Försvarshögskolan

Cyberepidemiologi

Hur kan utbrottsdetektion inom folkhälsa hjälpa IT-incidentsövervakning?

Försvarshögskolan

Statsvetenskap, inriktning krishantering och säkerhet

Delkurs 3: Uppsats.

Höstterminen 2018

Författarens namn: Andreas Richter

Handledaren: Eva-Karin Olsson

Antal ord: 12 719

Andreas Richter
Kandidatuppsats 15 hp
HT 18

Abstract

This study aims to shed light on what a comparison between cybersecurity intelligence and public health surveillance systems can yield in practical improvements. The issue at hand is best described by the amount of threats both systems must detect. Intelligent malicious software, malware, designed by humans to spread and reap havoc in the abundance of unprotected networks worldwide and contagious diseases with millions of years of evolution behind their design to bypass human defences, infect and multiply. These two threats stand as mighty competitors to actors who try to monitor their presence to be able to give advice on further action to hinder their spread. The sheer amount of experience in public health of dealing with surveillance of contagious disease can contribute with important lessons to cyber intelligence when malware is becoming an even more alarming threat against everybody who uses the Internet.

To compare them both this study uses high reliability theory to understand how Folkhälsomyndigheten, Sweden's main authority in public health surveillance, and CERT-SE, Sweden's national computer emergency response team, operate to make their surveillance as reliable as possible to detect emerging threats. Some key findings of the study points to the lack of regional or global binding policy's to share information in the cyber security sector of which CERT-SE takes part in. The major roll of trust-based information sharing can be subject to shifts in relationships between states and excludes states with which no bilateral arrangements are made, but who may possess information of urgent necessity. The lack of arrangements in the cybersecurity sector, correspondent to the International health regulations by World Health Organization in public health, stands as a major difference between the two sectors access to information. However, this study may not stretch as far as to prove that the greater access to information would have proved to be of ease in a specific cyberincident. Case studies of this kind or further research of how agreements can be made in an anarchistic domain like the Internet are to be continued from this study.

Key words: Cyber, cyber security, cyber intelligence, cyber surveillance, high reliability organisation, high reliability theory, public health, epidemiology, Folkhälsomyndigheten, CERT-SE

Innehåll

1.0 Introduktion

2008 började en ny typ av skadlig kod att spridas över världen. Mark Bowden (2012) beskriver i boken *Viruset* hur Conficker-masken spred sig från maskin till maskin. Efter mindre än en månad efter dess upptäckt var fler än 8 miljoner maskiner infekterade med ytterligare 1,5 miljoner infektioner tillkomna varje dygn (Bowden 2012:128). ”Varje ny maskin som angreps förvandlades till rena spridningsmonstret som snabbt och hungrigt började leta efter nya måltavlor […] De såg hur det strömmade in från Tyskland, Japan, Colombia, Argentina och olika platser runt om i USA. Det var en pandemi” (Bowden, 2012:31). Conficker-masken tycktes bygga ett större nät av förslavade datorer, så kallade botnet, än vad som någonsin tidigare skådats genom dess extrema smittsamhet och förmåga att motarbeta antivirusåtgärder. Med hjälp av botnätet spred den sedan bland annat program som försökte lura användare att betala för falska anti-virus program (The Rendon group, 2011:8). För att stoppa dess spridning organiserade sig flera olika grupper som ofta ovetandes om varandra arbetade för att döda botnätet och finna upphovsmakaren. En av de största kallade sig *Conficker Working Group* och inkluderade Microsoft som ägare av det huvudsakligen drabbade operativsystemet Windows, flera olika antivirus mjukvaruföretag, internetleverantörer och universitet. Amerikanska inrikessäkerhetsdepartementet, *Department of Homeland Security*, publicerade tillsammans med konsultbolaget *The Rendon Group* 2011 en utvärdering som poängterade flera brister i hanteringen av Conficker. De största lärdomarna hänvisade till bristen av samordningen mellan privata och offentliga initiativ, bristande infrastruktur för informationsdelning, ingen samlad strategi för arbetet och inga formella varningssystem som detekterar eller sprider informationen till berörda aktörer (The Rendon Group, 2011:37-41). Dessa lärdomar representerar ett decentraliserat arbetssätt som förlitar sig på fragmenterade lägesbilder.

Flera av dessa utmaningar påminner om utmaningar som det epidemiologiska fältet stod inför under början av 1900-talet när nya sjukdomar utvecklades i trångbodda städer och antalet människor som kunde sprida sjukdomen globalt nådde en kritisk massa (Rice et al, 2010:119). Exempelvis spanska sjukan som spreds 1918 dödade över 50 miljoner människor världen över, vilket är en av de dödligaste pandemierna någonsin (Folkhälsomyndigheten, 2018d). Flera forskare föreslår att folkhälsostrategier borde appliceras på cyberarenan för att minska sårbarheten för intrång och spridandet av skadlig kod likt de som infördes inom smittskyddet under 1900-talet (Rice et al, 2010. Smith III, 2016, Parker & Farkas, 2011). Cyberattacker kan ibland beskrivas i termer som cyberkrigföring vilket nationalstater är de mest aktiva med,

någonting som ligger långt från sanningen. Under 2018 var cirka 80% av de globalt genomförda cyberattackerna av kriminell natur riktade mot offer utan hänvisning till nationalitet vilket därför är ett gemensamt transnationellt hot (Hackmageddon, 2018). På cyberarenan introducerades 317 miljoner nya typer av skadlig kod endast under 2014, vilket innebar att nästan en miljon möjliga hot skapades varje dag (Smith III, 2016:306). Den ökade sårbarheten hos antalet mindre uppkopplade maskiner som inte är datorer eller telefoner, så kallade *internet of things*, sätter svår press på möjligheten för olika aktörer att dela information om sårbarheter mellan varandra och bidrar till explosionen av antalet uppkopplade enheter (Swaling & Johansson, 2018:3). Det är avgörande att det finns en gemensam nationell cybersäkerhetsbild för att kunna avvärja IT-relaterade kriser och detta är en nödvändig kugge i ett modernt krishanteringssystem (MSB, 2012:14). Denna lägesbild tecknas av CERT-SE på uppdrag av Myndigheten för Samhällsskydd och Beredskap, MSB, genom att insamla, samordna och förmedla information om olika typer av skadlig kod för att minska sårbarheten hos myndigheter och företag. Folkhälsomyndigheten har idag ansvar för övervakningen av spridandet av särskilt farliga sjukdomar på nationell nivå i Sverige och tillhandahåller system som kontinuerligt samlar in data, larmar och hjälper epidemiologer att se mönster i spridningen av sjukdomar för att tillsätta rätt åtgärder mot rätt hot.

Både Folkhälsomyndigheten och CERT-SE står inför en liknande utmaning. Hur ska de kunna förbereda sig för ett utbrott av en sjukdom eller skadlig mjukvara som de ännu inte vet existerar? Den amerikanska motsvarigheten till Folkhälsomyndigheten, *Center for Disease Control*, CDC, skrev i en rapport för strategisk hantering av smittsamma sjukdomar 1998 ”*because we do not know what diseases will arise, we must always be prepared for the unexpected*” (Weick & Sutcliffe, 2007:45). Att förberedda sig på det oförutsedda genom att öka möjligheten att upptäcka samt hantera det är något som *high reliability organizations*, HRO:s, är särskilt duktiga på. Den här studiens fokus på detektion kan förklaras med att ju tidigare ett problem eller hot kan upptäckas, desto bättre kan en organisation svara på det. För HRO:s är den stora svårigheten hur länge ett problem existerar, innan det blir synligt som gör att åtgärder kan vidtas (Weick & Sutcliffe, 2007:47). Ju tidigare ett problem kan upptäckas desto fler handlingsalternativ finns för att lösa det, men problemet är också som svårast att upptäcka ju tidigare organisationen söker efter det (Weick & Sutcliffe, 2007:47). Detta kräver flexibla och effektiva detektionssystem som kan upptäcka nya typer av hot.

1.1 Forskningsproblem, syfte och frågeställning

Svenska myndigheter har endast sedan 2016 bedrivit obligatorisk IT-incidentrapportering och MSB bedömer i den nationella risk- och förmågebedömningen 2018 att ”*Förmågan att upptäcka cyberangrepp mot samhällsviktig verksamhet och kritisk infrastruktur behöver öka*” (MSB, 2016b, MSB 2018c). Detta jämfört med den epidemiologiska övervakningen som pågått under organiserad lagstadgad form sedan 1968 i Sverige (Smittskyddslag, 1968:231). Om dessa områden nu metaforiskt kan jämföras med varandra borde det också finnas liknande utmaningar hos de båda som också kan ha gemensamma lösningar. Studiens syfte är därför att undersöka hur metoder inom smittskyddsövervakning kan påverka IT-incidentsövervakningen och hur dessa metoder kan tänkas appliceras, vilket mynnar ut i studiens frågeställning:

Vilka skillnader kan ses mellan Folkhälsomyndighetens utbrottsdetektion och CERT-SE:s nationella IT-incidentsövervakning inom ramarna för *high reliability theory*?

1.2 Avgränsning

Studien kommer att fokusera på organisationernas detektionsförmåga och kommer således inte att behandla andra enheter inom organisationen. Under studien kommer Folkhälsomyndigheten att beskrivas som aktuell organisation trots att avdelningen smittskydd och beredskap är den avdelning som kommer behandlas mest. Studiens resultat kommer hänvisa till principerna inom *high reliability theory*, HRT, på dessa utvalda delar, således inte i organisationen som helhet. CERT-SE är organisatoriskt en del av MSB men har samlat myndighetens detektionsförmåga hos enheten. Avgränsningen gjordes därför att i huvudsak fokusera på CERT-SE som enhet istället för MSB då deras verksamhet kan ses som mer spridd än Folkhälsomyndighetens.

Diskussion kan föras om någon av studiens organisationer är *high reliability organizations*, HRO:s, eller inte. För att kunna göra detta krävs ett betydligt mer omfattande material vilket sträcker sig bortom studiens syfte. En avgränsning har därför gjorts att inte diskutera detta då diskussionens resultat inte anses tillföra något till frågeställningens resultat.

1.3 Bakgrund. Vilka är Folkhälsomyndigheten och CERT-SE?

Folkhälsomyndigheten ansvarar för smittskyddsarbetet på nationell nivå. De ska bland annat förebygga sjukdomsspridning och samordna, följa och utveckla det svenska smittskyddet (SFS

2013:1020). Myndigheten har också som ansvar att vidta åtgärder som kan skydda befolkningen mot smittsamma sjukdomar genom att övervaka smittskyddets beredskap och ständigt analysera det epidemiologiska läget nationellt och internationellt (SFS 2013:1020, SFS 2004:168). Folkhälsomyndigheten är Sveriges internationella kontaktpunkt rörande smittskyddsfrågor som behandlar det internationella hälsoreglementet som beskrivs *i lagen om skydd mot internationella hot mot människors hälsa* (SFS 2006:1570). Det innebär att myndigheten måste rapportera till World Health Organizaton, WHO, inom 24 timmar från att de fattat misstanke om ett hot mot den internationella hälsan i Sverige (SFS 2006:1570). Det internationella hälsoreglementet är ett bindande avtal mellan alla WHO:s 196 medlemsländer (WHO, 2005). För att möjliggöra uppdraget mot den svenska befolkningen och ansvaret mot WHO bedriver Folkhälsomyndigheten omfattande folkhälsoövervakning. Detta sker huvudsakligen genom att särskilt smittsamma sjukdomar måste rapporteras till Folkhälsomyndigheten när de misstänks eller diagnostiseras i vården eller om individer misstänker att de bär på en av de anmälningspliktiga sjukdomarna (SFS 2004:168). De smittsamma sjukdomarna delas in i 26 allmänfarliga och tre samhällsfarliga sjukdomar. De allmänfarliga sjukdomarna inkluderar exempelvis HIV, rabies och tuberkulos medan de samhällsfarliga kan konstateras som de farligaste och mest smittsamma sjukdomarna mot samhället och består av smittkoppor, svår akut respiratorisk sjukdom (SARS) och infektion av ebolavirus. Utöver dessa allmän- och samhällsfarliga sjukdomar tillfaller också flera mindre allvarliga sjukdomar som är anmälningspliktiga (SFS 205:255).

Övervakningen av dessa sjukdomar sker på flera olika enheter inom Folkhälsomyndigheten. Avdelningen för smittskydd och hälsoskydd har det huvudsakliga ansvaret för övervakningen där flera enheter är inblandade i det operativa arbetet (Folkhälsomyndigheten, 2018a). I studien nämns därför hela myndigheten trots att det finns väldigt mycket av verksamheten som inte rör smittskydd och övervakning för att inte exkludera utfört arbete.

CERT-SE är en enhet som tillhör MSB och avdelningen för cybersäkerhet och skydd av samhällsviktig verksamhet. I MSB:s instruktion från regeringen innehar myndigheten ett samlat ansvar för samhällets informationssäkerhet (SFS 2008:1002). I uppdraget ingår att sammanställa rapporter angående svenska myndigheter, kommuner, landsting, företag och organisationers informationssäkerhetsarbete som kontinuerligt ska lämnas till regeringen. Myndigheten ska också enligt 11 b § i dess instruktion ansvara för en operativ funktion som

arbetar för att förebygga och hantera IT-incidenter (SFS 2008:1002). En IT-incident hänvisar här till en händelse som har betydande verkan på en samhällsviktig tjänst eller tillhandahållande av digital tjänsts kontinuitet (SFS 2018:1185). Detta kan exempelvis vara störning av mjuk- eller hårdvara, informationsförlust, angrepp, handhavandefel eller angrepp (MSB, 2016a).

CERT-SE har fyra huvudsakliga uppdrag:
”1. agera skyndsamt vid IT-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i det arbete som krävs för att avhjälpa eller lindra effekter av det inträffade,
2. återrapportera till berörda aktörer i samband med att en IT-incident har rapporterats,
3. samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet, och
4. vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa” (SFS 2008:1002).

CERT-SE är den funktion som är tilldelad ansvar för instruktionen i 11 b §. 2016 infördes obligatorisk IT-incidentrapportering för statliga myndigheter vilket utgjorde det första tvingande mandatet som CERT-SE fick del av (MSB, 2016). Under 2018 implementerades europaparlamentets direktiv om åtgärder för hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, något som också kallas NIS direktivet. Direktivet klargör varje EU-lands ansvar och instruktioner i hur de ska arbeta med cybersäkerhet. I direktivet beskrivs hur varje unionsmedlem ska ha en nationell kontaktpunkt i form av en CERT- , *Computer Emergency Response Team*, eller CSIRT-, *Computer Security Incident Response Team*, enhet med förmåga att ta emot incidentrapporter och samverka med andra unionsmedlemars motsvarande enheter (EU 2016/1148). Direktivet antogs i svensk lag 2018 och beskrivs i *lagen om informationssäkerhet för samhällsviktiga och digitala tjänster* (2018:1175). Lagen innebär att inte bara statliga myndigheter måste rapportera IT-incidenter utan även alla som levererar samhällsviktiga- eller digitala tjänster, det vill säga både offentliga och privata aktörer som bedriver samhällsviktig verksamhet (2018:1175). De rapporter måste aktörer skicka utan onödigt dröjsmål till CERT-SE och dessa rapporter blir då en del av organisationens dataflöde för övervakning. Tillsammans med de obligatoriska rapporterna som organisationer skickar kan även organisationer som inte omfattas av lagen rapportera IT-incidenter frivilligt till CERT-SE (SFS 2018:1175). Den andra delen baseras på flera publika

källor som sammanställer information om olika typer av skadlig kod, exempelvis shadowserver.org, malwarepatrol.net eller autoshun.org. Andra CERT organisationer i samverkansforum som CERT-SE deltar i är likaså en av de primära informationskällorna (CERT-SE, 2012). Informationen sammanställs bland annat i en karta som publiceras på www.cert.se som ger en överblicksbild över antalet infekterade datorer i Sverige och dess geografiska koncentration.

2.0 Teoretiskt ramverk

Nedan kommer forskningsfältet runt HRT att diskuteras med efterföljande forskning om sammansättning av folkhälsa och cybersäkerhet. Sedan kommer HRT att beskrivas med utgångspunkt ur Karl Weick och Kathleen Sutcliffes (2007) bok *Managing the unexpected*. Teorin kommer först att beskrivas i en övergripande form för att sedan gå djupare i dess fem principer, för att slutligen presentera teorins begränsningar.

2.1 Tidigare forskning

Den tidigare forskningen inom fältet har under denna rubrik delats in tre kategorier. Inledningsvis kommer forskningsfältet runt HRT att presenteras för att få en översiktlig teoretisk bild. Sedan presenteras forskning som på olika sätt sätter samman strategier inom folkhälsa och cybersäkerhet på en teoretisk nivå. Slutligen diskuteras tidigare forskning som undersökt praktiska tillvägagångssätt översatt från folkhälsa till cybersäkerhet för att bevisa jämförelsens relevans utöver en teoretisk liknelse.

2.1.1 Organisationsforskning kopplat till pålitlighet

Flera organisationsforskare har undersökt större olyckor och misslyckanden och ställt sig frågan, varför är det så svårt att bygga 100% säkra system som är vattentäta mot alla typer av missöden? Charles Perrow var en av de första stora organisationsforskarna som försökte besvara frågan genom att studera komplexa organisationer. I synnerhet studerades kärnkraftverk, och hans slutsatser vilade på att olyckor är oundvikliga i organisationer som förlitar sig på komplicerade system som är tätt integrerade med varandra (Perrow, 1999). Detta kom senare att mynna ut i teorin *Normal accident theory* som poängterar att allting kan misslyckas. Ingenting kan konstrueras med perfekt pålitlighet och att olyckor sker är något som måste accepteras i komplicerade miljöer (Perrow, 2007:261). Som svar på Perrows

resonemang undersöktes organisationer som tycktes ha nästintill felfri verksamhet för att förklara varför vissa organisationer klarar sig bättre från dessa ”normala olyckor” än andra. Dessa organisationer kom att kallas *high reliability organisations,* HRO:s.

Forskningen av HRO:s tar ofta sitt avstamp i tre studier utförda i USA på ett kärnkraftverk, ett hangarfartyg och på flera olika kontrolltorn för flygtrafik (Weick et al, 2008:32). Forskningen baseras på deskriptiva fältstudier om hur dessa organisationer undviker misslyckanden och bibehåller en hög tillförlitlighet i sin produktion. Weick et al (2008) beskriver en stor del av forskningen runt HRO:s och dess konceptuella bakgrund i artikeln *Organizing for high reliability: Processes of collective mindfullnes.* Där beskrivs också fler fallstudier där organisationer undersökts ur ett HRO perspektiv. Några av de som nämns är kärnkraftverket Three Mile Island och dess havererande kärnreaktor som nästan orsakade en härdsmälta, rymdfärjan Challenger och dess katastrofala explosion som dödade sju astronauter samt kollisionen av två flygplan på flygplatsen i Teneriffa som är den flygolycka med flest omkomna i historien (Weick et al, 2008:32). Ingen tidigare forskning där HRT är applicerad på Folkhälsomyndigheten eller dess amerikanska motsvarighet CDC kan hittas av författaren. Flera studier av HRT inom sjukvården har gjorts med betoning på akutsjukvårdsteam och för att minska antalet infektioner efter nålstickningar men inget som författaren av den här studien kan koppla till utbrottsdetektion (Pronovost et al, 2005 & Baker et al, 2006). Trots att Weick och Sutcliffe (2007:44-45) nämner CDC explicit finns ingen forskning om CDC som en HRO vad den här studien kan finna. Inte heller finner författaren bakom denna studie forskning på CERT-team inom ramen för HRT. Detta kan dock inte ses som ett problem då meningen med HRT är att se gemensamma drag i vilt skilda organisationer, så länge de fyller i de kriterier som beskrivs under avsnittet 2.2 teori. Två av de kriterierna beskriver faktumet att organisationen måste verka under komplicerade förhållanden och i en oförlåtande miljö. Detta möjliggör en bred tolkning för vilka organisationer som kan vara en HRO. Med detta sagt diskuteras nedan en artikel som applicerar HRT på en organisationen som inte riktigt kan ses som en stereotyp HRO men ändå lyckas använda dess principer för att göra verksamheten mer pålitlig.

Ciravegna och Brenes (2016) argumenterar för att HRT även kan appliceras inom handeln för att göra företag mer konkurrenskraftiga. Ett exempel på detta är en matvarukedja i El Salvador som stod inför att bli utkonkurrerad av en större amerikansk matvarukedja som skulle etablera

sig på marknaden. Genom att investera tid, resurser och energi i att skapa en organisation som prioriterar kontinuitet, tar tillvara på misslyckanden som en lärande resurs samt investerar i spelrum istället för minutprecisa leveranser av varor kunde kedjan bättre hantera oförutsägbara händelser som naturkatastrofer och marknadsfluktuationer (Ciravegna & Brenes, 2016:4500). Resultatet visade att El Salvador var det enda land i Centralamerika där den amerikanska matvarukedjan inte lyckades vinna en majoritet av marknaden (Ciravegna & Brenes, 2016:4505). Artikeln är relevant för denna studie för att argumentera mot kritik som kan väckas mot att Folkhälsomyndigheten eller CERT-SE inte verkar under tillräckligt pressade förhållanden för att kunna applicera principer likt HRO:s.

2.1.2 Sammansättning av folkhälsa och cybersäkerhet

Att applicera olika metaforer eller analogier på cybersäkerhetsområdet för att inspirera till nya lösningar och perspektiv är ingenting nytt. 2008 anordnade Sandia National Labratories en workshop med namnet ”CyberFest” där målet var att finna nya cybersäkerhetslösningar och koncept med hjälp av inspiration från andra fält (Karas et al, 2008:3). Resultatet blev rapporten *Metaphors for Cyber security* där flertalet olika metaforer applicerade på cybersäkerhetsområdet och diskuterades. Deltagarna motiverade användandet av metaforer på cybersäkerhetsområdet som någonting hjälpsamt då området är abstrakt och tämligen nytt (Karas et al, 2008:10). Några av de metaforer som nämns är att se cyberarenan med biologiska ögon och jämföra det med ett stort ekosystem av flera beroende småsystem i en biologisk mångfald (Karas et al, 2008:18). Jämförelsen gav idén till överföring av biologisk programmerad celldöd till cyberarenan där infekterade datorer själva kopplar bort sig från nätverk då de upptäcker skadlig kod. En annan metafor som diskuterades var att se internet som ett fysiskt utrymme, ofta det som kallas cyberrymden eller *cyberspace*. Amerikanska *Air force Cyber Command* beskriver cyberrymden som en domän, likt land, sjö och luft som måste försvaras (Karas et al, 2008: 20). Att se cyber som ett utrymme kan också ge lösningar som har att göra med hur stater kan lyckas förhandla om ansvar och reglering i ett område som ingen ensam stat äger. Tom Ridout (2017) ger förslag i artikeln *Developing an international cyberspace governance framework: comparisons to outer space* hur länder under rymdkapplöpningen reglerade den faktiska rymden ovanför jorden och föreslår att liknande avtal på samma sätt bör ingås angående cyberrymden.

En av de metaforer som rapporten diskuterar mest grundligt är dock den författarna kallar ”*cyber wellnes*” (Karas et al, 2008:30). Detta synsätt betonar det individuella ansvaret hos internetanvändare att själva ansvara för de vardagliga IT-relaterade hoten med hjälp av god ”cyberhygiene”. Skadlig mjukvara ses som en typ av sjukdom som kan bekämpas med samma typ av system som vi bekämpar smittsamma sjukdomar. Rapporten föreslår därför, att det likt på hälsovårdssidan, borde ingå samma typ av hälsoövervakning av användare på internet som det görs i många länder av myndigheter ansvariga för smittskydd och folkhälsa. En rekommendation är därför att de nationella CERT organisationerna ges större befogenheter att insamla information för att sammanställa lägesbilder över IT-incidenter då de bättre kan varna och motverka konsekvenserna av skadlig mjukvara (Karas et al, 2008: 32).

En av de mest utomvetenskapligt inflytelserika rapporterna heter *The internet health model for cybersecurity* och är ett samarbete mellan fler än 20 författare från privata mjukvaruföretag, universitet, telekombolag och nationella CERT-grupper (Sullivan, 2012). Rapporten beskriver på en abstrakt nivå skillnader och likheter mellan cybersäkerhetsarenan och arbete för en bättre folkhälsa. Det huvudsakliga problemet som rapporten behandlar är att inom cybersäkerheten finns ingen global aktör som har ansvar för att skydda eller koordinera insatser för att minska risken att människor och system utsätts för skadlig kod (Sullivan, 2012:9). Rapporten väljer att benämna detta som internetets hälsa. ”*For the internet health model to be successful, necessary monitoring activities must be matched with approproate controls*” (Sullivan, 2012: 16)

För att utforska hur en sådan aktör eller system skulle kunna se ut hämtar rapporten inspiration från WHO som har ett globalt hälsoansvar (Sullivan: 10). Utan att använda WHO som en fullständig ritning kan huvuddragen översättas och användas inom cybersäkerhet. Argumentet för detta vilar huvudsakligen på att internet och cyberrymden är ett offentligt utrymme. Om internet innehåller så lite skadlig kod som möjligt och är så säkert som möjligt hjälper det hela jordens befolkning, därav betoningen på en global aktör (Sullivan, 2012:14). Rapporten tar upp två huvudsakliga problem med hälsomodellen applicerad på internet. För det första förlitar sig flera nationella och globala folkhälsoaktörer på en jämn datatrafik om diagnoser för att kunna sätta insatser mot sjukdomar vilket kräver ett omfattande övervakningssystem. Som patient inom sjukvården har vi generellt sett lättare att acceptera insamlande av information av en auktoritet än vad vi har som en användare av internet. Global övervakning klingar därför mer negativt inom cybersäkerhet än vad det gör inom hälsovården (Sullivan, 2012:12). Det andra

problemet med jämförelsen behandlar verktyget karantän som sjukvården har tillgång till. Karantän kan användas för att både avskilja de sjuka från befolkningen men också genom att avskilja de friska från en sjuk befolkning. Detta är ett oerhört kraftfullt verktyg som en global aktör inom cybersäkerhet kan behöva ha tillgång till för att effektivt förhindra spridning av skadlig kod. Båda dessa problem är identifierade som integritetskränkande och kan förhindra att en struktur inom global cybersäkerhet kan direktöversättas från sjukvården (Sullivan, 2012:12). Ett i första hand paradoxalt argument är hur övervakning som leder till ett mer hälsosamt internet kommer skydda dess användares integritet från kriminellas möjlighet att insamla dyrbar data med hjälp av skadlig kod (Sullivan, 2012:15).

Frank Smith III (2016) håller inte med om att informationsinsamlingen inom cybersäkerhet nödvändigtvis måste innebära integritetskränkande åtgärder. Urskillningslös insamling av metadata från en befolkning, liknande de program som *National security agency*, NSA, avslöjades iscensätta, skiljer sig från att med samtycke dela med sig av information om specifika system eller om en IT-incident. Detta är på samma sätt som att insamlandet av sjukdomsdata inte kan tolkas som spioneri av sjukvårdsmyndigheterna (Smith III, 2016:307). Smith III (2016) ser hur framväxten av epidemiologiska och cybersäkerhets-övervakningssystem har olika grogrund, då insamlandet av sjukdomsdata främst startade i offentlig sektor och de första cybersäkerhetsaktörerna startades i den privata sektorn. Detta är relevant då det kan förklara skillnaden i mandat för de båda. Myndigheter inom offentlig sektor har mandat att utföra en uppgift med tillhörande verktyg, ett privat företag har ofta inte samma tydliga mandat att utföra en liknanden uppgift (Smith III, 2016:309). Smith III (2016) påvisar detta genom att referera till det presidentiella dikretet, PDD-63, som USA:s president Bill Clinton skrev under 1998. Dekretet manar till den privata sektorn att starta en liknande organisation som CDC, *Center for Disease Controll and prevention*, fast för cybersäkerhet som bygger på frivilligt deltagande. Utan något tydligt mandat om vad denna organisation skulle kunna göra stannade förslaget till att bli ett flertal olika samverkansforum, liknande de som redan fanns inom varje bransch och de bidrog därför med föga mycket (Smith III, 2016:309). På liknande sätt beskrivs internationella samarbeten inom cybersäkerhet som tandlösa då de inte innefattar några mandat att vidta åtgärder. WHO beskrivs som effektfull då organisationen grundar sig på internationell lag som tydliggör medlemmarnas rättigheter och skyldigheter inom sjukdomsövervakning samt att de kan straffa de länder som inte lyder det internationella hälsoreglementet (Smith III, 2016:310). Motsvarande samarbete inom cybersäkerhet lyser med

sin frånvaro. De globala samarbetsorganisationer som kan jämföras med WHO är antingen FIRST, *Forum of Incident Response and Security Teams*, som är ett frivilligt samarbetsforum för cybersäkerhetsfrågor eller IMPACT, International Multilateral Partnership Against Cyber Crime, som är en del av FN organet ITU, *International Telecommunication Union*, men som också saknar mandat eller tunga medlemmar som USA, Ryssland, Storbritannien, Tyskland, Frankrike, Australien och Japan (Smith III, 2016:310. IMPACT, 2012).

2.1.3 Epidemiologisk metod applicerad på cybersäkerhetsområdet

Till skillnad från artiklar nämnda ovan skiljer sig följande två artiklar från dem då de applicerar epidemiologiska metoder på cyberarenan. Tidigare nämnd forskning etablerar jämförelsen mellan folkhälsa och cybersäkerhet som relevant på systemnivå. Dessa två studier visar att jämförelsen är relevant också på lägre praktisk nivå. David Parker och Csilla Farkas (2011) använder SEIR-, *Susceptible, Exposed, Infectious, Recovered*, modellen, som används inom flera epidemiologiska utbrottsdetektionssystem, för att bedöma risken av lyckade cyberattacker och för att mer effektivt rikta offentliga medel för att försvara sig mot dem. Genom att översätta de medicinska faserna hos SEIR-modellen till cyberarenan kunde Parker och Farkas se att ett liknande utbrottsdetektionssystem kunde konstrueras och effektivt beräkna riskerna för spridning av skadlig mjukvara (Parker & Farkas, 2011:36). I sitt exempel använder de sig av en biologisk blodbärande smitta samt en mask av skadlig mjukvara som reproducerar sig själv för att se hur SEIR-modellen kan översättas inom cybersäkerhet (Parker & Farkas, 2011: 33). Resultatet visar att en översättning är möjlig och att modellen väl kan appliceras på cybersäkerhetsarenan för att bedöma risker med olika typer av cybervirus (Park & Farkas 2011:36). Deras forskning utmynnade i ett förslag till ett cyberövervakningssystem som baseras på epidemiologiska övervakningssystem kallat *Cyber Security Surveillance System* (Brantly, 2017:95). Aron Brantly (2017) fortsätter på Park och Farkas (2011) forskning genom att titta närmare på hur detta cyberövervakningssystem skulle stämma överens med WHO:s riktlinjer för effektiva epidemiologiska övervakningssystem (Brantly, 2017:95). Riktlinjerna riktar sig till de sex huvudsakliga funktioner som övervakningssystem bör ha.

- Detektion och varning om hälsohändelser.
- Insamling och befästande av relevant data.
- Undersökande och bekräftande av fall eller utbrott.
- Rutinmässig analys och författande av rapporter.
- Feedback av information till de som delger datan.

- Feedforward av information till högre beslutande nivåer.

Brantly (2017) tror att dessa riktlinjer även går att applicera som ett ramverk för nationella eller globala cybersäkerhetövervakningssystem. Nuvarande system som är på plats är enligt Brantly (2017:96) för fragmenterade mellan olika organisationer, geografiska områden och styrda av olika lagstiftningar och regleringar. Det finns inget övergripande system för att skapa överblick och etablera lägesbilder varken nationellt eller globalt vilket gör att även om de system som är på plats idag är effektiva så finns ingen tillräcklig samverkan mellan dem för att knyta ihop deras aktuella lägesbilder (2017:96).

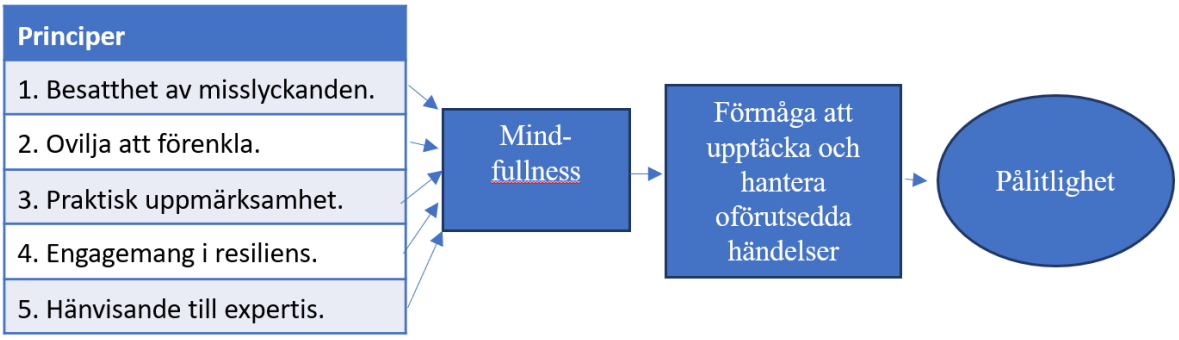
Denna studie ämnar fylla en kunskapslucka i forskningsfältet som beskrivits ovan. Genom att utöka empirin av HRT undersöks två svenska organisationer som inte tidigare undersökts med med hjälp av teorin. Studien ämnar också bygga vidare på forskning som genomförts på anammande av folkhälsostrategier inom cybersäkerhet, detta på en empirisk nivå som kan komma att öka relevansen av användandet av metaforen.

2.2 Teori, High reliability theory

High reliability theory (HRT) behandlar den brinnande frågan som är på många organisationers läppar, hur kan vi fortsätta producera vår produkt tillförlitligt även under störda förhållanden eller i en komplex miljö? Produkten som produceras kan vara flygstarter från ett hangarfartyg, el från ett kärnkraftverk eller säkra landningar med minutprecision på en större internationell flygplats för att nämna några exempel (Weick, Sutcliffe & Obstfeld, 2008:32). Det som dessa producenter har gemensamt är att de befinner sig i en oförlåtande riskfylld miljö där misslyckanden står dem dyrt i människoliv, ekonomiska medel eller politiskt förtroende och att misslyckanden inte *får* hända. Ursprunget till teorin kopplas till den fascination som väcktes av undran hur dessa tre organisationer nämnda ovan kunde operera nästintill felfritt trots den uppsjö av friktioner och möjliga felkällor som presenterade sig. En veteran från den amerikanska flottan beskriver däcket på ett hangarfartyg som en av de farligaste platserna på jorden. Flygplan startar och landar samtidigt, de tankas och laddas med motorerna på, vatten och olja sköljer över från havsgången, radarhjälpmedel används till ett minimum för att undgå upptäckt och allt hanteras av tjugoåringar medan en fiende aktivt försöker döda dem (Weick & Sutcliffe, 2007:24). Hur arbetar en organisation som hanterar dessa risker för att minimera

olyckor och ändå säkerställa sin funktion? Svaret visade sig vara väldigt likt mellan organisationerna trots skillnaden i deras arbetsfält (Weick, Sutcliffe & Obstfeld, 2008:32).

Den särskilda hotmiljön och kravet på att aldrig misslyckas gör att dessa organisationer måste vidta särskilda åtgärder för att tillförlitligt kunna prestera även under svåra förhållanden. Dessa organisationer kallas för *high reliability organizations* (HRO) och särskiljer sig på flera punkter från andra organisationer (Weick, Sutcliffe & Obstfeld, 2008:32). HRO:s prioriterar säkerhet högt på strategisk nivå, de är redundanta, de strävar efter decentraliserat beslutsfattande, de har en organisationskultur av att agera på olyckor samt övar ofta på eventuella scenarion (Weick, Sutcliffe & Obstfeld, 2008: 33). De många olika åtgärder och processer som dessa HRO:s ägnar sig åt kan delas in i fem olika principer. Tre första principerna hanterar hur en HRO kan bli bättre på att förvänta sig det oförutsägbara och förhindra det. De två resterande principerna beskriver hur en HRO kan hantera situationen om händelsen är ett faktum (Weick & Sutcliffe, 2007:44, 65). Dessa totalt fem principer gör en organisation medveten om sig själv och sin verksamhet på ett sätt som författarna Weick och Sutcliffe (2007) kallar ”*mindfull*”. Denna självmedvetenhet leder till ökad förmåga att upptäcka och hantera oförutsägbara händelser, vilket leder till ökad tillförlitlighet och pålitlighet. Se figur 1.



Figur 1. (Weick, Sutcliffe & Obstfeld, 2008:37)

Nedanför kommer de fem principerna samt deras två huvudkategorier mer utförligt att beskrivas under vardera rubrik.

2.2.1 Anticipation. Att förutse det oförutsägbara

De tre första principerna delar Weick och Sutcliffe (2007) in i en kategori de kallar *anticipation*, eller förväntning. De beskriver vad de menar med förväntning som ”*To anticipate is to foresee or imagine an eventual unchecked outcome, based on small disparities… Anticipation,*

however, is not just an exercise in sensing; it is also an exercise in stopping the development of undesirable events" (Weick & Sutcliffe, 2007:45). HRO:s förväntar eventuella utfall mycket bättre än andra organisationer genom att de mer lyhört uppfattar svaga signaler från verksamheten om en kommande händelse, som också gör dem bättre förberedda att hantera den (Weick & Sutcliffe, 2007:45). Weick och Sutcliffe (2007) besvarar också den givna kritiken, att ingenting går att säkert förutse då de möjliga utfallen är alltför många och mängden svaga signaler kan vara överväldigande, genom att HRO:s inte avser att "se in i framtiden". Genom att aktivt arbeta med att identifiera möjliga utfall har de en kortare startsträcka än andra organisationer när de väl upptäcker det oönskade scenariot eller då olyckan slår till. Hos organisationer som utför detta väl har Weick och Sutcliffe (2007) identifierat tre principer som nedan förklaras.

2.2.2 Princip 1: Besatthet av misslyckande

Weick och Sutcliffe (2007:46-52) beskriver den första principen som förmåga att detektera små signaler som kan förvarna om ett större ankommande fel, förmåga att sedan detektera det huvudsakliga felet samt att felet rapporteras korrekt och inte mörkas av personalen med rädsla för reprimander. Med fel menar författarna här en oönskad händelse. Det kan alltså vara både ett mänskligt misstag som får allvarliga konsekvenser, system som oavsiktligt kraschar eller antagonistiska hot som utsätter organisationen för påfrestningar. Åtgärder som HRO:s använder för att arbeta med misslyckanden är exempelvis att implementera avvikelsehanteringssystem samt säkerställa att personalen använder dessa (Weick & Sutcliffe, 2007:47-51).

2.2.3 Princip 2: Ovilja att förenkla

I alla komplicerade miljöer finns en vilja att förenkla för att få begripligare lägesbilder. Det är omöjligt att till viss del undvika att förenkla då en helhetsbild ska presenteras eller databaser ska bildas (Weick & Sutcliffe, 2007:55). I förenklingen försvinner dock också nyanser, kontext och världsbild (Weick & Sutcliffe, 2007:53). En mer detaljrik beskrivning, utrymme för ifrågasättande och en förmåga att problematisera ger en större möjlighet att se händelsers konsekvenser och möjliga signaler som antyder på fel kan lättare detekteras. För att förhindra att förenkling sker föreslår Weick och Sutcliffe (2007:56) att flera olika människor ska delta i problemformuleringen när ett problem ska förstås för att inkludera olika perspektiv och nyanser som kan bidra med en komplex beskrivning. Förutom antalet människor bör också de som

deltar i interaktionen besitta olika sorters expertis interdisciplinärt för att möjliggöra en så nyanserad bild som möjligt. ”*Teams composed of at least some individuals with different expertise are better able to grasp variations in their enviroments and to see specific changes that need to be made*” (Weick & Sutcliffe, 2007:56). Den blandade kompetensen är något som Weick och Sutcliffe (2007) betonar som avgörande för att undvika förenkling.

2.2.4 Princip 3: Praktisk uppmärksamhet.

Weick och Sutcliffe (2007:59) skriver om ”*sensitivity to operations*” när de poängterar betydelsen av uppmärksamhet mot organisationens huvudverksamhet, det som i denna studie beskrivs som praktisk uppmärksamhet. De beskriver hur fokuset huvudsakligen ska vara vid ”frontlinjen”, det vill säga mot organisationens kärnverksamhet för att där kunna upptäcka fel eller förbättra pågående arbete. Det som kan försvåra förmågan till praktisk uppmärksamhet är prioritering av kunskap, rutiner som blir tanklösa och utvärdering av nära misslyckande som en framgång (Weick & Sutcliffe, 2007:60-61). För att behålla denna uppmärksamhet kan flera paralleller dras till Mica Endsleys koncept om *situational awarness,* det vill säga förmåga att uppfatta pågående skeenden i komplicerade situationer (Weick et al, 2008:44). Men hos HRO:s är den pågående verksamheten för komplicerad för att en individ ska kunna inneha hela bilden av vad som pågår; den kognitiva förmågan hos människan räcker inte. Praktisk uppmärksamhet hos HRO:s beskriver därför mer organisationens förmåga att uppfatta situationen än individers förmåga vilket gör att begreppet innefattar en mer dynamisk och ständigt pågående förståelse för verksamheten (Weick et al, 2008: 45). Den praktiska uppmärksamheten hänvisar till organisationens kollektiva kunskap och förmåga att omsätta denna för att förstå pågående verksamhet. I denna studie kommer denna princip stark kopplas till de studerade organisationernas tillgång till information som kopplas till kärnverksamheten övervakning.

2.2.5 Containment: Om det ändå händer, hur ska det hanteras?

Om tidigare principer inte hjälper organisationen att förutse en negativ händelse är de resterande två principerna hängivna till hur en händelse kan hanteras och hur konsekvenserna kan begränsas. Weick och Sutcliffe (2007:65) har sett att HRO:s utmärker sig från andra organisationer i två huvudsakliga områden, hängivet engagemang i resiliens samt hänvisning till expertis i beslutsfattande (Weick & Sutcliffe, 2007:65).

2.2.6 Princip 4. Engagemang i resiliens.

För en HRO är resiliens avgörande för att kunna ha en pålitlig verksamhet. För att definiera resiliens har Weick och Sutcliffe använt Brad Allenby och Jonathan Finks definition från 2005, som beskriver att resiliens är ”*capability of a system to maintain its function and structure in the face of internal and external changes and to degrade gracefully when it must*” (Weick & Sutcliffe, 2007:69). I begreppet resiliens infinner sig tre huvudsakliga egenskaper. Först ska en resilient organisation kunna absorbera en motsättning och kvarhålla en övergripande systemfunktion även fast den drabbas av en överraskande händelse. För det andra ska en resilient organisation också under påfrestning tänjas för att sedan ”studsa tillbaka” för att återfå sin tidigare form efter att påfrestningen är över. För det tredje ska en resilient organisation ha förmågan att lära sig och anpassa sig efter en påfrestning eller förändrad miljö (Weick & Sutcliffe, 2007: 71).

2.2.7 Princip 5. Hänvisande till expertis.

Den sista principen som utmärker en HRO är den konstanta hänvisningen av beslut till där kunskapen och expertisen finns. Detta innebär att för snabba beslut ska kunna fattas måste också de som är närmast händelsens centrum ha befogenhet att fatta dem (Weick & Sutcliffe, 2007:74). För att detta ska vara möjligt måste ibland hierarkiska strukturer åsidosättas då inte alltid tjänstens hierarkiska befattning och dess expertis inom området korrelerar. Den som vet bäst ska ta beslut, oavsett hierarki (Weick & Sutcliffe, 2007:73-21, Weick et al, 1999:48-50).

2.2.8 Kritik mot HRT och teorins begränsningar.

LaPorte och Consolini (1991) lämnar värdefull kritik och insikt mot HRT genom sin artikel *Working in practice but not in theory: Theoretical challenges of ”high reliability organizations*”. De driver tesen att det är väldigt svårt att veta vad exakt det är som gör att organisationer som kan ses som HRO:s presterar bättre än andra organisationer. Många studier visar att HRO:s har gemensamma drag men att det är dessa drag som är det som leder till tillförlitlighet och pålitlighet är desto svårare att utröna (LaPorte & Consolini, 1991:43). Argumenten som LaPorte och Consolini presenterar visar att HRO:s angreppsätt inte skiljer sig nämnvärt från andra ramverk inom organisationsteori för att ordna pålitliga organisationer (LaPorte & Consolini, 1991:43). Likt titeln i artikeln beskriver de att det empiriska underlaget är väl efterforskat men att teorin saknar teoretiskt djup som särskiljer den från andra konkurrerande teorier. En annan invändning är att de huvudsakliga organisationerna som undersöktes hade råd att bygga redundanta system då de förfogar över nästintill gränslöst med

resurser (LaPorte & Consolini, 1991: 23). Med gränslösa resurser kan en oförmåga att bygga tillförlitliga system istället vara förvånande. Ett motargument mot detta kan vara att även organisationer som inte behöver oroa sig för konkurrens och vars verksamhet ses så vital att de har till synes oändligt med resurser fortfarande konkurrerar mot sig själva och egna uppsatta mål. Ineffektiva organisationer som trasserar budgetar kommer fortfarande att dömas hårt oavsett om uppdragsgivaren är aktieägare eller staten.

Intressanta invändningar lyfts också från teoretiker inom *normal accident theory*. Kritik lyfts mot svårigheten att etablera förtroende och pålitliga vägar för medarbetare att rapporter fel inom organisationen, då komplicerade sociala och politiska faktorer korrumperar möjligheten att göra detta ärligt. Det är därför i princip omöjligt att etablera helt säkra visselblåsningssystem för organisationens medarbetare som HRO:s till stor del förlitar sig på (Weick et al, 2008:33). En andra invändning är också paradoxen med att bygga redundanta system för ökad tillförlitlighet. Enligt *normal accident theory* är olyckor omöjliga att undvika i komplicerade miljöer, därför innebär utbyggnaden av parallella system för att öka redundansen en ökad komplexitet, vilket paradoxalt också ökar risken för att olyckor sker (Weick et al, 2008:33).

3.0 Tillvägagångssätt

Nedan kommer studiens tillvägagångssätt att presenteras. Den valda metoden kommer presenteras tillsammans med en kort beskrivning av materialet som analyserats.

3.1 Metod

Den metod som har valts för att söka efter svar till frågeställningen baseras på kvalitativ textanalys av offentliga dokument och två intervjuer med representanter från Folkhälsomyndigheten och CERT-SE.

Den kvalitativa textanalysen av tillgängliga dokument passar väl för att besvara studiens något pragmatiska frågeställning. De frågor som ställs till materialet är främst av en utredande art där undersökning efter specifika förmågor ställs. Det material som analyseras fokuseras därför runt de beskrivningar som de valda aktörerna ger om sin verksamhet hänvisat till kriterier om god källkritisk kvalitét angående autenticitet, trovärdighet, representativitet och meningsfullhet (Bryman, 2008:489). Relevant kritik mot materialet är att då aktörerna själva beskriver sin

verksamhet finns det en chans att informationen förskönas för att verksamheten ska ses i bättre dager eller att verksamhet som finns på pappret beskrivs, och inte den som faktiskt är aktuell. Detta kan bemötas genom att analysera utomstående utredningar av verksamheten för att säkerställa materialets trovärdighet. Offentliga utredningar från externa aktörer kopplat till organisationernas detektionsförmåga kan av studiens begränsade möjligheter inte hittas. En annan metod vore att delta i verksamheten som bedrivs och analysera den som observatör, något som tillämpas i flera studier relaterat till HRT. Deltagande observation används genom att undersöka en grupp eller miljö för att närvara, intervjua, uppleva och observera under en längre tid (Bryman, 2008:378). Metoden är tidskrävande och kräver att efterforskaren observerar föremålet för undersökning under en längre tid. I tidsomfånget som en kandidatuppsats lämnar är en god studie utförd med deltagande observation som metod olämplig. Det finns möjlighet att genomföra mikro-etnografiska studier där inbäddningen endast är ett par veckor till en månad, vilket skulle kunna vara möjligt för att genomföra denna studie (Bryman, 2008: 379). Dock vilar studiens syfte på en komparativ grund och skulle således kräva att två mikro-etnografiska studier skulle behöva genomföras vilket är utanför tidsramarna för vad denna studie kan behandla. De brister som materialet kan ha får därför kontrolleras mellan de offentliga dokumenten om verksamheten som finns tillgängliga och den information som lämnas vid intervjutillfällena, vilka är tillfredställande nog för att kunna finna resultat till studiens frågeställning.

Sökningar efter dokument skedde till största del på internet med hjälp av tillgängliga sökmotorer samt i särskild benämning sökmotorn Google Scholar för att finna artiklar rörande tidigare forskning. Både Folkhälsomyndigheten och CERT-SE har egna sökfunktioner på sina hemsidor där offentligt material kan hämtas. Den huvudsakliga inhämtningen kan därför beskrivas som internetbaserad vilket kan ses som kutym inom modern forskning. Detta i stark kontrast till det något gammalmodiga citatet från Alan Bryman ”*I och med att internet är en förhållandevis ny företeelse är detta ett område som ännu inte använts särskilt mycket av samhällsvetarna*” (Bryman, 2008:499).

Två kortare intervjuer genomfördes med en vardera representant från Folkhälsomyndigheten och CERT-SE. Intervjuerna baserades på Alan Brymans (2008) kapitel om kvalitativa intervjuer. Den form som valdes för dessa två intervjuer är den semistrukturerade. Denna form skiljer sig från den strukturerade på det sättet att den är mer flexibel och öppnar upp för

följdfrågor till skillnad från den strukturerade som behåller samma frågor till alla respondenter (Bryman, 2008:413). I intervjuerna baserades de huvudsakliga frågorna runt de fem principer som beskrivs av Weick och Sutcliffe (2007) med möjlighet till utveckling i det utrymme som följdfrågorna lämnar. Huvudfrågorna var därför desamma hos båda intervjutillfällena med skillnad i vad följdfrågorna kretsade kring, i enlighet med konstruktion av en semistrukturerad intervju (Weick & Sutcliffe, 2007:415). Syftet med intervjuerna var att få svar om inbördes förhållanden inom organisationerna som kan vara svåra att utläsa i offentliga dokument. Ett andra syfte rörde också de eventuella åsikter som de båda parterna kunde ha angående studiens frågeställning för att förankra studien hos verksamma personer i varder fält. Ambitionsnivån på dessa intervjuer kan konstateras som lägre än de studier som har sitt huvudsakliga material från intervjuer. Det huvudsakliga materialet bedöms vara offentliga dokument men intervjuerna kan ge ledtrådar om vad som inte får missas eller insikter som annars skulle vara svåra för författaren själv att finna.

3.2 Material

Materialet som rör CERT-SE kommer primärt att hämtas från MSB:s publikationer samt EU. 2016/1148, eller NIS-direktivet, som utförligt beskriver CERT/CSIRT verksamhet. Materialet som rör Folkhälsomyndigheten kommer primärt hämtas från Folkhälsomyndigheten, dess instruktion från regeringen samt Smittskyddslagen 2004:168 som beskriver smittskyddets huvudsakliga lagutrymme.

Två intervjuer har genomförts med en från vardera organisations ledande representant:

- Robert Jonsson, biträdande chef på CERT-SE. Intervjun genomfördes på MSB:s kontor på Fleminggatan 14 Stockholm, torsdag den 13 december 2018.

- Annette Richardsson, enhetschef på enheten för beredskap och krishantering på Folkhälsomyndigheten. Intervjun genomfördes på Folkhälsomyndighetens kontor på Nobels väg 18 Solna, den 17 december 2018.

Då mängden tillgänglig information om Folkhälsomyndighetens övervakning i större grad är offentlig än CERT-SE:s arbete kommer analysen kopplad till CERT-SE vara mer beroende av intervjun som fördes med dess representant. Om kunskap om detta hade framkommit tidigare

hade den intervjun varit djupare och förts med flera respondenter för att öka tillgängligt material att analysera. Mängden material som är tillgängligt i denna studie är av tillräcklig mängd för att tillfredsställa frågeställningen men en större mängd material hade gett studien ett större analytiskt djup.

4.0 Resultat och analys

Nedan presenteras fynd uppdelade under vardera princip och sedan under vardera aktör. Resultaten presenteras sammanvävda med analys löpande i texten. Avslutningsvis följer en sammanfattning av resultatet med påföljande analys.

4.1 Hur arbetar Folkhälsomyndigheten och CERT-SE med misslyckanden?

4.1.1 Folkhälsomyndigheten

I arbetet med misslyckanden eller nära misslyckanden borde organisationen ha ett system för att rapportera brister. Folkhälsomyndigheten har ett avvikelsehanteringssystem där både arbetsmiljö och verksamhetsrelaterade rapporter hanteras (Richardsson, intervju 2018). En avvikelse kan vara en oavsiktlig händelse som kan ha påverkat eller påverkade verksamheten i negativ benämning. Richardsson uppmuntrar sin personal att anmäla alla typer av avvikelser oavsett vad det rör. Hon betonar också vikten av att inte bara systemet för rapportering finns på plats utan att även informationen tas på allvar hos personer i ledande befattningar (Richardsson, intervju, 2018). Att ett system för hantering av avvikelser finns och att informationen tas tillvara på hos ledningen är en nyckelfaktor hos HRO:s (Weick & Sutcliffe, 2008:50). Folkhälsomyndigheten ansvarar för det enda nordiska laboratorium med den högsta säkerhetsklassningen som möjliggör undersökning av de farligaste och mest smittsamma sjukdomarna (Folkhälsomyndigheten, 2013). För att möta de internationella säkerhetsföreskrifter som tillåter laboratoriet att vara verksamt måste ett avvikelsehanteringssystem vara kopplat till det, vilket också möjliggör att andra delar inom verksamheten kan ta del av samma system (Folkhälsomyndigheten, 2017a. Richardsson, intervju 2018).

I myndighetens instruktion står det explicit att verksamheten ska stå på en vetenskaplig grund och att myndigheten själv ska bedriva den forskning som krävs för att myndigheten ska kunna lösa sitt uppdrag på smittskyddsområdet (SFS 2013:1020). Detta innebär att myndigheten

utvärderar egna metoder och utvecklar vetenskapliga lösningar för verksamheten vilket kan uppmuntra till ett klimat som stimulerar till diskussion om vad som fungerar och vad som behöver förbättras (Weick & Sutcliffe, 2008:51).

Enligt förordning 2006:942 om krisberedskap och höjd beredskap ska Folkhälsomyndigheten lämna in regelbundna sårbarhets- och riskanalyser till MSB. Denna analys ska identifiera hot eller risker inom myndighetens verksamhetsområde som kan försvåra för myndigheten att fullfölja sitt uppdrag. Tillsammans med analysen ska också förslag på planerade åtgärder redovisas som kan göra verksamheten mindre sårbar (SFS 2006:942). Detta kan vara en möjlighet att detektera brister i verksamheten som kan komma att bli framtida misslyckanden.

4.1.2 CERT-SE

Varje incidenthantering som CERT-SE är en del av har olika steg som fullföljs. Det näst sista steget inkluderar en utvärdering från deltagande personal och det sista steget behandlar hur lärdomar kan dras inför nästa incidenthantering. Detta sker oftast muntligt och i närtid till händelsen. Här finns en chans för organisationen att fånga upp konstaterade misslyckanden eller åtgärder som kunde ha misslyckats (Johansson, intervju 2018). CERT-SE har ingen typ av avvikelsehanteringssystem kopplad till verksamheten med förklaringen att enheten är för liten för att kunna förvalta något sådant (Johansson, intervju 2018). Det är möjligt att MSB har system för att rapportera avvikelser inom myndigheten relaterade till arbetsmiljön, men detta är inget som kan anses kopplat till CERT-SE:s cyberövervakningsverksamhet.

För att utveckla och förbättra svaga punkter i verksamheten förmedlar MSB stora mängder medel för forskning som är relaterat till cybersäkerhet. I MSB:s forskningstrategi 2014-2018 *Forskning för ett säkrare samhälle* (MSB, 2013) inkluderas informationssäkerhet som ett av fem forskningsområden. Forskningen runt informationssäkerhet behandlar både förmågan att hantera känslig information men också hur samhället kan öka sin motståndskraft mot digitala hot (MSB, 2013:33). MSB utlyser forskningsmedel som aktörer kan ansöka om för att fullfölja forskningsprojekt. De bedriver alltså inte forskning i egen regi på samma sätt som Folkhälsomyndigheten gör. I MSB:s forskningsplan inför år 2019-2020 pågår utlysning om forskningsprojekt kopplat till automatiserad och autonom cybersäkerhetsövervakning vilket ska kunna förbättra detektering och analys av cyberhot (MSB, 2018a:). Huruvida detta kommer påverka CERT-SE:s arbete kan dock inte fastställas.

Då MSB, likt Folkhälsomyndigheten, är en bevakningsansvarig myndighet ska de genomföra regelbundna sårbarhets och riskanalyser som ska rapporteras till regeringen enligt förordning 2006:942 (SFS 2006:942). I detta arbete analyserar alla avdelningars möjliga sårbarheter och lämnar förslag till förbättring för dessa.

4.2 Hur arbetar Folkhälsomyndigheten och CERT-SE med förenkling?

4.2.1 Folkhälsomyndigheten

På Folkhälsomyndigheten jobbar cirka 500 medarbetare och på enheten för krishantering och beredskap, som hanterar en stor del av övervakningen av anmälningspliktiga sjukdomar, arbetar det cirka 15 individer (Folkhälsomyndigheten 2016a. Richardsson, intervju, 2018). Personalen på enheten för krishantering och beredskap beskrivs av enhetschefen som av blandade yrkesgrupper där bland annat läkare, socionomer, mikrobiologer, statsvetare och apotekare nämns som exempel (Richardsson, intervju 2018). Denna blandning av perspektiv och erfarenhet från olika akademiska bakgrunder kan bidra till att förhindra förenkling inom enheten genom att en mer komplex bild kan målas upp av hälsoläget.

Likt många andra arbetsplatser har myndigheten ett gemensamt dagligt möte där alla olika enheter representeras. På mötet behandlas frågor som kan röra eller rör alla myndighetens enheter från den omvärldsbevakning som genomförs (Richardsson, 2018). Mötet ska säkerställa en gemensam lägesbild av det vardagliga arbetet och att information om enheters arbete når ut till övriga enheter. Till detta möjliggör också representationen från flertalet av de olika enheterna att frågor kan diskuteras från olika verksamhetsperspektiv.

4.2.2 CERT-SE

På MSB arbetar det cirka 850 personer och cirka 25 av dessa arbetar på enheten CERT-SE (MSB, 2018b. Johansson, intervju 2018). Personalen kan enligt Johansson (intervju, 2018) delas in i två kategorier, tekniskt orienterad personal och personal som har annan bakgrund. Den tekniska personalen, beskriver Johansson, har en teknisk akademisk bakgrund om de inte är självlärda. Förekomsten av att vara självlärd beskriver Johansson som något vanligt inom cybersäkerhetsbranschen då inte specifika cybersäkerhetsutbildningar funnits särskilt länge eller varit vanligt förekommande (Johansson, intervju 2018). Den omfattande kontakten mellan

incidenthanterare på enheten och drabbade aktörer bidrar till att förhindra förenkling då den drabbade aktören kan vara en it-säkerhetsspecialist, jurist eller en handläggare som fick till uppgift att rapportera IT-incidenten. Det gör att även deras perspektiv och kontext måste tas tillvara på och gör att CERT-SE kommer i kontakt med många vilt skilda miljöer (Johansson, intervju 2018).

4.3 Hur arbetar Folkhälsomyndigheten och CERT-SE med praktisk uppmärksamhet?

4.3.1 Folkhälsomyndigheten

Den praktiska uppmärksamheten hos Folkhälsomyndigheten vilar hos sjukdomsövervakning som riktar sig mot verksamhetens kärnuppgift, att upptäcka och förhindra utbrott av smittsamma sjukdomar. När Weick och Sutcliffe (2007) nämner att uppmärksamhet riktar sig mot verksamhetens frontlinje är det i Folkhälsomyndighetens fall förmåga att ha en så överstämmande bild av sjukdomsläget med verkligheten som möjligt. För att säkerställa detta förlitar sig myndigheten på olika sensorer som inhämtar information om det aktuella hälsoläget. Detta sker huvudsakligen från fyra större källor. Stora mängder av denna data inhämtas med hjälp av smittskyddslagen 2004:168 som kräver rapportering av anmälningspliktiga sjukdomar. Dessa sjukdomar rapporteras digitalt av sjukvårdspersonal till SmiNet, vilket är ett datorprogram som tillåter Folkhälsomyndigheten att ta del av förekomsten av de anmälningspliktiga sjukdomarna på nationell nivå (SmiNet, 2018). Programmet *Computer Assisted Search for Epidemics*, CASE, hämtar data från SmiNet och varnar personal vid Folkhälsomyndigheten vid avvikande värden (Folkhälsomyndigheten, 2017b). För att hämta data om sjukdomar som inte är anmälningspliktiga finns möjlighet för vårdpersonal att frivilligt skickar in prover kopplade främst till luftvägsinfektioner för att exempelvis undersöka förekomsten av influensa, så kallad sentinelövervakning (Folkhälsomyndigheten, 2018b). För att stärka båda dessa system genomförs syndromövervakning genom att data från sjukvårdsupplysningen 1177 hämtas och analyseras. Exempelvis analyseras hur många som söker hjälp för influensasymtom eller vinterkräksjuka för att kunna sammanställa prognoser om dess spridning. Detta görs för att övervaka hur många som är sjuka men som inte uppsöker vård (Folkhälsomyndigheten, 2016b).

Den fjärde större källan av data kan hänvisas till samarbetet med internationella samarbetsorganisationer. Inom ramarna för det internationella hälsoreglementet har

Folkhälsomyndigheten skyldighet att rapportera om utbrott i Sverige och rättighet att bli underrättad om utbrott i utlandet som kan komma att påverka Sverige (WHO, 2005). Inom EU samarbetar unionens medlemsländer i ett system som samlar information om ländernas sjukdomsövervakning i varningssystemet EWRS, *Early Warning Response System*. Genom detta system måste övriga unionsmedlemmar varnas inom 24 timmar från att en EU medlem uppfattat ett allvarligt gränsöverskridande hälsohot (EU, 2017/253).

En förutsättning för att alla dessa källor av data ska produceras är att ett utbrott måste ha skett. Vissa prognoser om återkommande säsongsjukdomar, exempelvis influensan, kan produceras för att förutspå händelseförlopp. Men för att upptäcka nya typer av influensa eller nya typer av smittsamma sjukdomar måste någon bli sjuk som dessutom uppsöker vård för att prover ska kunna tas. Dessa kan sedan användas för att undersöka sjukdomens utbredning bland populationen. Robin Henig (1994) lyfter denna generella problematik med övervakningens efterdröjsamhet genom att poängtera att det är omöjligt att förvänta sig att sjukdomar ska detekteras innan spridningen har börjat. Kortfattat beskriver Henig det som ”*there is no good way of anticipating the next disease outbreak short of waiting for a few people to get sick*” (Henig, 1994:68).

4.3.2 CERT-SE

CERT-SE har inget eget intrångsystem som söker efter skadlig kod eller intrång hos myndigheter eller aktörer som bedriver samhällsviktig verksamhet i nuläget. I årsrapporten om IT-incidenter för 2017 föreslår MSB möjligheten att de får installera egna tekniska sensorsystem på inbjudan av myndigheter för att förbättra CERT-SE:s övervakning (MSB, 2018d:18) Detta är något som i skrivande stund inte har implementerats. Den data som enheten har tillgång till för analys måste lämnas av andra aktörer (Johansson, intervju 2018). CERT-SE:s cyberövervakning förlitar sig på tre huvudsakliga källor. Den mest omfattande källan rör de publika sidor som för olika typer av register över infekterade maskiner och IP (internet protocol) adresser (Johansson, intervju 2018). Några av dessa publika källor som CERT-SE använder sig av, exempelvis Shadowserver.org och DroneBL.org, drivs som helt ideell verksamhet av frivilliga aktörer (Shadowserver, 2019. DroneBL, u.å). Det finns också tjänster som tillhandahåller liknande data men som inte är publika som CERT-SE använder sig av (CERT-SE, 2012).

Den andra huvudsakliga källan är andra nationella CERT:s eller CERT:s från privata företag. Det finns flera samarbetsforum med syfte att delge information mellan medlemmarna. Ett sådant forum som Johansson (intervju, 2018) poängterar som extra värdefulla är EGC (European govermental CERT:s). Organisationen är ett informellt forum för delning av information där 14 europeiska nationella CERT enheter ingår (EGC group, u.å). En annan värdefull källa för information är organisationen TF-CSIRT som samlar privata och offentliga CERT/CSIRT enheter från framförallt Europa (TF-CSIRT, 2018. Johansson, intervju 2018). På global nivå medverkar CERT-SE i samarbetsforumet FIRST som består av cirka 400 medlemmar från privat och offentlig sektor (FIRST, u.å). Samtliga ovan nämnda forum är förtroendebaserade, det vill säga att de inte har bindande avtal som reglerar medlemmarnas engagemang utan medlemmarna bidrar med den information som de är trygga med att lämna. Detta förtroende kännetecknar mycket av samverkan mellan olika CERT enheter enligt Johansson (intervju, 2018). Den samarbetsgrupp och europeiska CSIRT-nätverk som beskrivs i NIS-direktivet under artikel 11 och 12 har som beskrivna uppgifter att finna bästa praxis för informationsutbyte och delta i informationsutbyte i högsta möjliga mån. En medlemsstat kan dock neka att delta i diskussion eller bidra med information om denne finner anledning för det (EU. 2016/1148).

En mindre del av den data som CERT-SE har till sitt förfogande är baserad på de rapporter som är obligatoriska för aktörer med samhällsviktig verksamhet (Johansson, intevju 2018). Innan NIS-direktivets implementerande hade endast myndigheter ett obligatoriskt ansvar att rapportera IT-incidenter (MSB, 2016). Efter dess implementering innebar det en utökning av antalet aktörer som har ansvar att rapporter IT-incidenter. Det kan därför vara möjligt att antalet rapporter kraftigt ökar när föreskrifter kopplade till lagen implementeras och den allmänna kunskapen om rapporteringsansvaret ökar.

4.4 Hur arbetar Folkhälsomyndigheten och CERT-SE med resiliens?

4.4.1 Folkhälsomyndigheten

Weick och Sutcliffe (2007:71) beskriver tre komponenter som tillsammans utgör resiliensens kärna. Förmåga att absorbera påfrestning, förmåga att återhämta och förmåga att lära efter påfrestningen. De två första komponenterna behandlar Folkhälsomyndigheten genom att organisera sig i en krisledningsorganisation vid extrem påfrestning. Den nuvarande

krisledningsorganisationen beslutades under 2017 och har övats under året (Folkhälsomyndigheten 2018c). Richardsson (intervju, 2018) beskriver krisledningsorganisationen som en gränslös stegring av olika förmågor och inte en dikotomisk organisation som antingen är i normalläge eller stabsläge. Krisledningsorganisationen är myndighetens förmåga att anpassa ledningsstrukturen från mindre utbrott till globala pandemier. Beslut om krisledningsorganisation kan beslutas av myndighetens generaldirektör, en avdelningschef eller chefen vid enheten för krishantering och beredskap. Vid ofred och när höjd beredskap gäller går Folkhälsomyndigheten in i krigsorganisation som kraftigt reducerar antalet verksamhetsområden (Richardsson, intervju 2018). För att arbeta med den tredje komponenten, förmåga att lära efter påfrestning, identifierar Weick och Sutcliffe (2007:73) svårigheter med att identifiera hur en HRO kan lära sig något om det oförutsägbara. En lösning är att öva för att kunna simulera händelser som tidigare inträffat för att slipa verksamhetens operativa arbete och finna nya scenarion som ännu inte inträffat. I sin övningsverksamhet beskriver Richardsson (intervju, 2018) mängdövning internt på sin enhet men också nationella övningar där totalförsvarsövningen 2020 beskrivs spela en stor roll. Regelbundna table-top övningar, mindre simulerade teoretiska övningar utan personal som utför handlingarna praktisk, genomförs med den nordiska övningsgemenskapen Svalbard, andra länder inom EU och med WHO (Richardsson, 2018).

4.4.2 CERT-SE

Enheten är organiserad för att kunna hantera två större samtidiga incidenter med en uthållighet på en vecka (Johansson, intervju, 2018). Vid särskilda incidenter kan MSB besluta om en särskild organisation som etableras för att arbeta med en specifik händelse eller arbetsuppgift. Om denna händelse har ett cyberelement kan CERT-SE i olika utsträckning vara en del av detta för att bistå med expertis och resurser (Johansson, intervju 2018). Det finns också förmåga att använda personal från andra enheter på den avdelning som CERT-SE tillhör, avdelningen för cybersäkerhet och skydd av samhällsviktig verksamhet, för att få en styrketillväxt på personalstyrkan vilket kan komma att förlänga uthålligheten bortom en vecka (Johansson, intervju, 2018). Detta bidrar med flexibilitet i organisationen för att kunna stå emot överraskande påfrestningar. Användning av särskild organisation kan användas ända till beslut om höjd beredskap fattas. Vad höjd beredskap skulle innebära för CERT-SE och enhetens uppgifter är i skrivande stund inte klargjort (Johansson, intervju 2018).

I sin övningsserie deltar CERT-SE i flera internationella övningar, exempelvis Cyber Storm som arrangeras av amerikanska *Department of Homeland Security*, NATO:s övning Cyber Coalition och Cyber Europe som arrangeras av ENISA, *European Network and Information Security Agency* (Johansson, intervju 2018). Nationella övningar förs kontinuerligt med de myndigheter som är en del av SAMFI, Samverkansforum för Informationssäkerhet, där bland annat Försvarets radioanstalt, Säkerhetspolisen, Post- och telestyrelsen samt Försvarsmakten ingår. Tillsammans med dessa för också enheten mindre egna övningar inom CERT-SE (Johansson, intervju 2018).

4.5 Hur arbetar Folkhälsomyndigheten och CERT-SE med expertis?

4.5.1 Folkhälsomyndigheten

Richardsson (intervju, 2018) beskriver en strikt hierarkisk struktur på Folkhälsomyndigheten och på sin enhet. Mandat att påbörja större åtgärder följer en beslutsordning där generaldirektörens mandat kan delegeras till avdelningschefer som i sin tur kan delegera mandat till enhetschefer. Utredarna på enheten för krishantering och beredskap har instruktioner om vad de ska arbeta med och när de bör kontakta överordnade. Användandet av SOP, *Standard Operating Procedure*, instruktion om rutinbaserat arbete, beskrivs som omfattande. Enheten för krishantering och beredskap ansvarar för myndighetens tjänsteman i beredskap, TIB. (Folkhälsomyndigheten 2018a). Denna funktion har möjlighet att åsidosätta den annars vardagliga organisatoriska hierarkin med långtgående mandat att besluta om bland annat krisledningsorganisation om särskild tidspress infinner sig eller om generaldirektören inte kan nås (Richardsson, intervju 2018).

4.5.2 CERT-SE

Den hierarkiska strukturen på CERT-SE utgår från befattningen vakthavande som har det vardagliga operativa ansvaret för verksamheten. Denne styr incidenthanterarnas arbete. Till vakthavandes stöd finns det en operativ chef som kan stödja vid behov för att koordinera större insatser. Tillsammans har de mandat att vidta alla åtgärder som enheten har tillgång till förutom att kalla in personal från semester. Tjänstemannen i beredskap på MSB kan be vakthavande på CERT-SE att undersöka uppgifter som kommit till dennes kännedom (Johansson, intervju 2018). Annars beskriver Johansson enheten som en egen funktion frånkopplad av MSB:

> *” Vi har valt att lägga upp det så att cyberdelen är en svart låda som de [MSB] kan ställa frågor till. Men de kan inte gå in och styra i den svarta lådan. För där är det vår vakthavande som styr… När vi har haft större händelser har det funnits en tendens att MSB vill gå in i den här svarta lådan som jag pratade om och styra den direkt, det blir aldrig bra. Det innebär att du har folk som är inne och styr över en funktion som de inte förstår hur den fungerar.”*
> (Johansson, intervju 2018).

Johansson (intervju 2018) beskriver svårigheter att rekrytera personal med formell akademisk cybersäkerhetsutbildning, så som det beskrivs under rubrik 4.2.2. Detta resulterar i att erfarenhet och praktisk expertis skattas högt på enheten då beslut ska tas. Detta kan vara en anledning till varför funktionen beskriv som en ”svart låda” och frånskiljs från andra enheter på MSB.

4.6 Sammanfattning

I stora drag har både Folkhälsomyndigheten och CERT-SE mycket gemensamt inom ramarna för de fem principerna som anammas av HRO:s. Båda organisationerna har omfattande utvärderings- och sårbarhetsanalysverksamhet som söker att skänka ljus på möjliga misslyckanden. Trots att båda aktörer är verksamma i komplicerade miljöer, tekniskt- och epidemiologiskt vilket gör dem sårbara för förenkling, har båda en variation av personal som tillsammans med samverkan med externa aktören kan ge nyanserade bilder inom respektive övervakningsområde. I arbetet med resiliens har de olika typer av ledningsstrukturer som kan ta över vid ökad påfrestning. Båda krisorganisationer kan anpassas flexibelt till uppgiften och skalas upp eller ner beroende på påfrestning. Användande av övningar internt inom organisationerna och tillsammans med externa aktörer, både nationellt och internationellt, har bekräftats. Övningsfrekvensen kan ses som hög hos båda organisationer och i synnerhet CERT-SE:s deltagande i internationella övningar utmärker sig som omfattande. Även mandat för personal som hanterar pågående verksamhet är stor. Den hierarkiska strukturen som betonas på Folkhälsomyndigheten kan bero på den större strukturen som omfattar jämförelsen. CERT-SE beskrivs som mer frånkopplat från MSB vilket gör mandat att hantera pågående verksamhet som stor. Båda myndigheter har en TIB-funktion med långtgående möjligheter att starta åtgärder för att hantera hastigt uppkomna situationer dygnet runt.

Den stora skillnaden mellan Folkhälsomyndigheten och CERT-SE inom studiens ramar kan hänvisas till deras tillgång till information för att säkerställa deras praktiska uppmärksamhet. Den obligatoriska rapporteringen av sjukdomar och IT-incidenter tjänar samma syfte och funktion hos båda organisationer. Däremot skiljer sig samverkan med internationella aktörer omfattande mellan organisationerna. Eftersom båda organisationerna hanterar gränslösa hot spelar underrättelse från internationella aktörer stor roll som förvarning om vad som snart kan komma att drabba Sverige. Utan detta begränsas förmågan att uppfatta hälso/cyber lägesbilden i stor utsträckning. Båda organisationer är medlemmar i flera internationella forum för samverkan men skillnaden ligger i de bindande avtalen som ligger till grund för den epidemiologiska samverkan och de förtroendebaserade som bas för cybersäkerhetsforum. Detta behöver inte betyda att den tillgängliga cybersäkerhetsinformationen inte fyller sin funktion men det innebär en möjlighet för nationer och organisationer att ”mörka” eller undanhålla information som kan komma att påverka CERT-SE:s förmåga att hålla sig underrättad om kommande, pågående eller överspelade hot. Detta på ett sätt som inte i lika hög utsträckning är möjligt inom ramarna för bindande epidemiologiska samarbeten inom EU och WHO. Detta resultat anses ha hög generaliserbarhet inom andra nationella CERT-enheter då den förtroendebaserade samverkan inom cybersäkerhet beskrivs som närvarande inom hela sektorn, både av materialet som studien behandlar och baserat på tidigare forskning.

5.0 Diskussion och vidare forskning

Nedan kommer diskussion av studien att presenteras. Diskussionen är uppdelad i en teori- och resultatdiskussion som behandlar resultatets tänkbara möjligheter och konsekvenser samt diskuterar eventuella etiska dilemman med resultatet. Förslag på vidare forskning från studiens resultat presenteras sedan under egen rubrik.

5.1 Teori- och resultatdiskussion

I ljuset av resultaten från undersökningen kan vissa diskussioner lyftas angående den aktuella teorin och studiens resultat. I första hand kan teorins lämplighet för studien diskuteras. Teorin är ursprungligen inte en normativ teori som beskriver hur organisationer ska arbeta för att bli mer pålitliga, utan en deskriptiv teori som beskriver hur några särskilda organisationer arbetar för att vara mer pålitliga. Det finns däri en begränsning i teorin gällande hur man kan mäta relevansen av åtgärder vidtagna av en organisation inom någon av de fem principerna som

presenteras. Det finns exempelvis ingen möjlighet att värdera vilket sätt som är det mest effektiva eller bättre av Folkhälsomyndigheten och CERT-SE:s olika krisorganisationer kopplat till teorin. Det kan endast konstateras att de båda har en möjlig organisation på plats vilket tydliggör att de arbetar med frågan. I den utsträckningen kan de flesta organisationer konstateras arbeta med resiliens i någon mån. Hur omfattande detta arbete måste vara för att det ska räknas är något som lämnas obesvarat. Ett annat exempel kan väckas kring organisationernas arbete med forskning. Där kan forskningsmedel jämföras för att finna skillnader i mängd som organisationerna spenderar på utveckling. Men hur mycket av forskningen som sedan implementeras i verksamheten kräver djupare analys och hur sedan detta påverkar den faktiska produktionen kräver ännu en nivå av analys. Teorin kan därför sägas lämpa sig sämre om studiens jämförelse baserades på vilken organisation som är en HRO eller ligger närmast i att vara det. Då studiens syfte istället är att använda teorin som ramverk för att finna skillnader mellan dem kan den i detta avseende ses som väl lämplig.

Studiens resultat finner att CERT-SE:s övervakning, i relation till folkhälsoövervakningen, skulle gynnas av multilateralt bindande avtal om informationsutbyte. Detta stämmer väl överens med Smith III (2016) och Brantlys (2017) slutsatser om cybersäkerhetsarenans problem med fragmenterade lägesbilder och brist på samverkan vid större incidenter. Om ett avtal likt det internationella hälsoreglementet eller motsvarande på regional nivå kunde implementeras för cybersäkerhet skulle ansvar och säkerställande av fördelning av information tydliggöras. Detta skulle innebära större tillgång till information för CERT-SE och om bindande avtal om informationsspridning skulle etableras skulle de också kunna vara än mer säkra på att de skulle bli underrättade vid större händelser. Om inte ens en integrerad region som EU kan säkerställa bindande avtal om informationsdelning angående IT-incidenter och skadlig kod, kan detta ge en fingervisning om hur långt bort ett globalt bindande avtal ligger. Den frivilliga och förtroendebaserade samordningen som sker inom fältet idag är bräcklig då säkerhetspolitiska skiftningar kan förändra förtroendet mellan länder väldigt snabbt. En annan risk med det förtroendebaserade systemet som finns idag är att stora aktörer på cybersäkerhetsområdet utelämnas på grund av säkerhetspolitiska anledningar. Samverkan med ansenliga cybersäkerhetsaktörer som Ryssland och Kina blir begränsad eller uteslutande. Dessa aktörer har betydande resurser inom området och är själva hårt ansatta av cyberattacker, vilket kan ge värdefull information till CERT-SE om möjliga typer av skadlig kod som kan förväntas göra entré i Sverige inom kort. Användandet av skadlig kod som vapen och säkerhetspolitiskt

verktyg måste erkännas vilket kan försvåra bindande globalt samarbete inom cybersäkerhet. Ett sätt att kringgå denna låsning är att det bindandet avtalet uppdateras med vissa typer av skadlig kod som medlemmarna kommer överens om är av kriminell natur och som samtliga förlorar på att det fortsätter spridas, liknande en anmälningspliktig sjukdom. Exempelvis skulle Conficker-masken, vars syfte var att sprida falsk reklam, kunna sättas på denna ”lista” så att en mer komplett lägesbild skulle kunna målas och åtgärder mot den lättare samordnas. Detta skulle kräva universell konsensus inom området för att kunna möjliggöras, något som tidigare inte kunnat nås då hotets grad kanske inte uppfattas som så gravt att det tillåter nödvändiga kompromisser.

Tidigare organisationer för globalt samarbete inom cybersäkerhet som FIRST och IMPACT eller helt nya organisationer kan komma att spela större roll i framtiden då fler enheter kopplas upp, digitaliseringen av tidigare utvecklingsländer slår igenom och fler samhällsviktiga system sammankopplas med internet. Det kraftigt eftersatta cybersäkerhetsarbetet har en lång väg att vandra i jämförelse med det epidemiologiska arbetet. Möjligheten att se cybersäkerhet med folkhälsoögon kan underlätta detta. Internet ägs av alla som är sammankopplade till det. Sverige är beroende av alla andra stater som använder internet och för att öka Sveriges motståndskraft mot cyberhot ligger många av lösningarna globalt. Ansvaret för internets hälsa kan därför inte läggas på en skild stat eller företag utan måste säkerställas av ett globalt ansvarstagande.

En etisk diskussion kan väckas från resultatet. Framsidan av denna studie pryds av ett öga som ofta symboliserar övervakning. Denna bild tillsammans med begrepp om övervakning inom det fria internet kan ge integritetsvärnande människor rysningar i kroppen och tankar till dystopiska framtidsscenarion i stil av Orwells (1984) massövervakning i boken 1984. Om en global organisation skulle etableras där länder var tvungna att dela information med varandra i cyberrelaterade hot skulle det kunna vara en möjlighet för totalitära regimer att ursäkta insamlandet av metadata för att spionera på sina medborgare. Det finns en risk att diskussionen lutar åt detta hål när frågan om informationsdelning på global nivå diskuteras och det är en invändning som måste respekteras. I nuläget kan det dock anses att Sullivans (2012) argument om att ökad övervakning och samordning inom cybersäkert kan minska risken för att användares integritet kränks genom att en säkrare cyberarena etableras. Vilket som är det

största hotet, möjligheten att en supranationell organisation olovligen övervakar dig eller att skadlig kod från kriminella kränker din integritet är dock självklart öppet för diskussion.

5.2 Vidare forskning.

Det huvudsakliga förslaget till forskning som kan ta vidare denna studies resultat är empiriska undersökningar om specifika IT-incidenter som CERT-SE, eller motsvarande länders enheter, skulle prestera bättre i hanteringen av om de hade tillgång till ett regionalt eller globalt bindande avtal om informationsutbyte. Det kan vara lätt att bara be om mer data för effektivare övervakning men det måste vägas mot investeringens kostnad och om andra lösningar kan ge motsvarande resultat. Det måste framförallt vägas mot den integritetsvärnande kulturen, som bland annat Sullivan (2012) belyser, som präglar diskussioner om regleringar och tvingande mandat av internet och information. Ett annat område att forska vidare om vore hur globala överenskommelser kan bestämmas om ett sådant decentraliserat och anarkistiskt utrymme som internet. Den här studiens fokus på folkhälsa ger IHR som en föregångare, men det är i ljuset av ett geografiskt områdesansvar där stater ansvarar för varje människa och rapporteringssystem. Internet är svårare att reglera via geografiskt ansvar då information kan ligga geografiskt delad i flera länder för att sammanställas i ett annat. Det kan vara intressant att ta vid Tom Ridouts (2017) forskning om användandet av avtal för yttre rymden som ramverk för områdesansvar av internet. Ett givande alternativ vore att undersöka om det finns andra anledningar till varför inte omfattande globala överenskommelser redan dikterats inom cybersäkerhet. En vinkel skulle kunna vara att cyberhotet inte är tillräckligt erkänt som ett reellt hot mot nationalstater att de behöver ingå avtal om det. En annan vinkel vore att förtroendebaserad samverkan är det enda sättet som aktörer är villiga att dela med sig av information om egna sårbarheter av rädsla för att bli utnyttjad av illvilliga stater. Möjligheten för ett omfattande globalt samarbete inom cybersäkerhet är relevant att undersöka vidare om den nuvarande kursen mot mer digitalisering fortsätter.

6.0 Referenslista

Baker, D.P, Day, R & Salas, E. (2006). Teamwork as an Essential Component of High-Reliability Organizations. *Health service research*. Volume 41, issue 4p2, 1576-1598.

Bowden, M. (2012). *Viruset, det första digitala världskriget*. Falun: ScandBook AB.

Brantly, Aaron F. (2017). Public health and epidemiological approaches to national cybersecurity: a baseline comparison i Van Puyvelde, D. & Brantly, A.F. (red.). *US national cybersecurity: international politics, concepts and organization*. Abingdon, Oxon: Routledge.

Bryman, A. (2011). *Samhällsvetenskapliga metoder*. (2., [rev.] uppl.) Malmö: Liber.

CERT-SE, (2012). Om lägeskartan.
https://www.cert.se/megamap/ Hämtad 02-01-2019

Ciravegna, L & Brenes, E.R. (2016). Learning to become a high reliability organization in the food retail business. *Journal of Business Research.* Volume 69, Issue 10, 4499-4506

DroneBL, (u.å). Make donation.
https://dronebl.org/donate%20 Hämtad 02-01-2019

EGC group (u.å). Home.
http://www.egc-group.org/index.html Hämtad 03-01-2019

EU. 2017/253. *Om förfaranden för utfärdande av varningar inom ramen för det system för tidig varning och reaktion som inrättats för allvarliga gränsöverskridande hot mot människors hälsa och förfaranden för informationsutbyte, samråd och samordning av insatserna vid sådana hot i enlighet med Europaparlamentets och rådets beslut nr 1082/2013/EU.*
https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32017D0253&from=EN
Hämtad 30-12-2018

EU. 2016/1148. Europaparlamentets och rådets direktiv av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016L1148&from=SV Hämtad 08-01-2019

FIRST, (u.å.). About. https://first.org/about/ Hämtad 03-01-2019

Folkhälsomyndigheten. (2018a). Avdelningen för smittskydd och hälsoskydd. https://www.folkhalsomyndigheten.se/om-folkhalsomyndigheten/organisation/avdelningar-och-enheter/smittskydd-och-halsoskydd/ Hämtad 21-12-2018

Folkhälsomyndigheten. (2018b). Sentinelövervakning influensa. https://www.folkhalsomyndigheten.se/smittskydd-beredskap/overvakning-och-rapportering/sentinelovervakning/ Hämtad 30-12-2018

Folkhälsomyndigheten. (2018c). Årsredovisning 2017. https://www.folkhalsomyndigheten.se/contentassets/2c5deead35ff4f02ba8d651629efce48/folkhalsomyndighetens-arsredovisning-2017.pdf Hämtad 01-01-2019.

Folkhälsomyndigheten. (2018d). Pandemisk influensa. https://www.folkhalsomyndigheten.se/smittskydd-beredskap/krisberedskap/pandemiberedskap/pandemisk-influensa/ Hämtad 09-01-2019

Folkhälsomyndigheten. (2017a). Ledningssystem för hantering av biorisker i laboratorier (CWA 15793). https://www.folkhalsomyndigheten.se/mikrobiologi-laboratorieanalyser/biosakerhet-och-bioskydd/ledningssystem-for-hantering-av-biorisker-i-laboratorier/ Hämtad 21-12-2018

Folkhälsomyndigheten. (2017b). Datorstödd utbrottsdetektion. https://www.folkhalsomyndigheten.se/publicerat-material/publikationsarkiv/d/datorstodd-utbrottsdetektion/ Hämtad 30-12-2018

Folkhälsomyndigheten. (2016a). Kort fakta om oss. https://www.folkhalsomyndigheten.se/om-folkhalsomyndigheten/korta-fakta-om-oss/ Hämtad 28-12-2018

Folkhälsomyndigheten. (2016b). Syndromövervakning. https://www.folkhalsomyndigheten.se/smittskydd-beredskap/overvakning-och-rapportering/syndromovervakning/ Hämtad 30-12-2018.

Folkhälsomyndigheten. (2013). P4 laboratoriet vid Folkhälsomyndigheten. https://www.folkhalsomyndigheten.se/mikrobiologi-laboratorieanalyser/mikrobiologisk-beredskap-247-diagnostik/sakerhetslaboratorierna/p4-laboratoriet/ Hämtad 21-12-2018

Hackmageddon, (2018). January – September 2018 Cyber Attack Statistics. https://www.hackmageddon.com/?s=2018+cyber+attack+ Hämtad 05-01-2019

Henig, R.M. (1994). *A dancing matrix: how science confronts emerging viruses*. (1. Vintage Books ed.) New York: Vintage.

IMPACT, (2012). https://www.itu.int/ITU-D/cyb/publications/2012/IMPACT/IMPACT-en.pdf Hämtad 07-01-2019

LaPorte, T. R & Consolini, P. M. (1991). Working in practice but not in theory: Theoretical challenges of "High reliability organizations*". Journal of Public Administration Research and Theory: J-PART*, Vol. 1, No. 1. 19-48.

MSB. (2018a). Forskning planeras för ett säkrare samhälle: MSB:s forskningsplan 2019-2020. https://rib.msb.se/filer/pdf/28737.pdf%20 Hämtad 02-01-2019

MSB. (2018b). Organisation. https://www.msb.se/Templates/Pages/Page.aspx?id=6763&epslanguage=sv Hämtad 04-01-2019

MSB. (2018c). Nationell risk- och förmågebedömning 2018.
https://www.msb.se/RibData/Filer/pdf/28470.pdf
Hämtad 09-01-2019

MSB. (2018d). Årsrapport it-incidentrapportering: 2017.
https://www.msb.se/RibData/Filer/pdf/28463.pdf
Hämtad 09-01-2019

MSB. (2016a). Exempel på it-incidenter: Typexempel inklusive bedömning.
https://www.msb.se/Upload/Forebyggande/Informationssakerhet/exempel/Exempel%20p%C3%A5%20it-incidenter%20april%202016.pdf
Hämtad 09-01-2019

MSB. (2016b). Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters rapportering av it-incidenter.
https://www.msb.se/externdata/rs/f21ae5f7-b655-4462-a2e6-9939b952a751.pdf
Hämtad 02-01-2019

MSB. (2013). Forskning för ett säkrare samhälle: ny kunskap för framtidens utmaningar MSB:s forskningsstrategi 2014–2018.
https://www.msb.se/RibData/Filer/pdf/27246.pdf Hämtad 02-01-2019
Hämtad 02-01-2019

MSB. (2012). Nationellt system för it-incidentrapportering, svar på regeringens uppdrag till Myndigheten för samhällsskydd och beredskap (Fö2012/717/SSK, Regeringsbeslut II:1, 2012-04-12.
https://www.msb.se/Upload/Forebyggande/Informationssakerhet/MSB_uppdragsredovisning_it-incidentrapportering.pdf Hämtad 02-01-2019

Orwell, G. (1984). *1984: Nitton åttiofyra*. ([Ny utg.]). Höganäs: Bra böcker.

Shadowserver, (2019). Job opportunities.

https://www.shadowserver.org/wiki/pmwiki.php/Shadowserver/JobOpportunities Hämtad 02-01-2019

SFS 2008:1002. *Förordning med instruktion för Myndigheten för samhällsskydd och beredskap*.

SFS 2018:1175. *Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster*.

SFS 2018:1174. *Lag om informationssäkerhet för samhällsviktiga och digitala tjänster*.

SFS 2004:168. *Smittskyddslag*.

SFS 1968:231. *Smittskyddslag*

SmiNet. (2018). Om SmiNet.
http://sminet.se/?page_id=4 Hämtad 30-12-2018

Sullivan, K (2012). The internet health model for cybersecurity. Eastwest Institute.
https://www.files.ethz.ch/isn/143900/Internethealth_0.pdf
Hämtad 07-01-2019

Swaling, V. H & Johansson, J. (2018). Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem. https://www.msb.se/RibData/Filer/pdf/28550.pdf
Hämtad 07-01-2019

TF-CSIRT, (2018). Team database.
https://www.trusted-introducer.org/directory/alpha_LICSA.html Hämtad 03-01-2019

The Rendon Group, (2011). Conficker Working Group: Lessons Learned.
http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf%20 Hämtad 02-01-2019

Parker, R. D & Farkas, C. (2011). Modeling Estimated Risk for Cyber Attacks: Merging Public Health and Cyber Security. *Information Assurance and Security Letter*, volume 2, 32-36.

Perrow, C. (1999*). Normal Accidents: Living with High Risk Technologies (Updated*). New Jersey: Princeton University Press:

Perrow, C. (2007). *The next catastrophe: reducing our vulnerabilities to natural, industrial and terrorist disasters.* New Jersey: Princeton University Press.

Pronovost, P. J., Berenholtz, S.M., Goeschel, C. A., Needham, D. M., Sexton, J. B., Thompson, D. A., Lubomski, L. H., Marsteller, J. A., Makary, M. A., Hunt, E. (2005). Creating High Reliability in Health Care Organizations. *Health service research*. Volume 41, issue 4p2, 1599-1617.

Rice, Mason. Butts, Jonathan. Miller, Robert. Shenoi, Sujeet. (2010). Applying public health strategies to the protection of cyberspace. *International Journal of Critical Infrastructure Protection*. Volume 3, Issues 3–4, 118-127.

Ridout, Tom (2017). Developing an international cyberspace governance framework: comparisons to outer space. Van Puyvelde, D. & Brantly, A.F. (red.). *US national cybersecurity: international politics, concepts and organization*. Abingdon, Oxon: Routledge.

Weick, Sutckliff & Obstfeld, (1999). Organizing for High Reliability: Processes of Collective Mindfulness. *Research in Organizational Behavior*, Volume, 81–123.

World health organization. (2005). International health regulations, third edition. http://apps.who.int/iris/bitstream/handle/10665/246107/9789241580496-eng.pdf;jsessionid=5A63451FEFFE7B80A1CF5C60AD862E2E?sequence=1 Hämtad 21-12-18