Försvarshögskolan

Cyberattacker - unika fall eller en möjlighet till lärande?

En kvalitativ fallstudie av den nationella hanteringen av cyberattacker inom Sverige

Olivia Malmström

Självständigt arbete, 15HP

Statsvetenskap med inriktning krishantering och säkerhet

Påbyggnadskurs i statsvetenskap, HT20

Handledare: Magnus Ekengren

Antal ord: 12 743

Abstract

In the last decades the world has become more and more digitalized which has led to a new kind of threat, known as cyberattacks. The statistics show that the amount of attacks are increasing every year even though the increasing experience should help to contain the threat. This creates questions regarding the learning capacity when it comes to cyberattacks.

The aim of this paper is to explore whether or not there has occurred an organizational learning within the Swedish crisis management linked to cyberattacks. By analyzing four different cases of cyberattacks within Sweden and the measures in-between, the paper searches for signs of organizational learning. The analysis uses a theory of organizational learning summarized into three indicators representing different levels of learning; single loop learning, double loop learning and meta learning, which are used to identify the learning.

The thesis finds that there are signs of organizational learning on a shallow as well as on a deep level but that there is a lack of connection between the learning. It is difficult to tell if the learning is based on experience from prior cyberattacks or if there are other influential aspects playing a larger part in the learning process. Further research could focus on finding a more distinct connection within the learning and its origins with the purpose of a better understanding of crisis management linked to cyberattacks.

1. Inledning

1.1 Bakgrund

Dagens samhälle har förändrats snabbt under de senaste tjugo åren avseende vilken teknik som används och hur man använder tekniken. Teknikens utveckling har inom flera områden bidragit till nya möjligheter som har effektiviserat samhällens funktioner och skapat en ökad globalisering. Under de senaste åren har fokus legat på de möjligheter och risker som främst informationsteknik och digital teknik kan ge. Teknikens växande roll i samhället har skett samtidigt som den tekniska utvecklingen skett i allt högre fart. Det har lett till krav på en kontinuerligt fungerande anpassning till den senaste utvecklingen av tekniken. Bland annat finns det ett behov av ett säkerhetsarbete som hela tiden måste uppdateras och utvecklas i samma takt som den senaste tekniken för att undvika att system blir sårbara för cyberattacker, vilket kan leda till att de positiva faktorer tekniken bidrar med istället används emot oss och utnyttjas av andra aktörer på ett hotfullt sätt (Cybersäkerhet i Sverige, 2020:6).

Hoten om cyberattacker blir allt mer uppmärksammade men trots ökade åtgärder verkar antalet cyberattacker ständigt att öka. En undersökning från 2019 visade att hälften av de bolag som svarat på undersökningen hade blivit utsatta för cyberangrepp under 2018 och mer än hälften trodde att angreppen skulle fortsätta i större utsträckning under 2019 (PwC, 2019). Vidare skriver FRA i sin årsrapport från 2018 att det ständigt pågår cyberattacker och att de dessutom ökar, då metoderna för angrepp hela tiden blir mer sofistikerade och svårare att upptäcka (FRA:s årsrapport, 2018:17). I en undersökning från 2019 svarade 63 procent av bolagen att de hade blivit utsatta av cyberangrepp, vilket var en ökning på 14 procent sedan året innan (PwC, 2020). Lägesrapporten om ökade fall av cyberattacker har inte förändrats sedan 2018 och i samband med utbrottet av Covid-19 har man dessutom noterat en intensifiering av angreppen. Bland annat har man sett att sjukhus har blivit särskilt drabbade under årets pandemi, vilket är oroande då sjukhusen inte har personal som arbetar med att rapportera intrång och avvikelser i systemen (SvD, 2020).

1.2 Problemformulering

Som bakgrunden visar ökar antalet cyberattacker för varje år samtidigt som det riktas mer och mer uppmärksamhet mot hotet. Det skapar en fråga hur det kommer sig att antalet cyberangrepp blir fler samtidigt som erfarenheten av fenomenet ökar. Baserat på teorier om lärande ska erfarenhet underlätta krishanteringen av liknande framtida fall, både i form av att förhindra och att hantera.

Bland annat skriver Boin et al. i boken *The politics of crisis management* (2017) att kriser skapar möjligheter till lärande baserat på den erfarenhet som uppkommer i samband med krisen. Lärandet skapas genom den nya information som tillkommer vid en kris. Informationen översätts sedan till konkreta policyförändringar vars syfte är att förebygga och underlätta hanteringen av framtida jämförbara kriser (Boin et al., 2017:128). Det gör att ökningen av antalet cyberattacker som sker varje år inte ter sig stämma överens med den traditionella idén om lärande.

Kriser refereras ofta som stora exceptionella situationer som naturkatastrofer eller terroristattacker (Roux-Dufort, 2007:105). Cyberattacker däremot är snarare långdragna, anonyma och svåra att upptäcka direkt (Cybersäkerhet i Sverige, 2020:8). Eftersom konceptet av lärande efter kriser är baserat på en definition av kris som inte ter sig vara fullständig för cyberattacker som kris, går det att vidare spekulera kring vilken utsträckning lärande går att applicera på cyberattacker.

Denna studie syftar till att undersöka frågeställningen genom en analys av fyra fall av cyberattacker mot Sverige och hur dessa har hanterats. De utvalda fallen benämns inom studien som; Operation Cloud Hopper, Wannacry, kinesiskt cyberspionage och phishingkampanjer. Syftet är att försöka identifiera huruvida ett lärande har skett under och mellan fallen. Analysen kommer att använda sig av teori kring organisatoriskt lärande för att försöka mäta nivån av lärande kopplat till cyberattacker. Den utvalda teorin är organisatoriskt lärande, då krishanteringen av större cyberattacker hanteras av aktörer som organisationer och myndigheter. Det blir därmed mer relevant att se på lärande inom organisationer i jämförelse med lärande hos individer.

Studien baseras på antagandet att det finns en märkbar skillnad mellan cyberattacker och den traditionella definitionen av kris. Antagandet ligger till grund för påståendet att det finns en risk att konceptet av lärande efter kriser inte går helt i linje med cyberattacker. Det skulle kunna anses vara en anledning till att antalet angrepp ökar istället för minska trots den utökade erfarenheten. Vidare har uppsatsen valt att undersöka enbart lärande som förklaringsfaktor till antalet cyberattacker, vilket gör att det finns ett antagande om att denna faktor är av betydelse.

1.3 Tidigare forskning

Bland den tidigare forskningen inom ämnet cyberattacker relaterat till lärande finns artikeln *One-pass-throw-away learning for cybersecurity in streaming non-stationary environments by dynamic stratum network* (2018) som utifrån ett tekniskt perspektiv behandlar lärande inom cybersäkerhet på

en teknisk nivå. Artikeln uppmärksammar läsaren om att det finns en skillnad mellan stationär och icke stationär data men att de säkerhetssystem som används inte alltid tar hänsyn till det. Författarna förklarar problematiken som medföljer och hur viktigt det är för cybersäkerheten att man hanterar olika system efter behov. Lösningen som föreslås är ett ”one-pass-throw-away” lärande som använder den dynamiska strukturen inom ett nätverk för att lösa de problem som inte kan tas hänsyn till om systemen inte separeras (Thakong et al., 2018:1-2). Artikeln redogör sedan för ett flertal algoritmer för att visa mer exakt hur det skulle gå till och vad det skulle innebära (ibid:5-10).

Ytterligare en artikel som behandlar lärande inom cyber är *Structural relationships among self-regulated learning, learning flow, satisfaction, and learning persistence in cyber universities* (2014) som utifrån ett beteendevetenskapligt perspektiv diskuterar hur individer undervisas inom lärande. Författarna menar att det saknas psykologiska komponenter inom utbildningen som tålamod och uthållighet för att det arbete som individerna senare kommer att utföra inom cyber ska ha så bra förutsättningar som möjligt. Man menar att ett tillägg av psykologisk natur bland annat skulle öka individernas motivation att hela tiden växa och förbättra sitt arbete, vilket skulle hjälpa individernas förmåga att lära sig. Artikelns syfte är att visa på samband mellan de psykologiska faktorerna och se hur dessa kan komma att påverka andra variabler inom lärande (Young Ju et al., 2014:752-755).

Fortsättningsvis beskriver artikeln *Gaussian process learning for cyber-attack early warning* (2010) det viktiga i att lära sig upptäcka cyberattacker i tid. Författarna redogör för det svåra i att urskilja och prioritera vilka hot som är mest relevanta för olika system, eftersom det konstant sker hotfulla aktiviteter. Författarna visar upp en modell, kallad ”Gaussian Process Learning”, vars syfte är att lokalisera vilka hot som är mest troliga att angripa ett visst nätverk genom att lyfta fram faktorer som aggressivitet och tidigare mönster som kan indikera på relevans (Zhang et al., 2010:56-57). Vidare består artikeln av algoritmer och uträkningar som ska visa på hur modellen skulle kunna se ut och fungera (ibid:58-64).

Specifikt organisatoriskt lärande inom cyber diskuteras i boken *Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training* (2013). Bland annat redovisades en undersökning bestående av en gruppintervju och enkätundersökning. Syftet med undersökningen var bland annat att försöka förstå hur det organisatoriska lärandet upplevdes av individerna och vilka eventuella ändringar som skulle kunna göras inom organisationer utifrån upplevelserna. Vidare använde man undersökningen för att få en bättre uppfattning om vilken typ

av organisationskultur som är bäst anpassad till att hantera cyberattacker (Trim & Upton, 2013:119). Slutsatsen som dras av undersökningen är att en stabil riskbedömning är grundläggande för att det ska kunna fattas relevanta beslut kring hur man ska skapa en så fullständig säkerhetsstrategi inom cyber som möjligt (ibid:134).

Den tidigare forskningen visar på att det finns ett intresse för lärande kopplat till cyberattacker inom såväl statsvetenskap som andra forskningsfält. En stor del av den forskningen som redan har gjorts fokuserar på ett specifikt område inom lärande, så som ett visst beteende eller särskilda tekniska aspekter. Vad som är mindre vanligt är ett bredare perspektiv som studerar det generella lärande som koncept jämsides cyber. Det öppnar upp för en utveckling inom det statsvetenskapliga forskningsfältet kopplat till ämnet. Utifrån den tänkta analysen syftar uppsatsen till att bidra till ämnet och forskningsfältet utifrån ett bredare perspektiv.

1.4 Syfte

Syftet med studien är att undersöka huruvida det har skett ett organisatoriskt lärande på såväl ytlig som djup nivå inom den svenska krishanteringen, med fokus på statliga aktörer; regering, riksdag och relevanta myndigheter inom cyber; Försvarsmakten, MSB, Säkerhetspolisen och FRA, i samband med cyberattacker i Sverige. Uppsatsen ämnar bidra till det statsvetenskapliga fältet genom en utvecklad förståelse av cyberattacker som fenomen och i vilken utsträckning de kan förstås utifrån konceptet av lärande. En utökad kunskap inom området har potential att bidra till förståelsen av fenomenet, vilket i sin tur kan hjälpa till att utveckla krishanteringen kopplat till cyberattacker.

1.5 Frågeställning

I vilken utsträckning har Sveriges nationella krishantering lärt sig utifrån erfarenheter från cyberattacker?

1.6 Utvecklad problemformulering

Många menar att lärande efter kriser är allmänt svårt att uppnå, oavsett kris. På organisatorisk nivå talar till exempel Hede i sin artikel *Lull after the storm? Municipal leaders reflect on multiple crisis experienc*e (2011) om vad hon kallar för ”over-learning” som handlar om svårigheten att bearbeta och koppla samman informationen efter en kris på ett sätt som leder till användbar kunskap. Vid over-learning drabbas organisationen av en form av tunnelseende som gör att aktörerna misslyckas

med att se framtida scenarion bortom den kris som precis har inträffat (Hede, 2011:281). Vidare menar Drennan et al. att en annan orsak till varför lärande inte alltid sker inom en organisation är på grund av en för svag vilja till att genomföra förändringar, till exempelvis i organisationer med en djupt rotad policy att de uppsatta aktörerna inte gynnas av att genomföra ändringar (Drennan et al., 2014:204).

Det finns flera aspekter som gör att man skulle kunna hävda att ett lärande i samband med cyberattacker är extra svårt. Till exempel menar Boin et al. i boken *Governing After Crisis : The Politics of Investigation, Accountability and Learning* (2008) att en stor del av det lärande som sker (i ett fall av effektivt lärande) efter en kris kan ske utanför den organisatoriska sektorn. Författarna talar om ett politiskt lärande som baseras på att informationen bearbetas av politiska aktörer till en förståelse av vad som har hänt och vad som gick fel. Kunskapen som inhämtas ska sedan göras tillgänglig i syfte att förhindra att liknande kriser sker i framtiden. Det för att motarbeta spekulationer och skapa en klarhet kring situationen (Boin et al., 2008:14). Svårigheten med påståendet kopplat till cyberattacker är att informationen som tillkommer efter ett angrepp kan anses vara känslig. Om förövaren till exempel är en rivaliserande stat kan det ligga i den angripna statens intresse att inte öppet dela med sig av den nya kunskapen för att inte avslöja sin egen kapacitet (SvD, 2017). På så vis får medaktörer inte alltid all information, vilket försvårar processen av lärande.

Vidare talas det om att en välutvecklad lärandeprocess består av tre komponenter, vilka beskrivs som erfarenhet, förklaring och kompetens. Den förstnämnda grundas i att aktörer inhämtar erfarenhet i samband med att de utsätts för en kris. I och med att krisen sker får aktören en insikt i krisens innebörd, det vill säga orsaker, konsekvenser och respons. Tanken är att den erfarenhet som skapas efter en kris läggs på minnet för att sedan kunna användas vid nästa likartade kris. Det påpekas dock att denna form av lärande är mest effektiv inom yrken där en viss typ av kris sker så pass ofta att det blir rutin att hantera dessa (Boin et al., 2017:129). Svårigheten inom cyberattacker är att angreppen hela tiden utvecklas och blir mer och mer sofistikerade. Det innebär att det inte räcker med att förstå tidigare attacker. Ett försvar mot cyberangrepp kräver att cybersäkerheten växer i samma takt som hoten, vilket inte alltid är fallet (Cybersäkerhet i Sverige, 2020:20). Därmed går det inte att helt förlita sig på minnet när det kommer till cyberattacker. Vad som ytterligare försvårar denna komponent är att angripare kan använda sig av tidigare hotaktörers strukturer för att skapa en så kallad ”false flag” operation som går ut på att förvirra den drabbade

(ibid:8). I detta fall hjälper inte ett tidigare minne eftersom angriparen utnyttjar just detta i sin attack.

Förklaringsfaktorn går ut på att försöka hitta de bakomliggande orsakerna till de misslyckanden som skedde innan och under krisen samt vilka följder responsen hade på situationen. En förutsättning för att detta ska kunna genomföras är att det finns en mängd kvalificerade individer inom ämnet som kan göra en bedömning av situationen. Ytterligare en förutsättning är att dessa aktörer får utföra sitt arbete utan yttre påverkan och att det finns tillräckligt med tid och resurser för genomförandet (Boin et al., 2017:129). Den tredje faktorn som benämns som kompetens syftar till att beskriva de nya förmågor som krävs i samband med en kris. Kriser kan i många fall kräva en expertis som inte alltid existerar sedan innan. Därför behöver ofta det berörda yrket lära sig nya färdigheter samtidigt som de hanterar krisen. Krishanteringen blir därmed experimentell och inte nödvändigtvis effektiv. Processen är dock nödvändig för att aktören ska kunna införskaffa en förståelse av krisen inför framtida likartade situationer (Boin et al., 2017:130). Kopplat till cyberattacker kan detta bli problematiskt i och med att ett angrepp kan drabba vem som helst och att alla aktörer inte är lika utrustade med personal och resurser anpassade för krisen. Till exempel, som tidigare nämnts, har sjukvården blivit extra utsatt för cyberattacker under utbrottet av Covid-19, vilket är oroande, då de hanterar känslig information men saknar specialister inom cybersäkerhet (SvD, 2020:a). På så vis krävs det inte enbart en ökad specialisering inom cybersäkerhet utan även en installation av personal för att förklarings- och kompetensfaktorn ska kunna genomföras.

Ytterligare en påverkande faktor till ett försvårat lärande kan vara att cyberattacker som kris är ett relativt nytt fenomen i jämförelse med andra typer av kriser, så som naturkatastrofer. I och med att det har skett en så pass snabb utveckling inom tekniken kan det verka som att det har gått en lång tid sedan digitaliseringen påbörjades. I verkligheten har det dock gått en relativt kort tid i kontrast till de framsteg som har skett inom området. Cyberattacker som tidigare brukade kräva enorma resurser för att kunna genomföras kan nu verkställas genom en enda dator och med tanke på det omfång som datorer produceras och säljs kan ett angrepp orkestreras av betydligt fler aktörer med betydligt mindre besvär (SvD, 2012).

Slutligen bör det noteras att komplexiteten av cyberattacker ökar i och med att en attack inte bestämt innebär ett visst utfall. Det går visserligen inte att förutspå någon kris exakt men det problematiska med cyberangrepp är att de kan ta form på flera olika sätt. Bland underkategorierna

inom cyberattacker finns det till exempel vad som kallas för ”Malware” som inkluderar virus och spionprogram, ”Ransomware” som krypterar data och ofta kräver en lösensumma för att försvinna och ”Phishingkampanjer” vars syfte är att få fram personlig information så som lösenord och personuppgifter (Advenica). Inom andra kriser ser man ofta olika nivåer av samma typ av kris medan cyberattacker kan visa sig i helt olika former. Att ha varit utsatt för en cyberattack innebär alltså inte att aktören nödvändigtvis har införskaffat sig erfarenhet som kan nyttjas inför nästa attack då denna kan se helt annorlunda ut. Därmed går det att hävda att cyberangrepp har förutsättningar som gör att det blir extra svårt att lära sig av erfarenhet.

Detta ligger till grund för antagandet om att det finns en märkbar skillnad mellan cyberattacker och andra kriser när det kommer till lärande samt att denna är av betydelse.

1.7 Avgränsning

Studien avgränsas till att endast analysera större fall av cyberattacker som har drabbat Sverige. Det inkluderar både fall där Sverige är det enda drabbade landet och fall där Sverige är ett av flera drabbade länder. Avgränsningen större fall inom Sverige är gjord då mindre enskilda cyberangrepp sker kontinuerligt varje dag och inte är jämförbara med de större angreppen. I ett förtydligande definieras större attacker som de attacker som antingen har drabbat organisationer eller myndigheter samt massattacker av samma sort mot ett flertal individer under ett visst tidsspann. Avgränsningen inom Sverige är för att analysobjekten ska bli jämförbara. Resultatets trovärdighet ökar i och med att det går att hävda att samtliga ageranden och beslut som analyseras är gjorda inom samma land med liknande förutsättningar, i jämförelse med en analys av blandade länder.

Vidare är fallen begränsade till tidsperioden senare delen av 2010-talet för att begränsa och specificera empirin. Utöver det avgränsas analysen ytterligare till att endast undersöka beslut och agerande kopplat till nationella aktörer inom Sverige så som myndigheter och organisationer. Därmed syftar uppsatsen till att enbart undersöka lärande för nationella aktörer som arbetar med cybersäkerhet så som MSB, FRA, Säkerhetspolisen och Försvarsmakten. Ytterligare aktörer som kommer inkluderas är Sveriges riksdag och regering, då det är dessa aktörer som ansvarar över vissa betydelsefulla beslut vars grund har skapats av myndigheterna.

Myndigheterna är som tidigare nämnts utvalda baserat på relevans kopplat till uppsatsens ämne, det vill säga cyber. Alla fyra myndigheter arbetar på något sätt med cyberattacker och/eller

cybersäkerhet. MSB ansvarar bland annat för förebyggande av incidenter inom IT och analysen av omvärldsutveckling inom cyber (Myndigheten för samhällsskydd och beredskap). FRA har en egen avdelning för verksamhet inom cyber som arbetar med att identifiera och skydda Sverige mot utomstående cyberangrepp. FRA samarbetar även med Säpo i ett arbete vars syfte är att skydda myndigheter från cyberattacker (FRA). Försvarsmakten arbetar med cyberförsvar, vilket handlar om cyberoperationer på både offensiv och defensiv nivå (Försvarsmakten). Begränsningen av myndigheter utesluter eventuella andra viktiga aktörer som gör att resultatet kan komma att påverkas. Dock, som den korta beskrivningen av respektive myndighet visar, är de utvalda myndigheterna av hög relevans inom uppsatsens ämne, vilket gör att de kan anses vara representativa. Vidare går det att hävda att ett utökat antal av myndigheter hade krävt en studie bortom uppsatsens omfång.

Till sist har en avgränsning gjorts inom materialet. Eftersom information om cyberattacker, särskilt de som har drabbat i en större skala, kan anses vara känslig så ger uppgifterna som offentliggjorts ibland inte en fullständig bild av händelsen. Att få en full redogörelse av såväl krisen som beslut och åtgärder anses vara bortom studiens räckvidd, vilket gör att uppsatsen endast kommer hantera material som offentliggjorts. Materialet består enbart av andrahandskällor, då förstahandskällor kräver mer tid än vad studien hinner med. Det kan komma att påverka resultatet men anses inte förhindra studiens syfte.

1.8 Disposition

Uppsatsen är indelad i sex större delar; inledning, teori, metod, analys, avslutning och referenser. Inledningen inkluderar flera underrubriker som bland annat presenterar uppsatsens ämne och syfte. Teoridelen introducerar den utvalda teorin som analysen senare använder sig av samt centrala begrepp för studien. Den tredje delen kallad metod innehåller flera underrubriker i liknelse med inledningen. Vidare är analysen indelad i fyra delar som var och en beskriver ett fall av cyberattacker. Den avslutande delen knyter ihop uppsatsen genom att bland annat svara på forskningsfrågan och diskutera hur studien har genomförts. Slutligen presenteras en komplett referenslista.

2. Teori

2.1 Sammanfattning av teorin

Uppsatsen tar avstamp i teorin om organisatoriskt lärande, först presenterad av Argyris oh Schön, som redogörs i boken T*he politics of crisis management: Public Leadership under Pressure* (2017) av Boin et al. samt boken *Risk and Crisis Management in the Public Sector* (2014) av Drennan et al. Mer specifikt den definition av enkelspiralslärande, dubbelspiralslärande och metalärande som ges.

Inledningsvis menar Boin et al. att det finns vissa komponenter som ligger till grund för det generella lärandet, det vill säga aspekter som lärandemetoderna har gemensamt. Till att börja med menar författarna att lärande innebär en vilja att omkalibrera, ompröva och omvärdera den redan existerande förståelsen av den relevanta krisen. Det görs genom att ny information inhämtas och sedan används för att förändra organisationens krishantering. För att detta ska kunna genomföras menar författarna att det krävs en vilja och motivation till att utvecklas inom organisation (Boin et al., 2017:128).

Det som författarna kallar för enkelspiralslärande innebär att det sker en korrigering av till exempel organisationens policy, men på ett sätt som inte bidrar till en fundamental förändring (Boin et al., 2017:128). Vidare beskrivs den här formen av lärande som ett agerande som syftar till att ”bota symptom” snarare än att ta itu med de underliggande orsakerna till krisen (Drennan et al., 2014:203). Å ena sidan beskrivs enkelspiralslärande som en användbar metod av lärande i och med att det bidrar till en viss förändring. Å andra sidan påpekas det att metoden inte alltid räcker till, då lärandet endast rör ytliga faktorer och inte ändrar på djupet. Det finns således en sannolikhet att denna form av lärande inte fungerar långsiktigt. Det eftersom en organisations sårbarhet och begränsningar exponeras i samband med att en kris inträffar, vilket kräver en lösning på en djupare nivå än vad enkelspiralslärande kan erbjuda (Boin et al., 2017:128).

Dubbelspiralslärande tar lärandet till nästa nivå och inrättar nya normer inom organisationen i syfte att förbättra hur lärandet sker. Det kan till exempel innebära att organisationen sätter upp nya prioriteringar eller strukturerar om sin säkerhetsstrategi (Boin et al., 2017:128). I jämförelse med enkelspiralslärandet stannar inte lärandet vid att enbart påverka vad som ser ut att vara problemet i stunden, utan tar sig an det som ligger till grund för hur krishanteringen utförs. Vidare ifrågasätter

metoden organisationens kärnpolicy som definierar hur aktörer inom organisationen förstår och agerar i krävande situationer (ibid:129). Det innebär att dubbelspiralslärande bidrar med en mer långsiktig lösning än enkelspiralslärande (Drennan et al., 2014:203). Vad som kan ses som en risk med denna form av lärande är att en djupare förändring medför konsekvenser som är svåra att förutse och om dessa skulle visa sig vara negativa kan det som skulle bidra positivt bli kontraproduktivt (Boin et al., 2017:136-137).

Den tredje formen av lärande, kallad metalärande, innebär störst förändring av de tre metoderna. Metalärande beskrivs som den mest effektiva formen av lärande och kan beskrivas som ”att lära sig att lära”. Lärandet består av en kontinuerlig process där beslut och ageranden inom lärandet utvärderas. Processen innebär att organisationen inte bara reflekterar över de lärdomar som tillkommer i samband med kriser utan även hur man gör detta. Det innebär alltså att man inom denna form även försöker förstå lärandeprocessen i sig och hur den kan förbättras (Boin et al., 2017:129). Det problematiska med den här formen av lärande är att den är krävande i form av både resurser och vilja. För att ett lärande på en så pass djup nivå ska kunna genomföras behöver organisationen i fråga prioritera krishantering över andra mål, vilket inte alltid inte kan göras utan konsekvenser (Drennan et al., 2014:206).

Vad som bör noteras är att diskussionen kring nivån av användbarhet inte påverkar hur formerna av lärande används eller värderas inom studien, då syftet är att mäta ett eventuellt lärande och inte att testa metoderna i sig. Varje form av lärande bidrar till ett bredare perspektiv av lärande, eftersom det kan ske både ytligt och på djupet, för att öka förutsättningarna för ett resultat som visar på ett generellt lärande. Eftersom teorin som ska användas i studien har ett spann från ytligt till djupt lärande syftar analysen till att identifiera såväl effektivt lärande som enskilda strukturella förändringar som tyder på lärande. Då uppsatsen inte ämnar värdera det lärande som eventuellt kan urskiljas bör det också noteras att det som pekas ut som lärande inte likställs med effektivt lärande, det vill säga att ett resultat bestående av många tecken på lärande inte nödvändigtvis bör tolkas som att det sker en särskilt effektiv utveckling inom krishanteringen av cyberattacker, utan enbart att det sker ett lärande överhuvudtaget.

Varför just denna teori är vald är, som tidigare nämnts, på grund av att den anses ge en heltäckande bild av organisatoriskt lärande på flera nivåer. Ett exempel på en annan teori inom organisatoriskt lärande beskrivs i artikeln *”Organizational Learning: The Contributing Processes and the*

Literatures". Artikeln porträtterar organisatoriskt lärande med hjälp av fyra aspekter; kunskapsförvärv, tolkning av information, fördelning av information och organisatoriskt minne (Huber, 1991:88). Kortfattat representerar de fyra aspekterna olika processer i hur en aktör hämtar upp, tolkar och använder sig av information i ett lärande syfte (Huber, 1991:90). Anledningen till varför denna teori inte ansågs vara ideal för studien är bland annat på grund av att den inkluderar faktorer så som påverkan av utomstående aktörer. Det är inte relevant för uppsatsen, då den är begränsad till att endast analysera inom statliga aktörer. Vidare visar inte heller denna teori lika tydligt på en heltäckande bild, det vill säga lärande på olika nivåer, som den utvalda teorin gör. Uppsatsen syftar till att visa på ett generellt lärande, vilket teorin från Boin et al. och Drennan et al. anses göra på ett tydligare sätt.

2.2 Centrala begrepp

Centrala begrepp syftar till att definiera nyckelord inom uppsatsen som ur ett objektivt perspektiv inte har en ensam definition. Begreppsförklaringen som ges nedan är det som begreppen syftar till att beskriva specifikt i denna uppsats. Definitionerna ges för att läsaren ska få en bättre förståelse av dess innebörd och hur begreppen ser ut i kontrast till varandra. Det anses vara av vikt då uppsatsen bygger på att det finns en betydande skillnad mellan de utvalda begreppen, vilket ligger till grund för problemformuleringen och frågeställningen.

2.2.3 Kris

Begreppet kris syftar till att beskriva händelser som går under den traditionella definitionen av kris, vilken uppsatsen hävdar inte är heltäckande för cyberattacker som kris. Den traditionella definitionen talar om kriser som en händelse begränsad till tid och rum, det vill säga en händelse som har en tydlig början och ett tydligt slut. Det innebär även att begreppet refererar till händelser som sker på en viss plats inom geografiska gränser

2.2.4 Cyberattack/Cyberangrepp

Vad som i den här uppsatsen refereras till vid användandet av begreppet cyberattack respektive cyberangrepp är en digital attack av större form som antingen har drabbat en organisation/ myndighet eller en sammanhängande massattack av samma sort mot ett flertal individer under ett visst tidsspann. Attackerna är i sin natur svåra att identifiera, långdragna och ständigt skiftande. Krisfenomenet är i jämförelse med till exempel naturkatastrofer inte begränsat till geografiska platser utan kan drabba vem som helst, var som helst och när som helst. Fortsättningsvis begränsas

inte cyberangrepp till tid och rum i kontrast mot den traditionella krisen, vilket gör att en kris inom denna kategori kan pågå under längre period utan att bli upptäckt samt försvinna och återkomma i en liknande form. En cyberattack kan även drabba flera aktörer samtidigt och är inte begränsade av geografiska gränser.

3. Metod

3.1 Tillvägagångssätt och analytiskt verktyg

Uppsatsen genomförs som en kvalitativ fallstudie bestående av fyra olika fall av cyberattacker mot Sverige. Inom varje fall kommer, förutom själva händelsen i sig, beslut och ageranden att redogöras för. Efter varje fall kommer en analys med hjälp av den utvalda teorin att genomföras. Resultatet kommer sedan att studeras i ett försök att urskilja mönster eller liknande, som indikerar på ett sammanhängande lärande. Den kvalitativa metoden är utvald i syfte att ta fram det som anses vara mest väsentligt ur analysmaterialet (Esaiasson, 2017:33).

Det fördelaktiga med den kvalitativa metoden är att den, i jämförelse med den kvantitativa, är bättre på att lyfta fram specifika aspekter som sammanfattar analysmaterialet (ibid:198). Vidare bidrar den kvalitativa ansatsen med möjligheten att upptäcka sammanhang som kan bidra till förståelsen av de eventuella samband som upptäcks i analysen (Eliasson, 2018:27). Å andra sidan innehåller den kvalitativa ansatsen vad som kan anses vara brister i och med att den kräver mer tid åt varje fall än vad den kvantitativa ansatsen gör. Det innebär att en studie som genomförs med hjälp av en kvalitativ metod inte kan inkludera lika många analysobjekt som en studie som genomförs med en kvantitativ metod (Esaiasson et al., 2017:199). Det anses dock inte vara ett hinder för studien eftersom den kommer att undersöka ett bestämt antal fall på djupare nivå, vilket gör att det inte finns ett behov av ett breddat urval av analysobjekt.

Vad som också kan ses som en nackdel med den kvalitativa metoden är att generaliserbarheten blir sämre i och med att metoden inkluderar färre analysobjekt. Den kvantitativa metoden är mer effektiv när det kommer till att visa ett tydligt samband (Eliasson, 2018:50). Å andra sidan bidrar den kvantitativa metoden med en djupare analys än den kvalitativa, vilket ses som fördelaktigt för studien (ibid:21). Vidare bidrar den kvalitativa ansatsen med fördelen att analysobjekten är specifikt anpassade för den frågeställningen studien syftar till att besvara (ibid:27). Vad som också talar för den kvalitativa metoden och färre analysobjekt för denna uppsats är att det rent historiskt sätt inte

har skett alltför många cyberattacker som passar in i den kategori som ska undersökas i studien. Därmed fungerar de kvalitativa ansatsen bättre i relation till ämnet och analysen.

Det analytiska verktyget som kommer att användas i uppsatsen är processpårning. Syftet med verktyget är att urskilja samband och förklarande faktorer som visar på hur orsaker och resultat hänger ihop. Metoden hjälper till att förstå själva processen inom en händelse och identifierar relevanta beslut och ageranden (Esaiasson et al., 2017:129-130). Det anses vara passande för uppsatsens syfte, då verktyget hjälper till att urskilja faktorer och samband som kan visa på lärande.

3.2 Material

Materialet som används i studien är utvalt baserat på de fall som utgör analysobjekten samt den krishantering som sker emellan fallen. Objekten består av fyra fall av större jämförbara cyberattacker som har drabbat aktörer i Sverige. Det då studien syftar till att försöka urskilja ett lärande inom krishanteringen inom cyber. Genom att följa fallen får man en bild av krishanteringens utveckling, där förändringar kan visa på ett lärande. Det blir därför fördelaktigt för uppsatsen att undersöka de större attackerna, då empirin är bredare och mer omfattande än i de mindre fallen av angrepp. Dessutom blir de eventuella mönster som urskiljs mer legitima i och med att alla fall är ingår i samma kategori rent storleksmässigt och därmed är jämförbara. Materialet kommer som tidigare nämnts beröra fallen; Operation Cloud Hopper, Wannacry, kinesiskt cyberspionage och phishingkampanjer. Dessa fyra fall utgör även den tidsperiod som empirin förhåller sig till. Förutom de fyra fallen förhåller sig materialet även till de beslut och åtgärder som anses vara relevant för krishanteringen inom cyber mellan fallen. Analysobjekten utgör som tidigare nämnt en tidsram för den övriga krishanteringen.

Eftersom det generella begreppet cyberattacker inkluderar ett brett urval av angrepp har det, som tidigare nämnts, gjorts en egen definition av vad begreppet syftar till att mena i denna studie. De fyra fallen är valda utifrån definitionen för att de ska gå att hävda att de är jämförbara. Det går dock att ifrågasätta om den avgränsande definition som har gjorts fortfarande är såpass bred att fallen inte nödvändigtvis blir jämförbara. Å andra sidan behöver man ta hänsyn till det urval som existerar i förhållande till uppsatsens syfte. Som tidigare nämnts hävdas det i denna studie att det finns en skillnad mellan cyberattacker i jämförelse med andra kriser och en del av detta handlar just om den komplexa och varierade naturen hos cyberangrepp. I och med detta går det att hävda att cyberattacker i många fall delar färre likheter med varandra än andra kriser. Med tanke på att det

har skett flera avgränsningar inom ramen för studiens syfte anses fallen vara lämpade att jämföra med varandra.

3.4 Operationalisering

Indikator 1: Enkelspiralslärande

Indikator 1 visar på den mest ytliga nivån av lärande. Det lärande som sker är specifikt kopplat till en särskild händelse men hanterar inte nödvändigtvis kärnan av problemet. Indikatorn kan påvisas genom yttre korrigeringar eller förändringar i policyn eller strukturen gällande krishanteringen. Den kan även visas genom att aktören i fråga tar beslut i särskilt syfte att hantera den nyss inträffade krisen. Beslut och åtgärder som ska skydda mot ett specifikt problem men inte nödvändigtvis påverkar det generella problemet.

Indikator 2: Dubbelspiralslärande

Indikator 2 visar på en djupare nivå av lärande som inte enbart syftar till att hantera det nuvarande problemet utan även att skapa ett bättre lärande inom organisationen. Lärandet kan påvisas genom att det sker förändringar som påverkar krishanteringen på en djupare nivå, i jämförelse med indikator 1. Exempel på det skulle kunna vara omvärderade prioriteringar eller en ny strategi, det vill säga handlingar som utvecklar det som ligger till grund för den generella krishanteringen. Ytterligare tecken på indikatorn kan vara beteende eller agerande som ifrågasätter kärnpolicyn för krishanteringen.

Indikator 3: Metalärande

Indikator 3 är den mest utvecklade nivån av lärande som innebär djupgående förändringar för krishanteringen. Indikatorn påvisas genom att det sker utvärdering, beslut eller agerande som rör lärandeprocessen i sig. Förändringarna som sker i samband med indikator 3 handlar inte om konkreta handlingar i sig utan om hur processen sker som leder till konkreta handlingar. Vad som också kan anses vara tecken på denna indikator är om det sker en diskussion kring lärandeprocessen, det vill säga att det räcker med en förståelse om att en utveckling behövs och att det inte enbart behöver ske ett direkt agerande för att kunna räknas inom metalärande. Det eftersom lärandet beskrivs som en kontinuerlig process.

4. Analys

Analysen består av fyra olika fall av cyberattacker som har skett mot Sverige. Fallen är kronologiskt ordnade där varje del inleds med en redogörelse för vad som hände och vilket agerande som skedde kopplat till fallen. Förutom en redogörelse av själva fallet kommer beslut och åtgärder som har skett mellan analysobjekten att beskrivas. Dessa är också upplagda i en kronologisk ordning, vilket kan göra att det framstår som en ojämn fördelning. Det beror på att båda de två första fallen tog plats under 2017 och de två sista under 2019. Därför hamnar alla åtgärder och liknande som skedde under 2018 inom det senare fallet under 2017 och likaså det från 2020 i det senare fallet från 2019 för att följa den kronologiska ordningen. Materialet kommer sedan analyseras utifrån de indikatorer som beskrevs i teoridelen och som sedan kommer ligga till grund för ett resultat som diskuterar eventuella samband mellan det teoretiska ramverket kopplat till analysobjekten.

4.1 Operation Cloud Hopper

År 2017 upptäckte flera länder, bland annat Sverige, att de var utsatta för en cyberattack som gick under namnet ”Cloud Hopper” eller ”APT10”. APT står för Advanced Persistent Threat, en metod som spårades tillbaka till den kinesiska staten. Metoden är designad för utdragna och riktade cyberattacker som kan pågå under så lång tid som flera år där angriparen kontinuerligt får tillgång och stjäl information. Cloud Hopper är i nuläget den mest uppmärksammade APT-baserade cyberattacken (FOI Memo, 2019:6). Vad som bland annat gjorde att attackerna stack ut var att de skedde i en större skala än vad man hade behövt hantera tidigare (Omni Ekonomi, 2017)

Angreppen var särskilt inriktade på tjänsteleverantörer inom drift och it-infrastruktur. Efter att ha lokaliserat aktörerna fabricerades falska mejl vars syfte var att lura aktörerna på bland annat inloggningsuppgifter, vilka gjorde det möjligt för angriparen att installera skadliga koder hos tjänsteleverantörerna. Det slutgiltiga målet med attackerna var att få tillgång till information om tjänsteleverantörernas kunder som bestod av såväl företag som myndigheter (Cybersäkerhet i Sverige, 2020:23). Angreppen upptäcktes under år 2017 men misstänktes ha pågått redan så tidigt som år 2014. Att attackerna kunde pågå under så pass lång tid utan upptäckt menar man beror på att det var svårt att se samband mellan de enskilda angreppen, vilket gjorde att man inte direkt kunde identifiera dem som en enhetlig attack (SvD Näringsliv, 2017).

I och med upptäckten av attacken gick regeringen ut med ett pressmeddelande där man informerade det svenska folket att det pågick en kontinuerlig dialog mellan regeringen och de ansvariga myndigheterna samt att dessa var mitt i ett samarbete för att hantera attackerna. Vidare innehöll pressmeddelandet en försäkran om att cybersäkerhet prioriterades högt och att flera åtgärder hade vidtagits sedan regeringen tillträdde. Slutligen beskrevs det att attacken Cloud Hopper ytterligare hade tolkats som ett tecken på angelägenheten att ha en stabil informationssäkerhet och ett starkt arbete kring det (Regeringskansliet, 2017). Efter Operation Cloud Hopper insåg man sårbarheten som fanns relaterad till molntjänster, vilket är samlingsnamnet på det som angreps under attacken. Experter inom datasäkerhet uppmanade företag och privatpersoner att se över hur deras information delas och skyddas. Bland annat påpekade man att information och data av högt värde borde ges extra skydd i form av till exempel krypteringar (NyTeknik, 2017).

Beslutet att gå ut med information om förebyggande åtgärder efter Cloud Hopper visar på flera indikatorer. Med tanke på att direktiven var särskilt anpassade efter attacker mot molntjänster snarare än cyberattacker som generellt fenomen, så kan det ses som en yttre korrigering vars syfte var att skydda mot en specifik typ av situation. Å andra sidan går det att hävda att detta även kan visa på indikator 2. Uppmaningen om att se över hanteringen av bland annat skyddad information visar på början på en ny strategi och nya prioriteringar bortom den enskilda händelsen. Även regeringens pressmeddelande kan ses som tecken på indikator 2. Indikatorn visas genom att man påpekade att det är angeläget att arbeta mot en stabil informationssäkerhet, vilket skulle kunna tolkas som en form av kritik mot den säkerhet som redan fanns. Det kan ses som en typ av lärande eftersom insikten uppstod i samband med attacken. Varför detta räknas som indikator 2 och inte 1, trots den direkta kopplingen till den specifika situationen, är på grund av att slutsatsen som drogs av lärandet inte endast påverkade fallet utan cyberattacker överlag.

4.2 Wannacry

I maj 2017 utsattes flera organisationen runt om i världen, inklusive Sverige, för en synkroniserad attack i form av en skadlig kod kallad ”ransomware”. Koden användes för ekonomiskt utpressning och möjliggjordes genom att angriparen utnyttjade en sårbarhet i det program (Windows) som användes gemensamt av organisationerna (Cybersäkerhet i Sverige, 2020:17). När attacken inleddes var det svårt att identifiera exakt hur många aktörer som drabbades i Sverige. Även längden på attacken var svår att avgöra i och med att man misstänkte att viruset spreds via e-post. Det gjorde att antalet drabbade hela tiden riskerade att öka i antal (Svt Nyheter, 2017:a). Vad som ytterligare

gjorde att attacken blev svårhanterlig var att viruset hade det då hittills unika draget att kunna spridas utan att de drabbade klickade på länken som spreds via e-post. Det räckte med att en dator blev utsatt för viruset för att flera datorer som ingick i samma nätverk skulle kunna bli smittade (Wiklund, 2017).

I samband med att cyberattacken upptäcktes gick bland annat Sveriges nationella CSIRT (Computer Security Incident Response Team) ut med information om åtgärder, som kunde användas i syfte att skydda datorer mot den skadliga koden. De inkluderade bland annat nya säkerhetsuppdateringar särskilt skapade av Microsoft som skulle skydda datorer mot viruset. De hänvisade även till Microsofts hemsida där det fanns mer publicerad information om attacken och skyddande åtgärder (CERT, 2017). Vidare konstaterades det att en försvarsåtgärd mot viruset hade släppts redan en månad innan attacken blev uppmärksammad men att flera organisationer och företag hade missat detta (Svt Nyheter, 2017:b). Vad man även upptäckte var att det fanns en gemensam faktor mellan en stor majoritet av datorerna som blivit utsatta för viruset. Den gemensamma faktorn var en särskild version av Windows (Omni Ekonomi, 2019).

I stycket ovan går det att visa på indikator 1. Krishanteringen som beskrevs hade en direkt funktion att hantera det specifika problemet men inte nödvändigtvis det underliggande problemet eller cyberattacker utöver Wannacry. Säkerhetsfunktionen som gavs ut var särskilt designad för att stoppa den skadliga koden men inte tvunget andra cyberattacker som ett förtydligande. Ytterligare tecken på indikator 1 var att kännedomen kring vad som visade sig vara en gemensam faktor för den särskilda attacken även den gällde en särskild kontext. Det finns ingen information som tyder på att faktorn gäller utöver Wannacry, vilket gör att indikator 2 utesluts.

I en årsrapport från 2017 skriven av Försvarets radioanstalt konstaterades det att man förväntade sig att det skulle fortsätta ske en ökning av antalet cyberattacker mot Sverige. Men att hotet om angrepp och de utmaningar som medföljer blivit mer uppmärksammade under årets gång. Med det sagt blev de svenska myndigheterna under 2017 mer medvetna om styrkor och svagheter gällande sin informationssäkerhet. Vidare fastställdes det att en utvecklad kapacitet inom cybersäkerhet ligger till grund för att skydda landets suveränitet och infrastruktur inom den digitala världen (FRA:s årsrapport, 2017:7).

Den ökade förståelse som införskaffades under 2017 gällande cyberattacker visar på ett lärande i form av indikator 2 och 3. Indikator 2 uppvisas genom att det går att hävda att det har skett en ökad förståelse av cyberattacker under året som är så pass utvecklad att det kan komma att påverka grunden för krishanteringen inom området. Vidare visas indikator 3 genom att det skapades en ökad medvetenhet inom krishanteringsprocessen. Det gjordes en utvärdering av den egna kapaciteten där man upptäckte både styrkor och svagheter men också vad man ansåg vara en väsentlig faktor för en framtida bättre process. Även om det inte skedde en direkt konkret handling med denna insikt, visar årsrapporten på en utvecklad förståelse av processen, i linje med indikator 3.

Regeringen gick under 2018 ut med en uppdaterad nationell strategi för samhällets informations- och cybersäkerhet. Syftet med strategin var att redovisa vilka prioriteringar och målsättningar regeringen har inom området. Vidare skriver man att strategin hoppas skapa förutsättningar på lång sikt för en fungerande säkerhet men också skapa medvetenhet om situationen (Regeringskansliet, 2018).

Den uppdaterade säkerhetsstrategin kan ses som tecken på indikator 2. Det eftersom dess syfte var att visa på omvärderade prioriteringar och en ny strategi, vilka i sin tur ämnade förändra och utveckla kapaciteten inom cybersäkerhet. Vidare kan även indikator 2 hävdas genom viljan att öka medvetenheten hos andra aktörer, eftersom det var ett problem som upptäcktes året innan i samband med Wannacry. Agerandet kan ses som en del av den nya strategin. Vad som talar emot indikator 2 är att den nya strategin kan hävdas endast visa på påtänkta policyförändringar men att den tills vidare inte bidrar med en konkret förändring. Strategin visar å ena sidan på att det finns en vilja att göra omställningar som kan komma att skapa en ny grund för krishanteringen. Å andra sidan kan det ses som enbart en planering och inte en förändring i sig.

Under 2018 rapporterade även FRA att cyberattackerna fortsatte att öka både i kvantitet men även i kvalitet (FRA:s årsrapport, 2018:7). FRA förklarade samma år vilket värde en enhet specialiserad på cyberattacker skulle ha för Sveriges cybersäkerhet. Man föreslog ett fördjupat samarbete mellan relevanta myndigheter i syfte att skapa en kompetenshöjning inom området, som i sin tur skulle leda till ett bättre underlag för beslutsfattarna inom cybersäkerhet (ibid:19). Vidare påbörjades även bygget av ett nytt signalspaningsfartyg under 2018 vars syfte är att fånga upp främmande signaler som inte kan hämtas från fastlandet. Fartyget var en uppdaterad version av ett äldre fartyg med samma syfte. FRA skriver i sin årsrapport från 2018 att man under de kommande åren planerar att

arbeta med fler projekt inom teknikavdelningen i syfte att utveckla och förbättra sin signalspaning (ibid:15).

FRA:s rapportering från 2018 visar på indikator 2 och 3. Indikator 2 via planeringen av en utvecklad krishantering i form av ett fördjupat samarbete. Det kan anses vara en förändring som kan komma att påverka grunden inom krishanteringen. Vad som återigen talar emot indikator 2 är att åtgärden endast befann sig i en planeringsfas, vilket inte garanterat resulterar i förändringar. Ytterligare en motsägande faktor är att åtgärden inte nödvändigtvis behöver innebära en fundamental förändring eftersom samarbetet redan existerade och endast skulle utvecklas. Vidare visas indikator 3 genom att hävda att det har skett en förståelse kring behovet av en modifiering av krishanteringen i samband med att man tvingats konstatera att fallen ökade. Vad som talar emot båda indikatorerna är att det går att ifrågasätta vad utvärderingen är baserad på, det vill säga om planeringen faktiskt är gjorde för att man insett att krishanteringen är otillräcklig eller om det bara rör sig om en generell strävan att utveckla organisationen.

4.3 Kinesiskt cyberspionage

Under 2019 rapporterades ett flertal attacker i form av cyberspionage mot Sverige. Totalförsvarets forskningsinstitut (FOI) rapporterade att en omfattande mängd av dessa kunde knytas till Kina. Cyberspionaget rörde sig bland annat om stölder inom särskilda grenar av elektronik så som robot- och flygteknik. Enligt FOI var och är Sverige extra utsatta mot sådana angrepp, då vi bedriver en nyskapande och digitaliserad ekonomi (Mårtensson, 2019).

FOI gick under 2019 ut med en rapport om Kinas industriella cyberspionage mot Sverige. I rapporten sammanfattas bland annat huvudsakliga slutsatser så som att cyberspionaget främst inriktar sig på strategiska sektorer, som Kina anser kommer bidra till deras utvecklingsmål. Spionaget sker i syfte att understödja kinesiska intressen inom så väl politik som ekonomi men används också för att uppnå en vision om självförsörjande teknologi. Man konstaterade även att operationer inom cyber är en hög prioritet i Kina och att dess omfång verkar öka i både kvalitet och kvantitet (FOI Memo, 2019:1).

I och med den utvecklade förståelsen av Kina som hotaktör inom cyberspionage påpekade FOI i sin rapport att det kan finnas anledningar till att hålla uppsyn över de uppdateringar av 5G som började

diskuteras under 2018-2019. En uppdatering av 5G gjord av ett kinesiskt bolag skulle kunna utgöra en risk för dolda inbyggda vägar i utrustningen som staten Kina skulle kunna utnyttja för spionage, baserat på landets agenda och tidigare agerande (FOI Memo, 2019:16-17).

Förslaget om förebyggande försiktighetsåtgärder kan ses som ett tecken på indikator 2. Det eftersom att man skulle kunna hävda att det kan tolkas som en del av en ny strategi att införa förebyggande åtgärder. Vidare går det att formulera som om det drabbande hotet blev en erfarenhet som gjorde att man sedan kunde se risken för återkommande hot inom samma kategori, vilket gjorde att hotet blev en prioritering i vad som annars kanske enbart hade setts som en möjlighet till ytterligare teknisk utveckling.

I en interpellation från 2019 beskrevs det att Sverige hade en otillräcklig cybersäkerhet i kontrast till landets digitalisering. Det påpekades dock att det har skett en utveckling och att åtgärder så som en nyinrättad säkerhetsskyddslag visar på framsteg inom området. Å andra sidan skrevs det vidare i interpellationen att situationen, även om den ansågs förbättrad, inte var tillräckligt bra då man menade att Sveriges förmåga inom cybersäkerhet innehöll stora brister. Regeringens svar på interpellationen var att de delade uppfattningen och att man var medveten om den komplexa situationen gällande cyberhot. I svaret ingick även en redogörelse av beslut och ageranden som genomförts under 2017-2018 i syfte att stärka cybersäkerheten. Det i form av bland annat ökade resurser till myndigheter och ett påbörjat projekt kring ett center specialiserat för cybersäkerhet (Sveriges riksdag, 2019).

För att börja med den ifrågasättande biten av interpellationen går det att urskilja indikator 2 och 3. Interpellationen beskriver en problematik med krishanteringen runt cyberattacker genom att hävda att de framsteg som har gjorts inte är tillräckliga. Det kan tolkas som ett ifrågasättande av policyn för krishanteringen, i linje med indikator 2. Vidare är interpellationen baserad på en utvärdering av den dåvarande situationen som skapade en diskussion kring behovet av utveckling inom ämnet, vilket tyder på indikator 3. Fortsättningsvis, gällande svaret på interpellationen, visas även här indikator 2 och 3. Svaret består av en redogörelse av olika beslut åtgärder som har gjorts och planeras göra i syfte att förbättra kapaciteten inom cybersäkerheten. Varför detta ses som indikator 2 och inte 1 är att åtgärderna som beskrivs rör den generella krishanteringen och inte enbart ett specifikt fall. Ökade resurser och ett nytt center påverkar grunden inom krishanteringen, vilket visar på indikator 2. Dock går det att ifrågasätta i vilken utsträckning det rör sig om lärande eftersom det

inte ges en tydligare motivering än att cybersäkerheten inte är tillräcklig och att hotet om attacker ökar. På så sätt kan det handla om en ökad medvetenhet snarare en ett lärande. Å andra sidan går det att hävda att en ökad medvetenhet grundar sig i erfarenhet och lärdomar. Villigheten att göra förändringar och de konkreta handlingarna som beskrivs visar även på en utvecklande process inom ämnet, därav indikator 3.

I september 2019 fick FRA, Försvarsmakten, MSB och säkerhetspolisen i uppgift att tillsammans förbereda och planera för ett center för cybersäkerhet, som man hoppades kunna verkställa under 2020. Syftet med centret är att stärka landets förmågor inom cybersäkerhet, både inom förebyggande verksamhet och inom aktiv hantering (Regeringskansliet, 2019). Mer konkret avser centret att genomföra analyser, sammanställa lägesbilder och sprida information mellan myndigheterna, vilket förhoppningsvis bidrar till ett mer koordinerat arbete i samband med cyberattacker (Säkerhetspolisens årsbok, 2019:27).

Planeringen av ett nytt center för cybersäkerhet indikerar på lärande inom både indikator 2 och 3. Eftersom ett center för cybersäkerhet inte existerade innan kan ett införande av ett sådant ses som en fundamental förändring inom krishanteringen gällande cyber, men även som en del av ny strategi mot en förbättrad cybersäkerhet. Ytterligare tolkning av planeringen kan vara att cybersäkerheten har flyttats upp på prioriteringslistan, då centret är ett sätt att öka och förbättra resurserna inom den relevanta krishanteringen. Allt i linje med indikator 2, vidare kan planeringen av det nya centret ses som början av en process mot en bättre krishantering inom cyber. Det föreslås genom beskrivningen av syftet för centret, ett utvecklat samarbete mellan myndigheter gällande cyberattacker. På så vis hävdas indikator 3.

4.4 Phishingkampanjer

Under det senare halvåret av 2019 skedde flera angrepp under namnet phishingkampanjer. En av dem utfördes genom att förövaren skapade en falsk hemsida som förkläddes till en officiell registersida för Regeringskansliet. Länken till hemsidan skickades sedan ut till olika aktörer via e-post där de uppmuntrades att registrera sig. Sidans syfte var att samla information och uppgifter om de utsattas verksamheter. Ett annat angrepp skedde på liknande sätt där angriparen, igen via e-post, skickade ut en länk till en hemsida som var förklädd till att se ut som en säker webbplats. När aktören följde länken blev hen sedan ombedd att logga in på sitt Office-365. Vid inloggning gav aktören omedvetet ut sina inloggningsuppgifter till angriparen. Processen fortsatte sedan genom att

förövaren skickade ut falska mejl från aktörens mejladress med samma länk, i syfte att få tillgång till fler uppgifter (Cybersäkerhet i Sverige, 2020:16).

Efter att ha identifierat phishingkampanjer som en form av cyberangrepp, installerade verksamheter som var medvetna om hotet skydd för verksamhetens e-poster och man gick även ut och varnade sina anställda för falska mejl och länkar. Det visade sig vara en framgångsrik metod och de verksamheter som har uppmärksammat hotet är bättre på att hantera eventuella angrepp än de som inte har det (Cybersäkerhet i Sverige, 2020:16).

Den beskrivna åtgärden kan identifieras som indikator 1. Motivationen är att åtgärdernas syfte var att hantera den specifika situationen med phishingkampanjer. Resultatet av den rekommenderande handling är också specifikt kopplat till hotet i och med att det konstaterades att de som följde åtgärderna införskaffades sig ett bättre skydd mot phishingkampanjer men inte nödvändigtvis mot cyberattacker generellt.

I år, 2020, påbörjades för första gången en utbildning för cybersoldater inom Försvarsmakten. Utbildningens syfte är bland annat att förstärka Sveriges förmåga inom cyberförsvar och planeras vara en långsiktig åtgärd (Försvarsmakten, 2020). Det centrala i utbildningen är teoretiskt och praktisk kunskap inom it och hur försvar kan utföras i samband med en cyberattack. Vidare utbildas individerna i att urskilja sårbarheter i system och hur sårbarheterna skulle kunna utnyttjas av hotaktörer samt vilka åtgärder som kan användas för att laga intrång (Försvarsmakten, 2019).

Den nya utbildningen för cybersoldater kan ses som ett tecken på indikator 2 i och med att det kan komma att påverka grunden av krishanteringen inom cyber. Utbildningen bidrar med en ny och särskild inriktad kompetens inom ämnet som inte funnits tidigare inom organisationen, vilket har potential att göra stor skillnad. Med hjälp av cybersoldater skapas en utvecklad förmåga att förstå och använda införskaffad information och erfarenhet som i sin tur kan bidra till ett bättre lärande enligt indikator 2.

Säkerhetspolisen gick ut under 2020 med en rapport gällande Sveriges cybersäkerhet. I denna konstaterade man att Sveriges utveckling inom ämnet fortfarande går långsamt i jämförelse med hur snabbt digitaliseringen växer. Det innebär den kapacitet Sverige idag besitter inom cyberförsvar inte är tillräcklig för att kunna sätta upp ett stabilt försvar mot existerande hot och risker. Vidare tar

rapporten upp konkreta exempel på brister som verkar vara återkommande inom ämnet. De inkluderar bland annat bristfälliga hot- och riskanalyser i kombination med en avsaknad av policy och regler inom området. De visar även att det finns ett mönster av att beslutade säkerhetsåtgärder inte verkar genomföras och att engagemanget för ämnet inte är tillräckligt högt (Cybersäkerhet i Sverige, 2020:21).

Säkerhetspolisens rapport grundar sig på en undersökning av cybersäkerheten i Sverige där kapaciteten och behovet av utveckling utvärderas. Rapporten lyfter fram att den utveckling som hade skett hittills inte var tillräcklig, en kritik som gör att indikator 2 går att urskilja. Eftersom det är den allmänna krishanteringen och cybersäkerheten som ifrågasätts går det att göra ett antagande om att det är grundpolicyn som kritiseras. Vidare visar rapporten på en förståelse om att det behöver ske en utveckling inom området för att förbättra hanteringsprocessen. Uppmaningen kan ses som en möjlighet till konkreta handlingar som ökar effektiviteten, vilket tillsammans med förståelsen om utveckling visar på indikator 3.

Under september 2020 gick lämnade regeringen över budgetpropositionen till riksdagen där man valde att avsätta 50 miljoner kronor till att finansiera etableringen av det påtänkta nationella centret för cybersäkerhet. Det beskrivs av säkerhetspolisen som ett framsteg i processen att skapa en utvecklad och förbättrad förmåga inom cybersäkerhet (Säkerhetspolisen, 2020). Själva beslutet om centret togs i december 2020. Regeringen gick ut med ett pressmeddelande där det fastställdes att FRA, Försvarsmakten, MSB och Säkerhetspolisen har fått klartecken att inrätta ett nationellt center för cybersäkerhet vars syfte beskrevs som att utveckla den samlade svenska förmågan inom cybersäkerhet. Det påpekades även att Sverige har hög kapacitet inom digitalisering och att det är viktigt att säkerheten ligger på samma nivå. Det för att undvika hot såsom intrång och sabotage som kan komma att drabba de svenska intressena (Regeringskansliet, 2020).

Budgetbeslutet kan analyseras i linje med indikator 3 genom att se beslutet som en del av pågående process mot en bättre krishantering. Processen startade redan året innan beslutet om budgeten togs och med att man förstod att det behövdes utökade medel och började planera för centret. Att budgetbeslutet togs är ett ytterligare tecken på att processen med stor sannolikhet kommer leda till konkreta handlingar i form av både själva inrättandet av centret. Men också det arbete som är planerat att ske inom centret så som förbättrad utvärdering och ett mer utvecklat beslutsfattande. Själva beslutet om centret stärker ytterligare indikator 3, då det visar på slutet av den planerande

processen men även en början på en ny process av utförande. I och med att centret blev godkänt påbörjades en process mot en utvecklad cybersäkerhet. Det visar även på att det finns en förståelse kring behovet av en stärkt kapacitet inom området. Beslutet skulle även kunna hävdas visa på indikator 2, då inrättandet blir en fundamental förändring för både de inblandande organisationerna men också för den grundläggande krishanteringen inom cybersäkerhet.

4.5 Sammanställning av resultat

Indikator 1: Enkelspiralslärande

Av alla indikatorer går det att ur analysen konstatera att denna indikator förekommer i kortast utsträckning. Det mönster som går att urskilja gällande indikator 1 är att denna nivå av lärande uppstår direkt efter eller under en kris. Det är dock inte förvånande med tanke på att indikator 1 syftar till att beskriva ett lärande direkt kopplat till en specifik situation. I och med att det är den specifika krisen som sker och skapar konsekvenser för tillfället blir det också det specifika som behöver tas itu med först. Därför är det rimligt att indikator 1 uppstår nära i tid med krisen. Det är därför också rimligt att indikator 1 inte syns i de beslut som tas inom den allmänna utvecklingen inom cybersäkerhet, då det i många fall inte finns en given koppling till ett visst fall. Att denna nivå av lärande är den mest ytliga av de tre nivåerna bekräftas också genom att det inte går att urskilja tecken på att de lärdomar som har införskaffats i samband med indikator 1 inte tydligt dyker upp vid senare tillfällen. Återigen är detta inte överraskande eftersom de fall om har undersökts i studien inte är likadana när det kommer till typ av cyberattack eller vad som har blivit utsatt för angrepp och hur det gick till. Det gör att lärdomarna som dras inte är användbara på kriser med annorlunda modus operandi.

Indikator 2: Dubbelspiralslärande

Indikator 2 syns till skillnad från indikator 1 mer frekvent i analysen. Vilka fall indikatorn uppfattas inom är inte av särskild betydelse eftersom, som tidigare nämnts, de två första respektive de två sista skedde under samma år. Det gör att det blir naturligt att indikatorn hittas i större utsträckning under tidsperioden för de två senare fallen under 2017 och 2019. Med det sagt urskiljs indikator 2 i majoriteten av fallen i samband med beslut och åtgärder som sker mellan de utvalda cyberangreppen, det vill säga i kontexter utan särskild koppling till en specifik attack. På samma sätt som enkelspiralslärandet naturligt skedde nära i tid med fallen, så går det att hävda att det finns en naturlig koppling mellan dubbelspiralslärande och den självständiga kontexten. Det eftersom kraven för indikatorn insisterar på en mer generell natur kring lärandet. Det är svårare att

genomföra under eller precis efter en kris när det är just den relevanta attacken som behöver hanteras. Den kontinuerliga förekomsten av indikatorn visar på att det har skett ett lärande över tid inom cybersäkerhet men är sämre på att visa vad lärandet grundas ur, i jämförelse med indikator 1.

Indikator 3: Metalärande

I liknelse med indikator 2 syns indikator 3 i en större utsträckning mellan fallen. På samma sätt som för indikator 2 ligger det inte en djupare betydelse i var indikatorn förekommer av samma skäl som förklarat i stycket gällande dubbelspiralslärande. Ytterligare liknelse med indikator 2 är att indikator 3 uppstår i kontexter utan tydlig koppling till en cyberattack. Vidare går det att urskilja ett mönster som visar på att indikatorn vid många tillfällen förekommer i samma kontext som indikator 2. En anledning till detta är att indikator 3 delar den oberoende kontextfaktorn med indikator 2, det vill säga att det inte krävs att en särskild kris har inträffat nära i tid för metalärandet ska kunna ske. Förekomsten av indikator 3 visar på att det finns en förståelse kring behovet av en kontinuerlig utveckling av krishanteringen för att kunna uppnå en stabil cybersäkerhet. Indikatorn visar även på ett det förutom en förståelse även finns en pågående process som arbetar mot en bättre krishantering. Den visar sig både i form av planering och som utförande. Från analysen går det även att se att den utvecklande processen går framåt genom till exempel centret för cybersäkerhet som gick från att vara ett förslag till att ta form. I liknelse med indikator 2 finns en oklarhet kring vad lärandet kommer från då även denna indikator saknar kravet av anknytning till särskild kontext. Men eftersom metalärande är en mer abstrakt form av lärande, i jämförelse med både enkel- och dubbelspiralslärande, behöver detta inte nödvändigtvis ses som någonting negativt. Vad som dock kan diskuteras är dess effektivitet som indikator, då mätningen blir lite av en individuell tolkning och kan därmed hävdas vara för subjektiv för att bidra med ett generaliserbart resultat.

5. Avslutning

5.1 Sammanfattning

Uppsatsens syfte är att undersöka huruvida det har skett ett lärande i samband med cyberattacker i Sverige trots det stigande antalet attacker genom en kvalitativ analys av utvalda cyberattacker tillsammans med beslut och ageranden som har skett under och mellan fallen. Analysen sker med hjälp av en teori kring organisatoriskt lärande där definitionen av tre olika nivåer av lärande har valts ut specifikt för att representera teorin. Resultatet av analysen visar på att det har skett ett lärande inom alla tre nivåer men att det svårt att visa på ett samband mellan dessa.

5.2 Svar på forskningsfråga

Uppsatsens forskningsfråga är; I vilken utsträckning har Sveriges nationella krishantering lärt sig utifrån erfarenheter från cyberattacker? Utifrån studiens analys går det att konstatera att det har skett ett lärande på såväl ytlig som djup nivå, visat genom indikatorerna. Som tidigare nämnts förekommer indikator 1 i mindre utsträckning än indikator 2 och 3, vilket visar på att det i större utsträckning har skett ett lärande på en djupare nivå. Enligt teorin är det djupare lärandet att föredra men eftersom uppsatsens syfte inte är att värdera lärandet blir detta irrelevant. Vad som kan konstateras är att det har skett ett lärande i bred utsträckning eftersom alla nivåer av lärande har kunnat urskiljas. Vad som dock är svårare att visa på är huruvida lärandet har skett genom erfarenhet från tidigare cyberattacker eller om det finns andra aspekter som ligger till grund för lärandet. Eftersom majoriteten av det lärande som har urskilts i analysen rör sig om en djupare nivå av lärande vars koppling till tidigare kontext är otydlig finns det ingen garanti att lärandet faktiskt har hämtats i samband med tidigare erfarenhet, åtminstone inte i samband med de specifika kriser som har analyserats i studien.

5.3 Diskussion

5.3.1 Teori

Den utvalda metoden för uppsatsen är organisatoriskt lärande. Inom teorin har tre nivåer av lärande valts ut till att representera organisatoriskt lärande. Innebörden av respektive nivå har sedan omformulerats till tre indikatorer som var och en beskriver hur nivån av lärandet kan urskiljas i en kontext. Urvalet av tre nivåer av organisatoriskt lärande har bidragit till ett brett omfång som har gett studien goda förutsättningar till att upptäcka ett generellt lärande i linje med uppsatsens problemformulering och forskningsfråga.

Ur ett kritiskt perspektiv kan man ifrågasätta effektiviteten med indikatorerna. Syftet med dessa är att fungera som mallar för olika typer av lärande genom att beskriva vad som krävs för att räknas som ett lärande inom varje metod. Svårigheterna med indikatorerna är att mycket lämnas upp till individuell tolkning. Även om de bidrar med riktlinjer för varje nivå av lärande så saknas det en viss tydlighet som gör det möjligt för olika individer att uppfatta kraven olika. Det går inte att säga att det finns enbart en korrekt tolkning av vad som till exempel räknas som ”förändringar på en djupare nivå”, vilket gör att det går att hävda att analysen är subjektivt utförd utifrån författarens egna perspektiv. Detta gäller särskilt indikator 2 och 3 som i viss mån kan upplevas som lika och

svåra att helt skilja åt. Indikator 3 kan också anses vara särskilt svårtolkad i och med att den talar om förändringar inom lärandeprocessen i sig, vilket kan vara svårt att applicera i en kontext med konkreta handlingar. Eftersom innebörden av lärandeprocess inte definieras vidare kan det bli svårt att säga vad som inkluderas under begreppet. Vad som också kan ifrågasättas här är om det borde finnas en viss begränsning i tid inom lärandet då det som indikatorn hänvisar till som ”process” inte specificerar detta. Det går att spekulera kring huruvida lärandet verkligen är effektivt om det tar en märkbart längre tid. Ytterligare en bristande faktor kopplat till indikator 2 och 3 är att det saknas riktlinjer gällande huruvida det alltid krävs en konkret kris som grund för att det ska kunna ske ett lärande eller om det kan ske enbart genom en ökad medvetenhet av hotet. Teorin och indikatorerna hade gynnats av ett förtydligade av vad respektive nivå verkligen innebär.

5.3.2 Metod

Metoden som har använts i uppsatsen är av kvalitativ ansats och anses fortfarande var bra lämpad för syftet och frågeställningen. Metoden i kombination med det analytiska verktyget processpårning har skapat en fungerande process i att ta fram det centrala ur empirin som användes för att bemöta studiens frågeställning.

I ett utvecklande perspektiv av metoden går det att ifrågasätta den representativa faktorn i analysobjekten. I och med den kvalitativa ansatsen begränsades antalet analysobjekt, vilket vid studiens start inte ansågs vara ett hinder för uppsatsens syfte. I efterhand med resultatet från analysen i hand går det att hävda att det begränsade antalet fall kan ha påverkat studiens slutsatser. I och med den abstrakta naturen hos lärande hade ett bredare urval av analysobjekt kunnat gynna analysen genom att bidra med fler eventuellt påverkande faktorer. Det hade i sin tur kunnat hjälpa till med att bättre förklara vad den djupare nivån av lärande har grundats på, vilket hade skapat en mer komplett analys och slutsats. Vidare går det att kritisera urvalet i och med att studien avgränsades till att bara inkludera större fall av cyberattacker, det vill säga attacker som antingen har drabbat organisationer eller myndigheter samt massattacker av samma sort mot ett flertal individer under ett visst tidsspann. Det kan ha påverkat resultatet då det sker mindre individuella angrepp dagligen i en betydligt större skala än de större attackerna. I och med att de existerar i ett så pass stort omfång är det sannolikt att de påverkar den generella förståelsen av cyberattacker och cybersäkerhet. En studie med fler analysobjekt eller ett bredare omfång mellan små och stora angrepp hade kunnat resultera annorlunda. Ytterligare en avgränsning som kan ha påverkat resultatet är begränsningen till fall inom Sverige och de svenska myndigheterna. Det med tanke på

att digitaliseringen, inklusive cyberattacker, är ett globalt fenomen som inte hindras av geografiska gränser. Den globala faktorn gör att det kan finnas ett värde i att undersöka cybersäkerheten i Sverige, men att då också inkludera internationell påverkan och samarbeten med andra länder. Flera av de angrepp som har analyserats i uppsatsen drabbade ett antal länder samtidigt, vilket gör att det är sannolikt att ett samarbete skedde mellan länderna i samband med krishanteringen. Som resultatet visade saknas vissa förklarande faktorer till var lärandet har uppstått från, något som ett bredare perspektiv hade kunnat bidra med.

5.4 Generaliserbarhet

Studien anses vara bidragande genom att ligga till grund för fortsatt forskning inom ämnet. Som tidigare nämnt finns det ett behov av ett förtydligande inom teorin för att öka styrkan i resultatet. Även inom metoden finns det förbättringsområden som öppnar upp för vidare forskning som kan bidra till en utökad förståelse inom lärande kopplat till cyberattacker. Generaliserbarheten begränsas också i och med att studien har valt att enbart undersöka cyberattacker inom Sverige, vilket gör att den inte garanterat kan anses vara representativ för varken aktörer eller kriser utanför uppsatsens avgränsning. Detta gäller inte enbart för fall utanför Sveriges gränser utan även för cyberattacker som har skett inom Sverige men som ligger utanför den valda definitionen av attack i denna uppsats.

5.5 Vidare forskning

Uppsatsens resultat tillsammans med de utvecklingsområden som har diskuterats i avslutningen öppnar upp för vidare frågor inom ämnet. Bland annat hade vidare forskning kunnat undersöka väsentligheten av utomstående faktorer som uteslöts ur denna uppsats, så som globalisering och internationell påverkan. Även ett mer riktat fokus på tydligare samband mellan till exempel fall och lärande hade kunnat bidra till ökad förståelse inom ämnet. Som den tidigare forskningen i början på uppsatsen visar finns det utrymme för forskning gällande lärande kopplat till cyber inom det statsvetenskapliga fältet, då cyber ofta relateras till ett smalare perspektiv. Den tidigare forskningen visar även på att ämnet kan förstås utifrån flera olika perspektiv, vilket stärker sannolikheten att det finns en relevans i att inkludera flera olika faktorer i en framtida studie. Cyber är dessutom ett komplext område och kan därmed eventuellt kräva en förståelse inom ett smalare perspektiv för att i sin tur kunna analyseras bredare. Fortsatt hade vidare forskning även kunnat lägga fokus på relationen mellan cyberattacker som fenomen och lärande som koncept. Som tidigare nämnts

hävdar denna studie att det finns en märkbar skillnad mellan cyberattacker och andra typer av kriser samt att detta gör att det blir extra svårt att lära sig från cyberangrepp. Antagandet hade kunnat skapa en intressant forskningsfråga att undersöka för att fortsatt utveckla förståelsen av cyberattacker. Forskning inom cyber är viktigt oavsett perspektiv och fokusområden eftersom ämnet är relativt nytt och behöver utforskas i en bredare utsträckning. Dess roll är inte bara viktig för förståelsen utan även för krishanteringen, då en utvecklad förståelse har potential att förbättra krishanteringen kring cyber.

6. Referenslista

6.1 Böcker

Boin, A; McConnell, A & Hart, P (2008) *Governing After Crisis : The Politics of Investigation, Accountability and Learning.* Cambridge University Press.

Boin, A; Hart; P; Stern, E & Sundelius, B (2017). T*he politics of crisis management: Public Leadership under Pressure*. Cambridge University Press.

Drennan, Lynn T.; McConnell, Allan & Stark, Alastair. (2014). *Risk and Crisis Management in the Public Sector* (2nd edition). Routledge.

Eliasson, A (2018) *Kvantitativ metod från början.* Lund: Studentlitteratur.

Esaiasson, P; Gilljam, M; Oscarsson, H; Towns, A & Wägnerud, L (2017). *Metodpraktikan: Konsten att studera samhälle, individ och marknad*. Stockholm: Wolters Kluwer, 5:e uppl.

Trim, P & Upton, D (2013) *Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training.* Farnham: Routledge.

6.2 Elektroniska källor

Advenica, *Cybersäkerhet - vad är det?* https://www.advenica.com/sv/cybersakerhet-vad-ar-det (Hämtad 2021-01-06)

CERT (2017) *Pågående ransomware-kampanj (WannaCry/Wcry/WannaCrypt0r)* https://www.cert.se/2017/05/pagaende-ransomware-kampanj-wannacry-wcry-wannacrypt0r (Hämtad 2020-11-26)

FOI (2019) *Kinas industriella cyberspionage* https://www.foi.se/rest-api/report/FOI%20Memo%206698 (Hämtad 2020-11-27)

FRA, *Cyberförsvar* https://www.fra.se/jobbahososs/ettuppdragsomkraverdebasta/cyberforsvar.4.1c544a44165863dd11c19c.html (hämtad 2021-01-03)

FRA, Försvarsmakten, MSB, Polisen & Säkerhetspolisen (2020) *Cybersäkerhet i Sverige - Hot, metoder, brister och beroenden* https://www.msb.se/contentassets/8a5d2bb5d2024acb90feb5ebec0f645f/rapport-cybersakerhet-i-sverige-2020--hot-metoder-brister-och-beroenden.pdf (Hämtad 2020-11-09)

Försvarsmakten, *Cyberförsvar* https://www.forsvarsmakten.se/sv/var-verksamhet/det-har-gor-forsvarsmakten/cyberforsvar/?gclid=Cj0KCQiA88X_BRDUARIsACVMYD-T6Iaq8LODJivMzu_y5-jO7370yIXgCRUo6nvPvAo8P25UPhO4A6oaAhM5EALw_wcB (Hämtad 2021-01-03)

Försvarsmakten (2019) *Försvarsmakten utbildar cybersoldater* https://www.forsvarsmakten.se/sv/aktuellt/2019/02/forsvarsmakten-utbildar-cybersoldater/ (Hämtad 2020-11-27)

Försvarsmakten (2020) *Cyberförsvar* https://www.forsvarsmakten.se/sv/var-verksamhet/det-har-gor-forsvarsmakten/cyberforsvar/ (Hämtad 2020-11-27)

Hede, S. (2011). Lull after the storm? Municipal leaders reflect on multiple crisis experience. *Disaster Prevention and Management: An International Journal*, 20(3), 281-293 https://doi-org.proxy.annalindhbiblioteket.se/10.1108/09653561111141727 (Hämtad 2020-11-19)

Huber, George P. (1991). Organizational Learning: The Contributing Processes and the Literatures, *Organization Science*, Vol. 2, No. 1, Special Issue: Organizational Learning: Papers in Honor of

(and by) James G. March. (1991), ss. 88-115. http://links.jstor.org/sici?sici=1047-7039%281991%292%3A1%3C88%3AOLTCPA%3E2.0.CO%3B2-5 (Hämtad 2021-01-05)

Myndigheten för samhällsskydd och beredskap, *Informationssäkerhet, cybersäkerhet och säkra kommunikationer* https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/ (Hämtad 2021-01-02)

Mårtensson, R (2019) FOI:Omfattande kinesiskt cyberspionage mot Sverige, *Omni Ekonomi* https://omniekonomi.se/foi-omfattande-kinesiskt-cyberspionage-mot-sverige/a/8mqJ6x (Hämtad 2020-11-27)

NyTeknik (2017) *Expert: Cloud Hopper en väckarklocka* https://www.nyteknik.se/digitalisering/expert-cloud-hopper-en-vackarklocka-6839349 (Hämtad 2020-11-15)

Olsson, T (2012) Cyberattacker ett stort växande hot, *SvD* https://www.svd.se/cyberattacker-ett-stort-vaxande-hot (Hämtad 2020-12-05)

Omni Ekonomi (2017) *Hackarattack mot stora it-företag - Sverige drabbat* https://omniekonomi.se/hackarattack-mot-stora-itforetag-sverige-drabbat/a/Lz2m4 (Hämtad 2020-11-27)

Omni Ekonomi (2019) *Windows 7 på 98 procent av Wannacry-smittade datorer* https://omniekonomi.se/windows-7-pa-98-procent-av-wannacrysmittade-datorer/a/4pe3e (Hämtad 2020-11-27)

PwC Sverige (2019) *Domen från svenska storbolag: Sverige kan inte försvara sig mot cyberattacker* https://www.pwc.se/sv/cyber-security/cyberhot-sverige.html (Hämtad 2020-11-09)

PwC Sverige (2020) *Stor ökning av cyberattacker mot svenska bolag* https://news.cision.com/se/pwc/r/stor-okning-av-cyberattacker-mot-svenska-bolag,c3138790 (Hämtad 2020-11-09)

Regeringskansliet (2017) *Informationssäkerheten behöver stärkas för att öka motståndskraften mot it-angrepp* https://www.regeringen.se/pressmeddelanden/2017/04/informationssakerheten-behover-starkas-for-att-oka-motstandskraften-mot-it-angrepp/ (Hämtad 2020-11-28)

Regeringskansliet (2018) *Nationell strategi för samhällets informations- och cybersäkerhet* https://www.regeringen.se/regeringens-politik/krisberedskap/nationell-strategi-for-samhallets-informations--och-cybersakerhet/ (Hämtad 2020-11-27)

Regeringskansliet (2019) *Regeringen inleder arbetet med att inrätta nationellt cybersäkerhetscenter* https://www.regeringen.se/pressmeddelanden/2019/09/regeringen-inleder-arbetet-med-att-inratta-nationellt-cybersakerhetscenter/ (Hämtad 2020-11-13)

Regeringskansliet (2020) *Regeringen inrättar ett nationellt cybersäkerhetscenter* https://www.regeringen.se/pressmeddelanden/2020/12/regeringen-inrattar-ett-nationellt-cybersakerhetscenter/ (Hämtad 2020-12-13)

Roux-Dufort, C. (2007) Is Crisis Management (Only) a Management of Exceptions?, *Journal of Contingencies and Crisis Management*, Volume 15 Number 2 June, pp. 105-114. https://onlinelibrary-wiley-com.proxy.annalindhbiblioteket.se/doi/epdf/10.1111/j.1468-5973.2007.00507.x (Hämtad 2020-11-10)

SvD (2017) *FRA: Statlig aktör bakom massiv cyberattack* https://www.svd.se/fra-delger-statlig-aktor-bakom-massiv-cyberattack (Hämtad 2020-11-20)

SvD (2020) *”Center för cybersäkerhet får inte dröja längre”* https://www.svd.se/center-for-cybersaker-far-inte-droja (Hämtad 2020-11-10)

SvD Näringsliv (2017) *MSB: Skickliga angripare bakom cyberattack* https://www.svd.se/omfattande-cyberattack-mot-foretag-avslojad (Hämtad 2020-11-15)

Sveriges riksdag (2019) *Bristande cybersäkerhet* https://www.riksdagen.se/sv/dokument-lagar/dokument/interpellation/bristande-cybersakerhet_H610236 (Hämtad 2020-11-27)

Svt Nyheter (2017) **a:** *Datasäkerhetsblogg: 40 platser i Sverige drabbade av cyberattacken* https://www.svt.se/nyheter/inrikes/datasakerhetsblogg-40-platser-i-sverige-drabbade-av-cyberattacken **b:** *IT-attack kopplas till NSA – nära 100 länder drabbade* https://www.svt.se/nyheter/utrikes/virus-bakom-it-attack-kopplas-till-nsa (Hämtad 2020-11-26)

Säkerhetspolisen (2019) *Säkerhetspolisens årsbok 2019* https://www.sakerhetspolisen.se/download/18.a5cd4be16dfd84e1716a5/1585209341505/Arsbok2019.pdf (Hämtad 2020-11-27)

Säkerhetspolisen (2020) *Finansiering klar för nationellt cybersäkerhetscenter* https://www.sakerhetspolisen.se/ovrigt/pressrum/aktuellt/aktuellt/2020-09-21-finansiering-klar-for-nationellt-cybersakerhetscenter.html (Hämtad 2020-11-28)

Thakong, M ; Phimoltares, S ; Jaiyen, S & Lursinsap, C (2018) One-pass-throw-away learning for cybersecurity in streaming non-stationary environments by dynamic stratum network, *Public Library of Science* (PLoS), Vol.13 (9) http://europepmc.org/backend/ptpmcrender.fcgi?accid=PMC6126810&blobtype=pdf (Hämtad 2020-11-13)

Wiklund, K (2017) Det här vet vi om Wannacry-attacken, *NyTeknik* https://www.nyteknik.se/digitalisering/det-har-vet-vi-om-wannacry-attacken-6848974 (Hämtad 2020-11-26)

Young Ju, J; Sunyoung, J & Jiyeon, K (2014) Structural relationships among self-regulated learning, learning flow, satisfaction, and learning persistence in cyber universities, *Interactive learning environments*, Vol.22 (6), p.752-770; Abingdon: Routledge. https://doi.org/10.1080/10494820.2012.745421 (Hämtad 2020-11-14)

Zhang, J; Porras, P & Ullrich, J (2010) Gaussian process learning for cyber-attack early warning, *Statistical analysis and data mining*, Vol.3 (1), p.56-68; Hoboken: Wiley Subscription Services,

Inc., A Wiley Company https://onlinelibrary-wiley-com.proxy.annalindhbiblioteket.se/doi/epdf/10.1002/sam.10065 (Hämta 2020-11-15)

6.3 Övrigt

FRA (2018) *Årsrapport 2018*