Lunds universitet - Statsvetenskapliga institutionen
UNDA23 - Underrättelseanalys: Fortsättningskurs
Delkurs 4: Uppsats (9hp)
Handledare: Johan Matz

2023-05-28

En snabbt föränderlig värld

En förståelse för den svenska underrättelseinstitutionens bedömning av disruptiva teknologier och hot

Isac Ederberg
Olof Svarén

Innehållsförteckning

1. Inledning

Aldrig tidigare i världshistorien har den teknologiska utvecklingen fortskridit med en sådan oerhörd hastighet som den gör idag – somliga påstår till och med en samtida människa genomlever större vetenskapliga framsteg under dess livstid än alla dess förfäder har gjort tillsammans (Roser 2023). Förutom ett, åtminstone i västvärlden, ständigt växande välstånd innebär den teknologiska utvecklingen därtill, som en följd av tillämpningen av ny teknologi inom underrättelseverksamhet och krigföring, en omfattande förändring i hur mellanstatliga relationer ter sig (Nye 2004, s. 15-19). En häri central aspekt är att de hot som stater numera projicerar på varandra, och därigenom även deras bedömning av dito, är av aldrig tidigare skådad mångsidighet; en utveckling som i synnerhet får konsekvenser för världens underrättelsetjänster.

Sakläget – att den snabba teknologiska utvecklingen innebär allt mer komplexa mellanstatliga bedömningar av förmåga och intention – kan påstås ha sin kulmen i så kallade disruptiva teknologier. Dessa teknologier, vilka härvid definieras som sådana som är nydanande och kan medföra revolutionerande förändringar inom underrättelseverksamhet och krigföring, manifesterar nämligen ytterligheten i ett motsatsförhållande: å ena sidan gör stater allt i sin makt för att hålla den egna utvecklingen och användningen av dem hemlig; å andra sidan söker andra stater med alla till buds stående medel bedöma teknologierna samt vilka hot de konstituerar. Sålunda präglas staters bedömning av disruptiva teknologier och hot, annorlunda uttryckt av teknologierna som sådana samt det hot som de utgör i händerna på andra aktörer, av lika delar osäkerhet och vikt, vilket sammantaget bottnar för vansklighet i bedömningen.

Med utgångspunkt i ovanstående syftar föreliggande uppsats till att utröna en tudelad frågeställning: vilka narrativ går att urskilja i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot; och hur kan dessa narrativ förstås? Härvid åsyftar *den svenska underrättelseinstitutionen*, i syfte att avgränsa studieobjektet, Sveriges vedertaget tre mest centrala underrättelsemyndigheter: MUST, SÄPO och FRA. Därtill ämnar

uppsatsen undersöka deras *offentliga bedömning* genom att studera myndigheternas årsrapporter mellan 2014 och 2022, vilka i högsta grad är bearbetade och utgivna med offentligheten som tilltänkt läsare. Slutligen, med begreppet *narrativ*, avser föreliggande uppsats återkommande beskrivningar och berättelser i årsrapporterna, vilka genom sin förekomst vittnar om underrättelseinstitutionens gängse offentliga bedömning av disruptiva teknologier och hot.

2. Bakgrund

2.1. Disruptiva teknologier och hot

Med utgångspunkt i den i inledningen presenterade definitionen av disruptiva teknologier går det att konstatera att begreppet är vittfamnande och relativt godtyckligt. Som med de flesta paraplybegrepp är det emellertid inte dess definition i sig, utan vilka andra begrepp som faller inom dess omfång, som är intressant, och åsikterna kring vilka dessa bör vara skiljer sig åt. En för Sverige betydelsefull försvarsrelaterad entitet – Europeiska försvarsbyrån – identifierar sex disruptiva teknologier: kvantteknologi; artificiell intelligens; analys av stora datamängder; robotar och autonoma vapensystem; hypersoniska vapensystem och rymdteknologier; samt nya avancerade material (Clapp 2022, s. 1). Vidare identifierar en på Sverige måhända än mer inflytelserik aktör – NATO – samma disruptiva områden, samt därtill även bioteknologi, energi och propulsion (NATO 2022). Den svenska underrättelseinstitutionen torde således urskilja liknande, om inte samma, disruptiva teknologier, eftersom den i stor utsträckning kan förväntas influeras av de båda mellanstatliga organisationerna. Ett sådant antagande styrks därtill av att de svenska underrättelsemyndigheterna, i sina årsrapporter mellan 2014 och 2022, mer eller mindre återkommande genomför bedömningar av huvudsakligen fyra olika disruptiva teknologier och hot: *cyberdomänen*; *rymdteknologier*; *artificiell intelligens* och *kvantdatorer* (se ex. FRA 2015, s. 4; SÄPO 2021, s. 18; SÄPO 2018, s. 5; MUST 2020, s. 64).

Med *cyberdomänen* åsyftar föreliggande uppsats allt som är relaterat till informationsteknologi, och arenan har under senare år utvecklats till en av de mest framstående spelplanerna för underrättelseverksamhet; en trend som sannolikt kommer att hålla i sig (Kindvall & Tarras-Wahlberg 2021, s. 113-115). När mer och mer information, såväl öppen som hemlig, förläggs till databaser, intranät och internet följer ju cyberspionaget som ett brev på posten. Därtill utgör cyberdomänen en ny plattform för påverkansoperationer, vilket har resulterat i att metoder som desinformationskampanjer och angrepp på kritisk infrastruktur har fått en ny skepnad (Świątkowska 2020, s. 130). Vidare avser *rymdteknologier* sådant som på ett eller annat sätt är verksamt i rymden, och begreppet innefattar såväl sofistikerade resurser för övervakning som regelrätta vapensystem (Kindvall & Tarras-Wahlberg 2021, s. 13;53). På senare år har fler och fler stater tagit plats på rymdarenan samtidigt som dess centralitet i såväl civila som militära sammanhang har vuxit, vilket har renderat den allt mer kompetitiv (Kehler 2012, s. 26). Att rymden utgör allmänt territorium innebär därtill att maktutövning och diplomati försvåras, vilket generellt medför att domänen präglas av mellanstatlig instabilitet (Johnson-Freese 2018, s. 435). Vidare innebär *artificiell intelligens* maskiner som på ett eller annat sätt uppvisar ett beteende som förknippas med mänsklig intelligens, och ifrågavarande teknologis lavinartade utveckling har under senare år resulterat i enorma tillämpningsmöjligheter inom såväl den civila som militära sektorn (Dieu & Montasari 2022, s. 22-24). Kopplat till underrättelseverksamhet och hybridkrigföring innebär artificiell intelligens både defensiva och offensiva möjligheter, och i praktiken kan teknologin användas för allt mellan att detektera falskt bildmaterial till att iscensätta storskaliga desinformationskampanjer (Świątkowska 2020, s. 133-135). Därtill är artificiell intelligens av stort intresse för världens stater ur ett holistiskt perspektiv, då det i symbios med andra disruptiva teknologier kan skapa stora synergieffekter, såsom avancerad analys av cyberangrepp eller koordinering av rymdbaserad underrättelseinhämtning (Raska 2019, s. 66). Slutligen åsyftar *kvantdatorer* sådana maskiner som bygger på en annorlunda datorarkitektur jämfört med vanliga datorer, och som utnyttjar kvantfysik för att erbjuda användaren nya beräkningsmöjligheter

(Amselem et al. 2014, s. 9-11). Ifrågavarande teknologi skiljer sig från ovanstående i det faktum att utvecklingen ännu inte är så långt kommen att den är operativ, men forskare bedömer att fullt fungerande kvantdatorer kommer se dagens ljus inom tio till tjugo år (Grobman 2020, s. 56-57). Då kommer underrättelseverksamhet, och i synnerhet signalspaning, genomgå omvälvande förändringar, eftersom kvantdatorns revolutionerande beräkningsmöjligheter förutspås kunna forcera en icke oansenlig del av de krypteringsalgoritmer som stater använder idag.

I strävan att strukturera analysen av underrättelsemyndigheternas årsrapporter avgränsar sig föreliggande uppsats till att uteslutande beakta den svenska underrättelseinstitutionens bedömning av de ovan introducerade disruptiva teknologierna och hoten. Utöver att konstituera en lämplig avgränsning då det, såsom ovan belagt, faktiskt förekommer bedömningar av ifrågavarande teknologier och hot i årsrapporterna, är just dessa teknologier dessutom av särskilt intresse i förhållande till frågeställningen av två anledningar. För det första bär samtliga en tydlig koppling till underrättelseverksamhet, då de på olika sätt utgör revolutionerande verktyg i såväl underrättelseinhämtning som olika typer av otillbörliga påverkansförsök. Robotar och autonoma vapensystem lär exempelvis förvisso medföra stora förändringar i hur krig utkämpas, och därigenom även i hur mellanstatliga relationer ter sig, men deras inverkan på underrättelseverksamhet som sådan lär vara ringa, utöver att möjligtvis styra inhämtningens inriktning. För det andra konstituerar alla fyra teknologier så kallade produkter med dubbla användningsområden, vilket innebär att de kan utvecklas och användas i såväl ett civilt som militärt sammanhang. Föreliggande renderar ifrågavarande teknologier särskilt intressanta ur ett svenskt perspektiv, eftersom Sveriges öppna forskningsklimat och relativt framstående civila sektor riskerar bli måltavla för fientlig underrättelseinhämtning riktad mot just dessa.

2.2. Litteraturöversikt

Mellanstatliga förhållanden bör generellt betraktas som ett välutforskat fenomen inom ämnesområdena statsvetenskap, internationella relationer och underrättelseanalys. Vid efterforskning inför föreliggande uppsats återfanns emellertid inga vetenskapliga alster vars frågeställning eller metod låg i linje med dito i ifrågavarande arbete, vilket, utöver att skänka uppsatsen en viss inomvetenskaplig relevans, kan förklaras av dess nisch – disruptiva teknologier och hot. I strävan att ändå underbygga arbetet med lämplig litteratur introducerar föreliggande avsnitt därför inledningsvis tre övergripande teorier om mellanstatliga relationer, för att därefter presentera litteratur som mer djuplodat avhandlar hur stater bedömer disruptiva teknologier och hot. Förhoppningen är att de två typerna av alster i symbios ska konstruera ett vetenskapligt underlag som kan agera substitut för tidigare forskning kring narrativ i underrättelseinstitutioners offentliga bedömning av disruptiva teknologier och hot, och som således kan utgöra en god utgångspunkt för föreliggande uppsats i stort.

2.2.1. Mellanstatliga relationer

Mellanstatlig offentlighet och hemlighet

I sin bok *Secret Wars* (2018, s. 13-14;41-44) framför Carson en scenanalogi som förståliggör hur stater navigerar offentlighet och hemlighet på den internationellpolitiska spelplanen. Analogin grundar sig i att stater antingen kan interagera offentligt – framför publiken på scenen – eller hemligt – bortom publiken bakom scenen. Mellanstatlig interaktion som sker på scenen konstituerar därmed allmänt kända handlingar, medan sådan interaktion som sker bakom scenen endast är känd av andra statliga aktörer. Ifrågavarande sakläge kan utnyttjas av stater i det internationellpolitiska spelet genom att föra en viss agenda på scenen och en annan bakom, såväl i syfte att dupera varandra som att undvika ömsesidigt destruktiva utfall. Å ena sidan kan ju stater använda scenen för att vilseleda allmänheten och andra stater samtidigt som de undanhåller den verksamhet de faktiskt ägnar sig åt bakom scenen. Å

andra sidan kan stater också använda scenen för att vidmakthålla deras offentliga värdighet samtidigt som de når gemensamt fördelaktiga, men måhända ärekränkande, överenskommelser bakom scenen.

Mellanstatlig hotbedömning

I sin bok *Knowing the Adversary* (2014, s. 4-6) presenterar Yarhi-Milo en systemorienterad förståelseram för mellanstatliga hotbildskonstruktioner som bygger på tre teser, vilka i kombination med varandra ger upphov till staters sammantagna hotbedömningar. Den första – tesen om förmåga – anför att stater bedömer varandras intentioner baserat på militär kapacitet och rustningspolitik, och att en stat som utvidgar sin förmåga att medelst våld uppnå internationellpolitiska målsättningar således torde uppfattas som ett hot. Den andra – tesen om agerande – innebär att stater bedömer varandras intentioner baserat på mellanstatligt uppförande och beteende, och att en stat som agerar som ett hot på den internationellpolitiska spelplanen sålunda också torde tolkas som dito. Den tredje och sista – tesen om strategisk militärdoktrin – framhåller att stater bedömer varandras intentioner baserat på militär strategi, och att en stat vars doktrin eller sedvanliga handlingslinje präglas av internationellpolitisk aggressivitet därigenom torde uppfattas som ett hot.

Mellanstatlig säkerhet

I sin bok *People, States and Fear* (1991, s. 132) identifierar Buzan fem olika kategorier av hot som kan projiceras på stater – militära, politiska, samhälleliga, ekonomiska och ekologiska – och föreliggande uppsats avgränsar sig, med hänvisning till relevans, till de fyra förstnämnda. Militära hot åsyftar bekämpning av en stats elementära fysiska skyddsvärden, medan politiska hot avser underminering av den institutionella stabiliteten i en stat. Vidare kan samhälleliga hot vara en del av såväl militära som politiska diton, eller en kombination av båda, medan ekonomiska hot arbiträrt innefattar sådant som försvagar en stats ekonomi.

Därtill anför Buzan (1991, s. 93-96) att en stats säkerhet kan förstås som produkten av två av varandra oberoende systemorienterade variabler. Den första –

statens internationella makt – är dess förmåga att utöva externt inflytande över de stater som utgör dess internationellpolitiska omgivning, och kan exempelvis ta form av militär styrka. Den andra – statens sociopolitiska sammanhållning – är dess interna enighet och stabilitet, och kan exempelvis ta form av befolkningens tilltro till statliga institutioner. En stat är följaktligen olika mottaglig, eller annorlunda uttryckt olika sårbar, för olika typer av hot beroende på hur ifrågavarande variabler ter sig.

2.2.2. Staters bedömning av disruptiva teknologier och hot

Oberoende forskares perspektiv

I artikeln *International competition in the digital age* (2020, s. 14-16) för Rekowski ett resonemang om att stormakter numera betraktar digital teknologi, i vilket informationsteknologi ingår, som en avgörande aspekt i deras strävan efter global dominans. Sakläget, menar Rekowski, illustreras inte minst av att det har uppstått en sorts kapprustning inom området, samt av att verksamhet i cyberdomänen numera är av absolut central utrikes- och säkerhetspolitisk betydelse. Härvid påtalas därtill att flera av världens stater, i synnerhet dess stormakter, söker utveckla en fullständigt egen och oberoende förmåga inom ifrågavarande disruptiva område i syfte att undvika bilaterala interdependenser, vilka de bedömer som hot mot deras nationella säkerhet.

Vidare skriver Świątkowska, i artikeln *Offensive actions in cyberspace - A factor shaping geopolitical order* (2020, s. 127-129), att det finns en grundläggande skillnad mellan hur avskräckning och vedergällning ter sig på den konventionella spelplanen respektive i cyberdomänen, vilket gör arenorna till vitt skilda ytor för mellanstatlig interaktion. På den konventionella spelplanen är staters försvarsstrukturers kanske huvudsakliga syfte att agera som en avskräckande faktor, då de förkroppsligar den vedergällning som en antagonistisk aktör skulle utsättas för ifall den agerade fientligt. Vedergällningen, och därigenom den avskräckande effekt som hotet därom bär, är sålunda avhängigt den defensiva aktörens förmåga att fastställa vem som har agerat fientligt, samt att därtill genomföra en proportionerlig motåtgärd. I cyberdomänen är vedergällning emellertid sällan så rättframt, då det kan vara oerhört svårt att identifiera

vilken aktör som står bakom en fientlig handling. Därigenom förlorar också avskräckningen en del av sin tröskeleffekt, och antagonistiska stater bedömer det allt oftare som värt att ta större offensiva risker i sin cyberverksamhet för att uppnå strategiska målsättningar.

Vidare resonerar Johnson, i artikeln *Artificial intelligence & future warfare: implications for international security* (2019, s. 147-148), om att den snabba utvecklingen inom artificiell intelligens kommer ha en revolutionerande och potentiellt deterministisk inverkan på militär makt och strategiskt tänkande, samt därigenom även på världspolitiken i stort. Härvid talar han om att tekniken, ifall den lämnas oreglerad, tveklöst kommer att bidra till en växande mellanstatlig instabilitet och osäkerhet, i synnerhet stormakter emellan. Artificiell intelligens har nämligen redan börjat ge ringar på det internationellpolitiska vattnet, då det amerikanska försvarsdepartementet redan 2016 offentliggjorde en uppsättning studier kring hur tekniken ska kunna användas för att främja statens militära dominans. Kina har därtill, i sin strävan att bli världens nya supermakt, sjösatt en agenda för civil-militära synergieffekter med fokus på innovation inom just artificiell intelligens. Vidare genomför även Ryssland målmedvetna satsningar inom ifrågavarande teknikområde, då staten har som målsättning att robotisera betydande delar av sin militär under kommande år. Sammantaget, menar Johnsson, bör utvecklingen ses som ett bevis för att världens stater bedömer artificiell intelligens som en transformativ och potentiellt avgörande disruptiv teknologi, vilken de måste anamma för att värna sin fortsatta överlevnad.

Statstjänstemäns perspektiv

I artikeln *The impact of emerging and disruptive technologies on security* (2021, s. 261-262) skriver Oprișor, i egenskap av säkerhetsrådgivare åt Rumäniens president, att disruptiva teknologier, trots sina många civila fördelar, konstituerar ett annalkande hot mot individens, statens och det internationella samfundets säkerhet. Han menar nämligen att det har uppstått en global kapprustning inom forskning kring och implementering av disruptiva teknologier i underrättelseverksamhet och krigföring, vilket fordrar världens stater, i synnerhet dess stormakter, att fatta drastiska strategiska

beslut. Härvid påpekar han också att allt fler stater numera bedömer innovationsförmåga som en central egenskap på den internationellpolitiska spelplanen, då det, som ett resultat av kapprustningen, är förenat med stor statlig sårbarhet och osäkerhet att hamna på efterkälken. Vikten av disruptiv innovation förstärks därtill, oavsett om staten är en stormakt eller ej, av att ett försvar mot disruptiva hot förutsätter en viss kompetens inom området, vilket innebär att även mindre statliga aktörer måste hålla sig med en viss disruptiv förmåga för att värna sin överlevnad. Sammantaget menar följaktligen Oprişor att stater med stor förmåga inom disruptiva teknologier projicerar ett hot mot sin omvärld, och att innovationsförmåga har kommit att bli en allt viktigare indikator i mellanstatliga hotbedömningar.

Vidare skriver Kehler, i egenskap av general i det amerikanska flygvapnet, i artikeln *Implementing the national security space strategy* (2012, s. 18-21) att den amerikanska särställningen som hegemon på rymdarenan är oerhört fördelaktig, och att USA måste värna den även i framtiden. Han påpekar att den amerikanska statens beroende av rymdteknologi aldrig har varit större, och att USA, som ett resultat av en förändrad internationellpolitisk verklighet, därmed står inför en stor utmaning. Det långtgående beroendet av rymdbaserade förmågor kan nämligen utgöra en sårbarhet, och Kehler bedömer kallt att USA:s antagonister noggrant studerar hur den eventuellt kan utnyttjas. Härvid påtalar han därtill att hoten mot USA på rymdarenan har vuxit under senare år, då allt fler stater, som en följd av att rymdteknologi generellt har blivit billigare och allt mer tillgänglig, söker skörda de frukter som tidigare bara varit världens stormakter förunnade. Kehler bedömer följaktligen sammantaget att framtidens konflikter kommer att vara av flerdimensionell natur, och att avancerad rymdteknologi, i egenskap av kraftfull styrkemultiplikator, kommer att spela en central roll däri.

2.3. Teoretiskt ramverk

Den empiriska studien av den svenska underrättelseinstitutionens årsrapporter som utgör fundament för föreliggande uppsats identifierar, såsom klarläggs i det nedan presenterade operationaliseringsavsnittet, tre kategorier av narrativ i den svenska

underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot: sådana som tar sikte på disruptiva teknologier och hot i sig själva; sådana som tar sikte på krig, konflikter och hot; samt sådana som tar sikte på Sveriges sårbarheter. I strävan att – såsom frågeställningens andra del föreskriver – förståliggöra ifrågavarande kategorier av narrativ, eller närmare bestämt de narrativ som konstituerar kategorierna, lämpar sig därför ett tredelat teoretiskt ramverk. I det sedermera presenterade analyskapitlet tillämpas därför Carsons scenanalogi på den kategori av narrativ som avser underrättelseinstitutionens syn på disruptiva teknologier och hot i sig själva, eftersom ett sådant ramverk är användbart i att förståliggöra mellanstatlig offentlighet och hemlighet. Vidare appliceras Yarhi-Milos tre systemorienterade teser på den kategori av narrativ som avser myndigheternas syn på krig, konflikter och hot, eftersom ett sådant ramverk kan problematisera mellanstatlig hotbedömning. Slutligen används Buzans hotkategorier samt teori om starka och svaga stater för att analysera den kategori av narrativ som avser Sveriges sårbarheter, eftersom ett sådant ramverk skapar en djupare förståelse för mellanstatlig säkerhet.

3. Metod

3.1. Metodologisk utgångspunkt

Föreliggande arbetes frågeställning är av tudelad struktur, där den första är att uppsatsen söker identifiera narrativ i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot, och den andra är att den söker förstå desamma. Medan förståelsen för narrativen följaktligen utgör uppsatsens ändhållplats kan det föregående gedigna arbetet med att urskilja dito anses vara av större metodologisk vikt, då en förståelse för narrativen aldrig hade kunnat komma till stånd utan att de först hade identifierats. Härvid är det inledningsvis viktigt att påpeka att frågeställningens försök att förstå den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot i form av narrativ konstituerar ett metodologiskt vägval i sig självt. Vid efterforskning inför föreliggande uppsats återfanns

förvisso ingen litteratur att hämta inspiration från, men det är exempelvis inte omöjligt att föreställa sig en metodologi som snarare tar sikte på att identifiera trender över tid i underrättelsemyndigheternas offentliga bedömning av disruptiva teknologier och hot. En sådan angreppsvinkel hade kunnat skapa en djupare förståelse för huruvida deras bedömning har förändrats av särskilda internationellpolitiska händelser, och i praktiken hade den exempelvis kunnat realiseras genom en deskriptiv argumentationsanalys. Hade ett sådant tillvägagångssätt därtill kompletterats med ett värderande inslag hade det dessutom kunnat medföra en djupare insikt kring relevansen i de svenska underrättelsemyndigheternas offentliga bedömningar, och således problematisera vad som står bakom deras påståenden (Boréus 2018, s. 121-122). En nackdel med en sådan metod är emellertid att valet av tidsbundna bedömningar att jämföra med varandra riskerar bli alltför godtyckligt, samt att kopplingen till internationellpolitiska händelser, som förövrigt riskerar bli godtycklig i sig själv, inte nödvändigtvis bidrar till att besvara frågeställningens essens.

Vidare, oavsett om valet faller på att försöka identifiera narrativ, trender eller något annat, kan den svenska underrättelseinstitutionens bedömning av disruptiva teknologier och hot urskiljas ur flera olika typer av primärmaterial, och arbetet hade således inte nödvändigtvis behövt begränsa sig till dess årsrapporter. Härvid hade exempelvis avsekretessbelagt material, intervjuer med underrättelsetjänstemän eller rapporter av annat slag kunnat vara av stort intresse, då sådana källor lika väl, om inte än bättre, representerar underrättelsemyndigheternas faktiska bedömning. En nackdel med sådant material är emellertid att det, åtminstone i jämförelse med årsrapporter, präglas av en påtaglig inkonsekvens, samt att det därigenom även är särdeles svårt att motivera en rimlig avgränsning av detsamma. Dessutom fastslår frågeställningen att uppsatsen avser undersöka underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot, vilken inte på samma sätt kan påstås skina igenom i ifrågavarande alternativa material.

Den i föreliggande uppsats valda metodologiska utgångspunkten är således långt ifrån den enda, men bär med sig ett antal fördelar kopplat till det ämnesområde som den syftar till att studera. En första sådan är att är att valet att urskilja just narrativ i den

svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot möjliggör en relativt rättfram metod samtidigt som det minimerar godtycklighet. Det sistnämnda är av särskild vikt då frågeställningens andra del – hur narrativen kan förstås – är förhållandevis godtycklig i sig själv, och således gynnas av att vila på ett vederhäftigt fundament. En andra fördel är därtill att valet av underrättelseinstitutionens årsrapporter som primärmaterial skänker uppsatsen en viss reliabilitet, då de följer ett konsekvent format och därigenom lämpar sig för att studeras systematiskt.

3.2. Metodval

I strävan att besvara frågeställningens första del grundar sig föreliggande uppsats i ett egenkonstruerat textanalytiskt ramverk, vilket närmast påminner om en induktiv kvalitativ innehållsanalys med ett narrativanalytiskt bihang. Den svenska underrättelseinstitutionens 27 årsrapporter mellan 2014 och 2022 bearbetas nämligen först systematiskt utifrån ett på förhand stipulerat kriterium, i syfte att identifiera sådant textinnehåll som avser disruptiva teknologier och hot. Det relevanta materialet undergår sedermera en narrativanalytisk process, i syfte att tolka textinnehållet och identifiera narrativ i detsamma (Robertson 2018, s. 224-226). Analysens induktiva karaktär är följaktligen en konsekvens av att de narrativ som uppsatsen söker identifiera på intet sätt är förutbestämda, utan utkristalliserar sig under arbetets gång (Boréus & Kohl 2018, s. 50-51). Därtill är den att betrakta som kvalitativ då narrativen snarare identifieras på basis av bedömning än kvantitativ förekomst, även ifall det sistnämnda naturligtvis väger in i det förstnämnda.

Med frågeställningens första del besvarad genom ett antal narrativ i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot, besvaras dess andra del därefter genom att, med utgångspunkt i det teoretiska ramverket, förståliggöra ifrågavarande narrativ. Härvid tillämpas följaktligen redan existerande vetenskapliga teorier på det resultat som den empiriska analysen av

årsrapporterna ger upphov till, i syfte att problematisera och skapa en djupare förståelse för de identifierade narrativen.

3.3. Operationalisering

Frågeställningens tudelade natur fordrade en tudelad operationalisering, där den första delen ämnade urskilja narrativ i den svenska underrättelseinstitutionens 27 årsrapporter mellan 2014 och 2022, medan den andra delen syftade till att förstå dito.

Att urskilja narrativ

Ifrågavarande process tog utgångspunkt i en systematisk genomläsning av underrättelsemyndigheternas årsrapporter, under vilken författarna, i syfte att identifiera relevant material, löpande ställde sig en fråga: handlar föreliggande textavsnitt om någon av de fyra disruptiva teknologier och hot som ska studeras? Om svaret var jakande markerades textinnehållet, och efter genomläsning av samtliga årsrapporter återstod sålunda uteslutande material som på ett eller annat sätt avhandlade relevanta disruptiva teknologier och hot.

Därefter bearbetades det reducerade materialet med utgångspunkt i ytterligare en fråga: hur bedömer, beskriver och omtalar underrättelseinstitutionen teknologierna och hoten? Ur svaren kunde ett antal återkommande teman – annorlunda uttryckt narrativ – skönjas, varpå dessa sedermera sammanställdes till totalt nio stycken. I syfte att skapa ytterligare struktur, i synnerhet för att gagna det nedan beskrivna förståliggörandet av narrativen, delades dessa nio därtill upp i tre kategorier av narrativ, beroende på vad underrättelseinstitutionens bedömning tog sikte på.

Att förstå narrativ

Ifrågavarande process tog utgångspunkt i de nio identifierade narrativen, och sökte, genom att använda lämpliga vetenskapliga teorier, förstå desamma. Härvid var de ovan nämnda kategorierna av narrativ behjälpliga, då de, såsom redan diskuterat i det teoretiska ramverket, skapade goda förutsättningar för en strukturerad analys.

Respektive kategori av narrativ parades sålunda ihop med ett för den särskilt utvalt teoretiskt ramverk, varefter vardera narrativ i kategorin förståliggjordes med utgångspunkt i detsamma.

4. Material

4.1. Primärmaterial

Såsom framgår av metodkapitlet utgör den svenska underrättelseinstitutionens 27 årsrapporter – nio från vardera MUST, SÄPO och FRA – mellan 2014 och 2022 föreliggande uppsats tveklöst mest centrala material. Ifrågavarande rapporter, vilka sammanlagt spänner drygt 1500 sidor, konstituerar nämligen fundamentet på vilket hela arbetet vilar, då de narrativ som presenteras i analyskapitlet är ett destillat av textmaterialet. Det bör emellertid påpekas att de 27 årsrapporterna, i egenskap av underrättelsemyndigheternas egna och noggrant bearbetade utsagor, långt ifrån konstituerar en objektiv insyn i den svenska underrättelseinstitutionens inre, utan snarare bör beaktas som politiskt censurerade kommunikéer. Sakläget – att de offentligt kommunicerade narrativen inte nödvändigtvis utgör underrättelseinstitutionens sanna bedömning av disruptiva teknologier och hot – är naturligt, då underrättelsetjänstemän har ett ansvar att anpassa innehållet i sina rapporter, såväl hemliga som offentliga, utefter vem som är dess mottagare (Rescher 2017, s. 13-14). I strävan att, såsom frågeställningens första del anför, identifiera narrativ i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot utgör årsrapporterna emellertid ett ytterst lämpligt material, då dem mer än något annat är just offentliga. Läsaren bör således vara medveten om att årsrapporterna inte nödvändigtvis återger hela sanningen, men att deras eventuella brister som medium för objektiv genomskärning av underrättelseinstitutionen snarare bör beaktas som en styrka kopplat till frågeställningen.

Vidare använder föreliggande uppsats därtill en begränsad uppsättning övrigt primärmaterial, vilket består av information och rapporter som har hämtats från

svenska och utländska myndigheters samt internationella organisationers webbplatser. Till ifrågavarande kategori hör exempelvis information om USA:s vapengrenar från det amerikanska försvarsdepartementet samt en översiktsrapport om disruptiva teknologier från Europaparlamentet. Sådant material har valts med omsorg och ligger uteslutande till grund för specifika resonemang kopplade till den entitet som står bakom informationen, varför det inte torde medföra några källkritiska problem.

4.2. Sekundärmaterial

Utöver ovan diskuterade primärmaterial använder föreliggande uppsats en samling sekundärmaterial, vilket består av såväl tryckta som digitala vetenskapliga alster inom ämnesområden som på ett eller annat sätt tangerar uppsatsämnet. Härvid kan nämnas de tre böcker som konstituerar analysens teoretiska ramverk, en handfull artiklar från olika vetenskapliga tidskrifter samt diverse rapporter från Totalförsvarets forskningsinstitut. Ifrågavarande material har använts för att strukturera, grunda och fördjupa analysens resonemang och bör således huvudsakligen betraktas som ett komplement till primärmaterialet, av särskild vikt i den teoretiska förståelsen för de identifierade narrativen.

Vidare kan sekundärmaterialet, såsom redovisat i litteraturöversikten, delas upp i sådant som är ett resultat av oberoende forskares respektive statstjänstemäns arbete. Den förstnämnda typen av alster torde, som ett resultat av upphovsmännens oberoende, inte innebära några källkritiska problem, men den andra typen bör i föreliggande sammanhang åtminstone nämnas. Det faktum att upphovsmännen talar i egenskap av statsrepresentant medför ju att deras resonemang bör betraktas som politiserade, och därigenom, likt den svenska underrättelseinstitutionens årsrapporter, inte som en objektiv insyn i hur de faktiskt bedömer disruptiva teknologier och hot. Ifrågavarande alster används emellertid uteslutande som ett bollplank för resonemang kring de narrativ som uppsatsen urskiljer, och således inte som en fristående källa kring statlig hotbedömning, vilket torde minimera risken för att deras statsfärgare perspektiv påverkar uppsatsen negativt.

5. Analys

I strävan att till del undersöka vilka övergripande narrativ som kan urskiljas i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot, samt till del utröna hur ifrågavarande narrativ kan förstås, har föreliggande analyskapitel en tudelad struktur: ett empiriskt och ett teoretiskt avsnitt. Det empiriska avsnittet grundar sig i operationaliseringen och presenterar i tur och ordning de narrativ som genom analysarbetet har identifierats. Det teoretiska avsnittet grundar sig vidare i det teoretiska ramverket och analyserar i tur och ordning hur respektive narrativ kan förståliggöras.

5.1. Empiriska narrativ

Såsom tidigare nämnt identifierar ifrågavarande analys sammanlagt nio narrativ i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot. Dessa kan därtill, såsom tidigare påpekat, grupperas i tre så kallade kategorier av narrativ, beroende på vad det enskilda narrativet tar sikte på: disruptiva teknologier och hot i sig själva; krig, konflikter och hot; eller Sveriges sårbarheter. De tre kategorierna, vilka vardera består av tre narrativ, illustrerar sålunda den svenska underrättelseinstitutionens syn på vilka övergripande fenomen som tangerar disruptiva teknologier och hot, medan de enskilda narrativen konstituerar återkommande berättelser i deras offentliga bedömning av dito. Följaktligen är de tre kategorierna av narrativ i huvudsak av holistisk karaktär, medan respektive enskilt narrativ faktiskt går att belägga med citat och sidhänvisningar.

5.1.1. Synen på disruptiva teknologier och hot i sig själva

Disruptiva teknologier är ett hot snarare än en möjlighet

Det är angeläget att understryka både den stora omfattningen av de statsunderstödda cyberangreppen och det hot mot vårt samhälle, vårt välstånd och mot allas vår integritet som dessa innebär. (FRA 2018, s. 19)

Bearbetningen av årsrapporterna visar tydligt att den svenska underrättelseinstitutionen målar upp ett offentligt narrativ där den presenterar sig själv som en uteslutande defensiv part i förhållande till disruptiva teknologier. Att så är fallet beläggs emellertid inte bäst av sådana citat som det ovanstående, vilka det förvisso återfinns en myriad av i årsrapporterna, utan snarare av avsaknaden av textinnehåll som talar om vilka möjligheter disruptiva teknologier innebär för det svenska underrättelseväsendet. Medan underrättelsemyndigheterna återkommande talar om disruptiva hot och att Sverige ständigt måste värja sig mot sådana (se ex. MUST 2018, s. 39), talar de nämligen enbart ett fåtal tillfällen om hur de själva kan förbättra sin verksamhet genom att utveckla och implementera disruptiva teknologier (se ex. FRA 2018 s. 21). Därtill, när underrättelseinstitutionen väl omnämner en potentiell egen användning av disruptiva teknologier, talas det i stort sett uteslutande om vilka defensiva möjligheter ett sådant bruk skulle kunna medföra (se ex. SÄPO 2021, s. 44).

Det hotfulla omvärldsläget ökar behovet av samarbete mellan underrättelsemyndigheter

> *För att skydda Sverige mot ett föränderligt hot som avspeglar sig även på cyberarenan är samverkan med myndigheterna inom Nationellt cybersäkerhetscentrum (NCSC) värdefull. (SÄPO 2022, s. 7)*

Bearbetningen av årsrapporterna visar att den svenska underrättelseinstitutionen bygger ett offentligt narrativ där den påtalar vikten av samarbete mellan olika underrättelsemyndigheter, i syfte att bättre kunna möta det allt mer hotfulla disruptiva omvärldsläget. Att så är fallet beläggs i synnerhet av det i ovan citat omnämnda myndighetsgemensamma cybersäkerhetscentret, vilket upprättades 2020 och utgör en uppskattad samarbetsyta i kampen mot främmande hot i cyberdomänen (se ex. FRA 2020, s. 23). Den svenska underrättelseinstitutionen, såsom föreliggande uppsats avgränsar begreppet, utgör centrets kärna, och ett steg i arbetet har varit att samlokalisera personal (se ex. SÄPO 2021, s. 58). Utöver nationella samarbeten påtalar de svenska underrättelsemyndigheterna dessutom vikten av internationella samarbeten,

i synnerhet avseende teknikutveckling, i kampen mot de allt mer komplexa hoten som projiceras på Sverige (se ex. MUST 2022, s. 59).

Modern krigföring underlättar antagonistisk förnekbarhet

> *Konflikternas karaktär fortsätter att förändras. De utspelas på allt flera arenor, dolt och förnekbart, med en bred uppsättning av verktyg och ofta med snabbt skiftande intensitet. (MUST 2021, s. 35)*

Bearbetningen av årsrapporterna visar att den svenska underrättelseinstitutionen kommunicerar ett offentligt narrativ där den påpekar att den teknologiska utvecklingen inom krigföring och underrättelseverksamhet medför att Sveriges motståndare med större framgång kan dölja sina antagonistiska handlingar. En stor del av ifrågavarande utveckling anses vara ett resultat av att de nya påverkansmetoder som har blivit allt mer centrala i modern krigföring, såsom desinformationskampanjer och psykologiska operationer i cyberdomänen, är oberoende geografiska avstånd, och således lika väl kan bedrivas från antagonisternas egna territorium (se ex. SÄPO 2015, s. 62). Vidare talar underrättelseinstitutionen återkommande om gråzon, hybridkrigföring och icke-linjär krigföring, vilka de menar används av andra stater för att, medelst förnekbarhet, verka mot Sverige (se ex. MUST 2018, s. 29). Härvid omtalas i synnerhet Kinas och Rysslands cyberförmåga (se ex. MUST 2022, s. 15).

5.1.2. Synen på krig, konflikter och hot

Krig, konflikter och hot är inte lika konventionella som förr

> *För att få ett övertag i en konflikt behövs idag inte konventionella vapen. Det kan räcka med att slå ut kraftförsörjning, vatten och kommunikationer i några dagar. (FRA 2020, s. 26)*

Bearbetningen av årsrapporterna visar att den svenska underrättelseinstitutionen målar upp ett offentligt narrativ där den beskriver de hot som projiceras mot Sverige som allt mer komplexa, mångfacetterade och okonventionella. Sakläget anses vara en

följd av den snabba teknologiska utvecklingen som präglar vår samtid, vilken ökar såväl motståndarnas förmåga som den svenska statens sårbarheter, och därigenom får till följd att diskrepansen mellan hot och säkerhet växer (se ex. SÄPO 2018, s. 4). Därtill menar underrättelseinstitutionen att tröskeln för antagonistiska stater, i synnerhet Ryssland, att använda olika typer av icke-linjär krigföring har blivit allt lägre, vilket förstärker hotet mot Sverige (se ex. MUST 2022, s. 13). Härvid påtalas särskilt cyberangrepp, och att den svenska statens motståndare numera i allt större utsträckning använder dito för att uppnå strategiska och operativa målsättningar (se ex. FRA 2020, s. 5).

Sverige är särskilt eftersatt på den allt mer centrala rymdarenan

> *Fler länder ser rymden som en arena för konflikter i framtiden och den ses också redan i dag som en underrättelsearena. [...] Detta har betydelse för Sveriges säkerhet och måste ses ur ett totalförsvarsperspektiv. Kunskapen behöver öka. (SÄPO 2021, s. 8)*

Bearbetningen av årsrapporterna visar att den svenska underrättelseinstitutionen bygger ett offentligt narrativ där den omtalar rymdarenan som allt mer central för underrättelseverksamhet och krigföring, samt att Sverige är särskilt eftersatt inom ifrågavarande disruptiva område. Ståndpunkten tar utgångspunkt i att den snabba teknikutvecklingen och de minskade kostnaderna för att skjuta upp satelliter innebär att fler aktörer etablerar sig i rymden, vilket får konsekvenser för den svenska statens säkerhet och totalförsvar (se ex. SÄPO 2021, s. 18). Härvid omtalas i synnerhet Kinas rymdteknologiska satsningar, vilka utgör en del i statens målsättning att vara en världsledande militärmakt år 2049 (se ex. MUST 2022, s. 28), men även Rysslands prioritering av rymdförmåga nämns (se ex. MUST 2021, s. 20).

Motståndarnas auktoritära statsskick renderar dem ett allt större disruptivt hot

> *Våra motståndare följer inga regler, och kan dra full nytta av teknikutvecklingen. (SÄPO 2021, s. 43)*

Bearbetningen av årsrapporterna visar att den svenska underrättelseinstitutionen kommunicerar ett offentligt narrativ där den påpekar att dess demokratiska principer medför att auktoritära motståndare kan implementera disruptiva teknologier betydligt snabbare än den själv, då sådana regimer inte behöver ta hänsyn till begränsande lagstiftningar. Härvid påtalas i synnerhet Kina, vars lagstiftning fastslår att varje medborgare, företag och organisation är skyldig att bistå statens underrättelse- och säkerhetstjänster; ett tvång som möjliggör sömlösa civil-militära synergieffekter mellan statsmakten och näringslivet kopplat till teknologisk utveckling (se ex. MUST 2020, s. 26).

5.1.3. Synen på Sveriges sårbarheter

Cyberhoten växer och belyser Sveriges sårbarheter

> *Cyberangrepp som får konkreta konsekvenser för olika samhällsfunktioner är numera en del av vår vardagsverklighet, och behovet av att skydda känsliga uppgifter i myndigheters och företags IT-system har blivit alltmer uppenbart. (FRA 2017, s. 4)*

Bearbetningen av årsrapporterna visar att den svenska underrättelseinstitutionen målar upp ett offentligt narrativ där den beskriver att hoten i cyberdomänen är ständigt närvarande och växande, samt att det i sin tur renderar den svenska statens sårbarheter som alltmer påtagliga. Bedömningen grundar sig i att cyberangreppen som riktas mot Sverige präglas av tilltagande omfattning och komplexitet (se ex. FRA 2021, s. 9), och att stater eller statsunderstödda organisationer står för de allra mest avancerade hoten (se ex. FRA 2017, s. 21). Säkerhetsriskerna anses därtill förstärkas av att Sverige är en högteknologisk stat, då det innebär att mycket samhällsviktig verksamhet vilar på

informationsteknologi och därigenom lämnas sårbar för cyberangrepp (se ex. SÄPO 2022, s. 35). Kopplat till sårbarheterna talar underrättelsemyndigheterna dessutom flitigt om vikten av att utveckla Sveriges cyberförsvar, i syfte att kunna värja sig mot de växande hoten och minimera statens sårbarheter i cyberdomänen (se ex. MUST 2018, s. 33).

Sveriges högteknologiska industri är särskilt utsatt

> *Sverige är ett framstående land inom innovationer och högteknologi. [...] Att främmande makt på olika sätt tar del av denna teknologiska kompetens är problematiskt för Sverige. (MUST 2015, s. 11)*

Bearbetningen av årsrapporterna visar att den svenska underrättelseinstitutionen kommunicerar ett offentligt narrativ där den beskriver Sveriges framstående civila sektor som ett attraktivt underrättelsemål för antagonistiska stater. Kopplingen till disruptiva teknologier och hot är här tudelad: dels bedöms den främmande underrättelseinhämtningen inriktas mot Sveriges disruptiva innovation (se ex. SÄPO 2022, s. 13); och dels bedöms inhämtningen ske medelst spionage i cyberdomänen (se ex. MUST 2021, s. 55). Härvid omnämns i synnerhet Kina, som framförallt bedöms inrikta sin verksamhet mot Sveriges rymdindustri (se ex. MUST 2022, s. 29), och Ryssland, som bedöms ta sikte på all avancerad teknologi av militär relevans (se ex. SÄPO 2022, s. 23).

Sveriges myndigheter är inte dimensionerade för de växande hoten

> *Teknikutvecklingen ger statliga aktörer och ideologiskt motiverade aktörer ökade förmågor, men myndigheternas säkerhetsskydd har inte ökat i samma takt, vilket har inneburit att sårbarheterna i skyddsvärda verksamheter har ökat. (SÄPO 2018, s. 21)*

Bearbetningen av årsrapporterna visar att den svenska underrättelseinstitutionen bygger ett offentligt narrativ där den påtalar att svenska myndigheter har ett undermåligt skydd mot disruptiva hot. Härvid nämns såväl myndigheter med tydlig

koppling till Sveriges totalförsvar som sådana med, åtminstone i fredstid, uteslutande civila funktioner, och det framhävs därtill att samhällsviktig infrastruktur ägs av såväl offentliga som privata aktörer (se ex. MUST 2022, s. 59). I sammanhanget är cyberangrepp det disruptiva hot som omtalas i störst utsträckning, och underrättelseinstitutionen menar att antagonistiska stater riktar sådana otillbörliga attacker mot en bred uppsättning verksamheter i Sverige (se ex. SÄPO 2022, s. 35). Vidare bedömer myndigheterna att antalet cyberangrepp kommer fortsätta att tillta, och att den svenska staten därmed måste vidta åtgärder för att höja sin försvarsförmåga i cyberdomänen (se ex. FRA 2017, s. 7).

5.2. En teoretisk förståelse

Med de nio narrativen i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot presenterade och belagda söker föreliggande avsnitt förståliggöra respektive narrativ med utgångspunkt i det teoretiska ramverket. Såsom där klarlagt sker ifrågavarande på basis av de tre kategorierna av narrativ, då den svenska underrättelseinstitutionens syn på disruptiva teknologier och hot i sig själva kan förstås medelst Carsons scenanalogi, dess syn på krig, konflikter och hot kan förstås medelst Yarhi-Milos tre systemorienterade teser och dess syn på Sveriges sårbarheter kan förstås medelst Buzans hotkategorier och teori om starka och svaga stater.

5.2.1. Synen på disruptiva teknologier och hot i sig själva

Disruptiva teknologier är ett hot snarare än en möjlighet

Ifrågavarande narrativ i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot kan, med utgångspunkt i Carson, förstås som ett försök att belysa och offentliggöra den otillbörliga verksamhet som Sveriges antagonister söker bedriva bakom scenen. Såsom framgår av flertalet av de narrativ som presenteras i ovanstående delkapitel upplever ju den svenska staten sig som i tilltagande grad utsatt för disruptiva hot, och det faktum att antalet statsunderstödda

cyberangrepp mot Sverige ökar (RISE 2022, s. 2-3) skänker legitimitet åt en sådan tanke. Genom att på scenen klargöra att de är medvetna om den antagonistiska verksamhet som försiggår bakom scenen, såväl genom att påpeka specifika hot (se ex. SÄPO 2018, s. 5) som generella utvecklingar (se ex. MUST 2021, s. 54-55), söker de svenska underrättelsemyndigheterna sålunda måhända ta initiativet från motståndarna. Sådana uttalanden för ju antagonisternas internationellrättsligt olämpliga förehavanden framför publiken, och därigenom även framför det internationella samfundet, vilket i teorin kan medföra en avskräckande effekt. Officiella och offentliga underrättelseavslöjanden, såsom utsagor i årsrapporter om fientlig verksamhet kan anses vara, kan nämligen användas som ett internationellpolitiskt vapen mot sådan verksamhet som i sin natur är avhängig hemlighetsmakeri och doldhet (Reimer 2021, s. 556). Ryssland har ju exempelvis säkerligen ett intresse av att i största möjliga mån mörklägga sin inblandning i ovan nämnda cyberangrepp, och om Sverige återkommande uppmärksammar det internationella samfundet på dito kan det oönskade rampljuset tänkas avskräcka Ryssland från framtida oegentligheter.

De svenska underrättelsemyndigheternas offentliga bedömning av sig själva som offer i förhållande till disruptiva teknologier och hot kan därtill, utöver att förstås som ett försök att förhindra framtida antagonistisk verksamhet, vara ett led i att hemlighålla deras egen utveckling och användning av disruptiva teknologier i offensiva syften. På scenen framstår de sålunda som oskyldiga och rättrådiga, medan de bakom scenen i själva verket, åtminstone till viss del, uppträder lika aggressivt som de antagonistiska stater som omnämns i årsrapporterna. Det är förvisso svårt att föreställa sig svenska cyberangrepp eller desinformationskampanjer mot främmande makt, men det är likaledes otroligt att den svenska underrättelseinstitutionen inte utforskar disruptiva teknologiers offensiva möjligheter – ett av dess yttersta syften är trots allt att inhämta information om utländska förhållanden (Eriksson 2016, s. 59). Ett sådant resonemang förstärks vidare av det faktum att Sverige är en högteknologiskt stat med stor, och allmänt erkänd, civil kompetens inom produkter med dubbla användningsområden (ISP 2018, s. 12); något som torde medföra att Sverige även besitter relativt stor, men desto mer hemlighållen, militär kompetens inom disruptiva teknologier. Således

troliggörs den eventualitet där den svenska underrättelseinstitutionen, likt dess ovan diskuterade motståndare, använder scenen för att vilseleda allmänheten och andra stater, medan den bakom scenen i själva verket utvecklar och använder disruptiva teknologier i offensiva syften.

Det hotfulla omvärldsläget ökar behovet av samarbete mellan svenska underrättelsemyndigheter

Ifrågavarande narrativ i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot kan, i enlighet med Carson, förstås som ett försök att på scenen, framför såväl den egna befolkningen som andra stater, påvisa att Sveriges olika underrättelsemyndigheter arbetar tillsammans och står som en enad front mot de allt mer närvarande hoten från omvärlden. Samarbete mellan MUST, SÄPO och FRA, samt den styrkeuppvisning som blir följd av att göra det offentligt, kan nämligen tänkas medföra två gynnsamma effekter: en faktiskt starkare, samt en mer avskräckande, underrättelseinstitution. Den första effekten är ett resultat av det faktum att de tre underrättelsemyndigheterna besitter olika huvudsakliga kompetenser, vilka i samklang torde möjliggöra ett bättre försvar mot de växande hoten än om vardera myndighet hade mött dem på egen hand. Föreliggande synergieffekter kan därtill vara särskilt centrala i försvaret mot just disruptiva hot, eftersom sådana, såsom klarlagt i bakgrunden, ofta är av mångfacetterad natur (Raska 2019, s. 66). Vidare går den andra effekten hand i hand med den första, då de svenska underrättelsemyndigheternas val att offentliggöra sitt fördjupade samarbete på scenen kan vara ett försök att varsko andra stater om deras gemensamma styrka. Genom att göra det kommunicerar ju den svenska staten att den vidtar åtgärder för att värja sig mot de växande disruptiva hoten och att den kommer att vara mindre sårbar framöver; ett budskap som kan sända avskräckande signaler till Sveriges antagonister.

Vidare kan den svenska underrättelseinstitutionens offentliga bedömning av att det hotfulla omvärldsläget ökar behovet av samarbete mellan svenska underrättelsemyndigheter också förstås som ett försök att kommunicera dess existensberättigande till den inhemska politiska eliten, vilka utgör en del av publiken

som ser scenen. Genom att måla upp en bild av ett allt mer hotfullt omvärldsläge rättfärdigar ju den svenska underrättelseinstitutionen, medvetet eller omedvetet, sin existens, och äskar därtill indirekt om mer resurser. Fenomenet illustreras exempelvis av att det utökade samarbetet mellan MUST, SÄPO och FRA i kampen mot disruptiva hot har materialiserats i form av inrättandet av ett nationellt cybersäkerhetscenter (se ex. FRA 2019, s. 19), vars budget numera årligen uppgår till 60 miljoner kronor (NCSC 2023). Följaktligen kan det vara så att den svenska underrättelseinstitutionen, medvetet eller omedvetet, driver en sorts intern politisk agenda i syfte att värna sin fortlevnad och expansion.

Modern krigföring underlättar antagonistisk förnekbarhet

Ifrågavarande narrativ i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot kan, med utgångspunkt i Carson och i likhet med föregående två narrativ, förstås som ett försök att på scenen kommunicera till publiken att antagonistiska stater bedriver otillbörlig verksamhet bakom scenen. Disruptiva teknologier har nämligen, såsom klargjort i bakgrunden, revolutionerat möjligheterna till att medelst dolda eller förnekbara metoder bedriva mellanstatlig informationsinhämtning och påverkan (Świątkowska 2020, s. 127-130), vilket den svenska staten upplever att dess motståndare drar full nytta av (se ex. MUST 2022, s. 24). Den ökade förnekbarheten innebär ju att det är svårare att urskilja vilken stat som står bakom en viss handling, och därigenom även att vedergälla dito, vilket har sänkt tröskeln för antagonistiska stater att agera aggressivt bakom scenen. Utvecklingen illustreras inte minst av det faktum att allt fler statsunderstödda cyberangrepp har riktats mot Sverige under senare år, i synnerhet från Ryssland (RISE 2022, s. 2). Följaktligen kan den svenska underrättelseinstitutionens offentliga bedömning att modern krigföring underlättar antagonistisk förnekbarhet förstås som ett försök att stävja motståndarnas allt mer utmanande uppträdande bakom scenen, genom att på scenen och framför publiken påpeka dess existens trots dess förnekbara natur.

5.2.2. Synen på krig, konflikter och hot

Krig, konflikter och hot är inte lika konventionella som förr

Ifrågavarande narrativ i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot ter sig, med utgångspunkt i Yarhi-Milo, föga förvånande i en mellanstatlig verklighet som i allt större utsträckning präglas av högteknologisk underrättelseinhämtning och hybridkrigföring (Świątkowska 2020, s. 125-128). Enligt tesen om förmåga indikerar ju den drastiska kapacitetsutveckling inom cyberdomänen, rymdteknologier, artificiell intelligens och kvantdatorer som under det senaste årtiondet har varit norm bland världens stater, i synnerhet dess stormakter, att de ämnar förändra medelst vilka medel de bedriver underrättelseverksamhet och krigföring. Därigenom förändras även den hotbild som de projicerar på sin omvärld, från att tidigare främst ha varit av konventionellt slag till att numera i betydligt större utsträckning ta hybrid form. Utvecklingen illustreras inte minst av det faktum att USA, Kina och Ryssland har fördjupat sina investeringar i artificiell intelligens i syfte att transformera deras respektive underrättelseverksamhet och militärmakt (Johnson 2019, s. 147-148); något som tveklöst bör tolkas som ett hot av den svenska underrättelseinstitutionen. Vidare, enligt tesen om agerande, talar den ökning av fientliga inhämtnings- och påverkansoperationer mot Sverige som sker medelst disruptiva teknologier för att den svenska underrättelseinstitutionen bör uppfatta en hotbild som rör sig från konventionalitet mot hybriditet. Skiftet i hotens karaktär exemplifieras bland annat av att antalet cyberangrepp mot Sverige, såväl i syfte att komma över information som att påverka kritisk infrastruktur, har ökat avsevärt under senare år (RISE 2022, s. 2). Utvecklingen har omöjligtvis gått den svenska underrättelseinstitutionen obemärkt förbi, och förståliggör ifrågavarande narrativ i dess offentliga bedömning av disruptiva teknologier och hot. Slutligen, enligt tesen om strategisk militärdoktrin, torde det faktum att andra stater, i synnerhet stormakter, har introducerat disruptiva teknologier som beständiga element i deras underrättelseverksamhet och militärmakt medföra att den svenska underrättelseinstitutionen uppfattar ett växande disruptivt hot. Utöver ovan nämnda

generellt fördjupade investeringar i artificiell intelligens etablerade exempelvis Kina en så kallad strategisk stödstyrka i Folkets befrielsearmé under 2015, vars huvudsakliga ansvarsområde är att främja innovation och militär tillämpning av disruptiva teknologier (Kania & Costello 2020, s. 249-251). Ett sådant initiativ visar att stormakten beaktar området som en avgörande strategisk pusselbit i dess underrättelse- och militärdoktrin, såväl i nuläget som framöver, och det är följaktligen förståeligt att den svenska underrättelseinstitutionen bedömer att hoten mot Sverige inte är lika konventionella som förr.

Sverige är särskilt eftersatt på den allt mer centrala rymdarenan

Ifrågavarande narrativ i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot förefaller, i enlighet med Yarhi-Milo, rimlig med utgångspunkt i det faktum att ett tilltagande antal stater etablerar och expanderar sin militära närvaro i rymden (Kehler 2012, s. 26-27). Enligt tesen om förmåga indikerar ju en sådan rustningspolitik att omvärlden betraktar rymdarenan som en allt mer central domän för underrättelseverksamhet och krigföring, samt att de utvidgar sin rymdteknologiska kapacitet i syfte att kunna hävda sig på den. Det är följaktligen naturligt att den svenska underrättelseinstitutionen tolkar rymdteknologier som ett hot, men att den anser sig vara mer eftersatt inom föreliggande disruptiva område än inom cyberdomänen, artificiell intelligens eller kvantdatorer är intressant. Försvarsmakten och Rymdstyrelsen utredde nämligen redan i början av 2000-talet förutsättningarna för en svensk spaningssatellit (Andersson & Rydqvist 2008, s. 45-46), och Sverige har därtill en relativt välutvecklad civil rymdindustri (Edman 2019, s. 3-8). Ingetdera har emellertid medfört en utvecklad militär rymdförmåga, då projektet med spaningssatelliten ansågs vara för kostsamt och den svenska staten generellt har haft svårt att konkretisera civil-militära synergieffekter (Lindström et al. 2021, s. 21-24). Medan många stater under senare år har prioriterat rymdteknologier som ett av deras viktigaste disruptiva områden har Sverige sålunda inte intagit rymdarenan med samma beslutsamhet, och därigenom har diskrepansen mellan den svenska statens och omvärldens rymdförmåga utvidgats; en utveckling som förståliggör

att den svenska underrättelseinstitutionen betraktar sig som eftersatt på området. Vidare talar även tesen om agerande för att omvärldens mer handlingskraftiga inställning till rymdteknologier i underrättelseverksamhet och krigföring torde uppfattas som ett hot. Att allt fler stater etablerar och expanderar sin militära närvaro i rymden bör ju inte bara tolkas som att de förmår projicera ett allt mer kapabelt hot, utan också som att de hyser allt mer hotfulla intentioner mot sin omvärld. Den tilltagande animositeten i rymddomänen, vilken påverkar Sverige som både civil och militär aktör, illustreras inte minst av att världens stormakter under senare år har har genomfört fler tester av regelrätta rymdteknologiska vapensystem, såsom kinetiska antisatellitvapen (Lindström et al. 2021, s. 13). Slutligen, i enlighet med tesen om strategisk militärdoktrin och i likhet med resonemanget avseende föregående narrativ, talar det faktum att andra stater har introducerat rymdteknologier och tillhörande personal som beständiga element i deras underrättelseverksamhet och militärmakt för att den svenska underrättelseinstitutionen torde uppfatta sig som eftersatt inom föreliggande disruptiva område. Sedan 2020 beskriver Försvarsmaktens doktrin förvisso rymden som en fysisk domän, bredvid mark, sjö, luft och cyber, men andra stater, såsom Frankrike och Storbritannien, har kommit betydligt längre i att omsätta den ökade medvetenheten om rymdarenans centralitet till faktiska militärorganisatoriska förändringar (Lindström et al. 2021, s. 14). Därtill har världens stormakter såklart kommit än längre – USA har exempelvis introducerat en rymdstyrka som sin sjätte vapengren (U.S. DoD 2023) – och att den svenska underrättelseinstitutionen bedömer sig vara eftersatt på den allt mer centrala rymdarenan ter sig därigenom förståeligt.

Motståndarnas auktoritära statsskick renderar dem ett allt större disruptivt hot

Ifrågavarande narrativ i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot ter sig, i enlighet med Yarhi-Milo, naturlig med utgångspunkt i det faktum att de stater som anses bedriva mest antagonistisk verksamhet mot Sverige, nämligen Kina, Ryssland och Iran, är auktoritära regimer med stora geopolitiska ambitioner (Petersson et al. 2020, s.

45;59;66). Enligt tesen om förmåga konstituerar ju föreliggande statsmakters möjlighet att med stor frihet diktera alla statens resurser, såväl civila som militära, ett hot mot Sverige, då de kan dra full nytta av produkter med dubbla användningsområden och därigenom nå disruptiva förmågehöjningar inom underrättelseverksamhet och krigföring. Fenomenet illustreras inte minst av att Kinas lagstiftning klargör att varje kinesisk entitet, såväl inlands- som utlandsbaserad, är skyldig att bistå staten i frågor om nationell säkerhet, vilket i praktiken innebär att den kinesiska underrättelseinstitutionen förfogar över ett ofantligt nätverk av kunskap (Kristiansson 2019, s. 4-5). Medan Sverige, såsom diskuterat i ovanstående stycke, generellt har haft svårt att förverkliga civil-militära synergieffekter i rymddomänen kan Kina således uppnå dito medelst tvång, och det är därmed förståeligt att den svenska underrättelseinstitutionen bedömer att dess motståndares förkastelse av demokratiska principer renderar dem som ett allt större disruptivt hot. Vidare, i enlighet med tesen om agerande, torde även det faktum att Sveriges motståndare, som en följd av deras auktoritära natur, uppträder aggressivt och otillbörligt på den internationellpolitiska spelpanen tolkas som ett hot av den svenska underrättelseinstitutionen. Sådant oanständigt beteende, såsom Rysslands fortlöpande illegala cyberangrepp gentemot Sverige (RISE 2022, s. 5-7), indikerar ju naturligtvis att den ryska staten hyser hotfulla intentioner gentemot sin svenska motsvarighet, och förståliggör sålunda föreliggande narrativ. Slutligen, enligt tesen om strategisk militärdoktrin, talar motståndarnas ovan nämnda geopolitiska ambitioner, i vilka deras disruptiva förmågehöjning och auktoritära ageranden spelar en avgörande roll, för att den svenska underrättelseinstitutionen torde uppfatta dem som ett större disruptivt hot. Sakläget åskådliggjordes inte minst av gråzonsläget inför kriget i Ukraina, då Ryssland för första gången visade sig fullständigt villigt och, åtminstone till viss del, kapabelt att nyttja cyberkrigföring för att uppnå strategiska målsättningar (Lewis 2022, s. 7-8). Medan den aggressionen förvisso inte var riktad mot Sverige i sig påvisar den en förändring i Rysslands militära doktrin samt i den hotbild som den ryska staten projicerar på sin omvärld, och det är följaktligen förståeligt att den svenska underrättelseinstitutionen bedömer att disruptiva hot förstärks av motståndarnas auktoritära statsskick.

5.2.3. Synen på Sveriges sårbarheter

Cyberhoten växer och belyser Sveriges sårbarheter

Ifrågavarande narrativ i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot kan förstås med utgångspunkt i Buzans hotkategorier, då cyberangrepp, och hotet därom, kan vara av endera militär, politisk eller samhällelig karaktär beroende vad den otillbörliga verksamheten tar sikte på. I underrättelsemyndigheternas årsrapporter manifesteras detta inte minst av att det återkommande talas om cyberhot som mångfacetterade (se ex. SÄPO 2021, s. 44), vilket kan tolkas som ett uttryck för att de anses kunna slå mot flera av Sveriges olika typer av skyddsvärden.

Cyberangrepp kan inledningsvis förstås som ett militärt hot då en allt större del av den svenska statens kritiska infrastruktur numera vilar på digitala system (se ex. MUST 2021, s. 44), vilka, såsom diskuterat i bakgrunden, är sårbara för antagonistisk verksamhet i cyberdomänen (Rekowski 2020, s. 14-16). I samband med att den svenska underrättelseinstitutionen bedömer att cyberhoten växer är det därmed troligt att den också, mer eller mindre indirekt, bedömer utvecklingen som ett tilltagande militärt hot, då den belyser sårbarheter i Sveriges fysiska skyddsvärden. En sådan bedömning kan dessutom förväntas stärkas i kombination med det ovan analyserade narrativet som påtalar att krig, konflikter och hot inte är lika konventionella som förr, eftersom världens militärmakter numera bedöms använda cyberangrepp som en central del i deras moderna och hybrida krigföring (se ex. FRA 2022, s. 13). Härvid kan den svenska underrättelseinstitutionen därtill tänkas väga in sin uppfattning om en mellanstatlig spelplan där antagonistiska stater bedriver en allt mer aggressiv politik (se ex. SÄPO 2022, s. 12), då staters krigföring bör betraktas som en förlängning av deras politik (Clausewitz 1989, s. 7). Allt mer aggressiva militärmakter, vilka dessutom åtnjuter goda möjligheter till förnekbarhet (Świątkowska 2020, s. 127-129), torde ju därigenom bedömas ha en lägre tröskel för att tillgripa cyberangrepp som militärstrategiskt verktyg, vilket förståliggör att cyberhoten bedöms växa.

Vidare kan cyberangrepp förstås som ett politiskt hot då det i den svenska underrättelseinstitutionens årsrapporter återkommande påtalas att Sverige regelbundet utsätts för diverse påverkanskampanjer från främmande makt (se ex. MUST 2022, s. 15). En sådan typ av otillbörliga angrepp kan exempelvis vara spridning av kraftigt manipulerade uppgifter som marknadsförs som nyheter, så kallade *fake news*, vilka inte sällan får snabb och storskalig spridning på sociala medier. Ifrågavarande desinformation bör betraktas som en del av de växande cyberhoten, och det faktum att en stor andel av Sveriges befolkning, i synnerhet yngre (Skolverket 2021), skapar sin omvärldsuppfattning på sociala medier gör den svenska staten särskilt sårbar.

I nära koppling till dessa politiska hot kan cyberangrepp slutligen förstås som ett samhälleligt hot, då de kan riktas mot Sverige i syfte att bringa inomstatlig oreda och misstro. Ryssland har exempelvis på senare år genomdrivit omfattande satsningar på att försöka nå en större global publik med sin propaganda (Ekman et al. 2023, s. 61-62); en ambition i vilken cyberdomänen tveklöst spelar en avgörande roll. Kina är därtill ytterligare ett exempel på en stormakt som ständigt försöker destabilisera och påverka andra staters inomstatliga förhållanden i syfte att främja sina egna intressen (Ekman et al. 2023, s. 30), vilket inte minst återspeglar sig i att den svenska underrättelseinstitutionen återkommande påtalar det kinesiska cyberhotet (se ex. MUST 2022, s. 15). Sveriges sårbarhet påvisas härvid inte minst av den, måhända statsunderstödda, desinformationskampanj som under senare år har riktats mot socialtjänsten, vilken, genom sin stora genomslagskraft på sociala medier, har resulterat i en påtaglig inomstatlig polarisering (Törnquist & Al-Khameesi 2022).

Sveriges högteknologiska industri är särskilt utsatt

Ifrågavarande narrativ i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot kan, likt narrativet ovan, förstås med utgångspunkt i Buzans hotkategorier, då främmande underrättelseinhämtning mot Sveriges disruptiva innovation konstituerar ett uppenbart ekonomiskt hot. Sådana antagonistiska intrång kan nämligen resultera i att svensk industri i förlängningen förlorar konkurrenskraft, eftersom dess forskning och utveckling olovligen tas till vara

av andra stater. Sverige kan härvid, i antagonistiska staters strävan att tillskansa sig kunskap om högteknologi, tänkas vara en ytterst intressant måltavla, då FN:s immaterialrättsorganisation 2022 placerade Sverige på andra plats i sin årliga mätning av staters innovationsförmåga, i vilken exempelvis export av högteknologiska produkter väger in (PRV 2022). I kombination med att det därtill, åtminstone enligt den svenska underrättelseinstitutionen, föreligger en diskrepans mellan motståndarnas offensiva förmåga och Sveriges defensiva dito (se ex. MUST 2022, s. 53), torde antagonister bedöma den svenska statens disruptiva innovation som ett förhållandevis lätt byte. Sammantaget kan detta tänkas ge incitament åt främmande makt att prioritera sin underrättelseinhämtning mot svensk högteknologisk industri, och det är sålunda förståeligt att de svenska underrättelsemyndigheterna bedömer den som särskilt utsatt.

Sveriges myndigheter är inte dimensionerade för de växande hoten

Ifrågavarande narrativ i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot kan, utifrån Buzans teorier om mellanstatlig säkerhet, förstås som ett uttryck för att andra staters tilltagande disruptiva förmåga anses rendera Sverige som mer utsatt. I den mellanstatliga anarkin innebär ju den ena aktörens förmågehöjning den andres osäkerhet, och det är följaktligen rimligt att underrättelsetjänsterna bedömer svenska myndigheter som underdimensionerade inför det växande hoten från omvärlden.

Att svenska myndigheter och statliga bolag idag inte är dimensionerade för den rådande och alltjämt värre hotbilden, samt att det alltmer komplexa omvärldsläget ökar behovet att kvalificerad informationssäkerhet, kan därför ses som en indikation på att underrättelseinstitutionen bedömer att Sveriges säkerhet är på efterkälken i ifrågavarande avseende. Detta kan med Buzans teori om den internationella maktens koppling till staters säkerhet ses som att den svenska underrättelseinstitutionen uppfattar att Sveriges internationella makt, samt därigenom även dess säkerhet, lider. Flera nya satsningar som påtalas av myndigheterna ligger nämligen i linje med att den svenska staten strävar efter att stärka sin internationella makt, samt därigenom även dess säkerhet, exempelvis illustrerat av upprättandet av det nationella

cybersäkerhetscentret (se ex. MUST 2021, s. 48). Även narrativet där myndigheterna påtalar att försvar mot disruptiva hot gynnas av samarbete med internationella partners kan, med hjälp av Buzans teorier, tolkas som att den svenska underrättelseinstitutionen söker stärka Sveriges säkerhet med hjälp av andra länder inom de områden där brister råder. Som tidigare nämnt har nämligen antagonistiska stater idag en myriad verktyg att nyttja för att nå sina mål, vilket medför att statens sociopolitiska sammanhållning, vilken är en av nyckelfaktorerna i Buzans teorier om staters säkerhet, riskerar försvagas hos den aktör som står själv.

6. Slutsatser

Med utgångspunkt i frågeställningens tudelade natur åstadkommer föreliggande uppsats väsentligen två resultat: nio narrativ i den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot; samt en förståelse för desamma.

Inledningsvis går det att konstatera att de nio narrativen, i egenskap av direkt och koncentrerat svar på frågeställningens första del, bör betraktas som en slutsats i sig självt. Härvid är det emellertid viktigt att påtala att narrativen inte syftar till att vara uttömmande eller slutgiltiga, utan allena en möjlig tolkning av den svenska underrättelseinstitutionens offentliga bedömning av disruptiva teknologier och hot. Uppsatsen har ju i bearbetningen av dess primärmaterial förvisso eftersträvat objektivitet och regelbundenhet, men den aspirerar ingalunda läsas som en definitiv redogörelse för återkommande beskrivningar i underrättelsemyndigheternas årsrapporter mellan 2014 och 2022.

Vidare går det att konstatera att narrativen kan förståliggöras med utgångspunkt i tre teorier om mellanstatliga relationer, såsom presenterade i det teoretiska ramverket. Den svenska underrättelseinstitutionens syn på disruptiva teknologier och hot i sig själva kan nämligen förstås med utgångspunkt i Carsons scenanalogi, då staters disruptiva mellanhavanden är en balansgång mellan offentlighet och hemlighet. Vidare kan underrättelsemyndigheternas syn på krig, konflikter och hot i förhållande till

disruptiva teknologier förstås utifrån Yarhi-Milos tre systemorienterade teser, då staters bedömning av disruptiva hot i stor utsträckning vilar på samma indikatorer som konventionell hotbedömning. Slutligen kan underrättelseinstitutionens syn på Sveriges sårbarheter i relation till disruptiva teknologier och hot förstås genom Buzans hotkategorier och teori om starka och svaga stater, då de disruptiva hotens vitt och snabbt skiftande karaktär innebär nya utmaningar för Sverige på den internationellpolitiska spelplanen. Även härvid, likt i ovanstående stycke, är det emellertid viktigt att påpeka att ifrågavarande förståelse för narrativen är en av många, och att den bör läsas som ett bidrag till det vittomfattande forskningsfältet kring mellanstatliga relationer; dock med en nischad inriktning – disruptiva teknologier och hot.

9797 st. ord (varav 5167 analys)

Bibliografi

Amselem, Elias, Pontus Svenson & Linus Gisslén, 2014. "Kvantinformatik". Totalförsvarets forskningsinstitut, rapportnr: FOI-R--3920--SE.

Andersson, Christer & John Rydqvist, 2008. "MUSIS i ett svenskt perspektiv". Totalförsvarets forskningsinstitut, rapportnr: FOI-R--2667--SE.

Boréus, Kristina, 2018. "Argumentationsanalys" i Kristina Boréus & Göran Bergström (red.) *Textens mening och makt*. Studentlitteratur, s. 93-130.

Boréus, Kristina & Sebastian Kohl, 2018. "Innehållsanalys" i Kristina Boréus & Göran Bergström (red.) *Textens mening och makt*. Studentlitteratur, s. 49-89.

Buzan, Barry, 2016. *People, States and Fear*. ECPR Press.

Carson, Austin, 2020. *Secret Wars - Covert Conflict in International Politics*. Princeton University Press.

Clapp, Sebastian, 2022. "Emerging disruptive technologies in defence". European Parliamentary Research Service, rapportnr: PE 733.647.

Dieu, Oceane & Reza Montasari, 2022. "How States' Recourse to Artificial Intelligence for National Security Purposes Threatens Our Most Fundamental Rights", i Reza Montasari (red.) *Artificial Intelligence and National Security,* Springer, s. 19-47.

Edman, Tobias, 2019. "Särskild redovisning gällande företag". Rymdstyrelsen, rapportnr: 52/19.

Ekman, Ivar, Oscar Almén, Maria Engqvist, Karolina Lindén & Aron Lund, 2023. "Diaspora och påverkan från främmande makt", Totalförsvarets forskningsinstitut, rapportnr: FOI-R--5436--SE.

Eriksson, Gunilla, 2016. *Swedish Military Intelligence: Producing Knowledge*. Edinburgh University Press.

Grobman, Steve, 2020. "Quantum Computing's Cyber-Threat to National Security", *Institute for National Strategic Security, National Defense University*, vol. 9, nr. 1, s. 52-67.
Raska, Michael, 2019. "Strategic Competition for Emerging Military Technologies: Comparative Paths and Patterns", *PRISM*, vol. 8, nr. 3, s. 64-81.

ISP, 2018. *Verksamhet 2018*. Inspektionen för strategiska produkter.

Johnson-Freese, Joan, 2018. "Space and National Security", i Derek S. Reveron, Nikolas K. Gvosdev & John A. Cloud (red.) *The Oxford Handbook of U.S. National Security*, Oxford Handbooks, s. 435-452.

Johnson, James, 2019. "Artificial intelligence & future warfare: implications for international security", *Defense & Security Analysis*, vol. 35, nr. 2, s. 147-169.

Kania, Elsa B & John Costello, 2021. "Seizing the commanding heights: the PLA Strategic Support Force in Chinese military power", *Journal of Strategic Studies*, vol. 44, nr. 2, s. 218-264.

Kehler, Robert, 2012. "Implementing the National Security Space Strategy", *Air University Press*, vol. 6, nr. 1, s. 18-26.

Kindvall, Göran & Bo Tarras-Wahlberg, 2021. "Det framtida tekniklandskapet". Totalförsvarets forskningsinstitut, rapportnr: FOI-R--5049--SE.

Kristiansson, Stefan, 2019. “Om underrättelsehotet mot Sverige”. Fri värld, rapportnr: 7.

Lewis, James A, 2022. “Cyber War and Ukraine”, *Center for Strategic & International Studies*. Artikel i tidskrift. 2022-06-16. [Elektronisk] Tillgänglig: https://www.csis.org/analysis/cyber-war-and-ukraine . Hämtdatum: 2023-05-28.

Lindström, Sandra, Kristofer Hallgren, Seméli Papadogiannakis, Ola Rasmusson, John Rydqvist & Jonatan Westman, 2021. “Omvärldens rymdanalys 2020”, Totalförsvarets forskningsinstitut, rapportnr: FOI-R--5077--SE.

Nationellt cybersäkerhetscentrum [NCSC] webbplats, Om centret. [Elektronisk] Tillgänglig: https://www.ncsc.se/om-centret/ . Hämtdatum: 2023-05-28.

NATO webbplats, Emerging and disruptive technologies. [Elektronisk] Tillgänglig: https://www.nato.int/cps/en/natohq/topics_184303.htm . Hämtdatum: 2023-05-28.

Nye, Joseph S., 2004. *Power in the Global Information Age: From Realism to Globalization.* Routledge.

Oprisor, Ion, 2021. “The impact of emerging and disruptive technologies on security”, *Land Forces Academy Review*, vol. 26, nr. 4, s. 261-268.

Patent- och registreringsverket webbplats, Sverige - näst bäst i världen i år igen!. [Elektronisk] Tillgänglig: https://via.tt.se/pressmeddelande/sverige-nast-bast-i-varlden-i-ar-igen?publisherId=45876&releaseId=3317789 . Hämtdatum: 2023-05-28.

Petersson, Magnus, Oscar Almén, Carl Denward, Erika Holmquist, Tomas Malmlöv & Maria Ädel, 2020. “Utländska direktinvesteringar i skyddsvärda verksamheter”, Totalförsvarets forskningsinstitut, rapportnr: FOI-R--5069--SE.

Rekowski, Michał, 2020. “International competition in the digital age” i Izabela Albrycht, Michał Rekowski & Kamil Mikulski (red.) *Geopolitics of emerging and disruptive technologies*, The Kosciuszko Institute, s. 13-27.

Rescher, Nicholas, 2018. *Espionage, Statecraft and the Theory of Reporting: A Philosophical Essay on Intelligence Management*. University of Pittsburgh Press.

Riemer, Ofek, 2021. “Politics is not everything: New perspectives on the public Disclosure of intelligence by states”, *Contemporary Security Policy,* vol. 42, nr. 4, s. 554-583.

RISE, 2022. *Cyberhot mot Sverige- En sammanfattning för ledare och beslutsfattare*. Centrum för cybersäkerhet 2022.

Robertson, Alexa, 2018. “Narrativanalys” i Kristina Boréus & Göran Bergström (red.) *Textens mening och makt*. Studentlitteratur, s. 219-249.

Roser, Max, 2023. “Technology over the long run: zoom out to see how dramatically the world can change within a lifetime”. *Our World Data*. Artikel i tidskrift. 2023-02-22. [Elektronisk] Tillgänglig: https://ourworldindata.org/technology-long-run . Hämtdatum: 2023-05-28.

Skolverket webbplats, Skolutveckling. [Elektronisk] Tillgänglig: https://www.skolverket.se/skolutveckling/inspiration-och-stod-i-arbetet/inspiration-och-reportage/medieutvecklingen-forandrar-ungas-nyhetskonsumtion . Hämtdatum: 2023-05-28.

Świątkowska, Joanna, 2020. "Artificial intelligence - A driving force of geopolitical changes" i Izabela Albrycht, Michał Rekowski & Kamil Mikulski (red.) *Geopolitics of emerging and disruptive technologies*, The Kosciuszko Institute, s. 133-145.

Świątkowska, Joanna, 2020. "Offensive actions in cyberspace - A factor shaping geopolitical order" i Izabela Albrycht, Michał Rekowski & Kamil Mikulski (red.) *Geopolitics of emerging and disruptive technologies*, The Kosciuszko Institute, s. 123-133.

Törnquist, Hanna & Nahritha Al-Khameesi, 2022. "Nätkampanj mot Sverige oroar: "Vill skapa polarisering"". *Svenska Dagbladet*. Nyhetsartikel. 2022-02-07. [Elektronisk] Tillgänglig: https://www.svd.se/a/v5dk04/desinformationskampanj-mot-sverige-i-sociala-medier . Hämtdatum: 2023-05-28.

U.S. Department of Defense [U.S. DoD] webbplats, Our Forces. [Elektronisk] Tillgänglig: https://www.defense.gov/About/our-forces/ . Hämtdatum: 2023-05-28.

von Clausewitz, Carl, 1989. *On War*. Princeton University Press.

Yarhi-Milo, Keren, 2014. *Knowing the Adversary: Leaders, Intelligence, and Assessment of Intentions in International Relations*. Princeton University Press.

Ydén, Karl, Joakim Berndtsson & Magnus Petersson, 2019. "Sweden and the issue of NATO membership: exploring a public opinion paradox", *Defence Studies*, vol. 19, nr. 1, s. 1-18.

Den svenska underrättelseinstitutionens årsrapporter

FRA, 2014. *FRA årsrapport 2014*. Försvarets radioanstalt.

FRA, 2015. *FRA årsrapport 2015*. Försvarets radioanstalt.

FRA, 2016. *FRA årsrapport 2016*. Försvarets radioanstalt.

FRA, 2017. *FRA årsrapport 2017*. Försvarets radioanstalt.

FRA, 2018. *FRA årsrapport 2018*. Försvarets radioanstalt.

FRA, 2019. *FRA årsrapport 2019*. Försvarets radioanstalt.

FRA, 2020. *FRA årsrapport 2020*. Försvarets radioanstalt.

FRA, 2021. *FRA årsrapport 2021*. Försvarets radioanstalt.

FRA, 2022. *FRA årsrapport 2022*. Försvarets radioanstalt.

MUST, 2014. *MUST årsöversikt 2014*. Militära underrättelse- och säkerhetstjänsten.

MUST, 2015. *MUST årsöversikt 2015*. Militära underrättelse- och säkerhetstjänsten.

MUST, 2016. *MUST årsöversikt 2016*. Militära underrättelse- och säkerhetstjänsten.

MUST, 2017. *MUST årsöversikt 2017*. Militära underrättelse- och säkerhetstjänsten.

MUST, 2018. *MUST årsöversikt 2018*. Militära underrättelse- och säkerhetstjänsten.

MUST, 2019. *MUST årsöversikt 2019*. Militära underrättelse- och säkerhetstjänsten.

MUST, 2020. *MUST årsöversikt 2020*. Militära underrättelse- och säkerhetstjänsten.

MUST, 2021. *MUST årsöversikt 2021*. Militära underrättelse- och säkerhetstjänsten.

MUST, 2022. *MUST årsöversikt 2022*. Militära underrättelse- och säkerhetstjänsten.

SÄPO, 2014. *Säkerhetspolisens årsbok 2014*. Säkerhetspolisen.

SÄPO, 2015. *Säkerhetspolisens årsbok 2015*. Säkerhetspolisen.

SÄPO, 2016. *Säkerhetspolisens årsbok 2016*. Säkerhetspolisen.

SÄPO, 2017. *Säkerhetspolisens årsbok 2017*. Säkerhetspolisen.

SÄPO, 2018. *Säkerhetspolisens årsbok 2018*. Säkerhetspolisen.

SÄPO, 2019. *Säkerhetspolisens årsbok 2019*. Säkerhetspolisen.

SÄPO, 2020. *Säkerhetspolisens årsbok 2020*. Säkerhetspolisen.

SÄPO, 2021. *Säkerhetspolisens årsbok 2021*. Säkerhetspolisen.

SÄPO, 2022. *Säkerhetspolisens årsbok 2022*. Säkerhetspolisen.