Självständigt arbete (15 hp)

Författare		**Program/Kurs**
Kd Filip Banic		OP SA 16–19
Handledare		**Antal ord: 11675**
Fil. dr. Martin Neuding-Skoog	**Beteckning**	**Kurskod**
		1OP415

OM DU VILL HA FRED, RUSTA FÖR CYBERKRIG
SVERIGES CYBERFÖRSVAR UR ETT AVSKRÄCKNINGSPERSPEKTIV

In accordance with the EU Network and Information Security directive (NIS directive), the Swedish government made it mandatory for specific authorities and organizations to report IT-related incidents to the Swedish Civil Contingencies Agency (MSB). In their report from 2017, MSB stated that due to the low frequency of incoming information, the report doesn't give an accurate picture of the actual circumstances. The same year the European Commission adopted a cybersecurity package containing multiple initiatives aimed to further better member states resilience, deterrence and handling of cyber-attacks. Due to the insufficient information in MSBs' report, it´s difficult to determine whether the Swedish cyber defence has the ability to deter antagonistic states to conduct cyber operations or not.

The purpose of this theory-consuming single-case study was to examine the Swedish cyber defence from a deterrence perspective and thereby provide new understanding regarding Swedens' ability to deter within the cyber domain. To do this, a conceptual framework was constructed constituting of Phil Williams' theory on the requirements of successful deterrence, and David J. Lonsdales' model for cyber deterrence. Contemporary Swedish political documents, doctrines, reports and statements made up the empirical material that has been examined through qualitative text analysis.

The result of the analysis revealed that the Swedish cyber defence, from a deterrence perspective, can be described as inadequate. Despite meeting the basic requirements for deterrence to succeed, the Swedish cyber defence lacks what Lonsdale calls a comprehensive flexible cross-domain offensive capability. The absence of a cross-domain retaliatory capability in the Swedish cyber defence repertoire has a negative incidental impact on deterrence credibility. According to Williams, it's imperative that the defender possess necessary capabilities to fulfil a threat, otherwise the deterrence won't seem credible and therefor lack effectiveness.

Nyckelord:
Cyberförsvar, cyberavskräckning, cyberdomän, defensiva cyberförmåga, offensiv cyberförmåga

1. Inledning

1.1 Bakgrund

Skapandet av det allmänna internet har inneburit att privata, liksom statligt finansierade, aktörer sett en potential i att exploatera den nya domänen. I samband med att den estniska statsapparaten fattade beslut om att avlägsna en sovjetisk bronsstaty i april 2007 utsattes landet för långtgående komplexa cyberattacker. Angreppen var riktade dels mot landets myndigheter, dels mot andra samhällsbärande institutioner såsom bankväsendet. De, till synes, välkoordinerade attackerna varade i flera dagar och resulterade i en kollaps av landets offentliga sektor liksom dess finansiella system.[1] Liknade cyberangrepp förekom även i samband med den ryska invasionen av Georgien året därpå och lamslog initialt den georgiska krigsmaktens kommunikationssystem.[2] Andra exempel på statligt sanktionerade cyberangrepp är attacken mot Irans kärnkraftsprogram, där den skadliga programvaran *Stuxnet* angrep och saboterade anläggningarnas urananrikningscentrifuger.[3] Trots cyberoperationers ringa inverkan är Stuxnet det första bekräftade fallet på att en mjukvara kan åsamka fysiska skador på samhällskritiska anläggningar.[4]

Det frångår inte någon att digitaliseringen av samhällsstrukturer har inneburit stora förändringar, både till det bättre och det sämre. Den digitala utvecklingen har föranlett att cyberdomänen idag betraktas som en av flera konfliktarenor, där statsaktörer spionerar och angriper varandras skyddsvärda verksamhet och samhällsviktiga infrastruktur. All typ av nätverksbaserad verksamhet som i dagsläget är anslutet till internet riskerar att utsättas för cyberattacker och andra typer av intrångsförsök.[5] De utmaningar som uppstår till följd cyberdomänens utsatthet är ett angeläget problem för hela världssamfundet och därmed även Sverige.

Parallellt med att cyberdomänen i allt större utsträckning nyttjas för att tillgodose strategiska, ekonomiska och politiska målsättningar, har den politiska viljan att stärka motståndskraften mot cyberangrepp ökat. I samband med riksmötets öppnande 2019 deklarerade statsminister Stefan Löfven att ett nationellt center håller på att upprättas för att öka landets cybersäkerhet.[6] I dokumentet *Motståndskraft*, utgiven av försvarsdepartementet, belyses omvärldsutvecklingen och hur digitaliseringen möjliggör antagonistisk påverkan genom cyberattacker.[7]

[1] Sierzputowski 2019. s. 225–227.
[2] Collins & McCombie 2012. s. 83.
[3] Ibid. s. 84–86.
[4] Stuxnet: 2011. s. 1–3.
[5] Skr. 2016/17:213. s. 7.
[6] Regeringskansliet. Regeringsförklaringen: 21 januari 2019. 2019. s. 15.
[7] Ds 2017:66. s. 18.

Likaledes konkretiserar Försvarsmakten i *Militärstrategisk doktrin 2016 (MSD 2016)* cyberdomänens strategiska innebörd och stipulerar att myndigheten skall bistå för att stärka skyddet av landets cybersäkerhet.[8]

1.2 Problemformulering

Som medlem i den Europeiska Unionen (EU) omfattas Sverige av den gemensamma säkerhetspolitiken beträffande cybersäkerhet och det s.k. *Network and Information Security directive* (NIS-direktivet). De fastställda riktlinjerna i direktivet ställer krav på säkerhet i nätverk- och informationssystem med syfte att uppnå en hög gemensam nivå på säkerhet i nätverk- och informationssystem inom EU.[9] Som följd av NIS-direktivets krav fattade den svenska regeringen den 17 december 2015 beslut om obligatorisk IT-incidentrapportering för statliga myndigheter. Rapportering skall ske årligen till Myndigheten för samhällsskydd och beredskap (MSB) med start i 1 april 2016.[10] Syftet med ett obligatoriskt rapporteringssystem är b.la. att skapa gynnsamma förutsättningar för att vidta rätt skyddsåtgärder och utveckla totalförsvarets samlade cyberförmåga.[11] I sin senaste sammanställning, som omfattar kalenderåret 2017, konstaterade MSB att rapporteringen från berörda myndigheter varit bristfällig och således inte ger korrekt lägesbild av situationen.[12] Samma år lade EU:s kommission och höga representant för utrikes frågor och säkerhetspolitik fram ett gemensamt meddelande om att EU:s samlade cyberförsvar skall utvecklas. Ändamålet med utvecklingen är att ytterligare stärka unionens resiliens, *avskräckning* och hantering av cyberattacker.[13] Den låga rapporteringsgraden från berörda institutioner till MSB, innebär att det i nuläget är svårt att bedöma det svenska cyberförsvarets avskräckningsförmåga.

För att upprätthålla *status quo*, d.v.s. lyckas med avskräckningen, måste den avskräckande partens projicerade förmågor vara av en sådan karaktär att motståndaren uppfattar hoten som trovärdiga.[14] En lyckad avskräckning inbegriper i sin tur ett samspel mellan de tre grundläggande faktorerna *kommunikation*, *förmågor* och *trovärdighet*. Teoretikern Phil Williams åskådliggör i antologin *Contemporary Strategy* korrelationen mellan de bärande faktorerna och hur symbiosen mellan dem renderar i en effektiv och framgångsrik avskräckning.[15]

[8] Försvarsmakten 2016. s. 30.
[9] Ds 2017:66. s. 115, 118.
[10] Regeringskansliet. Regeringen inför krav på it-incidentrapportering för statliga myndigheter. 2015.
[11] MSB. Årsrapport It-incidentrapportering 2017. 2018. s. 5.
[12] Ibid. s. 7–9.
[13] Riksdagen. Resiliens, avskräckning och försvar: stärkt cybersäkerhet för EU. s. 8.
[14] Schelling 1960. s. 6.
[15] Williams 1987. s. 117–121.

Vidare konkretiserar David J. Lonsdale i sin artikel *Warfighting for Cyber Deterrence: a Strategic and Moral Imperative* vilka förmågor och handlingar som erfordras för att uppnå en lyckad avskräckning inom cyberdomänen. Genom att resonera utifrån de tre tidigare nämnda grundfaktorerna kombinerar Lonsdale idéer sprungna ur nukleär avskräckning och konstruerar ett konceptuellt ramverk för cyberavskräckning.[16]

Utgångspunkten för denna undersökning är följaktligen att studera Sveriges förutsättningar för att verka avskräckande mot cyberangrepp. Det svenska cyberförsvaret och den situation Sverige befinner sig i idag utgör studiens fall. Genom att utgå från Williams teoribildning och Lonsdales modell kan arbetet tydliggöra om Sveriges cyberförsvar i dagsläget är anpassat för att avskräcka en potentiell angripare inom cyberdomänen.

1.3 Forskningsöversikt

I *Deterring Russia in Europe: Defence Strategies for Neighbouring States* återfinns b.la. Tom Rostoks överläggning om avskräckning och dess konceptuella utveckling från kalla kriget, till dagens svåröverskådliga säkerhetspolitiska situation. Han åskådliggör hur nukleära förmågor i viss utsträckning tappat sin strategiska relevans. Vidare poängterar Rostoks att cyberdomänen i allt större grad ökat i betydelse och därav även staters förmåga till att avskräcka illasinnade cyberangrepp.[17]

I samma verk presenterar Robert Dalsjö också en analys av den säkerhetspolitiska utvecklingen i Sverige innan och i samband med den uppkomna krisen i Ukraina. Tesen han utgår från är att den svenska statsmakten varit snabb på att reagera på Rysslands aggressiva utrikespolitik men senfärdig med att de facto realisera sina säkerhetspolitiska målsättningar.[18] Hans huvudsakliga argument för varför Sverige misslyckats med att etablera en adekvat avskräckningsstrategi går att härleda till politikernas oförmåga att fatta konkreta beslut. Förutom historisk empiri underbygger Dalsjö sitt resonemang genom att hänvisa dels till den pågående säkerhetspolitiska debatten avseende svenskt medlemskap i NATO (*North Atlantic Treaty Organization*), dels till det faktum att satsningar på försvarsrelaterad verksamhet förblivit lågprioriterade.[19]

[16] Lonsdale 2018. s. 425–426.
[17] Rostoks 2019. s. 29–30, 33.
[18] Dalsjö 2019. s. 93.
[19] Ibid. s. 94–107.

Samlingsverket är intressant och relevant eftersom det avhandlar avskräckning i en nutida svensk och europeisk kontext utifrån de möjligheter och problem globaliseringen och den digitala revolutionen medför. Dock bottnar inte verket vare sig i hur avskräckning inom cyberdomänen skall manifesteras, eller huruvida de stater som avhandlas ur ett avskräckningsperspektiv besitter ett adekvat cyberförsvar.

En författare som däremot gör kopplingen mellan avskräckning och cybersäkerhet är Alex Wilner. I artikeln *Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation* driver han tesen att avskräckning är svårt att uppnå inom cyberdomänen. Problematiken, menar Wilner, grundar sig i sju olika dilemman en försvarande aktör tvingas bemöta om denne skall verka avskräckande.[20] Ett av dessa är särskilt intressanta att belysa kopplat till denna undersökning, nämligen problematiken kring vedergällning. Enligt Wilner kan en antagonist utan större svårigheter dölja sina spår, vilket i sin tur renderar i att vedergällning för en cyberattack blir svår att realisera.[21] Trots att en lösning inte presenteras i artikeln är den relevant då den belyser ett påtagligt problem alla statsaktörer som har ambitioner att försvara sin cyberdomän tvingas tackla.

En möjlig lösning till dilemmat presenteras istället av Emilio Iasiello. I sin artikel *Is Cyber Deterrence an Illusory Course of Action?* problematiserar han likt Wilner kring vedergällande attacker inom cyberdomänen. Problemet grundar sig i att utan information om vem som iscensatt ett cyberangrepp och varför, blir det svårt för en försvarande aktör att vedergälla ett cyberangrepp.[22] Utifrån det faktumet konkluderar Iasiello att en statsaktör som önskar verka avskräckande inom cyberdomänen, bör lägga tonvikten på defensiva cyberförmågor. Dock hävdar han att defensiva lösningar kontinuerligt måste evalueras i syfte att inte bli obsoleta.[23]

David J. Lonsdale delar till viss del Iasiellos ståndpunkt. I artikeln *Warfighting for Cyber Deterrence: a Strategic and Moral Imperative* hävdar Lonsdale att teoribildningen beträffande cyberavskräckning saknar en viktig variabel, nämligen viljan att verka offensivt. Idén, *warfighting*, är direkt hämtad från traditionell avskräckningsteori och medför, enligt författaren, en rad olika praktiska fördelar på cyberdomänen, däribland ökad trovärdighet i en aktörs strävan till att avskräcka sin motpart.[24]

[20] Wilner 2017. s. 309.
[21] Ibid. s. 313–314.
[22] Iasiello 2013. s. 65.
[23] Ibid. s. 67.
[24] Lonsdale 2018. s. 409.

Genom att tillföra idéer kring avskräckning sprungna ur kalla kriget i en ny digital kontext konstruerade han en alternativ modell till cyberavskräckning.[25] Trots att konventionell avskräckning skiljer sig från sådan som sker inom ramen för cyberdomänen, menar Lonsdale att detta inte utgör ett hinder då principerna för en lyckad avskräckning är allmängiltiga.[26] Han konkluderar att cyberavskräckning bör innefatta en offensiv liksom defensiv förmåga för att nå full potential. Kombinationen av olika förmågor stärker, enligt Lonsdale, trovärdigheten i en aktörs avskräckningsförsök och därmed effektiviteten i strategin.[27]

Artikeln är relevant då modellen som författaren skapar ingående beskriver vilka komponenter ett cyberförsvar bör innehålla för att verka avskräckande. Därav utgör den en del av arbetets teoretiska ramverk. En mer ingående beskrivning av modellen följer under teorikapitlet.

Andra artiklar som avhandlar avskräckning i en cyberkontext antar en juridisk utgångspunkt. Framförallt diskuteras legala implikationer som kan tänkas uppstå vid implementering av konceptet som en del av statsaktörers säkerhetsstrategier.[28] Merparten verk som återfunnits resonerar emellertid kring huruvida det är rimligt att applicera klassisk avskräckningsteori inom cyberdomänen. Vissa hävdar att det inte är lämpligt i och med teorins historiska arv. Mariarosaria Taddeo menar exempelvis att världssamfundet bör etablera normer som stipulerar statsaktörers agerande i cyberdomänen, istället för att förlita sig på obsoleta teoribildningar.[29] Matthew D. Crosston hävdar i sin tur, likt Lonsdale, att det är fullt gångbart och visar på i sin artikel hur logiken kring nukleär avskräckning kan appliceras i en cyberkontext.[30]

Phil Williams behandlar begreppet avskräckning och dess utveckling ur ett mer oberoende perspektiv. I verket *Contemporary Strategy* beskriver författaren avskräckningsteorin och de tre grundfaktorer som måste samspela såvida avskräckning skall uppnå sin önskade effekt. För att en aktörs avskräckningsstrategi skall uppnå sitt syfte hävdar Williams att den försvarande aktörens motpart måste uppfatta de kommunicerade hoten som trovärdiga utifrån de förmågor man som försvararen besitter.[31] Genom att lyfta begreppet ur det säkerhetspolitiska kontext som rådde under kalla kriget intar Williams en neutral ställning inom det berörda forskningsfältet.

[25] Lonsdale 2018. s. 410.
[26] Ibid. s. 417.
[27] Ibid. s. 426.
[28] Jensen 2012. s. 778.
[29] Taddeo 2018. s. 324–325.
[30] Crosston 2011. s. 115.
[31] Williams 1987. s. 117–121.

Författarens redogörelse renderar i en lättfattlig beskrivning kring avskräckningsteorins komposition. I och med att avskräckning som fenomen och strategiskt tillvägagångsätt kan anses vara allmängiltigt, är Williams bidrag intressant och relevant då det explicit redogör för dess grundfaktorer. Teoribildningen som presenteras lämpar sig således som konceptuellt ramverk utifrån vilket Lonsdales resonemang och cyberavskräckningsmodell kan begripas.

Forskning som avhandlar cyberavskräckning indikerar att konceptet fortfarande är i sin linda och således utgår från sin konventionella motsvarighet. Verkens teman varierar från att belysa juridiska aspekter, till att innefatta överläggningar kring skapandet av en adekvat avskräckningsteori lämpad för cyberdomänen. Den forskning som berör Sverige och andra småstater inom EU inbegriper enbart avskräckning ur ett konventionellt perspektiv. Detta är sålunda ett intressant men underforskat område som också är relevant att undersöka i svensk kontext.

1.4 Syfte och frågeställning

Arbetets övergripande syfte är att utifrån Williams teoribildning och Lonsdales modell undersöka det svenska cyberförsvarets förutsättningar för att verka avskräckande. Genom att studera det svenska cyberförsvaret utifrån ett avskräckningsperspektiv bidrar undersökningen med ny kunskap kring huruvida Sverige de facto möter EU:s vilja att verka avskräckande inom cyberdomänen. Undersökningen tydliggör en småstats avskräckningsförmåga och bidrar således även till det berörda forskningsfältet med en djupare insikt kring en småstats möjligheter att verka avhållande mot cyberangrepp. Därtill bidrar undersökningen till den svenska militära yrkesutövningen genom att belysa eventuella styrkor och svagheter i rikets cyberförsvar sett utifrån ett avskräckningsperspektiv.

Med det ovannämnda som grund har följande frågeställning formulerats:

Hur kan det svenska cyberförsvaret beskrivas utifrån ett avskräckningsperspektiv?

1.5 Avgränsningar

Undersökningen avgränsades till att behandla Sveriges aktuella cyberförsvar utifrån Willams teoribildning och Lonsdales modell, beträffande vilka förutsättningar som erfordras för att lyckas med avskräckning. Således har studien inte att förhållit sig till något tänkt motståndarperspektiv där en specifik motparts subjektiva uppfattning tagits i beaktande. Huruvida en illasinnad statsaktör under faktiska omständigheter upplever Sverige som avskräckande kan svårligen bevisas. Resultatet av undersökningen återger därmed enbart svensk förmåga till avskräckning inom cyberdomänen utifrån ett teoretiskt perspektiv.

Vidare hade undersökningen inga ambitioner att i detalj beskriva specifika förmågor, utan snarare ge en helhetsbild av det svenska cyberförsvaret utifrån ett avskräckningsperspektiv.

1.6 Disposition

Det första kapitlet inleds med en redogörelse av uppsatsens bakgrund och problemformulering. Därefter följer en presentation av tidigare forskning inom det berörda fältet samt undersökningens syfte och frågeställning. Kapitlet avslutas med en redogörelse av arbetes avgränsningar.

Kapitel två inleds med en motivering till valt teoretiskt ramverk där styrkor och svagheter belyses. Därefter följer en redovisning av Williams teoribildning och Lonsdales modell, varpå kapitlet avslutas med en presentation av den kritik som riktas mot avskräckningsteorin.

Det tredje kapitlet omfattar en beskrivning av uppsatsens metodologiska ansats samt en diskussion avseende valet. Kapitlet innefattar även en motivering till val av fall och en presentation av det empiriska underlaget med tillhörande källkritik. Avslutningsvis framställs undersökningens analysverktyg genom en syntes och operationalisering av arbetets teoretiska ramverk.

I det fjärde kapitlet analyseras undersökningens fall med stöd av framtaget analysverktyg. Analysen är av en argumenterande karaktär där ett resonemang förs utifrån indikatorerna och arbetets teoretiska ramverk. Analysen avslutas med en presentation och sammanfattning av erhållet resultat.

I det femte kapitlet, tillika arbetets avslutning, besvaras undersökningens forskningsfråga. Kapitlet inbegriper även en avslutande diskussion samt förslag till möjlig fortsatt forskning.

2. Teori

2.1 Motivering till vald teoretisk ansats

Oavsett vilka teoretiska åskådningar och perspektiv som används för att definiera och tolka avskräckning omnämns alltid faktorerna: *förmåga, kommunikation* och *trovärdighet* som bärande komponenter.[32] En framgångsrik symbios mellan faktorerna erfordras om en aktörs avskräckningsförsök skall nå sina strategiska målsättningar.[33] Williams lyfter grundfaktorerna ur kontext och för en mer allmän diskussion kring deras logik. Därav utgör dennes tolkning en del av arbetets teoretiska ramverk. Williams generella perspektiv bidrar med en lättfattlig förklaring kring den logik som omgärdar faktorerna och deras innebörd. Styrkan med vald teoribildning är följaktligen att den inte är belastad med specifika förmågor eller kringliggande kontext.

Svagheten torde dock vara att teorin är grundad under en period då digitaliseringen av samhället var marginell och således inte en faktor. Trots svagheten är Williams beskrivning av avskräckning och dess grundfaktorer mest adekvat för kommande undersökning då den är bredast och därmed tillämpbar i flera sammanhang.

Den andra delen av det teoretiska ramverket utgörs av Lonsdales teoretiska modell för lyckad cyberavskräckning. Författaren hämtar idéer främst från etablerad teoribildning kring nukleär avskräckning och applicerar dessa i en cyberkontext. Resonemanget han för utgår från avskräckningens tre grundfaktorer vilket möjliggör en syntes av dennes åskådning och Williams teoribildning. Modellen kompletterar således den generella teoribildningen kring lyckad avskräckning, vilket bistår vid operationaliseringen och sedermera preciseringen av undersökningens indikatorer. Williams generella tolkning är följaktligen det ramverk inom vilket Lonsdales mer systematiska beskrivning av vad som erfordras för att uppnå lyckad cyberavskräckning faller inom. Teoribildningen kastar ljus på modellen och bringar förståelse för det resonemang Lonsdale för utifrån de tre grundfaktorerna.

[32] Stone 2012. s. 108–120.
[33] Williams 1987. s. 117.

2.2 Teoretiskt ramverk

2.2.1 Williams teoribildning

En aktör som har ambitioner att genom hot verka avhållande gentemot en antagonistisk motpart och få denne att avbryta sina planerade handlingar, måste förhålla sig till avskräckningsteorins tre grundfaktorer. Tillsammans konstituerar grundfaktorerna en lyckad avskräckning där en symbios mellan dem bör eftersträvas ifall den eftersökta synergin skall uppnås. En framgångsrik samverkan mellan grundfaktorerna är följaktligen en förutsättning för att aktören som avskräcker och dennes hot skall upplevas som trovärdiga.[34]

Den första grundfaktorn, *kommunikation*, omfattar hur och vad en defensiv aktör signalerar till omvärlden beträffande konsekvenser en eventuell motståndare kan förvänta sig om denne fullföljer sina fientliga intentioner. De kommunicerade hoten måste vara tydliga och formulerade på ett sådant vis att de planerade motåtgärderna upplevs som trovärdiga. Vidare uppfattas den försvarande aktören som trovärdig om denne gör tillräckligt konkreta investeringar i sitt planerade försvar. Genom att göra kostsamma satsningar signalerar den defensiva aktören indirekt att denne underbygger sina hot med faktiska insatser. Kommunikationen behöver således inte enbart vara av verbal karaktär, utan även omfatta åtgärder och åtaganden som visar på ett engagemang. Det sistnämnda kan exempelvis innefatta demonstrativa övningar eller deltagande i skarpa insatser som gör tydligt vilken inställning man som defensiv aktör har gentemot en tänkbar angripare.[35]

Den andra grundfaktorn som Williams redogör för är kapabla *förmågor*, d.v.s. de förmågor den defensiva aktören projicerar i den uttalade konsekvensbeskrivningen. Vilka typer av förmågor som projiceras samt deras kapacitet är beroende av antagonistens tillvägagångssätt vid ett anfall och vilka intressen som hotas. Generellt gäller det att förmågorna skall vara av en sådan karaktär att de vid ett eventuellt angrepp skulle åsamka den offensiva aktören oacceptabla kostnader i relation till vad denne hade erhållit om aktionen fullföljts. Kostnadskalkyleringen skall sedermera driva motståndaren till att omvärdera sina avsikter och få denne att välja andra handlingsalternativ som inte utmanar rådande tillstånd.[36]

[34] Williams 1987. s. 121.
[35] Ibid. s. 117–120.
[36] Ibid. s. 120.

Den tredje och, enligt Williams, viktigaste grundfaktorn är *trovärdighet*. Framgångsfaktorn i den defensiva aktörens avskräckning är beroende av huruvida den offensiva motparten uppfattar de kommunicerade hoten som trovärdiga utifrån de förmågor försvararen besitter. För att avskräckningen skall få önskad effekt erfordras således, utöver en bedömning baserad på kostnadskalkyler, även en insikt hos den offensiva motparten att försvararen de facto avser effektuera sina hot. Trovärdighet tar följaktligen sin utgångspunkt i den defensiva statens uttryckta vilja att avvärja kränkningar med de medel som finns att tillgå. Därav är det nödvändigt för en stat som önskar avskräcka att influera sin motståndares förväntningar avseende det egna handlingssättet i händelse av en överträdelse. Därtill måste de hot som signaleras vara förenliga med det tänkta angreppets natur och omfattning samt praktiskt genomförbara för att uppfattas som trovärdiga.[37]

Sammanfattningsvis kan det konstateras att förhållandet mellan de olika faktorerna är att de är beroende av varandra. Grundfaktorerna innehar olika roller och bidrar därmed olika till avskräckningen. Williams poängterar dock att den centrala faktorn är att avskräckningen skall upplevas som trovärdig. En konkretisering av korrelationen mellan grundfaktorerna är att de förmågor som en försvarande aktör innehar samt hur denne förmedlar sitt budskap skall vara trovärdiga tillsammans. Ett politiskt uttalande som inbegriper en viss vilja måste enligt teorins logik alltså mötas med faktiska handlingar som visar att den försvarande aktören kan och vill agera.

2.2.2 Lonsdales modell för lyckad cyberavskräckning

Det fundamentala i warfighting är kombinationen av offensiva och defensiva förmågor. Genom att kombinera olika förmågor med varierande syften ökar avskräckningens trovärdighet och därav även chanserna till strategisk måluppfyllnad.[38] Lonsdale gör gällande att samma koncept går att tillämpa inom cyberdomänen, utifrån resonemanget att avskräckningens tre grundfaktorer och deras relation till warfighting-konceptet är universella.[39]

Modellen han konstruerar talar för att ett cyberförsvar bör inbegripa offensiva förmågor från olika domäner och aktiva samt passiva defensiva cyberförmågor. Den offensiva kapaciteten inbegriper utöver cyberförmågor även militära liksom icke-militära medel, där det sistnämnda kan involvera exempelvis ekonomiska sanktioner.[40]

[37] Williams 1987. s. 121.
[38] Lonsdale 2018. s. 411–412.
[39] Ibid. s. 410.
[40] Ibid. s. 424.

Avseende offensiva cyberförmågor utgörs dessa enligt Lonsdale av skadliga koder (virusprogram). De skadliga koderna kan konstrueras för att lösa olika typer av uppgifter, från vanlig underrättelseverksamhet till sabotage av samhällskritisk infrastruktur.[41]

Vad beträffar aktiva och passiva defensiva cyberförmågor särskiljer Lonsdale på dessa i sin modell. Brandväggar och nyttjandet av lösenord tillskrivs som aktiva defensiva medel, medan passiva omfattas av cyberdomänens resiliens och redundans. Vidare stipulerar författaren att ett cyberförsvar främst bör fokusera på defensiva medel för att uppnå en avskräckande effekt. Resonemanget grundar sig i faktumet att cyberattacker genom historien haft begränsad framgång.[42] Vilken typ av defensiv cyberförmåga som bör prioriteras framgår dock inte i Lonsdales modell.

Avseende den kommunikativa faktorn menar Lonsdale att en försvarande aktör bör besitta dedikerade cyberenheter vars uppgift är att leda operationer inom cyberdomänen. Detta signalerar enligt författaren att den försvarande parten har viss nödvändig kompetens att hantera de förmågor denne besitter. Han poängterar även vikten av att delta i cyberövningar där en försvarande aktör visar att denne kan och vill nyttja sina förmågor. Förekomsten av cyberenheter och deltagande i cyberövningar befäster således trovärdigheten i avskräckningen.[43]

2.3 Kritik mot teoretisk ansats

Vanlig kritik som riktas mot avskräckningsteori är att den utgår från idealiseringar där makthavare fattar beslut baserat på rationellt tänkande. Experterna Richard Ned Lebow och Janice Gross Stein hävdar exempelvis att den perfekta värld som teorier kring avskräckning bygger på saknar empiriskt stöd och är därav i grunden ofullkomliga.[44] Denna uppfattning delas även av Alexander George och Richard Smoke som hävdar att avskräckningsteori utgår från en rad olika simplifierade hypoteser, däribland synen på rationalitet. [45]

[41] Lonsdale 2018. s. 417, 420.
[42] Ibid. s. 424, 425.
[43] Ibid. s. 417.
[44] Lebow & Gross Stein 1989. s. 224.
[45] George & Smoke 1974. s. 71–78.

Förespråkare för avskräckningsteori menar i sin tur att antagandet avseende den rationellt tänkande människan inte utgör ett problem. Thomas Schelling hävdar exempelvis att irrationella handlingar i vissa situationer kan vara logiska och således paradoxalt nog betraktas som rationella utifrån ena partens perspektiv. [46]

Då debatten kring avskräckningsteori och dess validitet som teoretiskt ramverk till synes inte berör grundfaktorerna, har de svagheter som belyses av vissa ämnesexperter inte att underminera denna undersökning. Oavsett om det råder meningsskiljaktigheter kring huruvida teorin skall utgå från rationella eller irrationella aktörer föreligger konsensus avseende grundfaktorernas centrala roll. Därtill, eftersom undersökningen inte utgått från ett tänkt motståndarperspektiv och huruvida denne agerar rationellt eller irrationellt, påverkade kritiken inte undersökningen i någon utsträckning.

[46] Schelling 2008. s. 36–43.

3. Metod

3.1 Forskningsdesign – Teorikonsumerande fallstudie

Undersökningen genomfördes som en teorikonsumerande fallstudie[47]där fallet utgjordes av Sveriges cyberförsvar och det som studerades var cyberförsvarets avskräckningsförmåga. Då arbetet enbart berörde Sverige har undersökningen kategoriserats som en enkelfallstudie.[48] För att belysa det fenomen som studerats har en teori och modell nyttjats som båda gör anspråk på att förklara vad som erfordras för att uppnå en lyckad avskräckning. Teorin utgjorde ett konceptuellt ramverk utifrån vilket modellen skulle förstås. För att göra det teoretiska ramverket kompatibelt med valt fall genomfördes därefter en operationalisering, med syftet att urskilja och formulera indikatorer som sedermera utgjorde arbetets analysverktyg.[49]

Tillvägagångsättet möjliggjorde en djupgående analys av det empiriska materialet och bistod således med teoretiskt förankrade beskrivningar kring orsaker och konsekvenser avseende ett specifikt fenomen.[50] Visserligen kan resultatet som erhölls svårligen ses som allmängiltigt, i synnerhet eftersom undersökningen enbart inbegrep ett fall.[51] Dock behöver fallstudier av en teorikonsumerande karaktär inte nödvändigtvis ha ambitioner att överföra erhållet resultat till andra fall.[52] Det centrala argumentet med vald forskningsdesign var att pröva det unika fallet, inte huruvida vald teori eller fall hade en god förklaringskraft.[53] Arbetets resultat kan därmed inte anses som överförbart till andra nationer utan att nya undersökningar inom ämnet genomförs. Undersökningen belyste dock viktiga aspekter som i viss utsträckning kan bidra med perspektiv om övriga aktörer inom EU.[54] Det är rimligt att anta att de förutsättningar som råder i fallet Sverige även går att återfinna i andra EU-länder, i synnerhet de nordiska grannländerna.[55]

[47] Esaiasson et al. 2017. s. 42.
[48] Johannessen & Tufte 2003. s. 56.
[49] Esaiasson et al. 2017. s. 56.
[50] George & Bennett 2005. s. 21.
[51] Yin 2007. s. 57–59.
[52] Esaiasson et al. 2017. s. 154.
[53] Ibid. s. 89–90.
[54] Ibid. s. 159.
[55] Ibid. s. 165–166.

3.2 Val av fall

Valet av Sveriges cyberförsvar som fall grundade sig i att MSB i samband med sin IT-incidentrapportering för 2017 redovisade förvånansvärt bristfällig återrapportering från berörda myndigheter och organisationer. Kopplat till rapportens utfall och faktumet att EU vill verka avskräckande inom cyberdomänen, föreföll det både intressant och relevant att studera det svenska cyberförsvaret utifrån ett avskräckningsperspektiv. Därtill framgick det i forskningsöversikten att det aktuella fältet beträffande cyberavskräckning präglas av en överrepresentation av studier som enbart avhandlar USA:s cyberförsvar och dess avskräckningsförmåga. De studier som inbegriper Sverige antar ett konventionellt perspektiv och berör vare sig rikets cyberförsvar eller dess förmåga till avskräckning.

Ytterligare faktor som togs i beaktande vid val av fall var den stora tillgången till empiriskt material. Med hänseende till arbetets teoretiska ramverk och det resonemang som förs avseende avskräckningens tre grundfaktorer, erfordrades en stor mängd data för att återge en korrekt bild av det fenomen som avsågs undersökas. Genom att studera det svenska cyberförsvaret ur ett avskräckningsperspektiv tillför studien till det aktuella forskningsfältet och till ökad förståelse av EU:s samlade cyberförsvar.

3.3 Metod för dataanalys och datainsamling – Kvalitativ textanalys

För att samla in och analysera arbetets empiriska underlag utgick undersökningen från en kvalitativ textanalys.[56] Med hänsyn till att de handlingar som analyserades inte uttryckligen nämnde det eftersökta fenomenet, utgjorde vald metod ett adekvat tillvägagångsätt. Valet grundade sig på att metodens styrka ligger i att lyfta fram dolda budskap med hjälp av ett teoretiskt förankrat analysverktyg.[57] Vidare avsåg undersökningen att belysa de organisatoriska förhållanden som producerar ett fenomen, vilket ytterligare gav skäl för nyttjandet av en kvalitativ analysmetod.[58] Fenomenet var i detta fall det svenska cyberförsvarets avskräckningsförmåga och det som analysen ämnade åskådliggöra var förekomsten av avskräckningsteorins grundfaktorer.

Kvalitativ textanalys utgör ett av flera möjliga metodologiska tillvägagångsätt att samla in och analysera data. Eftersom logiken bakom avskräckning uppmuntrar öppen signalering av tillgängliga relevanta förmågor, uteslöts således intervjuer som datainsamlingsmetod.

[56] Esaiasson et al. 2017. s. 211.
[57] Ibid. s. 211.
[58] Johannessen & Tufte 2003. s. 123.

Diskursanalys bedömdes vara en alternativ analysmetod, men eftersom syftet med undersökningen ej varit att kritiskt granska det språkliga innehållet i det empiriska underlaget uteslöts även detta tillvägagångsätt.[59]

Då vare sig försökspersoner, informanter eller respondenter nyttjades för att samla in data, bedömde jag att forskningsetiska överväganden utgjorde en mindre betydelse i denna uppsats. Kopplat till arbetets karaktär och utformning har jag istället beaktat forskaretiska överväganden. Genom att redogöra för hur de operationaliserade indikatorerna avses tolkas, möjliggörs en transparens i tolkningsprocessen. I analysen har dessutom citat hämtade ur källmaterialet nyttjats föra att underbygga centrala resonemang. Nyttjandet av citat möjliggör att läsaren oberoende kan bedöma huruvida de tolkningar som gjorts är i enlighet med arbetets teoretiska ramverk.[60]

3.4 Empiriskt material och källkritik

3.4.1 Empiriskt material

Med hänsyn till den logik som avskräckning vilar på har studien avhandlats på en abstraktionsnivå som tillgängliga offentliga policydokument, uttalanden, rapporter och doktriner medgivit. Därmed uteslöts sekretessbelagd information avseende aktuella svenska förmågor och hemliga kommunikéer mellan Sverige och andra aktörer av förklarliga skäl. Valet av empiriskt material har baserats på att handlingarna explicit avhandlar det svenska cyberförsvaret och vilka förmågor berörda myndigheter förfogar över. Därmed uteslöts även dokument som återger EU:s syn på cybersäkerhet och cyberförsvar. De valda dokumenten speglar således enbart aktörer inom det svenska cyberförsvaret, vilka har i uppgift att skydda landets cyberdomän mot antagonistiska statsaktörer.

För att få en samlad bild av det svenska cyberförsvaret och viljan att försvara cyberdomänen ingick följande dokument i undersökningen:

- *Försvarsministerns anförande på Cyberförsvarsdagen den 14:e februari 2018*[61]
  Försvarsminister Peter Hultqvist talar om cybermiljön sett ur ett försvars- och säkerhetspolitiskt perspektiv. Anförandet är intressant då det inbegriper den svenska försvarsministerns syn på cyberförsvar.

[59] Esaiasson et al. 2017. s. 214–215.
[60] Ibid. s. 25–26.
[61] Regeringskansliet. 2018. Försvarsministern talade på Cyberförsvarsdagen 2018.

– *Överbefälhavarens anförande på rikskonferensen Folk och Försvar*[62]
Överbefälhavare (ÖB) Micael Bydén talar om Sveriges Försvarsförmåga. Talet är intressant att analysera då ÖB även pratar om cyberförsvaret och hans syn på ämnet.

– *Nationell strategi för samhällets informations- och cybersäkerhet*[63]
Handlingen redovisar regeringens strategi för samhällets informations- och cybersäkerhet och syftar till att utgöra en plattform för Sveriges fortsatta utvecklingsarbete inom området. Dokumentet är relevant då det kan sägas återge regeringens samlade vilja att försvara cyberdomänen. Därtill återger handlingen vilka cyberförmågor som finns och vilka som bör utvecklas.

– *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022*[64]
Dokumentet återkopplar till nationella strategin för informations- och cybersäkerhet och utgör en samlad redovisning av vilka åtgärder berörda myndigheter på eget initiativ planerar att vidta inom ramen för sina befintliga ansvarsområden. Handlingen är intressant att analysera då den återger en samlad bild av de myndigheter som utgör den svenska cyberförsvaret och hur de avser tillgodose den politiska viljan.

– *Motståndskraft*[65]
Handlingen är ett inriktande dokument och redogör för totalförsvarets och det civila försvarets utformning för åren 2021–2025. Dokumentet bidrar till undersökningen med en övergripande bild av omvärldsläget, vilka investeringar som måste göras samt vilka cyberförmågor som bör prioriteras. Rapporten är relevant då den dels kan sägas återge försvarsberedningens samlade vilja att försvara cyberdomänen, dels vilka cyberförmågor som bör prioriteras. Dokumentet redogör även för vilka roller olika myndigheter inom det svenska cyberförsvaret har.

[62] Försvarsmakten. 2019. ÖB Micael Bydén Rikskonferens Folk och Försvar 2019. s. 4–5, 7.
[63] Skr. 2016/17:213. s. 1.
[64] MSB. 2019. Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022. s. 9.
[65] Ds 2017:66. s. 113–119.

– *Myndigheten för samhällsskydd och beredskap (MSB) Årsredovisning 2018*[66]
Handlingen är en redovisning över de åtgärder som MSB gjort under året 2018, kopplad till diverse målsättningar inom olika ansvarsområden. Dokumentet innehåller även slutsatser på genomförd verksamhet samt vidare förslag på vad som bör göras för att utveckla samhällets förmåga att förebygga och hantera olyckor och kriser. Rapporten är relevant för undersökningen då den återger vad som gjorts för att stärka det svenska cyberförsvarets resiliens.

– *Försvarets Radioanstalt (FRA) Årsrapport 2018*[67]
Rapporten redovisar FRA:s verksamhetsår och vilka åtgärder som myndigheten gjort för att stärka det svenska cyberförsvaret. Rapporten är intressant att analysera då den även återger FRA:s roll inom cyberförsvaret samt dess bidrag avseende cyberförmågor.

– *Militärstrategisk doktrin 2016*[68]
Handlingen är ett inriktande dokument för hur Försvarsmakten skall använda sina maktmedel för att uppnå de säkerhetspolitiska målsättningar som regering och riksdag beslutar. Skrivelsen är relevant då den ger uttryck för vilka förmågor den svenska försvarsmakten bidrar med till rikets cyberförsvar. Doktrinen kan även sägas återspegla den politiska viljan att försvara cyberdomänen.

– *Försvarsmaktens årsredovisning 2018*[69]
Handlingen är en redovisning över de åtgärder som Försvarsmakten gjort under året 2018 kopplat till myndighetens stipulerade målsättningar och visioner. Dokumentet innehåller även slutsatser på genomförd verksamhet, skarp liksom sådan som relaterar till övningar. Rapporten är relevant då den återger vad Försvarsmakten gjort för att stärka sin cyberförmåga och således i förlängningen Sveriges cyberförsvar.

[66] MSB. 2019. Årsredovisning 2018. s. 35–36, 39.
[67] FRA. 2019. Årsrapport 2018. s. 9, 13, 21.
[68] Försvarsmakten 2016. s. 30, 56.
[69] Försvarsmakten. 2019. Årsredovisning 2018. s. 10, 13, 60.

3.4.2 Källkritik

Materialet som utgjorde undersökningens empiriska underlag ansågs tillgodose samtliga källkritiska kriterier. Merparten av dokumenten är parlamentariskt framtagna och utgivna av svenska myndigheter. Handlingarna utgör det senaste beslutsunderlaget och har med sin karaktär genomgått granskning av sakkunnig personal. Dock förekommer undantag. Vissa dokument kan vara politiskt färgade, vilket innebär att kriteriet för *tendensfrihet* i vissa fall kan ifrågasättas. Detta togs i beaktande i studiens analys genom att avvikande politiska uppfattningar exkluderades. Motiveringen bakom exkluderingen är att dessa inte ger uttryck för en samlad politisk vilja, något som teorin framhåller och undersökningen avsåg att undersöka.

3.5 Operationalisering av teoretiskt ramverk

Framställningen av relevanta indikatorer har skett genom en syntes av Williams teoribildning och Lonsdales modell. Williams definition av de tre grundläggande faktorerna utgjorde ramverket, medan Lonsdales modell bistod med relevant innehåll kopplat till aktuell cyberkontext. I analysen har indikatorerna eftersökts med avsikten att bedöma huruvida Sveriges cyberförsvar uppfyller de kriterier som erfordras för att uppnå en lyckad avskräckning. Som nämnts är samspelet mellan de olika grundfaktorerna en central del av avskräckningens logik. De förmågor som en försvarande aktör förfogar över samt hur denne förmedlar sitt budskap skall vara trovärdiga tillsammans. Interaktionen mellan grundfaktorerna innebär att avsaknaden av en faktor får implikationer för en annan. Nedan beskrivs operationaliseringsprocessen av indikatorerna samt hur de valt att tolkas i samband med analysen av det empiriska underlaget. Beskrivningen syftar till att visa hur sammanfogningen av Williams teori och Lonsdales modell renderat i operationella indikatorer och bidrar därmed till att stärka begreppsvaliditeten och öka reliabiliteten.[70] Resonemangen som förs kring operationaliseringen av respektive indikator bidrar dessutom till arbetets intersubjektiva prövbarhet.[71]

3.5.1 Indikatorer

Följande indikatorer har identifierats som grundläggande för att ett cyberförsvar skall verka avskräckande:

[70] Ekengren & Hinnfors 2012. s. 75–78.
[71] Esaiasson et al. 2017. s. 25.

Kommunikation

En grundbult i att verka avskräckande är att den försvarande aktören måste kommunicera sina intentioner till en tänkt motståndare. Enligt Williams finns det två olika typer av signalering: direkt och indirekt. Båda har olika betydelse och är som nämnts beroende av varandra, där direkt signalering måste mötas av indirekt signalering som inger trovärdighet i den försvarande aktörens uttryckta vilja. Härmed skiljer denna undersökning på direkt och indirekt signalering, då den sistnämnda faller under grundfaktorn trovärdighet och har därmed berörts separat. Vidare har en *uttryckt vilja att investera* i cyberförsvaret i denna undersökning tolkats som en *vilja att försvara* cyberdomänen. Utifrån detta resonemang och det som presenteras i teorisammanfattningen har följande indikatorer för grundfaktorn kommunikation identifierats:

– *Direkt signalering i form av uttalanden som utrycker en vilja att försvara cyberdomänen*
  Indikatorn eftersöker om det i uttalanden gjorda av politiska eller militära aktörer uttrycks en vilja att försvara cyberdomänen.

– *Direkt signalering i form av officiella dokument som uttrycker en vilja att försvara cyberdomänen*
  Indikatorn eftersöker om det i officiella dokument uttrycks en vilja att försvara cyberdomänen.

Förmågor

Williams stipulerar att en försvarande aktör måste besitta den fysiska kapaciteten att skada sin antagonistiska motpart. I en cyberkontext manifesteras dessa förmågor enligt Lonsdale dels i en kombination av offensiva och defensiva cyberförmågor, dels i en kombination av offensiva förmågor från olika domäner. Lonsdale poängterar även att defensiva förmågor skall premieras framför offensiva. Utifrån detta resonemang har följande indikatorer för grundfaktorn förmågor identifierats:

– *En kombination av offensiva och defensiva cyberförmågor*
  Indikatorn eftersöker huruvida det i empirin uttrycks att det svenska cyberförsvaret förfogar över offensiva och defensiva cyberförmågor.

Begreppet *aktiv cyberförmåga* har i samband med undersökningen likställts med begreppet *offensiv cyberförmåga*. Kopplingen mellan begreppen är i linje med den svenska statsmaktens rådande uppfattning.[72]

- *Betoning på defensiva cyberförmågor*
  Indikatorn eftersöker huruvida den svenska statsmakten med aktuella myndigheter prioriterar en defensiv cyberförmåga framför en offensiv.

- *En kombination av offensiva förmågor från olika domäner*
  Indikatorn eftersöker huruvida offensiva förmågor från olika domäner nyttjas inom ramen för cyberförsvaret.

Trovärdighet

Trovärdighet har enligt Williams sin utgångspunkt i den försvarande aktörens uttryckta vilja och uppnås genom att den underbyggs med faktiska handlingar. Handlingarna tar sig uttryck genom olika former av indirekt signalering som omfattar allt från konkreta investeringar, till deltagande i övningar och skarpa insatser där förmågor nyttjas. I enlighet med Williams resonemang konstaterar Lonsdale att trovärdighet uppnås genom att den försvarande aktören projicerar sina befintliga förmågor i samband med exempelvis arrangerade cyberövningar. Vidare kan förekomsten eller upprättandet av cyberenheter likaså signalera en nations vilja att försvara sin cyberdomän mot antagonistiska cyberangrepp. Utifrån detta och tidigare resonemang har följande indikatorer för grundfaktorn trovärdighet identifierats:

- *Indirekt signalering i form av investeringar i cyberförsvar*
  Indikatorn eftersöker om den svenska statsmakten gör investeringar i sitt cyberförsvar genom statsfinansierad forskning, inköp av nya system eller utveckling av befintliga system.

- *Indirekt signalering i form av deltagande i cyberövningar och skarpa insatser*
  Indikatorn eftersöker om de myndigheter som bidrar till Sveriges cyberförsvar deltar i cyberövningar eller bedriver skarpa insatser inom cyberdomänen.

[72] Sveriges Riksdag. Försvarsutskottets betänkande 2017/18: FöU4. 2017. s. 32.

– *Indirekt signalering i form av upprättande av cyberenheter*
  Indikatorn eftersöker om det i dagsläget finns dedikerade cyberenheter eller om sådana håller på att upprättas.

3.5.2 Analysverktyg

Nedan presenteras arbetets analysverktyg, tolkningsschema samt de mätvärden som har nyttjats i samband med undersökningen. Analysverktyget innehåller de grundfaktorer som tillsammans konstituerar lyckad avskräckning med tillhörande indikatorer.

Grundfaktorer	**Indikatorer**
Kommunikation	– *Direkt signalering i form av uttalanden som utrycker en vilja att försvara cyberdomänen*
	– *Direkt signalering i form av officiella dokument som uttrycker en vilja att försvara cyberdomänen*
Förmågor	– *En kombination av offensiva och defensiva cyberförmågor*
	– *Betoning på defensiva cyberförmågor*
	– *En kombination av offensiva förmågor från olika domäner*
Trovärdighet	– *Indirekt signalering i form av investeringar i cyberförsvar*
	– *Indirekt signalering i form av deltagande i cyberövningar och skarpa insatser*
	– *Indirekt signalering i form av upprättande av cyberenheter*

Figur 1-Analysverktyg

Mätvärden	**Tolkningar**
Ja	Indikatorn återfanns i texten
Nej	Indikatorn återfanns inte i texten
Indirekt	Indikatorn återfanns efter tolkning av texten

Figur 2-Mätvärden med tolkningsschema

4. Analys

4.1 Grundfaktor kommunikation

Indikator: Direkt signalering i form av uttalanden som utrycker en vilja att försvara cyberdomänen

Viljan att försvara cyberdomänen går att uttolka i uttalanden gjorda av politiska liksom militära aktörer. I ett anförande på Cyberförsvarsdagen den 14 februari 2018 sade försvarsminister Peter Hultqvist:

> […] Den tilltagande antagonistiska dimensionen i cyberrymden gör det nödvändigt att utveckla och stärka cyberförsvarsresurser. Vi kan se att ett flertal länder i världen har gjort just det. Det försvarspolitiska inriktningsbeslutet från 2015 innehöll ett tydligt och nytt steg i arbetet med svenskt cyberförsvar.[73]

Genom att hänvisa till det stagnerade omvärldsläget och betona vikten av att utveckla och stärka rikets cyberförsvarsresurser signalerade försvarsministern att den svenska cyberdomänen måste försvaras. Liknande budskap går även att uttolka i ett framförande gjort av ÖB Micael Bydén i samband med rikskonferensen Folk och Försvar 2019:

> Vi gör mycket. Men det krävs mer. Därför har jag beslutat att i det korta perspektivet gå vidare med fyra initiativ […] För det andra: Förmågan till cyberförsvar måste stärkas. Försvarsmakten kommer därför att senast år 2020 genomföra en pilotutbildning av upp till 30 ”cybersoldater” som ska stärka både vår egen och andra myndigheters cyberkompetens. Våra system måste skyddas mot en kvalificerad motståndare som söker påverka svensk militär verksamhet och andra samhällsfunktioner. Den insikten delar vi med andra myndigheter. Därför kommer Försvarsmakten också att fördjupa cybersamarbetet främst med FRA, Säkerhetspolisen och MSB.[74]

ÖB:s redogörelse av varför och hur cyberförsvaret skall stärkas kan, efter en tolkning av meningsinnehållet, sägas påvisa förekomsten av en vilja att försvara cyberdomänen. Utöver att åskådliggöra ÖB:s och försvarsministerns ståndpunkt och ambitioner, visar citaten även på en koherent samsyn inom den svenska statsmakten beträffande cyberförsvaret.

[73] Regeringskansliet. 2018. Försvarsministern talade på Cyberförsvarsdagen 2018.
[74] Försvarsmakten. 2019. ÖB Micael Bydén Rikskonferens Folk och Försvar 2019. s. 4–5.

Indikator: Direkt signalering i form av officiella dokument som uttrycker en vilja att försvara cyberdomänen

I *Nationell strategi för samhällets informations- och cybersäkerhet* ger regeringen uttryck för att det finns ett behov att utveckla samhällets informations- och cybersäkerhet. Att regeringen ger uttryck för att ett faktiskt behov existerar kan indirekt tolkas som att det finns en vilja från statsmaktens sida att försvara cyberdomänen. I samma stycke uttrycks en mer konkret faktiskt vilja från den svenska statsmakten:

> […] Regeringen vill genom strategin även stödja de insatser och det engagemang som redan finns i samhället för att stärka informations- och cybersäkerheten. […] [75]

Genom att vilja stödja redan pågående insatser med ändamålet att stärka informations- och cybersäkerheten, kan det tolkas som att regeringen signalerar en vilja att försvara cyberdomänen. Vidare i dokumentet åskådliggörs hur digitaliseringen av samhället medför möjligheter och risker. Faktumet avseende digitaliseringsprocessen avslutas med ett konstaterande att:

> […] Hur vi hanterar riskerna som följer av digitaliseringen har stor betydelse för vår förmåga att upprätthålla och stärka både vårt välstånd och vår säkerhet. […][76]

Utifrån citatet där riskerna med digitaliseringen framhålls går det att tolka som att det från regeringens sida existerar en vilja att försvara den svenska cyberdomänen. I handlingen framgår det även att:

> […] De regelverksförändringar som nu genomförs både nationellt och inom EU är ett sätt att höja säkerhetskraven samt stärka formerna och strukturerna för det samlade informations- och cybersäkerhetsarbetet. […][77]

Den uttryckta viljan återges ännu tydligare i och med att det i skrivelsen stipuleras hur regeringen, i egenskap av styrande organ, skall verka för att hantera riskerna.[78] En uttryckta vilja återfinns även i *MSD 2016* där det konstateras att:

> I cyberrymden ska Försvarsmakten aktivt skydda infrastruktur och skyddsvärd information. Det ska ske genom att verkan i cyberrymden möjliggörs enskilt eller tillsammans med andra myndigheter, stater och organisationer.[79]

[75] Skr. 2016/17:213. s. 1.
[76] Ibid. s. 3.
[77] Ibid. s. 3.
[78] Ibid. s. 21.
[79] Försvarsmakten 2016. s. 56.

Likaså återfinns försvarsberedningens ståndpunkt avseende cyberdomänen vid analys av inriktningsdokument *Motståndskraft*. I avsnittet *10.2 Utvecklingen av cyberförsvaret* uttrycks exempelvis:

> Försvarsberedningen konstaterar att ett kontinuerligt och systematiskt arbete med informations- och cybersäkerhet spelar en avgörande roll för en trovärdig totalförsvarsförmåga. För att öka förmågan inom totalförsvaret är det med andra ord centralt att bygga vidare på arbetet inom krisberedskapen och de strukturer för samhällets informations- och cybersäkerhet, som där har etablerats. […][80]

Påståendet kan tolkas som en uttryckt vilja att försvara cyberdomänen då försvarsberedning tydligt poängterar den centrala roll fortsatt arbete inom informations- och cybersäkerhet innehar kopplat till totalförsvarets förmåga. Viljan kan även uttolkas när försvarsberedningen i dokumentet fastslår att:

> […] För att möta den digitala utvecklingen på ett säkert sätt och öka möjligheterna att effektivt försvara t.ex. kritisk infrastruktur från störningar och yttre påverkan i konfliktsituationer behöver det strategiska och långsiktigt finansierade forsknings- och utvecklingsarbetet på informations- och cybersäkerhetsområdet stärkas. […][81]

Genom att uttryckligen presentera förslag på hur försvaret av kritisk infrastruktur skall effektiviseras, kan det efter tolkning av meningshållet sägas att försvarsberedningen ger uttryck för en vilja att försvara cyberdomänen.

Den uttryckta viljan som återfinns i berörda uttalanden och offentliga handlingar befästs i och med upprättandet av en samlad handlingsplan för de myndigheter som tillsammans konstituerar det svenska cyberförsvaret.[82] Handlingsplanen kan utifrån Williams resonemang betraktas som ett sätt att förmedla, eller t.o.m. förstärka ett budskap.

[80] Ds 2017:66. s. 116.
[81] Ibid. s. 117.
[82] MSB. 2019. Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022. s. 9.

4.2 Grundfaktor förmågor

Indikator: En kombination av offensiva och defensiva cyberförmågor

I *Nationell strategi för samhällets informations- och cybersäkerhet* går att återfinna vilka förmågor det svenska cyberförsvaret förfogar över. Där står exempelvis att FRA skall tillhandahålla andra myndigheter med ett tekniskt detekterings- och varningssystem (TDV). Systemet finns i dagsläget utplacerat hos svenska myndigheter och statliga bolag i syfte att varna för pågående angrepp.[83] Utvecklingen av FRA:s varningssystem sker fortlöpande och skall i framtiden även kunna hindra pågående angrepp.[84] Sensorn kan enligt Lonsdales modell kategoriseras som en defensiv cyberförmåga.

Avseende offensiva cyberförmågor framgår det i flera dokument att det svenska cyberförsvaret dels har ambitioner att besitta sådan kapacitet, dels redan gör det. I *Nationell strategi för samhällets informations- och cybersäkerhet* fastställs exempelvis:

> […] Ett nationellt cyberförsvar förutsätter en […] robust förmåga att kunna genomföra aktiva operationer i cybermiljön.[85]

Att bedriva aktiva operationer inom cyberdomänen förutsätter i sin tur att en aktör förfogar över en offensiv cyberförmåga. Efter tolkning av innehållet i den *Samlade informations- och cybersäkerhetshandlingsplanen 2019–2022*, kan det uppfattas som att Sverige redan förfogar över sådan kapacitet. I handlingsplanen står det skrivet att:

> Försvarsmakten med stöd av FRA förstärker förmågan att genomföra defensiva och offensiva operationer mot en kvalificerad motståndare i cybermiljön. […][86]

Försvarsmakten tillsammans med FRA skall alltså *förstärka* förmågan att bedriva defensiva och offensiva operationer. Utifrån citatet kan det tolkas som att specifika aktörer inom det svenska cyberförsvaret redan i dagsläget besitter en viss offensiv förmåga.

Sammantaget kan det utifrån det ovannämnda konstateras att det svenska cyberförsvaret besitter både defensiva och offensiva cyberförmågor. Andra bevis på cyberförsvarets förmågor återfinns även i *MSD 2016*.

[83] Skr. 2016/17:213. s. 20.
[84] FRA. 2019. Årsrapport 2018. s. 21.
[85] Skr. 2016/17:213. s. 21.
[86] MSB. 2019. Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022. s. 29.

I en redogörelse av cyberdomänens snabba utveckling och dess strategiska innebörd åskådliggör Försvarsmakten sin roll inom cyberförsvaret. Myndighetens resurser skall enligt skrivelsen:

> […] stödja defensiva och offensiva operationer i syfte att stärka skyddet av Sverige i cyberrymden.[87]

Liksom innehållet i tidigare dokument kan det utifrån *MSD 2016* tolkas som att Försvarsmakten, och därmed det svenska cyberförsvaret, besitter både defensiva och offensiva cyberförmågor.

Indikator: Betoning på defensiva cyberförmågor

Att den svenska statsmakten med berörda myndigheter i dagsläget prioriterar en defensiv cyberförmåga går att uttolka efter analys av texternas meningsinnehåll. I *Nationell strategi för samhällets informations- och cybersäkerhet* uttrycks exempelvis att skräddarsydda säkerhetsnät kan vara en metod för att *ytterligare* stärka skyddet kring skyddsvärd verksamhet från antagonistiska cyberangrepp.[88] Trots att det inte framgår huruvida ett sådant system existerar i dagsläget, visar innehållet i texten på en prioritering av defensiva förmågor. Liknande prioritering kan även att uttolkas i ett senare stycke där det fastställs att:

> Grunden i en robust cyberförsvarsförmåga är att säkerställa funktionalitet i samhällsviktiga funktioner och skydda de mest skyddsvärda verksamheterna, inklusive sådana system som är vitala för totalförsvaret, mot antagonistiska angrepp från kvalificerade statliga eller statsstödda aktörer samt andra aktörer med liknande förmåga.[89]

Citatet belyser att grunden i ett robust cyberförsvar bl.a. är att *skydda* skyddsvärd verksamhet och vitala system, vilket kan tolkas som en betoning på en defensiv cyberförmåga. Ett framhävande av defensiva cyberförmågor kan även uttolkas i försvarsberednings inriktningsdokument *Motståndskraft*. I kapitlet som avhandlar informations- och cybersäkerhet redogör försvarsberedningen för vilka risker digitaliseringen medför. Utifrån riskerna stipuleras vilka åtgärder som bör vidtas och hur utvecklingen av totalförsvarets cyberförsvar bör se ut för att möta den växande problematiken kring antagonistiska cyberangrepp. Fokus ligger främst på hur samhället skall *skyddas* mot cyberangrepp och hur nya tekniska lösningar skall öka *redundansen* i vitala IT-system och i förlängningen samhällsviktiga anläggningar.[90]

[87] Försvarsmakten 2016. s. 30.
[88] Skr. 2016/17:213. s. 20.
[89] Ibid. s. 20.
[90] Ds 2017:66. s. 113–120.

Förmåga till redundans kategoriseras enligt Lonsdale som en passiv defensiv förmåga. Vid analys av FRA:s årsrapport för 2018 framgår även där en betoning på defensiv cyberförmåga. I rapporten skriver FRA att:

> […] FRA har även uppgiften att vara statens resurs för teknisk informationssäkerhet. Det innebär att vi lämnar stöd till andra myndigheter och statliga bolag för att stärka deras förmåga att stå emot IT-angrepp.[91]

Indikatorn som eftersöker betoning på defensiv cyberförmåga kan uttolkas i sista delen av citatet där det framgår att FRA skall lämna stöd åt andra myndigheter i syfte att stärka deras förmåga att *stå emot* IT-angrepp.

Indikator: En kombination av offensiva förmågor från olika domäner

Inga indikationer återfinns som påvisar att offensiva förmågor från olika domäner nyttjas inom ramen för cybersäkerhet.

4.3 Grundfaktor trovärdighet

Indikator: Indirekt signalering i form av investeringar i cyberförsvar

Indikatorn som påvisar signalering i form av investeringar i cyberförsvaret förekommer i flera dokument. I *Nationell strategi för samhällets informations- och cybersäkerhet* framgår det exempelvis att:

> Utvecklingen inom it- och telekomområdet är ett naturligt steg i den alltmer globaliserade infrastruktur som byggs upp. Detta medför många möjligheter, men även att ökad forskning om digital säkerhet krävs för att kunna säkerställa att it-området förblir öppet, fritt och säkert. I dag bedrivs forskning inom informations- och cybersäkerhetsområdet i varierande grad på flera svenska lärosäten. Tillämpad forskning inom informations- och cybersäkerhet sker bl.a. vid Totalförsvarets forskningsinstitut, Försvarshögskolan och Swedish Institute of Computer Sciences (RISE SICS).[92]

Då forskningsverksamheten är statligt finansierad[93] kan det tolkas som en indikering på att det i dagsläget sker investeringar som ämnar stärka det svenska cyberförsvaret. Ytterligare bevis på att den svenska statsmakten satsar på sitt cyberförsvar påträffas i *MSB:s årsredovisning 2018*. I sin återrapportering för genomförd verksamhet skriver MSB:

[91] FRA. 2019. Årsrapport 2018. s. 9.
[92] Skr. 2016/17:213. s. 26.
[93] FOI. Om FOI.

> MSB:s samlade kostnader för att hantera information säkert har ökat med 14 mnkr jämfört med 2017. MSB har under 2018 förstärkt sin organisation inom informations- och cybersäkerhet med fler personella resurser vilket möjliggjort en ökad satsning inom området. De utökade resurserna har medfört att fler kunskapshöjande och samordnande åtgärder kunnat genomföras och förklarar ökningen för prestationstypen beslutsunderlag och kunskapsförmedling. […][94]

Det framgår ur citatet att MSB under 2018 har förstärkt sin organisation inom informations- och cybersäkerhet. Den ökade resurstilldelningen kan tolkas som ett bevis på att det de facto skett investeringar i cyberförsvaret.

Vidare, beträffande investeringar, framgår det i Försvarsmaktens årsredovisning att myndigheten erhållit ett tillskott på 103 miljoner kronor i syfte att förstärka cyberförsvarsförmågan. Det framkommer även att verksamhet som berör forsknings- och teknikutveckling utökats med 55 miljoner kronor. Delar av det ökade forsnings- och teknikutvecklingsanslaget har nyttjats för att utöka kunskapen avseende operationer inom cyberdomänen.[95]

Indikator: Indirekt signalering i form av deltagande i cyberövningar och skarpa insatser

Den indirekta signaleringen som berör övningsverksamhet påträffas i flera av de berörda dokumenten. I *Nationell strategi för samhällets informations- och cybersäkerhet* framgår exempelvis att FOI i dagsläget bl.a. bistår med myndighetsspecifika tekniska övningar via sin plattform CRATE (*Cyber Range and training environment*).[96] Plattformen omfattar drygt 800 servrar som tillsammans skapar ett simulerat internet där berörda aktörer, däribland Försvarsmakten och MSB, kan öva på att hantera olika typer av cyberangrepp.[97]

Träningsplattformen CRATE omnämns även i *MSB:s årsredovisning 2018*. I sin rapport skriver myndigheten att anläggningen har nyttjats flera gånger dels i samband med cyberövningar, dels för att utbilda tekniker i samhällsviktig infrastruktur. Vidare redovisar MSB i samma dokument att man tillsammans med sina nordiska samarbetspartner stärkt den gemensamma förmågan inom informations- och cybersäkerhet genom b.la. samfällda övningar och utbildningar. Utöver övningar har MSB även deltagit i diverse möten och konferenser inom ramen för sitt internationella samarbete.

[94] MSB. 2019. Årsredovisning 2018. s. 39.
[95] Försvarsmakten. 2019. Årsredovisning 2018. s. 13, 60.
[96] Skr. 2016/17:213. s. 28.
[97] FOI. CRATE - Cyber Range And Training Environment.

Myndigheten har medverkat på flera möten i EU:s strategiska NIS-samarbetsgrupp samt unionens operativa CSIRT-nätverk (*Computer Security Incident Response Team*).[98] Trots att verksamheten inte inbegriper övningar, signalerar MSB till en eventuell motståndare ett visst engagemang rörande cyberdomänen. Enligt Williams och Lonsdales resonemang kan deltagandet tolkas som en handling som underbygger den politiska viljan, vilket i sin tur bidrar till cyberförsvarets trovärdighet.

Cyberrelaterade övningar har även bedrivits av Försvarsmakten. I sin årsredovisning för 2018 framför myndigheten att man tillsammans med nationella och internationella samarbetspartner deltagit i övningarna LOCK SHIELD 18 samt SAFE CYBER 18. LOCK SHIELD 18 klassas som världens största cyberförsvarsövning och inbegriper både tekniska och strategiska aspekter. Övningen innefattar ett scenario där militäranläggningar och annan samhällskritisk infrastruktur utsätts för omfattande cyberangrepp. Samtidigt som tekniker skall försöka hålla igång de utsatta systemen, övas det på annat håll bearbetning av händelseförlopp på en högre beslutsnivå.[99] SAFE CYBER 18 kan sägas utgöras ett liknade koncept men på en nationell basis och omfattar således samtliga myndigheter som konstituerar det svenska cyberförsvaret.[100]

Utöver deltagande i relevant övningsverksamhet, framgår det i Försvarsmaktens årsredovisning att myndigheten kontinuerligt övervakat och avvisat flertalet intrångsförsök inom sina ledningsstödsystem.[101] Detta talar för att Försvarsmakten, i egenskap av central aktör inom det svenska cyberförsvaret, i dagsläget bedriver skarpa insatser inom cyberdomänen.

Vidare, avseende skarp verksamhet, har FRA enligt sin rapport bedrivit underrättelse i syfte att kartlägga tillvägagångsätt hos kvalificerade angripare.[102] Hur FRA har bedrivit sin underrättelseverksamhet framgår inte ur rapporten. Dock kan det utifrån Lonsdales resonemang konstateras att underrättelseverksamhet inom cyberdomänen kategoriseras som en offensiv förmåga. Om detta är fallet är det ovannämnda en indikation på att myndigheter inom det svenska cyberförsvaret bedriver skarpa insatser av både defensiv och offensiv karaktär.

[98] MSB. 2019. Årsredovisning 2018. s. 35–36.
[99] Försvarsmakten. Världens största cyberförsvarsövning. Högkvarteret. 23 april 2018.
[100] MSB. 2019. Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022. s. 33.
[101] Försvarsmakten. 2019. Årsredovisning 2018. s. 10.
[102] FRA. 2019. Årsrapport 2018. s. 13.

Indikator: Indirekt signalering i form av upprättande av cyberenheter

Det framgår i flera dokument att det svenska cyberförsvaret utgörs av en mosaik av flera olika myndigheter, alla med olika typer av ansvarsområden och uppgifter. MSB erbjuder exempelvis stöd vid hantering av incidenter som berör informationssäkerhet och digitala tjänster genom CERT-SE (*Computer Emergency Response Team*).[103] Enheten är Sveriges svar på de krav som ställs i det s.k. NIS-direktivet vad beträffar hantering och tillsyn av informations och cyberrelaterade frågor inom den Europeiska unionen.[104] FRA i sin tur har som huvuduppgift att dels utföra underrättelseverksamhet mot utländska cyberhot, dels understödja övriga myndigheter i deras cybersäkerhetsarbete.[105] Det som dock är relevant, kopplat till denna undersökning, är huruvida det inom det svenska cyberförsvaret existerar en enhet eller myndighet som har förmågan att koordinera cyberoperationer. I *Nationell strategi för samhällets informations- och cybersäkerhet* framgår det att:

> […] Försvarsmakten är den myndighet som ska verka inom alla delar av dator- och nätverksoperationer samt dimensionerat mot de högre konfliktnivåerna. Stöd från övriga berörda myndigheter är nödvändigt. […][106]

Utifrån citatet kan det tolkas som att Försvarsmakten är den myndighet som skall kunna koordinera alla kategorier av operationer inom cyberdomänen. Samtidigt uttrycks det att stöd från övriga myndigheter är en nödvändighet. Stödet återfinns i samverkansforumet *Nationell samverkan till skydd mot allvarliga it-hot* (NSIT). Forumet fungerar som en plattform där Säkerhetspolisen, FRA och Försvarsmakten tillsammans analyserar och bedömer hot och sårbarheter vad beträffar kvalificerade IT-angrepp som riktas mot rikets intressen.[107]

Ytterligare indikationer på att Försvarsmakten skall stå för koordinering av det svenska cyberförsvarets operationer återfinns i ÖB:s tal under Rikskonferensen Folk och Försvar 2019. Enligt ÖB skall Försvarsmakten senast 2020 genomföra en pilotutbildning av cybersoldater i syfte att stärka egen och andra myndigheters cyberkompentens. Det framgår även i dokumentet *Motståndskraft* vilken myndighet som bär det yttersta ansvaret beträffande operationer i cyberdomänen. I handlingen skriver försvarsberedningen att:

[103] Skr. 2016/17:213. s. 20.
[104] CERT-SE. Om CERT-SE. 22 januari 2019.
[105] FRA. 2019. Årsrapport 2018. s. 21.
[106] Skr. 2016/17:213. s. 21.
[107] Ibid. s. 12.

> […] Försvarsmakten ska bidra till totalförsvarets samlade cyberförsvar. Förutom att kunna skydda sina egna system, innebär det att Försvarsmakten ska ansvara för totalförsvarets aktiva cyberförsvarsförmåga. Detta måste ske med stöd av och i dialog med andra myndigheter, särskilt FRA och de övriga försvarsunderrättelsemyndigheterna samt Säkerhetspolisen. […][108]

Faktumet att den svenska statsmakten stipulerar att Försvarsmakten skall tillhandahålla en aktiv cyberförmåga påvisar att det finns en dedikerad myndighet som ansvarar för koordinering av cyberförsvarets operationer. Att Försvarsmakten skall utbilda cybersoldater stärker antagandet.

4.4 Presentation och sammanfattning av resultat

Nedan följer en presentation och sammanfattning av undersökningens resultat.

4.4.1 Presentation

Indikatorer	Mätvärden
– *Direkt signalering i form av uttalanden som utrycker en vilja att försvara cyberdomänen*	INDIREKT
– *Direkt signalering i form av officiella dokument som uttrycker en vilja att försvara cyberdomänen*	INDIREKT

Figur 3-Presentation av resultat för grundfaktorn kommunikation

Indikatorer	Mätvärden
– *En kombination av offensiva och defensiva cyberförmågor*	JA
– *Betoning på defensiva cyberförmågor*	INDIREKT
– *En kombination av offensiva förmågor från olika domäner*	NEJ

Figur 4-Presentation av resultat för grundfaktorn förmågor

Indikatorer	Mätvärden
– *Indirekt signalering i form av investeringar i cyberförsvar*	JA
– *Indirekt signalering i form av deltagande i cyberövningar och skarpa insatser*	JA
– *Indirekt signalering i form av upprättande av cyberenheter*	JA

Figur 5-Presentation av resultat för grundfaktorn trovärdighet

[108] Ds 2017:66. s. 120.

4.4.2 Sammanfattning

Sammanfattningsvis kan det konstateras att alla indikatorer utom en återfinns i samband med analysen. Inom grundfaktorn kommunikation påträffas båda indikatorerna efter tolkning av texternas meningsinnehåll. Den uttryckta viljan att försvara cyberdomänen går att uttolka i dels anföranden gjorda av centrala makthavare, dels i offentliga dokument.

Vidare påvisar undersökningen att det svenska cyberförsvaret förfogar över en offensiv, liksom defensiv, cyberförmåga. Den visar även efter tolkning av texternas meningsinnehåll en viss prioritering av defensiv kapacitet framför offensiv. Huruvida den svenska statsmakten kombinerar offensiva förmågor från olika domäner framgår emellertid inte.

Vad beträffar indikatorerna för grundfaktorn trovärdighet återfinns prov på att den svenska statsmakten de facto investerar i sitt cyberförsvar, både direkt och indirekt. Likaså återfinns tydliga indikationer på att berörda myndigheter deltar i cyberövningar och bedriver skarpa insatser inom cyberdomänen. Undersökningen kan även påvisa att Försvarsmakten axlar rollen som ansvarig myndighet avseende koordinering av cyberoperationer.

5. Avslutning

5.1 Svar på frågeställning

Hur kan det svenska cyberförsvaret beskrivas utifrån ett avskräckningsperspektiv?

Inom grundfaktorn kommunikation visar analysen att det från svenska makthavare uttrycks en vilja att försvara cyberdomänen. Den visar även att det inte finns någon diskrepans i vad som uttrycks mellan politiska och militära makthavare. Viljan att försvara cyberdomänen stärks dessutom i och med förekomsten av faktiska handlingsplaner och distinkta målsättningar. Denna typ av tydliga signalering till omvärlden är enligt Williams och Lonsdales resonemang ett robust första steg i att verka avskräckande.

Resultatet av analysen visar också att det svenska cyberförsvaret innehar det Lonsdale beskriver som offensiva och defensiva cyberförmågor. Därtill framgår det att defensiva förmågor premieras framför offensiva, vilket Lonsdale menar är en förutsättning för att verka avskräckande inom cyberdomänen. Den uttryckta viljan undergrävs dock eftersom det empiriska underlaget inte ger uttryck för huruvida antagonistiska cyberangrepp möts med en kombination av olika typer av offensiva förmågor. Avsaknaden av indikatorn kan tyckas vara anmärkningsvärd då empirin utgörs av dokument som manifesterar strategiska och politiska ambitioner. Inte heller har uttalanden från politiska eller militära makthavare indikerat förekomsten av ett koncept där offensiva förmågor från olika domäner nyttjas inom ramen för cybersäkerhet.

De förmågor som en försvarande aktör innehar måste enligt Williams resonemang åsamka den antagonistiska motparten oacceptabla kostnader och få denne att omvärdera sina avsikter. Att enbart nyttja offensiva cyberförmågor som medel för vedergällning skulle enligt det argument som Lonsdale framför inte vara tillräckligt. Om en försvarande aktör saknar en relevant förmåga, kan denne inte heller genom indirekt signalering visa för en tänkt motståndare att man kan och vill nyttja en viss kapacitet. Ur ett teoretiskt perspektiv blir effekten av en utebliven kombination av offensiva förmågor således att det svenska cyberförsvarets avskräckningsförmåga minskar i trovärdighet. Enligt Williams är det just grundfaktorn trovärdighet som är vital för att avskräckningen skall lyckas.

Bortsett från faktumet att illasinnade cyberangrepp inte möts med exempelvis ekonomiska sanktioner, visar undersökningen att Sverige utifrån de förmågor landet besitter skapar trovärdighet i sin uttryckta vilja att försvara cyberdomänen. Ambitionsyttringarna som texterna och uttalandena uttrycker stärks i sin trovärdighet tack vare ekonomiska investeringar ämnade att utveckla befintliga cyberförmågor.

Genom deltagande i återkommande cyberövningar signalerar Sverige dessutom att man vill och kan försvara sina intressen inom cyberdomänen, vilket ytterligare tillför till trovärdigheten.

Avslutningsvis kan det svenska cyberförsvaret ur ett avskräckningsperspektiv i vissa hänseenden beskrivas som ofullkomligt. För att en försvarande aktör skall upplevas som avskräckande måste denne enligt Williams teoribildning uppfylla vissa grundläggande förutsättningar. Därtill måste förutsättningarna samspela med varandra för att avskräckningen skall uppnå önskvärd strategisk effekt och få motparten att överväga sina avsikter. Å ena sidan går det att argumentera för att den svenska statsledningen, med berörda myndigheter, agerar på sin vilja genom att projicera befintliga förmågor som inger trovärdighet. Å andra sidan saknas kombinationen av offensiva förmågor från olika domäner, vilket får konsekvenser i den centrala grundfaktorn trovärdighet.

Syftet med undersökningen, att utifrån vald teoretisk ansats undersöka det svenska cyberförsvarets förutsättningar för att verka avskräckande, är härmed uppfyllt. Huruvida det svenska cyberförsvaret under faktiska omständigheter avskräcker antagonistiska cyberattacker riktade mot samhällsviktig infrastruktur återstår att se.

5.2 Avslutande diskussion

Trots ett fungerande samspel mellan avskräckningens tre grundfaktorer pekar resultatet i undersökningen på att det svenska cyberförsvaret har en begränsad avskräckningsförmåga. Enligt teorin är Sveriges cyberförsvar inte anpassat för att avskräcka en potentiell angripare inom cyberdomänen och möter således inte EU:s vilja att verka avskräckande. Resultatet av undersökningen och de slutsatser som dragits grundar sig enbart på källor som återger ett svenskt perspektiv på cybersäkerhet. Å ena sidan går det att argumentera för att de avgränsningar som gjorts kopplat till arbetets empiriska material kan ha inverkat på analysens resultat och i förlängningen slutsatsen. Vissa indikatorer kanske hade framkommit tydligare om dokument utfärdade av EU hade inkluderats i undersökningen. Exkluderingen av dokument som berör EU:s syn på cybersäkerhet kan vara en möjlig förklaring till att undersökningen inte kunde utröna huruvida det existerar ett sanktionssystem inom ramen för svenskt cyberförsvar. Å andra sidan var arbetets syfte att uteslutande undersöka det svenska cyberförsvaret. Ur den synvinkeln genererade det valda empiriska underlaget användbara data som kunde kopplas till arbetets teoretiska ramverk och de operationaliserade indikatorerna, vilket i sin tur gav en bild av det svenska cyberförsvarets avskräckningsförmåga.

Som en följd av att cyberdomänen har kommit att betraktas som en av flera konfliktarenor, kommer cyberkrigföring i allt större utsträckning utgöra en del i hur länder tillgodoser sina politiska målsättningar. Utvecklingen innebär att officerare och försvarsmakter måste anpassa sitt tankesätt beträffande krigföring och hur tillgängliga resurser på ett effektivt sätt skall nyttjas. Genom att betrakta cyberdomänen och försvaret av denna ur ett avskräckningsperspektiv skapas ett nytt synsätt i hur ett land såsom Sverige kan tänkas tackla digitaliseringens avigsidor. Mot bakgrund av undersökningens resultat torde det verkansfulla alternativet vara att utveckla redan befintligt samarbete mellan olika myndigheter inom ramen för totalförsvaret. Kontentan är att politiska och militära makthavare bör tänka utanför ramarna och inte betrakta cyberkrigföring som ett isolerat konfliktområde. Istället för att fokusera på olika typer av cyberförmågor, förordar författaren ett flexibelt och mångsidigt strategiskt tillvägagångsätt med inslag av varierande offensiva förmågor. En högre grad av integrering mellan militära och politiska förmågor skulle i teorin befästa det svenska cyberförsvarets trovärdighet och därmed öka effektiviteten i dess avskräckningsförmåga. Detta kan med fördel göras genom att det i offentliga handlingar signaleras en vilja att besvara cyberattacker med exempelvis ekonomiska sanktioner eller militära aktioner.

Undersökningen återkopplar till det aktuella forskningsfältet genom att problematisera det svenska cyberförsvaret och ge en helhetsbild avseende dess avskräckningsförmåga. Även om det erhållna resultatet svårligen kan överföras till andra nationer, bidrar studien med en relevant beskrivning av ett EU-lands cyberförsvar sett ur ett avskräckningsperspektiv. Därutöver tillför arbetet kunskap till det berörda forskningsfältet avseende småstaters avskräckningsförmåga inom cyberdomänen.

Trots att arbetets teoretiska ramverk gick att applicera i en cyberkontext, förelåg viss problematik med operationaliseringen av indikatorer. Samspelet och analogin mellan avskräckningens tre byggstenar gjorde att det inledningsvis var svårt att urskilja på grundfaktorerna kommunikation och trovärdighet. Enligt Williams resonemang gör båda anspråk på att vara någon typ av signalering, där den ena enligt teorin anses vara mer relevant än den andra. I samband med operationaliseringsprocessen fanns funderingar på att exkludera grundfaktorn kommunikation och inkorporera all typ av signalering inom grundfaktorn trovärdighet. Idén visade sig emellertid ha flera begränsningar, främst kopplat till att resonemanget som fördes vilade på en ostadig grund och därav upplevdes som tvivelaktig. Att med ologiska argument exkludera en grundfaktor skulle vara minst sagt vanskligt, eftersom den röda tråden och koppling mellan teoretiskt ramverk och indikatorer skulle bli uppenbart lidande.

Förutom en osund logik hade begreppsvaliditeten sjunkit, varvid analysen av det empiriska underlaget renderat i felaktiga resultat. För att behålla samtliga grundfaktorer valdes istället alternativet att dela på direkt signalering och indirekt signalering. Den direkta varianten av signalering innefattade en uttryckt vilja och placerades inom grundfaktorn kommunikation. Den andra typen av signalering inbegrep handlingar som gick att koppla till den uttryckta viljan och placerades således inom grundfaktorn trovärdighet. Tillvägagångsättet finner stöd i det resonemang som Williams och Lonsdale för avseende logiken bakom avskräckning och visade sig vara adekvat för undersökningens ändamål.

5.3 Förslag på fortsatt forskning

Resultatet av undersökningen visar att det inom ramen för svenskt cyberförsvar inte förekommer en kombination av offensiva förmågor från olika domäner för att stävja cyberangrepp. Eftersom arbetet enbart omfattar handlingar utgivna av svenska myndigheter, vore det intressant att i en liknade studie också inkludera dokument utfärdade av styrande organ inom EU. Ändamålet med en sådan undersökning vore att placera Sverige i en vidare kontext och utifrån ett utökat empiriskt underlag utforska huruvida det svenska cyberförsvarets avskräckningsförmåga får ökad trovärdighet.

I analysen framgår det bl.a. att svenska myndigheter bedriver omfattande och regelbundna samarbeten med olika samarbetspartner i syfte att stärka den egna cybersäkerheten. Ytterligare förslag på framtida forskning skulle sålunda vara att studera hur ett eventuellt NATO-medlemskap påverkar det svenska cyberförsvaret sett ur ett avskräckningsperspektiv. En sådan studie skulle kunna ha sin utgångspunkt i rådande politiska debatt kring huruvida ett svenskt medlemskap i NATO är till gagn för landet eller inte. Ett möjligt tillvägagångsätt vore exempelvis att genomföra undersökningen i form av en jämförande fallstudie. Sveriges cyberförsvar skulle i en sådan undersökning ställas mot ett NATO-lands cyberförsvar, där resultatet sedermera skulle jämföras med ändamålet att utröna fördelar respektive nackdelar. Förslagsvis skulle Danmark i en sådan undersökning kunna utgöra NATO-landet, då det liknar Sverige i många hänseenden. Genom att analysera Danmark skulle det erhållna resultatet dessutom bredda förståelsen avseende EU:s samlade cyberförsvar.

6. Litteratur och referensförteckning

6.1 Källor

6.1.1 Tryckta

Försvarsmakten. *Militärstrategisk doktrin 2016: MSD* 16, Stockholm, 2016.

Försvarsberedningen. Ds 2017:66. *Motståndskraft - Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025.* Regeringskansliet. Försvarsdepartementet. Stockholm, 2017.

Regeringskansliet. Skr. 2016/17:213. *Nationell strategi för samhällets informations- och cybersäkerhet,* 2017.

6.1.2 Digitala

FRA. Årsrapport 2018. 2019. https://www.fra.se/nyheter/nyhetsarkiv/news/arsrapporten-for2018publicerad.5.69cf97cd167832fc038242.html (Hämtad 2019-04-17).

Försvarsmakten. Årsredovisning 2018. 2019. https://www.forsvarsmakten.se/sv/om-myndigheten/dokument/arsredovisningar/ (Hämtad 2019-04-06).

Försvarsmakten. ÖB Micael Bydén Rikskonferens Folk och Försvar 2019. 2019. https://www.forsvarsmakten.se/siteassets/3-organisation-forband/overbefalhavaren/tal-och-debattartiklar/nuvarande-obs-tal-och-debattartiklar/190114-ob-general-micael-byden-tal-vid-folk-och-forsvars-rikskonferens-i-salen-2019.pdf (Hämtad 2019-04-16).

MSB. Årsredovisning 2018. 2019. https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Arsredovisning-2018/ (Hämtad 2019-04-06).

MSB. Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022. 2019. https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Samlad-informations--och-cybersakerhetshandlingsplan-for-aren-20192022/ (Hämtad 2019-04-14).

Regeringskansliet. Försvarsministern talade på Cyberförsvarsdagen 2018. 2018. https://www.regeringen.se/artiklar/2018/02/forsvarsministern-talade-pa-cyberforsvarsdagen-2018/ (Hämtad 2019-04-16).

6.2 Litteratur

6.2.1 Tryckta

Collins, Sean & McCombie, Stephen. Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*. *Vol.* 7, no. 1, 2012: 80-91. doi: 10.1080/18335330.2012.653198.

Ekengren, Ann-Marie & Hinnfors, Jonas, *Uppsatshandbok: [hur du lyckas med din uppsats]*, 2., [rev.] uppl., Studentlitteratur, Lund, 2012.

Dalsjö, Robert. Sweden and its deterrence deficit: Quick to react, yet slow to act. I *Deterring Russia in Europe: defence strategies for neighbouring states*, Vanaga, Nora & Rostoks, Toms (red.), 93-110. London: Routledge, Taylor & Francis Group, 2019.

Esaiasson, Peter, Gilljam, Mikael, Oscarsson, Henrik, Towns, Ann E. & Wängnerud, Lena, *Metodpraktikan: konsten att studera samhälle, individ och marknad*, Femte upplagan, Wolters Kluwer, Stockholm, 2017.

Försvarsberedningen. Ds 2017:66. *Motståndskraft - Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025.* Regeringskansliet. Försvarsdepartementet. Stockholm, 2017.

Försvarsmakten. *Militärstrategisk doktrin 2016: MSD* 16, Stockholm, 2016.

George, Alexander L. & Bennett, Andrew, *Case studies and theory development in the social sciences*, MIT, Cambridge, Mass., 2005.

George, Alexander L. & Smoke, Richard, *Deterrence in American foreign policy: theory and practice*, New York, 1974.

Iasiello, Emilio. Is Cyber Deterrence an Illusory Course of Action?. *Journal of Strategic Security. Vol.* 7, no. 1, 2013: 54–67. doi: 10. 5038/1944–0472.7.1.5.

Johannessen, Asbjørn & Tufte, Per Arne, *Introduktion till samhällsvetenskaplig metod*, 1. uppl., Liber, Malmö, 2003.

Lebow, Richard Ned & Gross Stein, Janice. Rational Deterrence Theory: I Think, Therefore I Deter. *Cambridge University Press*. *Vol*. 41, no. 2, 1989: 208–224. doi: 10.2307/2010408.

Lonsdale, J. David. Warfighting for Cyber Deterrence: a Strategic and Moral Imperative. *Springer Philosophy & Technology*. *Vol*. 31, no. 3, 2018: 409–429. doi: 10.1007/s13347-017-0252-8. s.425–426.

Regeringskansliet. Skr. 2016/17:213. *Nationell strategi för samhällets informations- och cybersäkerhet*, 2017.

Rostoks, Tom. The evolution of deterrence from the Cold war to hybrid war. I *Deterring Russia in Europe: defence strategies for neighbouring states*, Vanaga, Nora & Rostoks, Toms (red.), 19-36. London: Routledge, Taylor & Francis Group, 2019.

Schelling, Thomas C. *Arms and influence*, Yale University Press, New Haven, CT, 2008[1966].

Schelling, Thomas C. *The strategy of conflict*, Harvard University Press, Cambridge, Mass, 1960.

Sierzputowski, Bartłomiej. THE DATA EMBASSY UNDER PUBLIC INTERNATIONAL LAW. *The International and Comparative Law Quarterly*. *Vol*. 68, no. 1. 2019: 225–242. doi:10.1017/S0020589318000428.

Stone, John. Conventional Deterrence and the Challenge of Credibility. *Contemporary Security Policy*. *Vol.* 33, no. 1, 2012: 108–123. doi: 10.1080/13523260.2012.659591.

Stuxnet: targeting Iran's nuclear programme. *Strategic Comments, Routledge. Vol.*17, no. 2, 2011: 1–3. doi: 10.1080/13567888.2011.575612.

Taddeo, Mariarosaria. Deterrence and Norms to Foster Stability in Cyberspace. *Springer Philosophy & Technology*. *Vol*. 31, no. 3, 2018: 323–329. doi: 10.1007/s13347-018-0328-0.

Wilner, Alex. Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation. *Routledge, Taylor & Francis Group*. *Vol.* 36, no. 4, 2017: 309–318. doi: 10.1080/01495933.2017.1361202.

Williams, Phil. Nuclear Deterrence. I *Contemporary strategy*, 2. ed., rev. Baylis, John (red.), 113–134. New York: Holmes & Meier, 1987-. s.117–121.

Yin, Robert K., *Fallstudier: design och genomförande*, 1. uppl., Liber, Malmö, 2007.

6.2.2 Digitala

CERT-SE. Om CERT-SE. 22 januari 2019. https://www.cert.se/om-cert-se (Hämtad 2019-04-08).

Crosston, D. Matthew. World gone cyber MAD: How ‘mutually assured debilitation’ is the best hope for cyber deterrence. *Strategic Studies Quarterly*. *Vol*. 5, no. 1, 2011: 100–116. https://search-proquest-com.proxy.annalindhbiblioteket.se/docview/857934287/fulltextPDF/886F94B63583402FPQ/1?accountid=8325 (Hämtad 2019-03-13).

FOI. CRATE - Cyber Range And Training Environment. https://www.foi.se/kurser-och-resurser/resurser-och-anlaggningar/crate---cyber-range-and-training-environment.html (Hämtad 2019-04-08).

FOI. Om FOI. https://www.foi.se/om-foi.html (Hämtad 2019-04-17).

Försvarsmakten. Världens största cyberförsvarsövning. Högkvarteret. 2018. https://www.forsvarsmakten.se/sv/aktuellt/2018/04/varldens-storsta-cyberforsvarsovning/ (Hämtad 2019-04-15).

Jensen, Eric Talbot. Cyber deterrence. *Emory international Law Review*. *Vol.* 26, no 2, 2012: 773–824. https://heinonline-org.proxy.annalindhbiblioteket.se/HOL/Page?lname=&public=false&collection=journals&handle=hein.journals/emint26&men_hide=false&men_tab=toc&kind=&page=773&t=1556260190 (Hämtad 2019-02-11).

MSB. Årsrapport It-incidentrapportering 2017. 2018. https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Arsrapport-It-incidentrapportering-2017/ (Hämtad 2019-02-18).

Regeringskansliet. Regeringsförklaringen: 21 januari 2019. 2019. https://www.regeringen.se/tal/20192/01/regeringsforklaringen-den-21-januari-2019/ (Hämtad 2019-02-19).

Regeringskansliet. Regeringen inför krav på it-incidentrapportering för statliga myndigheter. 2015. https://www.regeringen.se/pressmeddelanden/2015/12/regeringen-infor-krav-pa-it-incidentrapportering-for-statliga-myndigheter/ (Hämtad 2019-03-18).

Sveriges Riksdag. Försvarsutskottets betänkande 2017/18: FöU4. 2017. https://www.riksdagen.se/sv/dokument-lagar/arende/betankande/nationell-strategi-for-samhallets-informations-_H501F%C3%B6U4 (Hämtad 2019-04-14).

Sveriges Riksdag. Resiliens, avskräckning och försvar: stärkt cybersäkerhet för EU. https://www.riksdagen.se/sv/dokument-lagar/dokument/fakta-pm-om-eu-forslag/resiliens-avskrackning-och-forsvar-starkt_H506FPM5 (Hämtad 2019-04-26).