och Andersson (2022) visar hur delade mentala modeller och konfirmationsbias påverkar innovationsprocesser och förändringsbenägenhet i en svensk kontext. Vidare har forskning belyst hur politisk styrning och strategiska prioriteringar påverkar utvecklingen av militära förmågor (Farrell & Terrif 2002:266; Jakobsen & Ringsmose 2018).

Sammantaget präglas forskningsområdet av ett brett perspektiv på militär förmågeutveckling. Samtidigt visar Liwång et al. (2023:414) att det finns få studier som integrerar dessa perspektiv i ett sammanhållet teoretiskt ramverk. Mot denna bakgrund efterlyses tvärvetenskapliga studier vilket utgör utgångspunkten för denna studie.

1.4.4. Doktrin och doktrinutveckling

Doktriner och styrande dokument utgör centrala verktyg för att omsätta strategiska styrningar och föreställningar till praktisk verksamhet. Samtidigt menar Høiback (2011:879) att forskningen på området är relativt underutvecklat. Han framhåller vidare att doktriner inte enbart fungerar som vägledning utan som styrdokument vilka syftar till att leda, utbilda eller förändra befintlig organisation och förmåga samt att de representerar en institutionell, snarare än individuell militär kunskap (Høiback 2011:879, 887).

Flera studier kompletterar denna bild genom att visa att doktrin och andra styrande dokument aldrig uppstår i ett vakuum, utan formas av de aktörer som inriktar, formulerar och implementerar dem (Kier 1995; Farrell & Terrif 2002:3; Nisser 2025:33). Även Høiback (2011:885–886) understryker att doktrinutveckling är en social process där kultur, institutioner och professionell kunskap utgör centrala påverkansfaktorer.

I den svenska kontexten har studier visat att Försvarsmakten saknar en fullt institutionaliserad process för doktrinutveckling (Thunholm & Palmgren 2017:21; Thunholm et al. 2018:32).

HOP SA

Avsaknaden av formaliserade metoder kan innebära att normer, traditioner och personliga uppfattningar kan få stort genomslag. Doktrin och andra styrande dokument utgör därmed den arena där STF om cyberdomänen, framtida hot och behov av förmågeutveckling möts, stabiliseras och omsätts i praktik.

1.5. Forskningslucka

Sammantaget visar tidigare forskning att cyberdomänen präglas av begreppslig osäkerhet, konkurrerande tolkningar samt att militär förmågeutveckling formas i ett samspel mellan tekniska, organisatoriska, politiska och kognitiva faktorer.

Trots ett omfattande forskningsläge saknas studier som analyserar hur STF om cyberdomänen formuleras, institutionaliseras och förändras i styrande dokument samt hur dessa påverkas av säkerhetspolitiska omdaningar såsom Rysslands invasion av Ukraina. Vidare har tidigare forskning i begränsad utsträckning undersökt hur STF omsätts i doktrin och styrande dokument och därigenom formar förutsättningarna för militär förmågeutveckling.

Mot denna bakgrund identifieras ett behov av tvärvetenskapliga studier som integrerar STF och förmågeutveckling. Genom att använda Jasanoffs och Kims (2015a:4) ramverk om STF adresserar denna studie denna lucka genom att analysera hur sådana föreställningar uttrycks och förändras i styrande dokument mellan 2017-2025 samt hur de påverkar utvecklingen av svensk militär cyberförmåga.

1.6. Vetenskapligt bidrag

Mot bakgrund av den identifierade forskningsluckan beskrivs studiens avsedda inomvetenskapliga och utomvetenskapliga bidrag.

Inomvetenskapligt förväntas studien bidra till en fördjupad förståelsen för hur STF formar utvecklingen av nya militära förmågor. Genom att analysera cyberdomänen med utgångspunkt i STF adresserar studien den brist på tvärvetenskapliga perspektiv som tidigare forskning efterfrågat (Liwång et al. 2023).

Utomvetenskapligt förväntas studien synliggöra hur STF påverkar militär förmågeutveckling samt bidra till att beslutsfattare får en fördjupad förståelse för hur föreställningar formar

HOP SA

utvecklingen av nya förmågor. Slutsatserna kan även vara relevanta för andra framväxande domäner där liknande osäkerheter och föreställningar påverkar förmågeutvecklingen.

1.7. Studiens disposition

Kapitel 1 introducerar studiens bakgrund, problemformulering, syfte och forskningsfrågor samt positionerar studien i relation till tidigare forskning.

Kapitel 2 presenterar det teoretiska ramverket om sociotekniska föreställningar samt specificerar de fyra processer som utgör studiens teoretiska lins.

Kapitel 3 redogör för studiens metodologiska ansats, forskningsdesign, empiri och urval samt genomförande av analys.

Kapitel 4 presenterar studiens resultat och analys utifrån studiens teman.

Kapitel 5 sammanför resultaten med tidigare forskning genom diskussion samt presenterar studiens slutsatser, bidrag och vidare forskning.

HOP SA

2. Teori

Kapitlet presenterar studiens teoretiska ramverk: sociotekniska föreställningar (STF) och de ingående fyra processer som i denna studie används som teoretisk lins vid analysen. Vidare diskuteras hur ramverket tillämpas i en militär kontext.

2.1. Sociotekniska föreställningar

Jasanoff (2015a:2) menar att teknologisk utveckling ofta förstås som frikopplad från den sociala världen, som om teknologisk utveckling uppstår i ett vakuum utan ett kontinuerligt samspel med den sociala kontext som skapat och upprätthåller densamma.

Teorin om STF utvecklades för att bryta denna uppdelning och synliggöra hur teknik och samhälle formas i ett ömsesidigt förhållande samt för att fylla tomrummet mellan studier av politik, kultur samt sociotekniska system (Jasanoff 2015a:4).

Teorin vilar på idén om *samproduktion*, enligt vilken naturvetenskapliga och samhällsliga ordningar skapas tillsammans och är ömsesidigt beroende (Jasanoff 2004b:2; a:17; 2015a:17–18). Samhället kan inte fungera utan kunskap lika lite som kunskap kan existera utan ett samhälle (Jasanoff 2015a:3). Genom samproduktion undviks därmed enligt Jasanoff (2004b:3) den ensidiga förklaringslogik som tidigare präglat akademiska debatter om framtida teknologier.

Det centrala i teorin är att teknisk utveckling förstås som sammanflätad med sociala praktiker, identiteter, normer och institutioner vilka tillsammans formar kollektiva visioner om framtiden (Jasanoff 2015b:2). Studien utgår från Jasanoff och Kims (2015a:4) definition av STF vilken fritt översatt till svenska är: “kollektivt hållna, institutionellt stabiliserade och offentligt framförda visioner om önskvärda framtider, formade av gemensam förståelse om socialt liv och samhällslig ordning som kan uppnås genom, och som understöds av, vetenskapliga och teknologiska framsteg”

STF utvecklas i samspelet mellan vetenskap, politik och samhällsliga institutioner och bidrar till att stabilisera vissa utvecklingslinjer samtidigt som andra försvagas eller trängs undan. Genom processer av uppkomst, institutionalisering, motstånd och utvidgning blir föreställningar bärare av makt, normer och prioriteringar som påverkar möjligheterna till

HOP SA

förändring över tid (Jasanoff 2015a:3). STF kan därmed användas för att analysera både kontinuitet, förändring och konflikt i utvecklingen av nya förmågor.

Vidare betraktas STF som en process genom vilka föreställningar uppstår, institutionaliseras, förändras och möter motstånd, snarare än som ett statiskt uttryck av en framtidsbild (Samimian-Darash et al. 2025:542).

Vidare identifierar Jasanoff (2015b:3–16) fyra analytiska processer genom vilka STF kan analyseras och förstås:

- **Uppkomst** (origins) – hur föreställningar uppstår
- **Institutionalisering** (embedding) – hur föreställningar stabiliseras och institutionaliseras
- **Motstånd** (resistance) – hur konflikter och alternativa föreställningar utvecklas
- **Utvidgning** (extension) – hur föreställningar sprids, förändras och omformas

Studiens empiri analyseras med stöd av dessa processer och fungerar som en teoretisk lins vid tolkningen av materialet. Genom att analysera hur svenska styrdokument formulerar föreställningar om cyberdomänen kan studien synliggöra hur dessa formas och förändras, särskilt i relation till den säkerhetspolitiska omvälvningen 2022.

2.2. Teoretisk reflektion

Jasanoffs och Kims teoretiska ramverk är framtaget för att analysera hur samhällen i bred mening kopplar samman kunskap, teknik, makt och normer. I denna studie tillämpas ramverket inom en mer avgränsad militär kontext, med fokus på utvecklingen av svensk cyberförmåga. Trots tillämpning i en ny kontext har inga principiella anpassningar av ramverket bedömts nödvändiga eftersom relationerna mellan politik, professionell kunskap, institutionella strukturer och teknologisk utveckling är centrala även i militär verksamhet.

HOP SA

3. Metod

I detta kapitel redogörs för studiens metodologiska ansats, forskningsdesign, empiriska material, analysförfarande samt etiska överväganden.

3.1. Metodansats

Studien utgår från en kvalitativ och tolkande ansats, där verklighet och kunskap förstås som socialt och språkligt konstruerade (Bryman 2018:58). Styrande dokument betraktas därmed inte som neutrala beskrivningar av verkligheten, utan som uttryck för hur olika aktörer förstår och ger mening åt cyberdomänen. Den tolkande ansatsen är ändamålsenlig då studien syftar till att skapa en fördjupad förståelse för hur idéer och föreställningar som uttrycks i styrande dokument påverkar militär förmågeutveckling.

Analysen genomförs induktivt; det teoretiska ramverket styr därmed inte kodningen eller temagenereringen, utan används som en tolkande lins vid analysen av de empiriskt framvuxna temana. Studien får därmed en teoriutvecklande snarare än teoriprovande inriktning (Bryman 2018:61–62).

3.2. Forskningsdesign

Studien är utformad som en kvalitativ, dokumentbaserad fallstudie med tolkande ansats (Vennesson 2010:227; Bryman 2018:62). Syftet är att undersöka hur STF om cyberdomänen kommer till uttryck i svenska styrande dokument och hur dessa förändras över tid samt hur de påverkar förmågeutvecklingen av området.

Fallstudien avgränsas till svenska offentliga dokument som formulerar STF om cyberdomänen under perioden 2017–2025. Denna design motiveras av att STF, enligt Jasanoff (2015a:24), formas och institutionaliseras genom nationella policyprocesser och därmed görs synliga i styrande dokument. Vilka i sin tur påverkar militär förmågeutveckling, politiska prioriteringar och strategisk inriktning.

Den nationella avgränsningen motiveras av att STF enligt Jasanoff (2015a:18) är nära kopplade till nationell kontext i form av kultur, historiska erfarenheter och självbild.

HOP SA

Tidsperioden har valts då den omfattar en omvälvande säkerhetspolitisk förändring i och med Rysslands fullskaliga invasion av Ukraina 2022, vilken antas ha påverkat svenska beslutsfattares föreställningar om cyberdomänens roll och utveckling.

3.3. Empiri och urval

Empirin består av offentligt tillgängliga dokument från Regeringen, Försvarmakten och Försvarsberedningen. Dessa aktörer innehar institutionell auktoritet och inflytande över styrande dokument som ger uttryck för STF om cyberdomänen. Urvalet är målstyrt och har genomförts i relation till studiens forskningsfråga (Bryman 2018:496, 498).

Urvalet av dokument baseras på följande kriterier, vilka tar sin utgångspunkt i Jasanoff och Kims (2015a:4) definition av STF:

- ger uttryck för kollektiva visioner
- är offentligt publicerade och uttrycker institutionella föreställningar
- innehåller framåtriktade perspektiv såsom visioner eller riktlinjer
- har en styrande eller vägledande funktion för militär förmågeutveckling
- innehåller formulering avseende cyberdomänen

I syfte att möjliggöra analys av förändring över tid, delas empirin in i två korpusar:

- **Korpus A (2017–2022):** dokument publicerade och framtagna före Rysslands invasion av Ukraina
- **Korpus B (2022–2025):** dokument publicerade efter invasionen

Korpusindelningen baseras på dokumentens innehåll och analytiska karaktär snarare än enbart publiceringsår. Dokument som huvudsakligen bygger på föreställningar formulerade före 2022 placeras i korpus A, medan dokument med en tydligare framtidsinriktning placeras i korpus B. Den säkerhetspolitiska omdaning 2022 används som analytisk referenspunkt snarare än som ett strikt tidsmässigt brott och en fullständig dokumentförteckning återfinns i bilaga 1.

Målsättningen har varit att välja jämförbara dokument från respektive tidsperiod, såsom propositioner och perspektivstudier. Därav har studien avgränsats till tidsperioden 2017–2025 då den möjliggör ett sådant upplägg. I de fall motsvarande dokument saknas har funktionellt

HOP SA

likvärdiga dokument använts. En strävan har även varit att uppnå balans mellan dokument från politisk och militärstrategisk nivå i syfte att belysa båda perspektiven.

Nationell strategi för cybersäkerhet 2025-2029 (Regeringen 2024a) samt liknande dokument övervägdes men valdes bort då dessa i huvudsak avhandlar cybersäkerhet i vidare bemärkelse och inte militär cyberförmåga.

3.4. Analysmetod

I studien används tematisk analys (TA) som verktyg för att identifiera och strukturera återkommande mönster av mening i styrande dokument. TA anses vara ett flexibelt verktyg för kvalitativ forskning och metoden saknar egen fast ontologisk eller epistemologisk position och kan därav tillämpas inom olika vetenskapsteoretiska inriktningar (Braun & Clarke 2006:77; Bryman 2018:272–273; David & Sutton 2019:272–273; Alvinus et al. 2023:5).

I denna studie används inte TA som ett fullständigt metodologiskt ramverk utan primärt som ett struktureringsverktyg för empirin. De teman som genereras genom TA utgör underlag för tolkning genom Jasanoffs teoretiska ramverk (2015b:3–15).

Vidare har latent kodning genomförts, vilket innebär att analysen inte enbart fokuserar på explicita utsagor, utan även på underliggande antaganden och problemformuleringar (David & Sutton 2019:274).

3.5. Genomförande och kodning

Analysen genomfördes i två analytiska steg. I det första steget användes TA för att strukturera det empiriska materialet. Syftet var att identifiera återkommande mönster i hur STF om cyberdomänen kommer till uttryck i dokumenten. I det andra steget tolkades de empiriskt framvuxna temana genom Jasanoffs (2015b:3–15) analytiska processer.

Kodningen genomfördes induktivt, utan att teman i förväg härleddes ur studiens teoretiska ramverk. Samtidigt fungerade Jasanoff och Kims (2015a:4) definition av STF som *sensitizing concept*, det vill säga som analytiska utgångspunkter som vägleder tolkningen utan att fungera som fasta kodningskategorier (Blumer 1954). Det riktade uppmärksamheten mot formuleringar som motiverar, definierar eller uttrycker önskad utveckling av cyberdomänen. Jasanoffs

HOP SA

processer operationaliserades till kodningsindikatorer (se bilaga 2) som användes för att identifiera relevanta uttryck för STF i materialet. Dessa fungerade som analytiskt stöd men var inte styrande för tolkningen.

Teman utvecklades initialt utifrån korpus A och de användes därefter som sensitizing concepts vid analysen av korpus B. Kodningen av korpus B genomfördes iterativt, med möjlighet att lägga till eller justera koder och teman vid behov. Detta möjliggjorde analys av både kontinuitet och förändring över tid. Kodningen utgick från meningsbärande formuleringar som uttrycker föreställningar om cyberdomänen, oavsett tempus vilka exemplifieras i bilaga 3.

Sammantaget utgjorde TA studiens huvudsakliga struktureringsverktyg, medan Jasanoffs processer fungerade som tolkningslins vid analysen.

3.6. Forskningsetiska överväganden

Studien baseras uteslutande på offentligt tillgängliga dokument och omfattar inga personuppgifter. Det innebär att etiska risker kopplade till deltagarskydd bedöms som begränsade. De etiska överväganden som aktualiseras rör i stället forskningsintegritet såsom transparens och hantering av forskarens förförståelse.

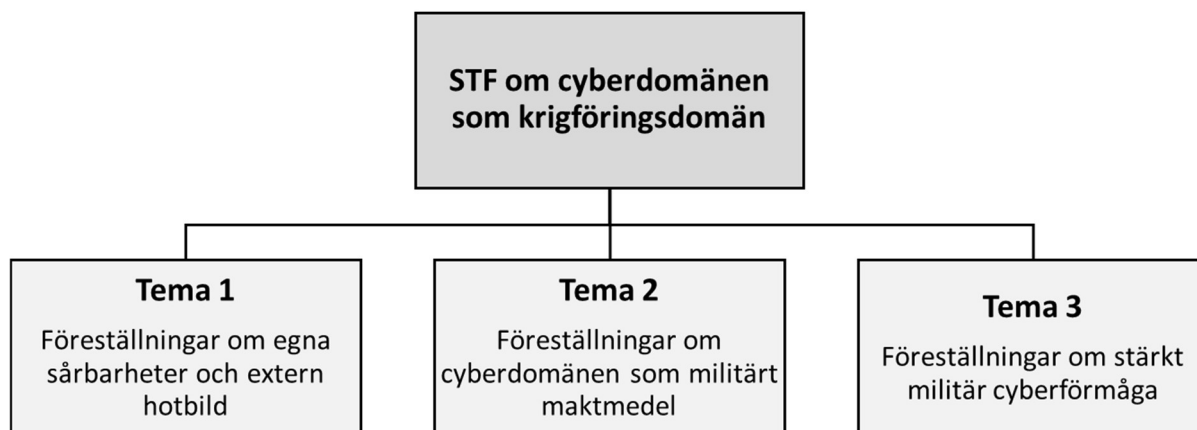
Eftersom författaren är verksam inom Försvarmakten kan studien klassificeras som insiderforskning (Drake & Heath 2011:47). Författarens position bidrar till en fördjupad kontextuell förståelse vilket är en tillgång i en tolkande studie. Samtidigt innebär denna position att analys och tolkning präglas av författarens förförståelse. I stället för att försöka motverka detta har generell och professionell reflexivitet tillämpats som ett genomgående förhållningssätt, där reflektion över författarens roll, antaganden och analytiska val kontinuerligt har genomförts och synliggjorts (Alvinus et al. 2023:32–33).

4. Analys och resultat

I detta kapitel presenteras analysen av det empiriska materialet, strukturerat utifrån tre huvudteman som genererats genom kodning av korpus A och B. Analysen fokuserar på hur STF om cyberdomänen formas, stabiliseras och förändras över tid. Fokus ligger därmed på STF, inte faktisk militär förmåga.

4.1. Temaöversikt

Figur 1 presenterar studiens teman, under respektive tema analyseras dess ingående kategorier genom en integrerad analys- och resultatdel, där empirin tolkas med stöd av studiens teoretiska ramverk. Vid analysen av temana används därför Jasanoffs begrepp (2015b:3–15) – uppkomst, institutionalisering, utvidgning och motstånd – utan att dessa explicit refereras till i varje enskild analys.

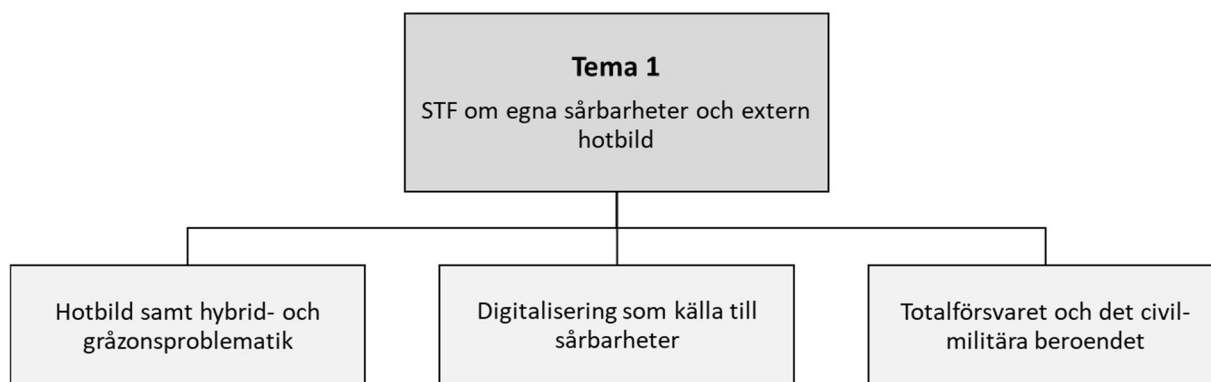


Figur 1: Översiktsbild över studiens teman.

4.2. Tema 1 – STF om egna sårbarheter och extern hotbild

Tema 1 beskriver en komplex hotbild samt tillhörande sårbarheter och civil-militära beroenden vilken motiverar behovet av en militär cyberförmåga. Analysen inriktas i huvudsak på processerna uppkomst, institutionalisering och till del utvidgning, då empirin i begränsad utsträckning ger uttryck för motstånd.

HOP SA



Figur 2: Översiktsbild över Tema 1 och dess ingående kategorier.

Hotbilden framställs genomgående i både korpus A och B som komplex, där cyberdomänen ofta beskrivs som en integrerad del av hybrida aktiviteter med potential att påverka såväl det militära försvaret som samhället i stort (Försvarsberedningen 2017:114; Försvarsmakten 2018:30; Regeringen 2024b:15). I korpus A framställs cyberhotet som ett framväxande problemområde med successivt ökande påverkan på svensk säkerhet. Hotbeskrivningar fungerar här som ett sätt att etablera cyberdomänen som ett nytt militärt problemområde vilket utifrån Jasanoffs processer (2015b:3–8) kan förstås som uppkomst och till del institutionalisering av föreställningen kring cyberdomänen som ett militärt problem.

Cyberförmågan kopplas i korpus A i stor omfattning till påverkan under tröskeln för väpnat angrepp. Den kopplas även till statliga aktörers användning av cyberförmåga som komplement till traditionella maktmedel även om referenser till cyberdomänen som krigföringsförmåga förekommer (Försvarsmakten 2018:106; Försvarsberedningen 2019:47). I korpus B sker en delvis förskjutning, där denna hotbild breddas genom att cyberhotet framställs som ett reellt militärt hot med relevans över hela konfliktskalan (Regeringen 2024b:146). Denna utveckling kan förstås som en utvidgning av redan existerande STF avseende cyberdomänen som säkerhetshot.

Cyberangrepp beskrivs i båda korpusar som potentiellt allvarliga och samhällspåverkande men ges delvis olika status. I korpus A framställs cyberangrepp ofta som möjliga framtida händelser med risk för omfattande konsekvenser, även om hotet i viss utsträckning också beskrivs som reellt. I de senare dokumenten i korpus B där den säkerhetspolitiska kontexten präglas av Rysslands invasion av Ukraina och dess följdverkningar, framträder en tydligare normalisering

HOP SA

av hotet. Cyberangrepp beskrivs i högre grad som ett ständigt pågående inslag i den säkerhetspolitiska vardagen, vilket följande formulering visar: ”olika former av antagonistiska cyberaktiviteter utgör idag en del av normalbilden” (Regeringen 2024b:146). Att cyberhotet i ökande grad framstår som en given utgångspunkt för militär planering och verksamhet kan förstås som en rörelse från uppkomst till institutionalisering av föreställningarna om cyberdomänen som ett säkerhetshot.

Cyberhotet beskrivs i både korpus A och B som oberoende av geografiskt avstånd. Denna egenskap framställs i dokumenten som särskilt problematiskt, då den möjliggör påverkan utan fysisk närvaro. I korpus B kopplas denna gränsöverskridande karaktär tydligare till strategiska konsekvenser, såsom påverkan på svensk suveränitet, handlingsfrihet och det kollektiva försvaret (Regeringen 2024b:18, 146). Cyberhotet framstår därmed som ett hot med tydliga strategiska implikationer vilket ytterligare bidrar till institutionalisering av cyberdomänen som en säkerhetspolitisk utmaning.

Vad avser hotaktörer, identifieras statliga aktörer som de normerande i båda korpusar men där Ryssland tydligare pekas ut som det dimensionerande hotet i korpus B (Försvarmakten 2023:4). I korpus B breddas dessutom synen på cyberhotet genom att även belysa kommersialiseringen av cyberförmågor, vilket möjliggör att även mindre och icke-statliga aktörer kan orsaka oproportionerligt stora effekter vilket Försvarmakten lyfter fram i *Doktrinansats cyberförsvar 2024* (2024:27). Detta bidrar till bilden av ett mer komplext och svåravgränsat hotlandskap där traditionella maktstrukturer delvis luckras upp och där synen på cyberhotbilden utvidgas.

Vidare beskrivs i båda korpusar, digitalisering som en grundläggande förutsättning för samhällets funktion och totalförsvarets förmåga, samtidigt som den framställs som en central källa till sårbarhet (Regeringen 2020:63; 2024b:17; Försvarmakten 2022b:32, 34; a:86). I korpus A betonas digitaliseringens roll i att skapa komplexa och svåröverblickbara system (Försvarsberedningen 2019:30). I korpus B fördjupas denna föreställning genom beskrivningar av hur digitaliseringen skapar komplexa beroendekedjor, där enskilda aktörers svagheter kan få konsekvenser för aktörer inom andra sektorer eller nationer (Försvarsberedningen 2023:36; Regeringen 2024b:17). Cyber- och informationssäkerhet framställs därmed i ökande grad som ett gemensamt ansvar snarare än ett sektorsvist problem, vilket stabiliserar föreställningen om digitaliseringens risker som en långsiktig utmaning för hela samhället.

HOP SA

Det civil-militära beroendet framstår slutligen som ett grundvillkor för totalförsvaret i båda korpusar (Regeringen 2020:63; 2024b:150). Gränsen mellan civil och militär IT-infrastruktur beskrivs genomgående som otydlig (Försvarsberedningen 2017:113). Cyberdomänen konstrueras därmed som en sammanhållande arena där cybersäkerhet och militärt cyberförsvar framstår som ömsesidigt beroende och förstärkande samt integrerade delar av totalförsvaret (Regeringen 2024b:150). Det tyder på att föreställningar kring digitaliseringens konsekvenser är institutionaliserade och uppvisar kontinuitet över tid.

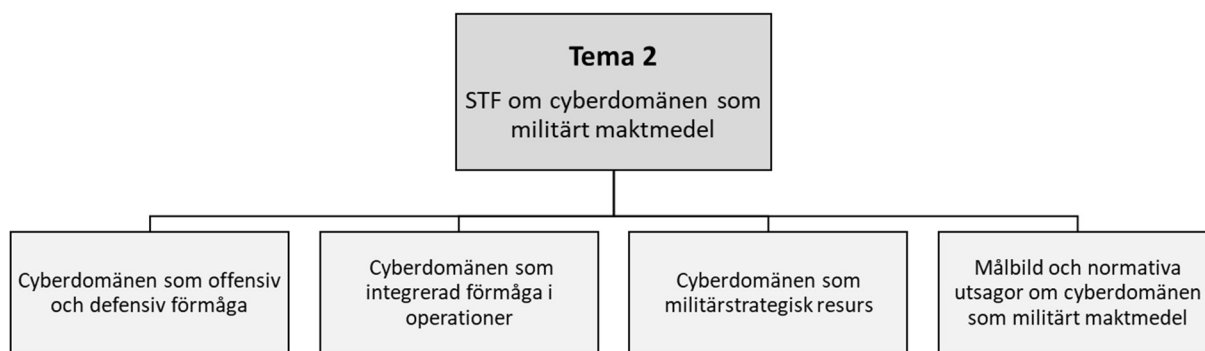
Sammantaget konstrueras cyberhotet inte enbart som ett externt antagonistiskt problem, utan som något som får säkerhetspolitisk betydelse genom digitaliseringens inbyggda sårbarheter och totalförsvarets civil-militära beroenden.

Tema 1 har visat hur föreställningar om hot, sårbarheter och samhällsberoenden successivt institutionaliseras och till del utvidgas. Förskjutningen mellan korpus A och B består mindre i vad som uppfattas som hot och mer i hur hotet förstås: från potentiellt och framtida till permanent, normaliserat och styrande för planering och förmågeutveckling. Temat visar därmed på de föreställningar som utgör motiv till utvecklingen av cyberdomänen.

4.3. Tema 2 – STF om cyberdomänen som militärt maktmedel

I detta tema analyseras hur cyberdomänen ges militär mening genom att beskriva domänenens olika förmågor. I kontrast till Tema 1 som främst motiverar behovet av en militär cyberförmåga, fokuserar Tema 2 på hur domänenens funktion, användning och betydelse definieras. Analytiskt dominerar Jasanoffs (2015b:3–15) processer institutionalisering och utvidgning samtidigt framträder inslag av motstånd i form av konkurrerande sätt att definiera förmågans roll, medan processer av uppkomst är mindre framträdande.

HOP SA



Figur 3: Översiktsschema över Tema 2 och dess ingående kategorier.

I både korpus A och B framställs den militära cyberförmågan som en kombination av offensiva och defensiva förmågor vilka tillsammans utgör ett militärt maktmedel (Försvarsberedningen 2017; 2019; Försvarmakten 2018; 2022b; 2024). I de tidiga delarna av korpus A beskrivs dessa förmågor mer implicit genom formuleringar avseende behovet av att kunna skydda egna system och förhindra intrång samt ha förmågan till defensivt och offensivt agerande (Försvarmakten 2018:63). Cyberförmågan relateras tidigt till kända militära begrepp såsom bekämpning och skydd, men ofta på en övergripande nivå där det saknas närmare precisering avseende ledning, ansvar eller effekt (Försvarmakten 2018:27, 46, 106). Sammantaget tyder detta på att föreställningar kring cyberdomänen som krigföringsförmåga ännu inte fullt ut har institutionaliserats genom tydliga definitioner och ledningsförhållanden.

I senare dokument inom korpus A, sker en tydligare operationalisering av förmågan, defensiva och offensiva cyberoperationer definieras och det tydliggörs att cyberförmågan utgör ett militärt maktmedel. Dessutom ges förmågan en uttalad roll i samtliga konfliktnivåer och det formuleras att Försvarmakten är ansvarig för den offensiva cyberförmågan (Försvarsberedningen 2019:253; Regeringen 2020:152). Förmågan kopplas därmed tydligare till militär planering och genomförande. Dessa formuleringar kan förstås som en rörelse från uppkomst till institutionalisering, där cyberdomänen inte längre enbart framstår som ett framväxande problemområde utan som en naturlig del av militär verksamhet.

I korpus B förstärks föreställningen om cyberdomänen som militärt maktmedel ytterligare. *Doktrinansats cyberförsvar 2024* (2024:11–15, 35) preciserar och operationaliserar förmågan genom definitioner av offensiva och defensiva cyberoperationer, dess syften, begränsningar

HOP SA

och användning i militära operationer. Förmågan till offensiva och defensiva operationer beskrivs nu som ”central för hela totalförsvaret” (Regeringen 2024b:150). Föreställningarna kring cyberförmågan har därmed utvidgats och institutionaliserats ytterligare, inte främst genom synen på behovet av offensiv och defensiv förmåga, utan genom hur förmågan förstås.

En annan central del i Tema 2 är hur cyber föreställs i förhållande till övriga domäner. I både korpus A och B återfinns beskrivningar som relaterar förmågan till andra militära förmågor. I tidiga dokument i korpus A framställs cyber ofta genom tekniska beroenden och behov av skydd alternativt att förmågan beskrivs ingå som en del i andra militära operationer (Försvarsmakten 2018:106; 2024:86). I senare dokument i korpus A, ges cyber dock en mer operativ roll (Försvarsmakten 2022b:55, 57).

Samtidigt förekommer i korpus A en parallell föreställning om cyberdomänen som ett alternativt handlingsalternativ till stöd för den strategiska, militärstrategiska och operativa nivån som innehar förmågor som ligger utanför de reguljära förbandens förmågor (Försvarsmakten 2022b:56). Detta tydliggörs genom formuleringen: ”cyberförmågan som verkanssystem existerar parallellt med de traditionella försvarsförmågorna och ger tillgång till alternativa sätt att uppnå ett visst mål” (Försvarsmakten 2018:105). Att cyberförmågan beskrivs som både integrerad och som en parallell strategisk förmåga indikerar en ambivalens i hur cyberdomänens roll förstås i förhållande till övriga domäner. I Jasanoffs termer (2015b:8–11) kan detta förstås som ett uttryck för motstånd, inte mot föreställningen om cyberdomänen som militärt maktmedel, utan hur förmågan skall integreras med övriga domäner.

I korpus B sker en tydligare inordning av cyberdomänen som integrerad krigföringsdomän och som en självklar del av militär verksamhet som ska samordnas och utgör en förutsättning för övriga domäner (Försvarsmakten 2022a:41; 2024). Samtidigt tydliggörs att offensiva och defensiva cyberoperationer kan genomföras inom ramen för gemensamma operationer men även att de kan genomföras som en autonom strategisk operation. Där den autonoma operationen tydligt kopplas till behovet att omsätta militärstrategiska inriktningar till operativ effekt, särskilt när tempo, sekretess eller okonventionellt uppträdande är centralt (Försvarsmakten 2024:36, 38, 41). Sammantaget ger detta en mer utvecklad och institutionaliserad bild av cyberförmågans dubbla roll i krigföring (Försvarsmakten 2024:39, 41).

HOP SA

Detta kan ses som en utvidgning och institutionalisering av föreställningar kring cybers roll. I korpus B tillåts båda roller samexistera och det motstånd som i korpus A tar formen av ambivalens mellan parallell och integrerad förmåga framträder i korpus B snarare som en uttalad strategi.

Utöver föreställningar om förmågans användning återfinns även normativa och målbildsinriktade föreställningar om cyberdomänens roll i det militära försvaret. I både korpus A och B uttrycks en tydlig ambition att cyberdomänen ska utgöra ett centralt inslag i försvaret av Sverige (Försvarsberedningen 2017; 2019; Regeringen 2020; 2024b). I de tidiga dokumenten motiveras detta ofta genom Sveriges omfattande digitalisering och behovet av proaktiv förmåga i gråzonen för att skapa tröskeleffekter (Försvarsberedningen 2017:118–119). Även om cyberdomänen i dessa sammanhang ibland framställs som ett komplement, indikerar målbilden en tidig normativ ambition att cyberdomänen ska fungera som ett eget militärt maktmedel.

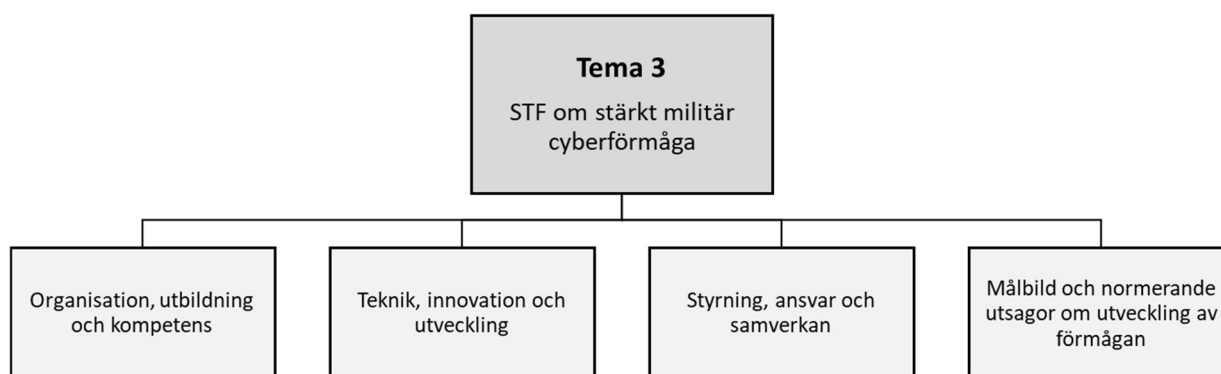
I korpus B fördjupas och breddas denna målbild. Cyberdomänen beskrivs här som en förmåga som ska kunna bidra över hela konfliktskalan och som en central komponent i såväl nationellt som kollektivt försvar, inklusive inom ramen för NATO (Försvarsmakten 2023:9; Regeringen 2024b:150–151). Efter Rysslands invasion av Ukraina och det efterföljande svenska medlemskapet i NATO sker en omdaning av synen på svensk cyberförsvarsförmåga till att även omfatta cyberoperationer inom ramen för NATO (Regeringen 2024b:41, 151).

Sammantaget visar Tema 2 hur föreställningar om cyberdomänen som militärt maktmedel utvecklas genom en kombination av kontinuitet och omdaning. Cyber etableras tidigt som relevant militär förmåga, men genomgår successiva processer av uppkomst, institutionalisering, utvidgning samt motstånd. Resultatet är en gradvis stabilisering där cyber framträder som en institutionellt förankrad och normativt legitim krigföringsdomän både i en svensk och internationell kontext.

4.4. Tema 3 – STF om stärkt militär cyberförmåga

Tema 3 visar hur STF om framtida utveckling, organisering och vidmakthållande av militär cyberförmåga formuleras. Processerna institutionalisering och utvidgning dominerar, medan uppkomst främst ses i de äldre dokumenten. Motstånd framträder i form av spänningar mellan etablerade militära strukturer och cyberdomänens egenart.

HOP SA



Figur 4: Översiktsbild över Tema 3 och dess ingående kategorier.

Redan i korpus A formuleras behovet av kompetens och utbildning för att upprätthålla ett adekvat cyberförsvar. I slutet på korpus A påbörjas en förskjutning från behovsidentifiering till en mer systematiserad och långsiktig kompetensförsörjning. Det visar sig genom etablering av särskilda utbildningar, karriärvägar och värnplikt inom cyberområdet, vilket följande formulering exemplifierar: “Cyberförmågan förstärks genom att Försvarsmakten [...] organiserar ett personal- och kompetensförsörjningssystem för cyberförsvarsfunktionen” (Försvarsmakten 2022a:67). Detta visar på en institutionalisering, där identifierad kompetensbrist omhändertas genom inrättandet av organisatoriska strukturer och utbildningar.

Denna utveckling förstärks ytterligare i korpus B (Försvarsmakten 2024:12). Där sker även en utvidgning av synen på utbildning, från en föreställning om dess nödvändighet för att uppnå grundläggande cybersäkerhet till att framställas som operativt avgörande för uppbyggandet av krigföringsförmågan.

Behovet av teknikutveckling framställs genomgående i korpus A och B som centralt för att uppnå militär effekt i cyberdomänen. Redan 2018 formuleras föreställningen att det även krävs stridsteknik, taktik och doktrin vid införandet av ny teknik för att uppnå militär effekt (Försvarsmakten 2018:29). I korpus B tydliggörs ytterligare att den militära cyberförmågan behöver byggas i samverkan mellan teknik, metoder och kompetent personal (Försvarsmakten 2024:12). Det kan ses som institutionalisering och utvidgning av synen på förmågeutveckling som inte enbart teknisk utan att även kompetens och den mänskliga aspekten behöver omhändertas.

HOP SA

Vidare uttrycks tidigt i korpus A, behovet av forskning till stöd för teknikutveckling i syfte att möta snabba förändringar i hotbilden. Dock formuleras detta i mer generella ordalag (Regeringen 2020:152). I korpus B specificeras behovet tydligare, där formuleras att teknikutveckling och forskning behöver ske i ett samspel mellan myndigheter, akademi och näringsliv samt att utbildning, träning och övning är väsentligt för att uppnå en teknologisk förmåga i framkant (Försvarmakten 2022a:88; 2023:37; 2024:16, 43). Här kan stabilisering och utvidgning av föreställningen ses, där behovet av teknikutveckling institutionaliseras samtidigt som det sker en utvidgning till att även inkludera aktörer utanför Försvarmakten (Försvarmakten 2023:5). Motstånd framträder samtidigt i spänningar mellan att militär förmågeuppbyggnad går långsamt och cyberdomänens behov av snabb teknikutveckling.

Genomgående i båda korpusar beskrivs cyberdomänen som ett område där flera aktörer delar på ansvaret, även om Försvarmakten pekas ut som ansvariga för cyberförsvaret (Försvarsberedningen 2019:254). Problem med samordning beskrivs återkommande samt behovet av samverkan framhävs i båda korpus men i korpus B ses en tydligare formuleringar av mandat och ansvarsfördelning (Försvarsberedningen 2017:115; Regeringen 2020:153). Upprättandet av en nationell samordnings- och samverkansstruktur, såsom Nationellt cybersäkerhetscentrum samt en cyberförsvarsledning bidrar till att behovet av samordning i större utsträckning framställs som institutionaliserad genom organisatoriska lösningar och tydlig ansvarsfördelning (Regeringen 2024b:150). I den senare säkerhetspolitiska kontexten, efter 2022 och genom svenskt NATO-medlemskap förskjuts behovet av samverkan samt samordning från ett nationellt fokus till ett alliansfokus vilket kan ses som en relativt tydlig omdaning och inte enbart utvidgning av tidigare föreställningar.

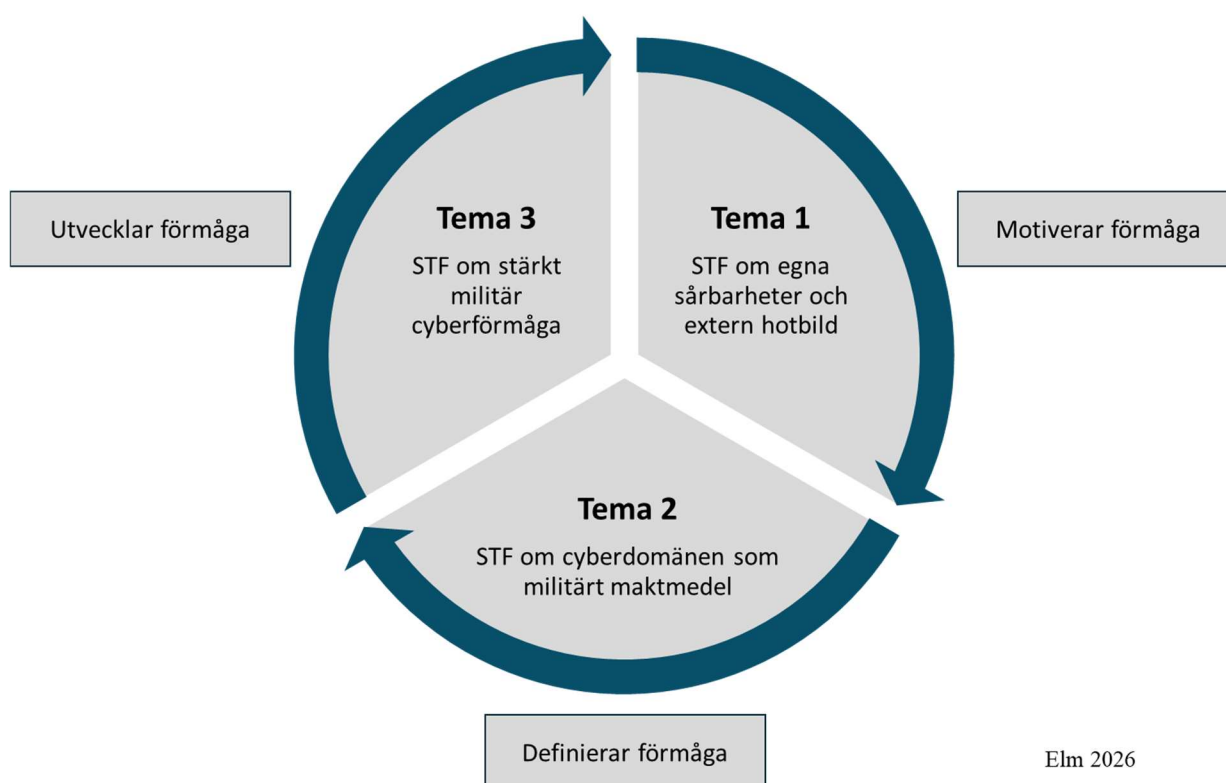
Slutligen syns ett skifte i hur framtidsvisioner och planeringsinriktning formuleras. Från långsiktiga och mer svepande beskrivningar av behov av förmågeutveckling till att tydligare inriktas mot att skapa förmåga här och nu, vilket följande citat är ett exempel på: "På militärstrategisk nivå bedöms tyngdpunktsförskjutningar behöva ske från i huvudsak långsiktig planering till ökat fokus på förmåga här och nu." (Försvarmakten 2023:5). Det sker även ett skifte i hur inriktningen av förmågeplaneringen beskrivs efter NATO inträdet, från ett nationellt fokus till ett kollektivt fokus. Där förmågeutveckling enligt Försvarmakten (2023:6) bör utformas utifrån alliansens militärstrategiska målsättningar. Båda dessa förändrade formuleringar kan ses som omdaning snarare än utvidgning av tidigare föreställningar, där en

HOP SA

tydligt förändrad säkerhetspolitisk kontext skapar nya krav på hur svensk militär cyberförmåga bör utvecklas.

Sammantaget visar Tema 3 hur STF formar utvecklingen av den militära cyberförmågans organisation och inriktning. Den förändrade säkerhetspolitiska kontexten omdanar föreställningar avseende internationalisering och tempo men föreställningar avseende organisation och kompetens fördjupas och institutionaliseras ytterligare.

4.5. Sammanfattning och syntes



Figur 5: Figuren visar hur de tre temana relaterar till varandra. Tema 1 motiverar behovet av cyberförmåga, Tema 2 definierar förmågan och Tema 3 beskriver hur förmågan bör utvecklas. Pilarna illustrerar en tolkningsmässig rörelse mellan temana och ska inte förstås som ett kausalt samband. Figuren utgör den empiriska grunden till studiens analytiska modell (figur 6).

Sammantaget visar analysen att de tre identifierade temana inte bör förstås som fristående delar utan som en sammanhängande process där STF successivt formar utvecklingen av militär cyberförmåga. Som illustreras i figur 5 kan denna process förstås som en rörelse från

HOP SA

föreställningar om hot och sårbarheter, via definition av cyberdomänen som militärt maktmedel, till föreställningar om hur förmågan bör utvecklas, organiseras och vidmakthållas. Processen bör förstås som cirkulär då förändrad kontext kontinuerligt förändrar de föreställningar som motiverar, definierar och utvecklar förmågan.

Tema 1 visar hur en komplex hotbild, präglad av hybrida hot, gråzonsproblematik, ökad digitalisering och civil-militära beroenden fungerar som grundläggande motiv till varför militär cyberförmåga behövs. Här etableras cyberdomänen som ett militärt problemområde genom beskrivningar av externa hot och interna sårbarheter, vilket skapar förutsättningar för att föreställa sig cyberdomänen som en nödvändig del av det militära försvaret.

Tema 2 bygger vidare på föreställningar om cyberdomänen som militärt problemområde. Detta görs genom att visa hur cyberdomänen successivt definieras och legitimeras som militärt maktmedel genom institutionalisering i doktrin och tydliggöranden om vad förmågan förväntas bidra med. Föreställningarna förskjuts från att initialt beskriva cyberdomänen som en främst stödjande eller teknisk funktion till att förstås som en integrerad och vissa avseende självständig krigföringsdomän genom kopplingar till etablerade militära begrepp, doktrin och ledningsstrukturer.

Tema 3 synliggör slutligen hur dessa föreställningar omsätts i idéer om konkret förmågeutveckling. Här framträder hur STF inte enbart motiverar och legitimerar cyberförmågan i begreppslig mening utan även omsätts genom uttryckt inriktning av ansvarsfördelning, kompetensförsörjning, teknikutveckling och internationell samverkan.

Tillsammans visar tema 1–3 att förändringar i STF om cyberdomänen i huvudsak präglas av gradvisa förskjutningar och kontinuitet snarare än tvära förändringar avseende hur cyberdomänen föreställs. Detta trots att Rysslands invasion av Ukraina 2022 utgjorde en omvälvande säkerhetspolitisk förändring. Dock framträder vissa mer genomgripande förändringar av uttryckta föreställningar, vilka kan kopplas till den säkerhetspolitiska förändring som skedde 2022 och dess efterföljande konsekvenser, såsom upplevd operativ omedelbarhet samt svenskt medlemskap i NATO. Här förändras föreställningar om internationell samverkan samt inriktning av utvecklingen av cyberdomänen mer genomgripande och hastigt.

HOP SA

Denna syntes tydliggör hur STF kan förstås som en sammanhållande länk mellan hotuppfattning, begreppsliggörande av cyberdomänen som militärt maktmedel och önskad förmågeutveckling. I nästa kapitel diskuteras vad dessa resultat innebär för förståelse av militär förmågeutveckling samt vilken analytisk relevans STF har som teoretisk tolkningsram för militär förmågeutveckling.

HOP SA

5. Avslutning

Kapitlet inleds med en resultatdiskussion utifrån studiens empiriska resultat. Därefter följer en metoddiskussion samt studiens huvudsakliga slutsatser. Avslutningsvis presenteras studiens teoretiska, metodologiska och praktikhäna bidrag och implikationer, varefter kapitlet avrundas med en diskussion om studiens kvalitet, styrkor och begränsningar samt förslag på vidare forskning.

5.1. Resultatdiskussion

5.1.1. Selektiv förändring av STF

Studiens analys visar att STF om cyberdomänen inte förändras på ett enhetligt sätt vid kontextuella skiften. Trots den omfattande säkerhetspolitiska omdaning som Rysslands invasion av Ukraina inneburit, uppvisar vissa föreställningar kontinuitet och stabilitet, medan andra har omformulerats snabbt och genomgående. I Jasanoffs (2015b) termer innebär detta att vissa föreställningar omprövas genom omdaning eller utvidgning medan andra förblir stabila och därmed mer trögrörliga. Förändring av STF framträder därmed som selektiv snarare än likvärdig och generell.

Skillnaden är särskilt tydlig mellan föreställningar som rör cyberdomänens grundläggande militära karaktär – såsom dess teknologiska förutsättningar, offensiva och defensiva dimensioner samt inordning i militär struktur – och de föreställningar som rör hur, när och i vilket sammanhang förmågan bör utvecklas och användas. De förra präglas av kontinuitet och förändras gradvis, medan de senare såsom synen på internationalisering, långsiktig förmågeutveckling och NATO-integration, omformuleras mer genomgripande och snabbt.

En möjlig tolkning av dessa skillnader är att när beslutet om NATO-medlemskap väl var fattat framstod en omställning mot ökad interoperabilitet och NATO-integration som ett icke-val. Tidigare föreställningar gick inte att upprätthålla utan behövde anpassas till de nya institutionella och operativa förutsättningarna. På motsvarande sätt kan skiftet från långsiktig förmågeutveckling till behov av förmåga ”här och nu” förstås. I takt med att hotbilden förändrades framstod omformuleringen som nödvändig.

Vidare kan dessa mer genomgripande förändringar av föreställningar tolkas som ett uttryck för att alternativa handlingsalternativ uppfattades som oacceptabla. Förändringen drevs på av en

HOP SA

upplevd nödvändighet snarare än av en internt efterfrågad omprövning. Säkerhetspolitiska vägval och hotuppfattningar fungerade därmed som styrande förutsättningar för hur föreställningar kunde förändras.

Denna dynamik ligger i linje med tidigare forskning som visar att förmågeutveckling i hög grad formas genom politiska och strategiska inramningar (Farrell & Terrif 2002:266; Jakobsen & Ringsmose 2018).

I kontrast uppvisar föreställningar om cyberdomänens grundläggande funktion, dess relation till övriga domäner samt roll i militär verksamhet, större kontinuitet och stabilitet. Förändring har här skett gradvis. En tolkning är att dessa föreställningar inte har upplevts behöva omprövas i samma omfattning eftersom cyberdomänens grundläggande funktion framstått som ändamålsenlig även efter den säkerhetspolitiska omdaning. Sådana föreställningar kan förstås som starkt sammanvävda med militär praktik och teknologiska förutsättningar vilket tillsammans med begränsad politisk styrning och en låg upplevd nödvändighet till förändring bidrar till deras stabilitet. Förändring av dessa föreställningar sker därmed främst i takt med cyberdomänens interna behov av teknologisk, organisatorisk och metodologisk utveckling.

Mot bakgrund av Modig och Andersson (2022) tidigare forskning kring kognitiva dimensioner av militär innovation kan det indikera att delade mentala modeller tillsammans med konfirmationsbias påverkar hur den säkerhetspolitiska förändringen tolkas och därmed bidrar till att befintliga föreställningar förblir stabila snarare än omprövas.

Ur detta perspektiv framträder selektiv förändring som ett resultat av hur säkerhetspolitiska förändringar möter institutionaliserade föreställningar om cyberdomänen. Omdaning av föreställningar koncentreras till ett begränsat antal områden där anpassningen uppfattas som nödvändig medan merparten av föreställningarna uppvisar kontinuitet eller gradvis utvidgning.

Selektiv förändring kan därmed förstås som en situationsbunden process där stabilitet och omdaning kan samexistera. Cyberdomänen utvecklas i spänningen mellan säkerhetspolitiska vägval, institutionaliserade föreställningar och militär praktik. Det återspeglar det sociotekniska perspektiv som vuxit fram avseende förmågeutveckling (Mumford 2006; Baxter & Sommerville 2011).

HOP SA

5.1.2. Institutionaliserings dubbla roll

Studiens empiriska resultat visar att föreställningar om cyberdomänen successivt har institutionaliserats genom doktrin och andra styrande dokument. Detta sker i ett forskningsområde som i sig präglas av betydande begreppslig osäkerhet. Forskare är oeniga om hur området skall förstås, där cyberdomänen omväxlande beskrivs som strategiskt maktmedel, stödande verktyg eller egen domän (Finlay 2018:357; Libicki 2021:112–114; Smeets 2022:3). Denna begreppsliga osäkerhet skapar särskilda utmaningar för militära organisationer där samordning och styrning förutsätter gemensamma förståelser. Tidigare forskning visar dessutom att politisk och militär ledning ofta har begränsad kunskap och cyberdomänen vilket försvårar dess integrering i den militära förmågepaletten (Hayden 2016:4). Den begreppsliga osäkerheten förstärks därmed av kompetensbrist vilket ytterligare ökar behovet av gemensamma tolkningsramar.

I akademiska sammanhang kan sådana konkurrerande perspektiv samexistera men för en militär organisation är ett motsvarande tolkningsutrymme svårare att hantera. För att planering, organisering och utveckling ska vara möjliga måste vissa förståelser enligt Høiback (2013:3) därför göras gemensamma och bindande i doktrin och styrande dokument. Det är utifrån denna bakgrund som dessa dokument får en särskild betydelse vid förmågeutveckling.

I denna studie framträder styrande dokument inte enbart som beskrivningar av existerande förmåga, utan som dokument där STF formuleras, ges legitimitet och institutionaliseras. De fungerar därmed som ramverk där en i grunden omstridd och framtidsorienterad domän ges en bestämd militär mening. I en domän präglad av begreppslig osäkerhet måste organisationen formulera gemensamma och institutionellt stabiliserade förståelser för att möjliggöra planering och samordning, vilket ligger i linje med Høibacks (2011:887) förståelse av doktrin som institutionell och normerande. Den stabilitet som därigenom skapas kan därför förstås som central för militär förmågeutveckling då den möjliggör ett gemensamt språk och delade referensramar. Samtidigt aktualiseras frågan om i vilken utsträckning denna stabilitet också kan innebära en inneboende tröghet för förändring.

För cyberdomänen, som präglas av snabb teknologisk förändring och strategisk osäkerhet, kan sådan institutionell tröghet få särskilda konsekvenser. Tidigare forskning visar dessutom att Sverige saknar en systematisk process för doktrinutveckling vilket ytterligare kan förstärka denna tröghet (Thunholm & Palmgren 2017:21; Thunholm et al. 2018:32).

HOP SA

När föreställningar väl har blivit institutionellt etablerade i doktrin riskerar de att fungera som tolkningsramar även bortom den kontext som en gång gav dem mening. Høiback (2011:879; 2013:6) framhåller dock att doktrin kan fungera som förändringsverktyg och möjliggöra kreativitet, men detta förutsätter att doktrinen kontinuerligt revideras och speglar verkligheten på ett trovärdigt sätt vilket även Thunholm et al (2018:42) lyfter fram. Utan formaliserade revisionsprocesser finns en risk att stabilitet förväxlas med relevans – det som varit stabilt uppfattas som beprövat, snarare än som potentiellt föråldrat. Förmågan kan framstå som tillräcklig därför att den fungerar enligt sina egna institutionaliserade föreställningar, snarare än den faktiskt svarar mot förändrade omvärldsvillkor.

Institutionaliseringen av föreställningar framträder därmed som både förutsättning och begränsning för militär förmågeutveckling. Den skapar ordning och handlingsbarhet, men formar samtidigt ramarna för vad som framstår som möjligt att tänka och göra. Snarare än att entydigt främja eller hindra förändring utgör institutionalisering en central del av den process där spänningen mellan stabilitet och anpassning ständigt pågår.

5.2. Metoddiskussion

Studiens tolkande ansats och dokumentbaserade design har möjliggjort en analys av hur STF om cyberdomänen konstrueras och förändras mellan 2017 och 2025. Utgångspunkten har varit att fördjupa förståelsen för hur cyberdomänen formas genom offentligt uttryckta föreställningar i styrande dokument.

Valet av STF som teoretiskt ramverk motiveras av studiens syfte att analysera hur framtidsinriktade idéer om cyberdomänen påverkar dess utveckling. Ramverket möjliggör en analys som går bortom en teknisk förståelse och synliggör samspelet mellan sociala och teknologiska dimensioner, vilken tidigare forskning efterfrågat (Liwång et al. 2023). Diskursanalys har övervägts som alternativ, men STF bedömdes bättre lämpat då perspektivet inte enbart analyserar språk, utan även hur idéer kopplas till materiell och organisatorisk utveckling (Jasanoff 2015a:18; Bryman 2018:640).

HOP SA

Användningen av dokumentanalys innebär samtidigt begränsningar. Officiella dokument representerar redan kollektivt sanktionerade föreställningar, vilket innebär att motstånd i form av konkurrerande tolkningar, interna konflikter och resurskamper endast synliggörs i begränsad utsträckning. Därmed fångar studien, institutionaliserade uttryck snarare än de processer genom vilka föreställningar förhandlas fram. Valet av dokumentanalys är en medveten avvägning i linje med att STF förstås som just offentligt och kollektivt uttryckta visioner.

Cyberdomänen utgör ett särskilt värdefullt empiriskt fall eftersom området är relativt nytt, saknar etablerade referensramar och utvecklas snabbt. Detta gör processer som uppkomst, institutionalisering, motstånd och utvidgning empiriskt synliga inom en hanterbar tidsrymd.

Den tematiska analysen med tolkande ansats har möjliggjort en systematisk hantering av ett omfattande material, men innebär samtidigt att resultaten är beroende av författarens tolkningar. För att stärka studiens tillförlitlighet redovisas analysprocessen utförligt i kapitel 3 och ett reflexivt förhållningssätt har tillämpats genom hela studien (Drake & Heath 2011:47).

5.3. Slutsatser

Denna studie har utgått från forskningsfrågan: ***Hur formar sociotekniska föreställningar, uttryckta i svenska styrande dokument mellan 2017–2025, utvecklingen av svensk militär cyberförmåga?***

För att besvara denna forskningsfråga har tre delfrågor formulerats:

1. Vilka centrala STF om cyberdomänen uttrycks i dokumenten och hur legitimeras dessa?
2. Hur påverkas dessa föreställningar av omvälvande säkerhetspolitiska förändringar såsom Rysslands invasion av Ukraina 2022?
3. Hur påverkar STF förutsättningarna för militär förmågeutveckling?

Studiens slutsatser besvarar sammantaget dessa delfrågor och därigenom den övergripande forskningsfrågan. Den första delfrågan behandlas i huvudsak i kapitel 4, där analysen visar hur STF formuleras och legitimeras i styrande dokument.

Analysen visar att cyberdomänen etableras som krigföringsdomän genom STF som motiverar förmågeutveckling, definierar förmågan som militärt maktmedel och formar hur verksamheten organiseras och utvecklas. Dessa föreställningar fungerar inte enbart som beskrivningar av

HOP SA

existerande förhållanden, utan som styrande ramar för vad som uppfattas som legitim och möjlig militär förmåga.

Vidare visar studien att förändring av STF om cyberdomänen sker selektivt i samband med den säkerhetspolitiska omdaning. Föreställningar kopplade till internationalisering, NATO-interoperabilitet och långsiktig förmågeutveckling omformas mer genomgripande, medan grundläggande föreställningar om cyberdomänens militära funktion och användning uppvisar hög grad av stabilitet och förändras gradvis.

Resultaten indikerar att förändring inte enbart styrs av säkerhetspolitisk omdaning eller institutionell stabilitet utan av hur handlingsutrymmet uppfattas. När alternativa föreställningar framstår som orealistiska eller oacceptabla möjliggör det snabbare och mer genomgripande omdaning. Vissa föreställningar framstår därmed som mer öppna för förändring medan andra fungerar som stabila ramar för fortsatt utveckling av cyberdomänen.

Slutligen visar analysen att institutionaliseringen av cyberdomänen genom doktrin och styrande dokument är förutsättningsskapande för förmågeutvecklingen genom att definiera förmågan och göra STF handlingsbara. Samtidigt bidrar denna process till att stabilisera vissa föreställningar över tid, vilket kan begränsa vad som uppfattas som möjligt att ompröva. Institutionaliseringen framträder därmed som både möjliggörande och begränsande.

Sammantaget visar studien att utvecklingen av cyberdomänen bör förstås som en process där föreställningar, organisation och teknik samproduceras. Förmågeutveckling framträder därmed inte som en direkt anpassning till nya hot, utan som en institutionellt förankrad process präglad av både selektiv förändring och stabilitet. Studien visar därigenom hur STF formar de institutionella och begreppsliga förutsättningarna för militär förmågeutveckling genom att påverka vad som blir tänkbart, legitimt och prioriterat. Studien analyserar däremot varken dess praktiska genomförande eller faktiska utfall. Studien bidrar därmed till en fördjupad förståelse av hur militära förmågor formas genom STF.

HOP SA

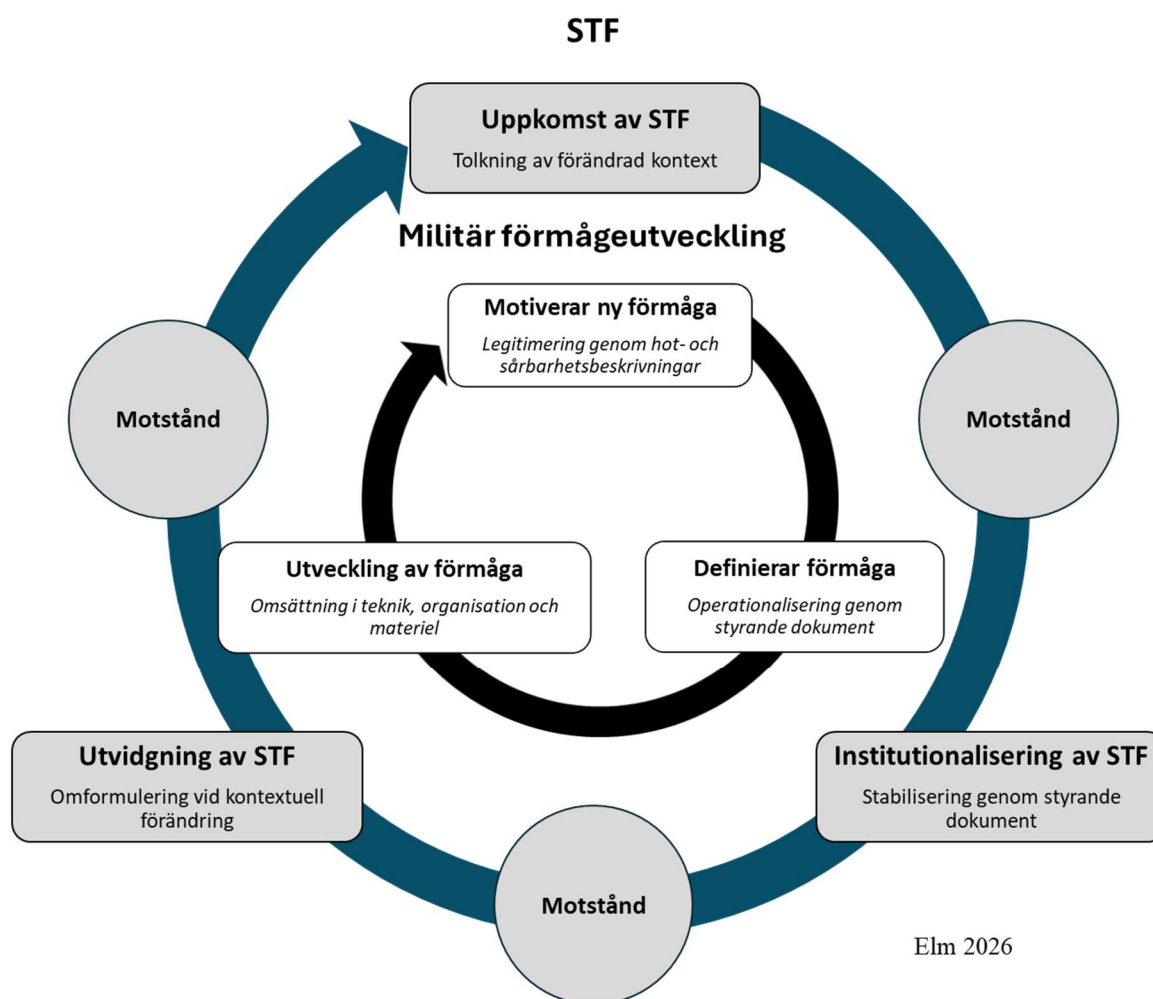
5.4. Teoretiskt bidrag och implikationer

5.4.1. STF som analytiskt raster

Analysens tillämpning av Jasanoffs (2015b:3–15) teoretiska ramverk på utvecklingen av cyberdomänen, har visat att STF kan användas för att analysera militär förmågeutveckling bortom teknologin i sig, vilket tidigare forskning har visat är önskvärt. Genom att fokusera på föreställningar möjliggörs en förståelse för varför vissa teknologier och förmågor utvecklas i en militär kontext medan andra inte gör det. Analysen visar vidare att STF inte enbart beskriver hur cyberdomänen förstås utan hur de aktivt formar hur förmågan utvecklas. Därmed fångar föreställningar som analytiskt raster inte bara innehållet i de förändringar som sker utan dynamiken i hur militär förmågeutveckling faktiskt sker, genom samproduktion och selektiv omformning.

5.4.2. Analytisk modell – Från generell teori till specifik tillämpning

Analysen i kapitel 4 har möjliggjort utvecklingen av en analytisk modell (figur 6) som visar hur Jasanoffs (2015b:3–15) processer påverkar militär förmågeutveckling. I modellen konkretiseras dessa processer genom tre empiriskt identifierade mekanismer: motivering, definition och utveckling av förmåga.



Figur 6: Analytisk modell som visar hur Jasanoffs (2015b:3–15) processer formar utvecklingen av militär förmåga.

Figur 6 visualiserar den samproduktion som beskrivs i kap 2.1 där dessa cirkulära processer motsvarar studiens teman och visar hur STF formar militär förmågeutveckling. Tema 1 motiverar förmågan genom hot- och sårbarhetsbeskrivningar som legitimerar behovet av nya förmågor. Tema 2 definierar och operationaliserar förmågan som militärt maktmedel genom styrande dokument. Tema 3 utvecklar och materialiserar STF genom organisatorisk, teknisk och metodmässig omsättning.

De grå figurerna operationaliserar Jasanoffs (2015b:3–15) processer genom att visa hur STF uppstår i relation till kontextuella förändringar (uppkomst), stabiliseras genom styrande dokument (institutionalisering) och omformas när förutsättningarna förändras (utvidgning).

HOP SA

Motstånd framträder som en varaktig del i processen och kan påverka samtliga faser, exempelvis genom motsägelsefulla föreställningar.

Modellens två cirkulära processer illustrerar att de är ömsesidigt beroende och pågår parallellt. Medan vissa STF institutionaliseras, omformas andra. Vid större kontextuella skiften kan även nya cykler initieras.

Genom denna koppling mellan Jasanoffs (2015b:3–15) ramverk och studiens empiriska teman visar modellen hur STF påverkar militär förmågeutveckling. Modellen bidrar därmed till att konkretisera hur föreställningar, organisation, teknik och metod samproduceras i en militär kontext. Modellen kan därmed vara användbar vid analys av andra framväxande militära områden.

5.5. Praktiska, samhälleliga och etiska implikationer

För den militära professionen visar studien att nya förmågor såsom cyberdomänen inte växer fram enbart genom teknologiska och organisatoriska satsningar, utan genom föreställningar vilka begreppsliggörs och institutionaliseras i doktrin och styrande dokument. Att förstå STF:s grundläggande roll möjliggör en mer informerad och reflekterad militär förmågeutvecklingsprocess.

Ur ett samhälleligt och etiskt perspektiv bidrar studien till ökad transparens i hur militära cyberförmågor motiveras och definieras i officiella dokument. Genom att synliggöra hur STF formar utvecklingen av cyberdomänen kan studien belysa de normer och antaganden som påverkar militära och politiska beslut på ett område med betydande säkerhets- och integritetsmässig påverkan. Detta kan stödja mer välgrundade och ansvarstagande beslut inom såväl politisk som militär nivå samt minska risken att empiriskt osäkra föreställningar får oproportionerligt stort genomslag.

Sammantaget kan studien därmed bidra till en mer reflexiv och medveten utveckling av nya militära förmågor och koncept.

5.6. Studiens styrkor och begränsningar

Givet studiens tolkande ansats är syftet inte att fastställa kausala samband mellan föreställningar och faktisk operativ effekt. I stället analyserar studien hur militär cyberförmåga

HOP SA

motiveras, definieras och görs handlingsbar på en institutionell nivå genom styrande dokument. Resultaten bör därför förstås som analyser av hur cyberdomänen begripliggörs i doktrin och andra styrande dokument, snarare än som utsagor om reell operativ förmåga.

Studien fokuserar på de STF som uttryckts offentligt, i linje med Jasanoff och Kims (2015a:4) definition av STF som kollektivt och offentligt uttryckta framtidsvisioner. Den omfattar därmed inte enskilda aktörers uppfattningar eller bakomliggande processer, utan de föreställningar som ges organisatorisk och politisk legitimitet.

Detta perspektiv utgör samtidigt studiens styrka. Genom att fokusera på offentliga styrdokument analyseras den nivå där föreställningar om framtida förmågor formuleras, legitimeras och omsätts i styrande riktlinjer. Det möjliggör en analys av hur militär cyberförmåga formas genom de föreställningar som etableras på politisk och militärstrategisk nivå.

I detta sammanhang utgör den analytiska modellen (figur 6) ett redskap för att synliggöra dessa processer. Modellen är inte empirisk generaliserbar men analytisk överförbar och kan användas för att studera andra framväxande militära områden.

5.7. Framtida forskning

Ett möjligt nästa steg är att empiriskt pröva den analytiska modellen (figur 6). Genom att tillämpa modellen på andra framväxande områden eller koncept såsom exempelvis multidomäna operationer (MDO) kan dess analytiska tillämpbarhet och överförbarhet undersökas och samtidigt visa på skillnader mellan specifika och mer generella mekanismer i militär förmågeutveckling.

Vidare skulle en jämförande fallstudie som kombinerar denna studies dokumentanalys av STF med studier av cyberdomänens faktiska militära förmåga, kunna belysa eventuella gap mellan föreställd och realiserad förmåga. En sådan studie skulle kunna ge ett tydligt professionsnära bidrag genom att synliggöra var i förmågeutvecklingsprocessen det finns spänningar mellan beslutsfattares föreställningar och organisatoriska, teknologiska och mänskliga förutsättningar.

HOP SA

5.8. Redovisning av generativ AI i skrivprocessen

Under arbetet med studien har generativ AI (ChatGPT, OpenAI) använts som språkligt stöd i skrivprocessen. Verket har använts för att pröva formuleringar och strukturera text. Samtliga analyser, tolkningar och slutsatser är författarens egna, och innehållet har granskats och redigerats innan publicering.

6. Litteraturförteckning

- Alvinius, A., Borglund, A. & Larsson, G. (2023). *Tematisk analys: din handbok till fascinerande vetenskap*. Upplaga 1. Studentlitteratur.
- Baxter, G. & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, 23 (1), 4–17.
- Boeke, S. & Broeders, D. (2018). The Demilitarisation of Cyber Conflict. *Survival*, 60 (6), 73–90.
- Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3 (2), 77–101.
- Bryman, A. (2018). *Samhällsvetenskapliga metoder*. Tredje upplagan. Liber AB.
- David, M. & Sutton, C.D. (2019). *Samhällsvetenskaplig metod*. 1:4. Studentlitteratur AB.
- Drake, P. & Heath, L. (2011). *Practitioner research at doctoral level: developing coherent research methodologies*. Routledge.
- Dunn Cavelt, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, 15 (1), 105–122.
- Farrell, T. & Terrif, T. (2002). *The sources of military change: culture, politics, technology*. Farrell, T. (red.) (Farrell, T., red.). Boulder. (Making sense of global security)
- Finlay, C.J. (2018). Just War, Cyber War, and the Concept of Violence. *Philosophy & Technology*, 31 (3), 357–377.
- Försvarsberedningen (2017). Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021-2025. Regeringskansliet, Försvarsdepartementet.
- Försvarsberedningen (2019). Värnkraft: Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021-2025. Regeringskansliet, Försvarsdepartementet.
- Försvarsberedningen (2023). Allvarstid: Försvarsberedningens säkerhetspolitiska rapport 2023. Regeringskansliet, Försvarsdepartementet.
- Försvarsmakten (2018). Tillväxt för ett starkare försvar: Slutredovisning av Försvarsmaktens Perspektivstudie 2016-2018. Försvarsmakten.
- Försvarsmakten (2020). *Doktrin Gemensamma Operationer 2020*. Försvarsmakten.
- Försvarsmakten (2022a). Ett starkare försvar för en utmanande framtid: Slutredovisning av Försvarsmaktens Perspektivstudie 2022. Försvarsmakten.
- Försvarsmakten (2022b). *Militärstrategisk doktrin – MSD 22*. Försvarsmakten.
- Försvarsmakten (2023). Utveckling av det militära försvaret 2025–2035. Försvarsmakten.
- Försvarsmakten (2024). *Doktrinansats Cyberförsvar 2024*. Försvarsmakten.
- Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*, 38 (2), 41–73.
- Gibson, W. (1984). *Neuromancer*. Nachdr. ACE Books. (ACE science fiction)
- Hayden, M.V. (2016). THE FUTURE OF THINGS CYBER. I: Yannakogeorgos, P.A. & Lowther, A.B. (red.) *Conflict and Cooperation in Cyberspace*. 0. uppl. CRC Press. 3–8.
- Hendriks, A., Karhunmaa, K. & Delvenne, P. (2025). Shaping the future: A conceptual review of sociotechnical imaginaries. *Futures*, 170, 103607.
- Høiback, H. (2011). What is Doctrine? *Journal of Strategic Studies*, 34 (6), 879–900.
- Høiback, H. (2013). *Understanding military doctrine: a multidisciplinary approach*. Routledge. (Cass military studies).

HOP SA

- Jakobsen, P. & Ringsmose, J. (2018). Victim of its own success: how NATO's difficulties are caused by the absence of a unifying existential threat. *Journal of Transatlantic Studies*, 16 (1), 38–58.
- Jasanoff, S. (2004a). Ordering knowledge, ordering society. I: Jasanoff, S. (red.) *States of knowledge: the co-production of science and social order*. Routledge.
- Jasanoff, S. (2004b). The idiom of co-production. I: *States of knowledge: the co-production of science and social order*.
- Jasanoff, S. (2015a). Future Imperfect: Science, Technology, and the Imaginations of Modernity. I: Jasanoff, S. & Kim, S.-H. (red.) *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*. University of Chicago Press.
- Jasanoff, S. (2015b). Imagined and Invented Worlds. I: Jasanoff, S. & Kim, S.-H. (red.) *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*.
- Jasanoff, S. & Kim, S.-H. (2009). Containing the Atom: Sociotechnical Imaginaries and Nuclear Power in the United States and South Korea. *Minerva*, 47 (2), 119–146.
- Jasanoff, S. & Kim, S.-H. (2013). Sociotechnical Imaginaries and National Energy Policies. *Science as Culture*, 22 (2), 189–196.
- Jasanoff, S. & Kim, S.-H. (red.) (2015). *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*. University of Chicago Press.
<https://www.bibliovault.org/BV.landing.epl?ISBN=9780226276663> [2025-10-07]
- Kerr, J.A. (2023). Assessing Russian Cyber and Information Warfare in Ukraine: Expectations, Realities, and Lessons. *CNA*,
- Kerttunen, M. (2023). The Absolute Ideal: Military Cyber Capabilities in War and Society. *German Institute for International and Security Affairs*,
- Kier, E. (1995). Culture and Military Doctrine: France between the Wars. *International Security*, 19 (4), 65.
- Libicki, M.C. (2021). *Cyberspace in peace and war*. Naval institute press. (Transforming war)
- Limnell, J. & Rid, T. (2014). Is Cyberwar Real? Gauging the Threats. *Council on Foreign Relations*, 2014
- Liwång, H., Andersson, K.E., Bang, M., Malmio, I. & Tärnholm, T. (2023). How can systemic perspectives on defence capability development be strengthened? *Defence Studies*, 23 (3), 399–420.
- Malmio, I. (2023). Ethics as an enabler and a constraint – Narratives on technology development and artificial intelligence in military affairs through the case of Project Maven. *Technology in Society*, 72, 102193.
- Modig, O. & Andersson, K. (2022). Military Innovation as the Result of Mental Models of Technology. *Scandinavian Journal of Military Studies*, 5 (1), 45–62.
- Mumford, E. (2006). The story of socio-technical design: reflections on its successes, failures and potential. *Information Systems Journal*, 16 (4), 317–342.
- Ní Mhurchú, A. & Shindo, R. (2016). *Critical Imaginations in International Relations*. Taylor and Francis. (Interventions)
- Nisser, J. (2025). *Implementing Military Doctrine*. Department of War Studies.
- Regeringen (2020). Regeringens proposition 2020/21:30: Totalförsvaret 2021–2025. Regeringskansliet, Försvarsdepartementet.
- Regeringen (2024a). Nationell strategi för cybersäkerhet 2025-2029. Skrivelse, Regeringskansliet, Försvarsdepartementet.

HOP SA

- Regeringen (2024b). Regeringens proposition 2024/25:34: Totalförsvaret 2025–2030. Regeringskansliet, Försvarsdepartementet.
- Robinson, M., Jones, K. & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, 49, 70–94.
- Samimian-Darash, L., Sheniak, A. & Rotem, N. (2025). Unboxing the imaginary: Typology of future imagination techniques in high-tech development. *Social Studies of Science*, 55 (4), 542–564.
- Sartori, L. & Bocca, G. (2023). Minding the gap(s): public perceptions of AI and socio-technical imaginaries. *AI & SOCIETY*, 38 (2), 443–458.
- Smeets, M. (2022). *No shortcuts: why states struggle to develop a military cyber-force*. Hurst & Company. (Oxford scholarship online Political Science).
- Thunholm, P. & Palmgren, A. (2017). Hur kan doktriner utvecklas och implementeras i Försvarsmakten. Försvarshögskolan.
- Thunholm, P., Widén, J. & Wikström, N. (2018). *Militära arbetsmetoder: en lärobok i krigsvetenskap*. Universus Academic Press.
- Venesson, P. (2010). *Approaches and methodologies in the social sciences: a pluralist perspective*. Della Porta, D. & Keating, M. (red.) (Della Porta, D. & Keating, M., red.) Reprinted with corr. Cambridge University Press.
- Zehfuss, M. & Vaughan-Williams, N. (2024). From Security-Space to Time-Race: Reimagining Borders and Migration in Global Politics. *International Political Sociology*, 18 (3), olae019.
- Ølgaard, D.M. (2025). The New Technopolitics of War: (Re)imagining Agency and Authority in Military Affairs. *Global Policy*, 16 (3), 474–479.
- Ördén, H. (2024). The neuropolitical imaginaries of cognitive warfare. *Security Dialogue*, 55 (6), 607–624.

HOP SA

Bilaga 1 – Dokumentöversikt*Dokumentöversikt Korpus A och B, dokumenten återfinns även i litteraturförteckningen.*

Korpus A	Korpus B
Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025, 2017	Ett starkare försvar för en utmanande framtid - Slutredovisning av Försvarmaktens Perspektivstudie 2022, 2022
Tillväxt för ett starkare försvar - Slutredovisning av Försvarmaktens Perspektivstudie 2016–2018, 2018	Utveckling av det militära försvaret 2025–2035, 2023
Värnkraft: Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025, 2019	Allvarstid: Förvarsberedningens säkerhetspolitiska rapport 2023, 2023
Doktrin Gemensamma Operationer, 2020	Doktrinansats Cyberförsvar 2024, 2024
Regeringens proposition 2020/21:30, Totalförsvaret 2021–2025, 2020	Regeringens proposition 2024/25:34: Totalförsvaret 2025–2030, 2024
Militärstrategisk doktrin – MSD 22, 2022	Överväganden om det militära försvarets utformning, 2025

HOP SA

Bilaga 2 – Kodningsindikatorer

Operationalisering av Jasanoffs (2015b:3–15) processer i syfte att göra dem användbara som kodningsindikatorer vid analysen av empirin.

Processer	Analytisk funktion	Analytiska frågor	Indikatorer i empirin
Uppkomst (Origins)	Möjliggör analys av hur cyberdomänen görs till ett militärt problemområde genom sårbarhet- och hotbeskrivningar	Vilket problem formuleras? Vilken sårbarhet eller hotbild lyfts fram? Vilka sårbarheter och hotbilder skall förmågan kunna hantera?	Hot- och sårbarhetsbeskrivningar. Nya problemdefinitioner, referenser till förändrad omvärld eller teknisk utveckling.
Institutionalisering (Embedding)	Möjliggör analys av hur föreställningar om cyberdomänen stabiliseras och görs styrande genom doktrin och styrande dokument.	Hur görs föreställningen självklar eller normerande? Hur definieras cyberdomänen och dess roll? Hur kopplas den till etablerade militära begrepp och strukturer?	Normativa formuleringar ("ska", "bör"), fasta definitioner, standardiserade begrepp, införlivande i doktrin eller styrande dokument samt koppling till etablerade domäner, roller eller strukturer.
Motstånd (Resistance)	Möjliggör analys av spänningar, osäkerheter och alternativa förståelser inom och mellan styrande dokument.	Finns osäkerhet eller tvekan? Förekommer motstridiga formuleringar? Undviks ställningstaganden? Indikerar texten organisatorisk eller professionell friktion?	Ambivalenta formuleringar, parallella förståelser, hänvisningar till kompetensbrist eller oklar ansvarsfördelning.
Utvidgning (Extensions)	Möjliggör analys av hur föreställningar förändras i takt med nya erfarenheter och kontextuella skiften.	Tillkommer nya roller eller funktioner? Förändras hur cyberdomänen beskrivs? Breddas dess användning? Skiljer sig formuleringar mellan dokument och över tid?	Nya användningsområden, förändrad tidshorisont, breddad funktion, koppling till nya domäner eller aktörer, omformuleringar mellan korpus A och B.

HOP SA

Bilaga 3 – Kodningsexempel tematisk analys

Kodningsexempel för respektive kategori och tema, innehållandes exempel från både korpus A och B.

Dokument	År	Meningsbärande enhet	Kod	Tema
Doktrinansats Cyberförsvaret 2024, 2024	2024	“En aktör med motivation, resurser och teknisk kapacitet kan agera i cyberdomänen och åstadkomma strategiska och storskaliga effekter som är oproportionerliga till aktörens storlek” (Försvarmakten 2024:27)	1.1 Hotbild samt hybrid- och gråzonsproblematik	Tema 1: STF om egna sårbarheter och extern hotbild
Militärstrategisk doktrin – MSD 22, 2022	2022	“Effekterna av en cyberattack kan få lika stora konsekvenser för samhällsviktiga funktioner som ett konventionellt väpnat angrepp.” (Försvarmakten 2022b:34)	1.2 Digitalisering som källa till sårbarheter	Tema 1: STF om egna sårbarheter och extern hotbild
Motståndskraft - Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025, 2020	2017	“Det blir allt svårare att säga var den civila infrastrukturen slutar och var den militära börjar.” (Försvarsberedningen 2017:113)	1.3 Totalförsvaret och det civil-militära ömsesidiga beroendet	Tema 1: STF om egna sårbarheter och extern hotbild
Ett starkare försvar för en utmanande fram-tid - Slutredovisning av Försvarmaktens Perspektivstudie 2022, 2022	2022	“Cyberförsvaret har förmåga att genomföra offensiva och defensiva cyberoperationer samt att upptäcka, identifiera och avvärja hot mot digitala informationssystem och elektroniska kommunikationstjänster.” (Försvarmakten 2022a:67)	2.1 Militär cyberförmåga - offensiv och defensiv	Tema 2: STF om cyberdomänen som militärt maktmedel
Tillväxt för ett starkare försvar - Slutredovisning av Försvarmaktens Perspektivstudie 2016–2018, 2018	2018	“Cyberförmågan kan också ingå som en komponent i påverkansoperationer.” (Försvarmakten 2018:106)	2.2 Cyberdomänen som en integrerad förmåga	Tema 2: STF om cyberdomänen som militärt maktmedel
Doktrin Gemensamma operationer, 2020	2020	“Vissa delar av en operation kan dock ledas centraliserat genom direktstyrning, till exempel då det är höga krav på samordning i tid och rum eller då en specifik resurs används, som till exempel vid sjömålsbekämpning och offensiva cyber- och informationsoperationer.” (Försvarmakten 2020:32)	2.3 Militärstrategisk resurs och ledning	Tema 2: STF om cyberdomänen som militärt maktmedel

HOP SA

Värnkraft - Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021– 2025, 2019	2019	“Ett väl fungerande cyberförsvaret behöver ha goda möjligheter att detektera cyberangrepp eller försök till cyberangrepp.” (Försvarsberedningen 2019:254)	2.4 Målbild och normativa utsagor om cyberdomänen som krigföringsdomän	Tema 2: STF om cyberdomänen militärt maktmedel
Ett starkare försvar för en utmanande fram-tid - Slutredovisning av Försvarsmaktens Perspektivstudie 2022, 2022	2022	“Vidare förstärks även nya områden som varit under uppstart till att bli fullstora områden. Exempel på sådana är cyberoperationer, artificiell intelligens och autonoma system.” (Försvarsmakten 2022a:88)	3.1 Organisation, utbildning och kompetens	Tema 3: STF om en stärkt militär cyberförmåga
Tillväxt för ett starkare försvar - Slutredovisning av Försvarsmaktens Perspektivstudie 2016–2018, 2018	2018	“En kontinuerlig forskning och utveckling av nya tekniker krävs för att i alla lägen kunna skapa en lägesbild och hantera incidenter.” (Försvarsmakten 2018:63)	3.2 Teknik, innovation och utveckling	Tema 3: STF om en stärkt militär cyberförmåga
Doktrinansats Cyberförsvaret 2024, 2024	2024	“Sammantaget ställer dessa ledningsförhållanden särskilda krav på cyberförsvarets förmåga att leda och samordna flera olika typer av cyberoperationer samtidigt” (Försvarsmakten 2024:41)	3.3 Styrning, ansvar och samverkan	Tema 3: STF om en stärkt militär cyberförmåga
Tillväxt för ett starkare försvar - Slutredovisning av Försvarsmaktens Perspektivstudie 2016–2018, 2018	2018	“Cyberrymden kommer att utgöra en allt viktigare förutsättning för att kunna genomföra både informationsoperationer och konventionella militära operationer.” (Försvarsmakten 2018:30)	3.4 Målbild och normerande utsagor om utveckling av förmågan	Tema 3: STF om en stärkt militär cyberförmåga