Bortom de tekniska riskerna

Cybersäkerhetens komplexitet och vikten av ett helhetsperspektiv i en sammanflätad värld

Beyond the technical risks

The complexity of cybersecurity and the importance of a holistic perspective in an interconnected world

Amanda Lilleberg

Fakulteten för humaniora och samhällsvetenskap
Utbildningsprogram: Riskhantering i Samhället, 120 hp
Examensarbete Masternivå, 30 hp
Handledare: Erik Persson Pavlovic
Examinator: Finn Nilson
Datum: 2024-05-30

Förord

Jag har alltid fascinerats av den antagonistiska arenan vilket gjort att det har varit ämnen för mina arbeten, studier och uppsatser ända sedan gymnasietiden. När jag började mina masterstudier inom riskhantering var min önskan att få integrera detta intresseområde med riskstudier, vilket jag har fått göra. Alltså var det mer eller mindre givet att min uppsats skulle hamna inom denna ram, vilket är en av anledningarna till valet av uppsatsämne: Cyberrisker. Likaså är cyberdomänen ett riskområde jag fått upp ögonen för under mina masterstudier, som dessutom aktualiseras alltmer i samtiden.

Jag vill rikta mitt största och varmaste tack till min handledare Erik Persson Pavlovic, för våra samtal, din kunskap, vägledning, all välbehövlig stöttning och ditt stora personliga engagemang. Det har varit ovärderligt under uppsatsen gång – tack!

Att skriva en masteruppsats på resande fot i Latinamerika har varit lika utmanande som givande för oss sammanboende uppsatsstudenter. Tack till alla inblandade, ni har gjort uppsatsresan till en fantastisk och minnesvärd tid, trots alla prövningar.

Några av mina studiekamrater som numera är kära vänner har gjort vägen till och under uppsatsskrivandet möjlig, då vi har stöttat varandra och kämpat tillsammans. Men framför allt har ni gjort tiden oerhört rolig och givande på så många sätt – tack till er!

Slutligen vill jag tacka min faster med familj som peppat och stöttat mig kontinuerligt. Specifikt tack till min faster som utöver allt annat, varit min konsult i angelägenheter som rört Word och som tvingats hjälpa mig när mina kunskaper varit bristfälliga. Tack för allt!

Amanda Lilleberg

Göteborg, 2024-05-30

Summary

The thesis takes its point of departure from the extensive technological advancements and digitalization in today's interconnected society, exploring their correlation with cyber risks. Based on increased vulnerability to cyberattacks and the growing threat from the cyber environment, the aim is to investigate whether risk management strategies and assessments for cybersecurity within the national policy sphere, adequately address the complex nature of cybersecurity risks. Furthermore, it aims to identify whether a systemic understanding of these risks is present, including the potential for extensive consequences. The thesis adopts a qualitative approach with a deductive stance, using documents as the primary data source. A directed content analysis was applied to the material, consisting of seven policy documents: Four agency reports authored by the National Cyber Security Center and three national security strategies, focusing on the national strategy for information and cybersecurity. The results of the directed content analysis indicate that the documents emphasize technological progression and digitalization as central factors contributing to vulnerabilities and cybersecurity risks. Dependency relationships that have emerged in the wake of technological applications in society are also highlighted. While there is a focus on protecting critical infrastructure and essential services in the documents, the results show limited discussion regarding cyberattacks effects and impacts on people's health, life as well as on the environment. Similarly, there are shortcomings in fully addressing the multidimensional nature of cyber risks. A systemic understanding of cyber risks is apparent in the documents, although it may not be fully comprehensive in its scope. Despite emphasis on vulnerabilities in critical infrastructure, there is a discrepancy in the focus on vital sectors. Detailed and extended discussions on cascading effects as a process and their relation to cybersecurity risks are limited, thereby restricting the understanding of the potentially extensive consequences of cyber risks. In conclusion, this raises questions about whether an adequate holistic view of contemporary cyber risks prevails within the policy sphere.

Keywords: Systemic risk, cyber risk, cybersecurity, critical infrastructure, cascading effects, systems theory, NCSS.

Sammanfattning

Uppsatsen tar avstamp i den omfattande tekniska utvecklingen och digitaliseringen i dagens sammanlänkade samhälle och dess samhörighet med cyberrisker. Baserat på ökad sårbarhet för cyberangrepp och tilltagande hot från cybermiljön är syftet att undersöka huruvida riskhanteringsstrategier och bedömningar för cybersäkerhet inom den nationella policysfären, adresserar den komplexa karaktären av cybersäkerhetsrisker. Vidare identifiera om en systemförståelse av dem återfinns, inklusive riskernas potential att medföra omfattande konsekvenser**.** Uppsatsen är av kvalitativ karaktär med en deduktiv ansats, där dokument används som dataunderlag. Vidare har en riktad innehållsanalys tillämpats på uppsatsens material, där empirin består av sju policydokument: Fyra myndighetsrapporter som är författade av Nationellt cybersäkerhetscenter samt tre nationella säkerhetsstrategier, med fokus på den nationella strategin för samhällets information- och cybersäkerhet. Resultatet av den riktade innehållsanalysen pekar på att dokumenten betonar teknologisk progression och digitalisering som en central faktor till sårbarheter och cybersäkerhetsrisker. Beroendeförhållanden som vuxit fram i kölvattnet av teknologisk tillämpning i samhället, som en annan. Fokus på att skydda kritisk infrastruktur och samhällsviktig verksamhet framträder i dokumenten, men resultatet visar begränsad diskussion om spridningseffekter från cyberangrepp gällande dess påverkan på människors hälsa, liv såväl som på miljön. Likaså brister i att fullständigt adressera den mångdimensionella karaktären av cyberriskerna. En systemisk förståelse för cyberrisker framträder i dokumenten, men inte i fullständig utsträckning. Trots betoning på sårbarheter inom samhällsviktig verksamhet och kritisk infrastruktur, förekommer en diskrepans i fokus på samhällskritiska sektorer. Utförliga resonemang om kaskadeffekter som process och dess relation till cybersäkerhetsrisker är småskaliga, vilket begränsar förståelsen för cyberriskernas potentiellt omfattande konsekvenser. Sammanfattningsvis medför det frågan huruvida en tillräcklig helhetssyn på samtidens cyberrisker råder inom policysfären.

Nyckelord: Systemisk risk, cyberrisk, cybersäkerhet, kritisk infrastruktur, kaskadeffekter, systemteori, NCSS.

Innehållsförteckning

1 Introduktion

Att vår samtid blir alltmer högteknologisk och digitaliserad är numera ett faktum. Den progressiva digitala övergången i samhället tillsammans med den tekniska utvecklingen, har bidragit till omfattande samhällelig tillväxt (Renn m.fl., 2022). Samtidigt är denna utveckling associerad med osäkra och komplexa konsekvenser utifrån den omfattade teknologiska tillämpningen i dagens samhälle. Dessa osäkra konsekvenser kan få effekter inom viktiga samhällssystem, eftersom den teknologiska utvecklingen medför potentiella hot och risker – exempelvis cyberrisker i form av cyberangrepp. Den teknologiska utvecklingen tillsammans med en alltmer globaliserad och sammankopplad teknologi i samhället, har på så sätt medfört förändringar och framträdande hot som påverkar och ökar samhällets sårbarhet (Olsen m.fl., 2007; Scholz, 2017). Sårbarheten är därtill sprungen ur att den digitala teknologins omfattande användning gjort samhället alltmer beroende av digital infrastruktur (Scholz, 2017). En annan faktor är att den ökade komplexiteten i teknologiska system resulterat i att det är svårare att förutse och hantera risker och hot. Gällande cyberrisker i en nationell kontext förmedlar Myndigheten för samhällsskydd och beredskap (2024) och Säkerhetspolisen (2022) att digitaliseringen och den tekniska utvecklingen sker hastigt varvid cybersäkerheten inte slutit upp i samma tempo – därför har hela vårt samhälle blivit sårbart för cyberhot och cyberangrepp sker dagligen mot Sverige. Likaså framhålls att digitaliseringen dessutom medfört uppkomsten av komplexa beroendekedjor och ett större beroende mellan IT-system som sträcker sig inom och mellan organisationer samt mellan länder, vilket resulterat i att cyberincidenter som påverkar flera organisationer blivit mer frekventa. Alltså har samhällets sårbarhet expanderat i relation med teknologisk progression och dess komplexitet, och den snabba takten i teknologiutvecklingen utgör en utmaning för att hålla jämna steg med säkerhetsåtgärderna för cyberrisker.

Cyberrisker inbegrips vanligtvis inom ramen för komplexa risker samt inom kategorin systemiska risker (Renn m.fl., 2022; Sonnsjö & Mobjörk, 2013). Systemiska risker är de risker som inte är avgränsade till nationella gränser eller enskilda sektorer, där riskernas skadliga effekter ofta är allvarsamma samt påverkar områden utanför det primära skadeområdet (Renn, 2021; van Asselt & Renn, 2011). Därtill är riskerna komplexa, i form av att de är multikausala samt omgivna av hög osäkerhet och/eller tvetydighet. Systemiska risker betraktas även som ett resultat av de hastiga och djupgående sociala, ekonomiska och tekniska förändringar i dagens moderna samhälle (Renn, 2021).

Parallellt med tilltagande digitalisering och teknologisk progression har vårt moderna samhälle blivit alltmer sammanlänkat – därav bärande av beroenden och beroendeförhållanden, vilket återspeglas i alla våra olika samhällssystem (Johansson & Hassel, 2016). Därigenom har även våra samhällsviktiga funktioner blivit alltmer sammankopplade, vilket gör att samhället numer är beroende av att samhällsviktiga funktioner fungerar utan avbrott. Att våra samhällsviktiga funktioner fungerar oavbrutet är viktigt för att kunna säkerställa leveransen av vitala funktioner såsom elektricitet,

vattentillgång, telekommunikation, transportnätverk och tillgång till sjukvård. Dessa centrala funktioner diskuteras vanligen inom ramen för kritisk infrastruktur. De här sektorerna och systemen har digitaliserats alltmer, vilket gjort infrastrukturen mer mottaglig och sårbar för cyberattacker (Atkins & Lawson, 2020). Inom den nationella kritiska infrastrukturen såsom energiförsörjning, livsmedelsförsörjning, transportsektorn samt hälso-och sjukvårdskedjan existerar kritiska beroenden – både inom och mellan systemen (Mittermaier m.fl., 2020). Likaså är dessa system starkt beroende av informationsteknologi och cyberdomänen, vilket genererar sårbarheter för cyberangrepp. Cyberangrepp mot kritisk infrastruktur och samhällsviktig verksamhet har inträffat världen över i närtid, där angreppen resulterat i allvarliga störningar flertalet gånger. Exempelvis skedde ett cyberangrepp mot Ukrainas elnät 2015, vilket gjorde att runt 230 000 personer var utan el i sex timmar (Dinku m.fl., 2021). Ytterligare exempel är när ett sjukhus i Tyskland 2020 utsattes för en cyberattack som stängde av vitala digitala resurser på sjukhuset (Eddy & Perlroth, 2020). Ett dödsfall betraktas ha orsakats av försenad behandling till följd av attacken, vilket kan vara det första kända indirekta dödsfallet av en cyberattack. Det uppmärksammas också att cyberattacker mot lantbrukare och attacker som påverkar livsmedelsäkerheten är en reell och föreliggande risk (Lindsten, 2024).

I takt med att våra samhällssystem blir alltmer sammankopplade ökar således riskerna för spridningseffekter, inom och utanför sektorer vid störningar relaterat till existerande beroendeförhållanden mellan olika system (Sonnsjö & Mobjörk, 2013). Ett cyberangrepp kan alltså både skapa störningar i enskilda sektorer och verksamheter men även potentiellt utlösa så kallade kaskadeffekter; exempelvis kan en attack riktad mot elnätet lamslå elförsörjningen och samtidigt störa kommunikationsnät, vilket i sin tur kan hindra olika räddningsinsatser (Atkins & Lawson, 2020). Likaså kan en vällyckad cyberattack mot säkerhetssystem inom vissa sektorer, såsom oljeraffinaderier, dammar, flyg eller kärnreaktorer – potentiellt resultera i skador på egendom såväl som förlust av liv.

Renn m.fl (2022) framhäver att systemiska risker (däribland cyberrisker) har genererat nya utmaningar för riskbedömning, riskhantering och riskstyrning, i relation till riskernas komplexa karaktäristika inklusive dess icke-linjära samband mellan orsak-verkan. En annan viktig aspekt i sammanhanget är att systemiska risker och dess potentiellt omfattande effekter tenderar att underskattas samt tilldelas förhållandevis liten uppmärksamhet i den offentliga diskursen, särskilt i relation till riskernas potentiella skada (Renn, 2021; Schweizer & Renn, 2019). Likaså anses det existera en generell, gedigen förståelse för enskilda risker och hot – men desto mindre för de risker och hot som bär potential att medföra kaskadeffekter (Panda & Bower, 2020). Risker förknippade med cybersäkerhet är en del av detta, vilket gör att riskbedömningar inom ramen för cyberrisker behöver beakta kaskadeffekter – relationellt med samtidens komplexa sammankopplade system. Detta utifrån att påverkan på små enheter i ett sammanlänkat system med beroendeförhållanden gör att cybersäkerhetsrisker bär potentialen att resultera i kollapser på en systemisk skala. Likaså eftersom cyberattacker kan få omfattande och allvarliga konsekvenser när attackerna är knutna till störningar på

infrastruktur, i synnerhet när kaskadeffekterna av cyberhoten skapar störningar i vitala samhällsfunktioner. Cybersäkerhet som fält har historiskt fokuserat på de tekniska aspekterna av informations- och säkerhetssystem (Burk & Kallberg, 2016). Och fastän skyddet av kritisk infrastruktur generellt sett är en nationell prioritet läggs fokus oftast på tekniska intrång – snarare än på att bedöma eller ta hänsyn till de eventuella konsekvenserna på samhället, människor och miljön om cybersäkerheten brister. En ytterligare aspekt i sammanhanget är att åtgärder mot cyberrisker som är teknikorienterade och fokuserade till informations- och kommunikationsteknik, endast fångar en del av en mycket bredare bild av cybersäkerhet (Chowdhury m.fl., 2021).

Sverige behöver precis som andra länder bemöta riskerna och hoten från cybermiljön, speciellt eftersom cybersäkerhet framträder som en alltmer omfattande problematik för stater världen över. En central aspekt i att bemöta problematiken kring cyberrisker är att utveckla policys för cybersäkerhet, där många regeringar på nationell nivå har utvecklat och implementerat cybersäkerhetsstrategier som en del av policybildningen (Azmi, m.fl., 2018; Zajko, 2015). Nationella säkerhetsstrategier har traditionellt behandlat hur säkerheten avseende externa militära hot ska uppnås (Craig m.fl., 2023). Men en förändrad hot- och riskbild i relation till globalisering och en mer sammanlänkad värld har medfört att nationella säkerhetsstrategier utvecklats: I samtiden omfattar de ytterligare säkerhetsrelaterade fenomen och frågor, såsom miljökatastrofer, pandemier och mänskliga rättigheter. I takt med teknisk expansion och digitalisering samt det ökade hotet från cybersfären har cybersäkerhet kommit att inbegripas i dessa nationella säkerhetsstrategier. Granskningen av nationella policydokument inom cybersäkerhetsdomänen är således viktig, då dessa representerar officiella riktlinjer och strategier som återspeglar en nationell syn på och hantering av cyberrelaterade risker och hot. Det i sin tur kan bidra till en fördjupad förståelse för regeringens och myndigheternas prioriteringar samt strategiska inriktningar, vilket ger insikter om Sveriges förmåga att adressera hela spektrumet av cyberrisker och hot.

1.1 Syfte och frågeställningar

Föreliggande uppsats tar avstamp i den omfattande tekniska utvecklingen och digitaliseringen i dagens sammanlänkade samhälle och dess samhörighet med cyberrisker, tillsammans med det tilltagande hotet från cybermiljön. Utifrån ett nationellt perspektiv med en kvalitativ ansats, syftar uppsatsen till att undersöka huruvida riskhanteringsstrategier och bedömningar för cybersäkerhet inom policysfären adresserar den komplexa karaktären av cyberrisker. Med särskilt fokus på om de speglar en system- och helhetsförståelse av cyberriskerna, inklusive riskernas potential att orsaka kaskadeffekter. Därigenom är avsikten att frambringa en utvidgad förståelse av cyberriskerna i en svensk kontext, med fokus på policydomänen. Följande frågeställningar har utformats för att undersöka studiens syfte närmare.

- På vilket sätt beskrivs relationen mellan cyberattacker och dess eventuella påverkan på liv, hälsa och miljö?
- Hur förhåller sig strategierna och bedömningarna till cyberattacker mot samhällsviktig verksamhet och kritisk infrastruktur?
- Vilka överväganden eller bedömningar görs i dokumenten angående risken för kaskadeffekter till följd av cyberattacker?

2 Bakgrund

Följande del presenterar begrepp som är centrala i sammanhanget, med avsikten att stödja förståelse för cybersfären som fenomen och dess associerade risker. Likaså syftar den till att ge en bakgrundförståelse kring Sveriges övergripande arbete med cybersäkerhet utifrån ett policyperspektiv.

Den hastiga digitaliseringen och samhällsförändringar som kommit med den, har resulterat i att frågor gällande cybersäkerhet ständigt blir viktigare (Strupczewski, 2021). En mängd olika termer existerar inom cyberområdet och utifrån den existerande litteraturen på området anses det inte råda tydlig universell konsensus kring alla termer (Kumar m.fl., 2018; von Solms & van Niekerk, 2013). Cyberrisker är ett tvärvetenskapligt område som framträtt relativt nyligen i den vetenskapliga diskursen (Strupczewski, 2021). En enskild vedertagen definition av cyberrisker existerar inte, antagligen relaterar till den tvärvetenskapliga karaktären av konceptet och den dynamiska karaktären av riskerna. Cyberrisker betraktas här som en term vilken syftar på en mängd olika riskkällor som påverkar tekniska och informationsrelaterade resurser, samt på risker som är förknippade med utförande av aktiviteter i cybersfären (Biener m.fl., 2015; Strupczewski, 2021). Cyberrisker omfattar inte bara den virtuella sfären utan även den fysiska världen, där de kan påverka olika system och verksamheter – termen innefattar därav diverse händelser som kan orsaka skada eller oönskad påverkan på olika nivåer, både inom privat och offentlig sektor samt på individnivå (Strupczewski, 2021).

Cybersäkerhet används som en allomfattande term i den övervägande delen av litteraturen på området (von Solms & van Niekerk, 2013). Likaså används den omväxlande med termen informationssäkerhet, varvid dessa överlappar men är inte helt identiska. Och ibland beskrivs nätverks- och informationssäkerhet som en del av cybersäkerhet (European Union Agency For Network and Information Security [ENISA], 2017). Termen i fokus för föreliggande uppsats är cybersäkerhet. FN:s specialiserade organ för informations- och kommunikationsteknologi: *The International Telecommunication Union* (ITU) definierar cybersäkerhet som samlingen av policyer, verktyg, riktlinjer, säkerhetsåtgärder, riskhanteringsmetoder och teknologier som kan användas för att skydda cybermiljön (ITU, u.å). ENISA (2017) beskriver att cybersäkerhet omfattar alla nödvändiga aktiviteter för att skydda cyberrymden, dess användare och berörda personer från cyberhot. Därtill att cybersäkerhet täcker alla aspekter av förebyggande, prognoser, upptäckter, analys och utredning av cyberincidenter. Cybersäkerhetspolicy i sammanhanget kan beskrivas som utvecklingen av olika säkerhetspolicys vilka är specifikt riktade mot cyberteknologin och dess system (Gorka, 2018).

Cyberrymden, även benämnt som cyberdomänen och cybermiljön betraktas här analogt med definitionen från Li & Liu (2018): Alla olika typer av sammankopplade nätverk, såsom IT-infrastrukturer, kommunikationsnätverk, datorsystem, virtuell informationsmiljö samt interaktionen mellan denna miljö och människor. Cyberhot betraktas som alla de händelser med förmågan att skada funktioner, uppdrag eller digitala

tillgångar via ett informationssystem, vilket kan ske genom obehörig åtkomst, förstörelse, avslöjande/ändring av information eller genom att hindra/störa leverans av tjänster (Li & Liu, 2018). Vidare existerar en samhörig term; cybersäkerhetshot vilket kan förstås som alla typer av försök och avsikter att skada eller störa ett nätverkssystem (Kumar m.fl., 2018). Cyberattacker och cyberangrepp betraktas här som alla obehöriga, avsiktliga handlingar i cyberdomänen som är riktade mot informationssystem, med syftet att orsaka skada, störning eller avbrott i tjänst eller åtkomsten till information (Li & Liu, 2018). Cyberattacker inbegriper även alla cyberincidenter som är sprungna ur skadliga avsikter och som resulterat i störningar, funktionsfel eller skador (ENISA, 2017).

Cybersäkerhet har tills relativt nyligen diskuterats främst i termer av en teknisk angelägenhet för riskhantering inom ramen för skyddet av kritisk informationsstruktur (Dunn Cavelty & Wenger 2020). Emellertid har detta förändrats i takt med teknisk progression och digitaliseringen ihop med de samhällsförändringar det medfört – och numera hanteras cybersäkerhet på högsta regeringsnivå som en nyckelutmaning för nationell säkerhet. Cyberattacker blir alltmer kostsamma, avancerade och mer strategiska än tidigare. Följaktligen har incidenter och attacker relaterat till cybersfären blivit framträdande element i säkerhetspolitiken. Både på nationell och internationell nivå, där stater och organisationer försöker finna adekvata sätt att bemöta dessa hot. I takt med att cyberhoten har utvecklats och avancerat, har alltså motåtgärder och politik som syftar mot ökad cybersäkerhet, expanderat. Men trots att cybersäkerhet numera är en integrerad del av cybersfären, är det fortfarande ett relativt nyvaket område inom policybildning (Tarhan, 2022).

I samtiden har de flesta stater utvecklat dokument som presenterar en uppsättning policyer för att uppnå mål och ambitioner inom cybersäkerhet, exempelvis i form av nationella cybersäkerhetsstrategier (NCSS) (Craig m.fl., 2022). Termen cyberstrategi avser inte endast regeringsdokument i form av NCSS, utan även andra ramverk från stater och myndigheter. Flertalet stater har mer än en NCSS, Sverige å andra sidan har i dagsläget endast en färdigställd där regeringen under 2023 inledde arbetet med att ta fram en ny NCSS (Regeringskansliet, 2023). Det nationella ansvaret för att hantera riskerna, hoten och sårbarheterna associerade med cybermiljön samt öka cybersäkerheten är delat, varvid ansvaret är fördelat inom både Regeringskansliet och mellan myndigheter (Riksrevisionen, 2023). I Sveriges NCSS beskrivs några av målsättningarna för arbetet med cybersäkerheten, och i ett försök att skapa en bättre struktur och enhällighet i arbetet med cybersäkerheten har regeringen ålagt uppdraget åt ett antal myndigheter att skapa ett nationellt cybersäkerhetscenter (NCSC).

2.1 Nationellt cybersäkerhetscenter

I december 2020 beslutade regeringen att upprätta ett nationellt cybersäkerhetcentrum (Försvarsdepartementet, 2020). Upprättandet beskrivs som en strategisk åtgärd i syfte att göra Sverige säkrare samt stärka den nationella samlade förmåga att bemöta cyberhot. Etableringen av centret framhålls initierats mot bakgrunden att cyberhoten mot Sverige är extensiva, där den utbredda teknikutvecklingen och digitalisering resulterat i att sårbarheterna såväl som hoten utökats – vilket medför att säkerheten behöver förstärkas nationellt. I Nationellt cybersäkerhetscenter (NCSC) ingår myndigheterna: FRA, Försvarsmakten, MSB och Säkerhetspolisen (NCSC, u.å.a). Arbetet görs även i samverkan med Polismyndigheten, Försvarets materielverk samt Post- och telestyrelsen. Uppgifter enligt regeringsuppdraget från 2020 är att koordinera arbetet för att förebygga, upptäcka och hantera cyberangrepp och andra IT-incidenter; kommunicera råd och stöd om hot, sårbarheter och risker relaterade till cyberdomänen, samt; utgöra en nationell plattform för samverkan och informationsutbyte för privata samt offentliga aktörer inom cybersäkerhetsområdet (MSB, 2024). Målsättningen är även att leverera lägesbilder och analyser avseende sårbarheter, hot och risker inom cyberområdet samt koordinera arbetet vid IT-incidenter och cyberangrepp. Inom ramen för centret har olika rapporter tagits fram, vilka beskrivs syfta till att uppmärksamma och sprida kunskap om cyberangrepp samt fungera som ett stöd. Detta för att möjliggöra att fler samhällsaktörer ska besitta fullvärdigt skydd samt kunna vidta åtgärder för att stärka sin motståndskraft mot olika typer av cyberangrepp.

3 Tidigare forskning

I följande avsnitt presenteras ett urval av tidigare forskning som positionerar uppsatsen i dess vetenskapliga sammanhang. Som tidigare nämnt är cyberområdet tvärvetenskapligt, vilket gör tidigare forskning på området diversifierad där cybersäkerhet som forskningsfält anses relativt färskt, speciellt inom policydomänen. Den forskning som presenteras nedan är inkluderad utifrån att den relaterar till cybersäkerhet och cyberrisker i en kontext kring kritisk infrastruktur och spridningseffekter, samt till den forskning som knyter an till granskning av nationella cybersäkerhetsstrategier och cybersäkerhet ur ett policyperspektiv.

3.1 Nationella cybersäkerhetsstrategier

Tidigare forskning som innefattar granskning av nationella cybersäkerhetsstrategier (NCSS) har framförts av exempelvis Gorka (2018), som jämfört strategier för länder inom Visegrádgruppen. Detta med syftet att belysa skillnader och likheter länderna emellan i en kontext kring deras framtida samarbete gällande en gemensam central- och östeuropeisk cybersäkerhetsstrategi. En annan studie involverar en kvalitativ analys av NCSS från 54 länder (Sverige inräknat) med syftet att identifiera motiv som driver utvecklingen av nationella cybersäkerhetsstrategier (Azmi m.fl., 2016). Luiijf m.fl. (2013) har studerat NCSS genom en jämförande innehållsanalys av 19 nationella cybersäkerhetsstrategier från 18 olika länder (Sverige exkluderat), för att hitta gemensamma tillvägagångssätt och brister i strategierna som sedan ska bidra till att belysa hur NCSS kan utvecklas. Luiijf m.fl. (2013) påvisar att det existerar betydande skillnader mellan strategierna i termer av fokus, struktur och innehåll. I studien poängteras att ENISA i sina rekommendationer för utformning av NCSS, dikterar att medlemsstaterna behöver erkänna utvecklingen och dynamiken i cybersäkerhetshoten genom att göra strategierna till levande dokument. Men Luiijf m.fl. (2013) pekar på att majoriteten av NCSS saknar ett dynamiskt förhållningssätt i avseendet att hantera teknologiska hot och utmaningar relaterade till cybersfären. Endast Tyskland och USA nämner specifikt dynamiken i hoten, och Japan är enda landet som betraktar dynamisk anpassning relaterat till de framväxande cybersäkerhetshoten samt planerar specifika åtgärder för det. Enligt Luiijf m.fl. (2013) speglar det att Japan betraktar cybersäkerhetsproblematiken från ett vidare, mer dynamiskt säkerhetsperspektiv än övriga länder. Ytterligare belyser studien relationen mellan NCSS, andra nationella säkerhetsstrategier och andra ramverk inom säkerhetsområdet, där många NCSS är otydliga i avseendet med sambandet till andra nationella säkerhetsstrategier eller internationella ramverk. Värt att notera i sammanhanget är att artikeln är över tio år gammal.

Vidare påvisar Luiijf m.fl. (2013) att de flesta NCSS explicit uttrycker cybersäkerhethoten mot nationell kritisk infrastruktur, men att sambandet mellan NCSS och nationella strategier för skydd av kritisk infrastruktur (CIP) är mindre explicit uttryckt. Luiijf m.fl. (2013) menar att det är anmärkningsvärt att nio av tio EU-

medlemsstater inte sammanlänkar relationen med sina NCSS till den europeiska direktivet för skydd av kritisk infrastruktur, där Estland är enda undantaget. Sammanfattningsvis betonar Luiijf m.fl. (2013) behovet av mer integrerade strategier för cybersäkerhet på nationell och internationell nivå, för att effektivt kunna hantera de växande hoten och utmaningarna härledda från cybersfären. Det inkluderar att tydligt definiera cybersäkerhetsbegreppet och anta dynamik i strategierna för att hantera de teknologiska hoten. Likaså rekommenderas ett fokus på harmonisering av policys för att uppnå effektivare hantering av cybersäkerhetshoten.

Ytterligare innehållsanalys av NCSS har genomförts av Craig m.fl. (2022), där 83 strategier från olika länder (Sverige inkluderat) ingår. Studien kastar ljus på att mycket av tidigare forskning gällande strategier mot cyberhot har gjorts ur andra perspektiv än på staters konkreta föreslagna politik för cybersäkerhet, vilket beskrivs i deras officiella dokument. Craig m.fl (2022) framhåller att staters olika policys och mål för cybersäkerhet beskrivs i de nationella cybersäkerhetsstrategierna, vilket gör dessa dokument till användbara källor att för att förstå hur stater betraktar och hanterar cyberhoten och dess tillhörande risker. Studien påvisar skillnader i fokus mellan samarbetsinriktade och icke-samarbetsinriktade strategier, både på nationell och internationell nivå. Likaså pekar Craig m.fl (2022) på att stater har olika prioriteringar och förhållningssätt i sina dokument, där vissa dimensioner av cybersäkerhetspolitiken och initiativ mot cyberhoten prioriteras högre jämfört med andra. Varvid det finns tydliga skillnader mellan hur olika politikområden prioriteras i dokumenten. Områden såsom mänskligt kapacitetsbyggande och standarder var mer vanligt förekommande, medan politikområden som rör internationell kapacitetsuppbyggnad desto mindre. Craig m.fl. (2022) framhåller att många länder lägger förhållandevis liten fokus på att presentera konkreta förslag i form av politikområden för ökad cybersäkerhet, och menar att denna aspekt kan indikera en bristande beredskap för cybersäkerhetsrisker hos många regeringar. Slutligen framförs att det existerar ett behov av fortsatt forskning på området.

Sammanslutningen av studierna som analyserat NCSS visar på variationen av perspektiv och fokus strategier kan ha, samt brister som existerar i strategier. Studierna av Craig m.fl. (2022) och Luiijf m.fl. (2013) antyder att det finns variationer i hur länder och prioriterar olika områden inom cybersäkerhet och existerande skillnader mellan NCSS i termer av fokus och innehåll. Studien av Craig m.fl. (2022) framför relevansen av att studera officiella policydokument för cybersäkerhet samt att det existerar ett behov av ytterligare forskning på området. Studierna av Gorka (2018); Luiijf m.fl. (2013); Craig m.fl. (2022) samt Azmi m.fl. (2016) speglar att det finns många perspektiv att anta i studiet av cybersäkerhetsstrategier. Således att forskning på NCSS utifrån det som presenterats, är diversifierat – men att många perspektiv behövs för att strategierna ska vara helomfattande.

3.2 Kritisk infrastruktur, samhällsviktig verksamhet och kaskadeffekter

Att cyberattacker riktade mot sjukhus, medicintekniska produkter och vårdinrättningar blir vanligare poängteras i forskning av Bernard m.fl. (2020). Trots att tidigare cyberattacker påvisat att hälsosektorn utgör ett betydande mål bland nationell kritisk infrastruktur, på grund av dess centralitet för samhället, får sjukvårdssektorn mindre uppmärksamhet än annan kritisk infrastruktur. Studien påvisar att störningar i tekniska system i sjukvårdsnätverk kan resultera i betydande destabiliserande konsekvenser samt leda till förlust av liv. Bernard m.fl. (2020) framhåller att det relaterar till att den potentiella attackytan är omfattande utifrån sjukhussystemets komplexitet, i form av det breda spektrumet av anställda samt användningen av leverantörer och programvara från tredje part i de tekniska systemen. Dessutom använder hälso- och sjukvårdssektorn ofta föråldrade IT-system, en mängd olika kliniska informationssystem och medicinska enheter med olika operativsystem vilka alla är sårbara för cyberattacker. Enheter som används på sjukhus, antingen för att övervaka patientstatus eller för att ge medicinsk vård såsom dialysenheter eller respiratorer, såväl som medicinsk utrustning implanterad i patienter (exempelvis pacemaker och insulinpumpar) är beroende av nätverksanslutningar. Bernard m.fl (2020) pekar på att komplexiteten i interaktionerna mellan dessa olika system och de personer som använder dem, lämnar hälsosektorn öppen och sårbar för en mängd olika cyberattacker. Slutsatser från studien belyser att det föreligger ett aktuellt och systemiskt hot mot sjukvårdssektorn från cyberattacker, vilket för närvarande inte behandlas på ett systematiskt sätt där vidare diskussion kring lagstiftning och regelverk för att hantera hotet behöver ske på policynivå. Bernard m.fl (2020) konstaterar att många fördelar har kommit med växande teknologi och inneburit viktig utveckling för hälso- och läkemedelssektorerna, men att konsekvenserna av cyberattacker mot dessa sektorer behöver övervägas på nationell säkerhetsnivå.

Utöver det forskningen från Bernard m.fl (2020) visat, existerar en samstämmighet kring vikten av att skydda kritisk infrastruktur. Kritisk infrastruktur är en av de mest avgörande sektorerna i samhället eftersom många viktiga verksamheter och tjänster är beroende av deras komplexa leverans (Atkins & Lawson 2020; Kumar m.fl., 2018). Den kritiska infrastrukturen är avgörande för det moderna samhällets funktion och verksamheterna inom dessa sektorer blir alltmer digitaliserade. Samtidigt är IT-komponenterna i digitaliserade system ofta sårbara för attacker eftersom de har exploaterbara funktioner, därav är det centralt att skydda sektorer inom kritisk infrastruktur eftersom de är frekventa mål för cyberattacker (Atkins & Lawson, 2020; Rulleau, 2023; Palleti m.fl., 2021). Albahar (2017) lyfter ytterligare aspekter kring vikten av att skydda nationell kritisk infrastruktur: Eftersom cybersfären inte har några konventionella gränser kan cyberattacker utföras från långa avstånd och med snabba hastigheter. Angrepp kan alltså genomföras på distans och kräver inte fysisk närvaro, vilket speglar att skador från cyberattacker numera kan bli lika dödliga som konventionell krigföring, om inte mer.

Pescaroli & Alexander (2015) beskriver att kaskadeffekter är den dynamik som uppstår när en fysisk händelse eller incident, utlöst av teknologisk eller mänsklig faktor, leder till en följd av händelser inom mänskliga delsystem som resulterar i ekonomiska, fysiska eller sociala störningar. Alltså en initial påverkan som utlöser andra fenomen och kedjereaktioner, vilket leder till konsekvenser av betydande omfattning. Vidare är processen komplex och utvecklas över tid, även starkt kopplad till systemens sårbarhet snarare än till de enskilda hoten: Om sårbarheterna är utbredda eller inte hanteras korrekt i systemet kan även mindre hot och händelser generera omfattande kedjeeffekter. Pescaroli & Alexander (2015) & Alexander (2018) pekar även på att ömsesidiga beroendeförhållanden och kritisk infrastruktur är viktiga faktorer som måste tas upp i riskreducerande metoder för att begränsa kaskadeffekter. Detta då kritisk infrastruktur ofta är kanalen genom vilken kaskadeffekter sprids, relaterat till att våra samhällssystem övergår till att bli mer komplexa och systemen därinom alltmer ömsesidigt beroende samt beroende av fungerande teknologi och digital infrastruktur.

Genom Cutter (2018) framhävs att kaskadkatastrofer är extremhändelser som innebär att kaskadeffekter ökar successivt och genererar sekundära, oväntade händelser med betydande påverkan. Vidare kastar Cutter (2018) viktigt ljus på att vad som skiljer kaskadkatastrofer från andra typer av katastrofer, vilket är inkluderingen av och förlitandet på komplexa och sammankopplade sociotekniska system, såsom den kritiska infrastrukturen. Cutter (2018) framhåller att kaskadeffekter och deras allvarliga konsekvenser oftast kan härledas till den kritiska infrastrukturen som har en avgörande roll för samhällets funktion. Vidare att det sociala funktionella beroendet på den kritiska infrastrukturen är resultatet av upparbetade sårbarheter hos det moderna samhället, där teknologin är tätt integrerad och sammanlänkad, vilket innebär att störningar och avbrott är mer eller mindre oundvikliga. Cyberattacker kan leda till sådana typer av allvarliga konsekvenser och kaskadeffekter, relaterat till att många av sektorerna inom kritisk infrastruktur är avgörande för samhällets funktion (Palleti m.fl., 2021; Rulleau, 2023). Likaså utifrån att det finns ömsesidigt beroende mellan olika infrastrukturer, vilket gör att effekterna kan överlappa och påverka andra infrastrukturer och system. Alltså kan en cyberattack i en komponent av ett ömsesidigt beroende system orsaka kaskadeffekter som potentiellt kan kollapsa hela system.

Utifrån ovanstående forskning kan det anses råda konsensus kring att cyberattacker besitter en potential i att resultera i kaskadeffekter, och att kaskadeffekter kanaliseras genom kritisk infrastruktur— där kritisk infrastruktur betraktas som särskilt sårbart för cyberattacker. Sammantaget speglar det samspelet mellan riskerna som existerar kring kritisk infrastruktur, cyberattacker och kaskadeffekter. Forskning gjord av Panda & Bower (2020) sammanfattar och kastar ljus på denna relation ytterligare: Händelser som resulterar i kaskadeffekter bortom det initiala området kan påverka samhället, medborgare och sammankopplade system allvarligt. Vidare framhålls att till skillnad från traditionella fysiska risker existerar cyberrymden i en virtuell domän, vilken är integrerad i och ansluten till majoriteten av de viktiga samhällssektorerna och systemen. Därav kan

cybersäkerhetsrisker leda till allvarliga och storskaliga problem när de kopplas till störningar på kritisk infrastruktur, utifrån potentiella kaskadeffekter som cyberattacker kan generera. Därtill påpekas att kaskadeffekter som fenomen försvårar förståelsen av enskilda risker samt gör det svårt att bedöma hur stora störningar som kan uppstå, eftersom många olika faktorer kan påverka händelseförloppet. Slutsatser från Panda & Bower (2020) betonar att tillvägagångssätt för riskhantering således behöver tillåta en integrering av cybersäkerhetsrisker och dess samhörighet med kaskadeffekter samt ett helhetsinriktat synsätt som tar hänsyn till hela samhället, för att kunna hantera dessa komplexa, sammanflätade risker.

Forskningen som presenterats belyser att cyberattacker mot kritisk infrastruktur, såsom sjukvårdssystem, inte bara utgör en teknisk utmaning utan också innebär en risk för samhällsviktig verksamhet och människors hälsa och liv såväl som för miljön. Studier som belyser dimensionen kring kaskadeffekter från cyberattacker på kritisk infrastruktur, som exemplifierats av bland andra Pescaroli & Alexander (2015); Cutter (2018) och; Panda & Bower (2020) visar på behovet av att betrakta cyberrisker ur ett systemiskt perspektiv. Därtill på att existerade sårbarheter i våra teknologiska sammankopplade system är problematiska – vilket pekar på att medvetenhet behöver råda kring riskernas potentiella kaskadeffekter och omfattande konsekvenser med dessa. Presenterad forskning har även bidragit till att spegla samspelet mellan riskerna som existerar kring kritisk infrastruktur, cyberattacker och kaskadeffekter. Det bidrar i sin tur till förståelsen av att cyberriskerna kan spridas över olika sektorer och system och förvärra konsekvenserna av en cyberattack betydligt. Policydokument som NCSS är centrala för att adressera dessa komplexa risker eftersom de representerar en politisk och samhällelig vision för att hantera cyberhoten, vilket innebär att policydokument behöver ta hänsyn till de potentiella konsekvenserna av cyberattacker på samhällets funktion och inte fokusera på attackerna enskilt. Likaså behövs en helhetsförståelse som betraktar cyberriskerna ur ett systemiskt perspektiv som inkluderar aspekter kring cyberriskers potential för kaskadeffekter. Trots att det finns forskning som inkluderar Sverige i analyser av NCSS föreligger en brist på studier som är specifikt inriktade på den svenska kontexten, vilket möjligen relaterar till att Sverige endast haft en NCSS i sju år.

4 Teoretisk referensram

I följande kapitel presenteras uppsatsens teoretiska perspektiv, vilka tillsammans utgör uppsatsens teoretiska referensram. Utgångspunkten är ett systemteoretiskt perspektiv, kombinerat med normal accident theory samt koncepten systemiska risker och riskstyrning.

4.1 Systemiska risker & risk governance

Sedan den internationella finanskrisen 2008 har systemiska risker som koncept blivit framträdande, både i litteraturen och i riskdiskursen generellt (Renn m.fl., 2019). I dagsläget diskuteras systemiska risker inte bara i ekonomiska termer utan även i sammanhang kring risker kopplade till pandemier, klimatförändringar och cybersäkerhet. En tidig definition av systemiska risker är den av Kaufman & Scott (2003, s. 371) som definierar begreppet i en ekonomisk kontext: "Systemic risk refers to the risk or probability of breakdowns in an entire system, as opposed to a breakdown in individual parts of components, and is evidenced by comovements (correlation) among most or all the parts". International risk governance council (2018) beskriver att system som är utsatta för dessa risker är de som är djupt sammanflätade med varandra, där denna sammankoppling genererar komplexa orsakssamband och strukturer. Systemiska risker är dessutom dynamiska i sin utveckling över tid, icke-linjära i sina orsak-verkan-samband samt vanligen slumpmässiga och oregelbundna (stokastiska) i termer av deras effekter, även potentiellt globala i räckvidd. Riskerna innefattar därutöver de potentiella hot och risker vilka kan skada funktionen av samhällets kritiska system (Renn m.fl., 2022). Likaså kännetecknas de av att dess konsekvenser kan sträcka sig bortom det ursprungliga systemet, för att följaktligen påverka andra system och funktioner bortom det initiala. Sammantaget belyser detta hur risker med systemisk karaktär är inbäddade i de större samhällsprocesserna och djupt integrerade i våra samhällssystem (Renn m.fl., 2011).

Vidare är systemiska risker fenomen som är kantade av stark komplexitet och bär ett beroende av varandra, där riskerna har sitt ursprung i tätt ihopkopplade system och kännetecknas av kaskadeffekter och icke-linjära utvecklingar (Schweizer, 2019). Således skiljer sig systemiska risker från konventionella, då de involverar många fler interagerande element vars effekter är oförutsägbara (Renn m.fl, 2022). Systemiska risker relaterar även till komplexitet och dynamik hos risker i det moderna samhället, vilket involverar flera ömsesidigt beroende orsak-verkan-samband mellan exempelvis samhällssektorer och tekniska komponenter. Det gör att systemiska risker även betraktas som ett resultat av de hastiga och djupgående ekonomiska, sociala och tekniska förändringarna i dagens moderna samhälle, där teknologisk progression i samhället föranlett potentiella hot som kan karaktäriseras som systemiska risker – såsom cyberbrottslighet och cybersäkerhetsrisker (Renn m.fl, 2022; Renn, 2021). Egenskaper hos systemiska risker är även typiska komponenter i komplexa teknologier, särskilt inom samhällets kritiska infrastruktur. Kritiska infrastrukturer fungerar som prototyper för

systemiska risker eftersom de påverkar system på vilket samhället är beroende av, där störningar i infrastrukturen kan orsaka kollaps av hela system samt påverka andra ihopkopplade (samhälls)system på ett oförutsägbart sätt. På så sätt är systemiska risker inte avgränsade till nationella gränser eller enskilda sektorer och komplexa i form av att de är multikausala samt omgivna av hög osäkerhet och/eller tvetydighet, där riskernas skadliga effekter är ofta allvarliga (van Asselt & Renn, 2011; Renn, 2021).

Teoritiseringar från Welburn & Strong (2022) belyser att cyberriskernas utbredning inte är helt förstådda än, och att betrakta dem som systemiska risker är en del av att öka förståelsen för dess allvarliga konsekvenser. Cyberrisker behöver benämnas och förstås som systemiska cyberrisker, vilket innebär att integrera fälten systemiska risker och cyberrisker mer tydligt. Riskerna behöver förstås som systemiska relaterat till cyberattackers potentiella dominoeffekter (kaskadeffekter), där cyberincidenters effekter och risker kan och historiskt har spridits över sammanlänkade system. Welburn & Strong (2022) menar vidare att tidigare cyberincidenter (exempelvis attacken mot Ukrainas elnät 2015) till skillnad från enskilda cyberincidenters isolerade effekter, påvisar de utbredda konsekvenserna och vanligen undermåligt förstådda kedjereaktionerna av cyberincidenter, vilket exemplifierar potentialen för systemisk risk i den digitala världen.

4.2 Risk governance

Renn m.fl. (2011) framhåller att traditionella perspektiv på riskhantering är otillräckliga i diskursen kring systemiska risker utifrån riskernas speciella karaktäristiska, därför kräver systemiska risker ett holistiskt tillvägagångssätt innefattade ett helhetsperspektiv vad gäller identifiering, bedömning och hantering. De systemiska riskerna behöver betraktas i termer av existerande beroendeförhållanden, spridningseffekter samt inkludera aspekter kring hur olika risker är beroende av varandra och hur deras konsekvenser sprids och påverkar andra områden utöver det initiala. Detta leder in på *risk governance* - *riskstyrning*. Riskstyrning i sammanhanget kring systemiska risker avser både den institutionella strukturen och policyprocessen som styr samt begränsar de gemensamma aktiviteterna hos ett samhälle, grupp eller en internationell gemenskap för att reglera, reducera eller kontrollera risker (Renn m.fl., 2011). Riskstyrning erbjuder en teoretisk såväl som en normativ grund för hur osäkra, komplexa och/eller tvetydiga risker bör hanteras, alltså en grund för hur systemiska risker bör hanteras eftersom dessa risker bär sådana egenskaper. En centralitet inom riskstyrning är erkännandet av att det finns olika typer av risker som också behöver hanteras på olika sätt – där idén kring riskstyrning syftar till att bidra till en förändring i form av att skapa en bredare uppfattning om risker.

Riskstyrning är enligt Renn m.fl., (2011) en dynamisk styrningsprocess som inbegriper kontinuerligt lärande samt justering för att kunna generera en adekvat hantering av risker som bär komplexitet, osäkerhet och/eller tvetydighet. I kontexten kring systemiska risker innefattar riskstyrning alltså ett dynamiskt förhållningssätt i styrningen och hanteringen av systemiska risker – således även i styrningen av risker relaterade till cyberdomänen.

Riskstyrning bör följaktligen vara adaptiv och kunna anpassa sig till föränderliga förhållanden och nya insikter om risker, vilket kräver en flexibel och dynamisk strategi för att hantera och reagera på nya och framväxande hot och risker (Renn m.fl., 2022; Renn m.fl., 2011). Även Schweizer (2019) menar att systemiska risker utgör en utmaning för riskstyrning eftersom riskerna är sammanlänkade, komplexa, icke-linjära i sina orsak-verkan-relationer samt att dess konsekvenser är allvarliga och omfattande. Dimensionen kring systemiska riskers förmåga att vara gränsöverskridande som leder till konsekvenser vilka inte är begränsade i tid och rum, är en ytterligare faktor. En följd av detta är att insatserna för styrning av systemiska risker blir höga enligt Schweizer (2019), och därav behöver de systemiska aspekterna beaktas i riskstyrningen.

4.3 Systemteoretiska perspektiv

Systemteori innebär enligt Sparf (2009) att betrakta samhället och dess olika ingående delar som integrerade system vilka är sammankopplade och påverkar varandra; ett perspektiv som innebär att betrakta världen som ett sammankopplat system. Utgångspunkten är att samhället består av flertalet system på olika nivåer: Från globala ekonomiska system till mindre avgränsade enheter såsom organisationer eller enskilda individer – många olika system var för sig, men som är sammanbundna och påverkar varandra. Sparf (2009) pekar på två grundtankar inom systemperspektivet: System betraktas som självreglerande enheter vilka försöker upprätthålla balans och överleva genom att interagera med sin omgivning, genom utbyte av energi och materia och: Att varje system är uppbyggt av en mängd mindre enheter som alla har egen funktion och att de påverkar varandra. Systemteori fokuserar således på systemen som helhet, inte på de separata ingående delarna och betraktas som komplexa strukturer där egenskaper och beteenden därinom uppstår från interaktionerna mellan dess olika komponenter – snarare än från egenskaperna hos de enskilda delarna (Larsson m.fl., 2010). Det betyder att det är nödvändigt att undersöka de samband som finns mellan systemets olika delar för att förstå ett system som helhet. En central aspekt inom systemteori är *emergens* vilket uppstår från interaktionen mellan fristående delar inom ett system när de slutar vara fristående och börjar påverka varandra. Olyckor kan betraktas som emergenta fenomen som inträffar när systemets komponenter interagerar med varandra, och påverkar varandra på sätt som inte var förutsägbara utifrån deras individuella egenskaper.

Översätts ovanstående till en riskkontext innebär det följaktligen att ett system är beroende av alla enheter inom systemet, vilket betyder att om en enhet utsätts för en risk – kan det påverka hela systemet (Sparf, 2009). Om en enhets funktion slås ut riskerar följaktligen även resterande delar i systemet att sättas ur funktion. Dessutom kan det faktum att olika system är nära sammankopplade innebära att om en enhet i ett system hotas, kommer även andra system att hotas. Sparf (2009) exemplifierar detta genom att det inte endast är transporter som skulle påverkas om olja tar slut, även affärsverksamheter, sjukvård, arbetsplatser, skolor och andra områden skulle påverkas eftersom varken tjänster eller människor skulle kunna nås normalt. Detta inflytande över

systemgränser speglar betydelsen av ett systemteoretiskt perspektiv på risker för att förstå hur olika system är sammanfogade med varandra. En betydelsefull aspekt av systemteorin gällande risker är att perspektivet ger insikt om att risker inte är isolerade till enskilda områden. I stället påverkar en risk för en del av samhället andra delar, vilket leder till att olika system existerar inuti varandra och är tätt sammankopplade på olika nivåer. System är inte heller isolerade enheter utan överlappar varandra i stor utsträckning. Enligt Shaked m.fl. (2017) är systemteoretiska perspektiv ett tvärvetenskapligt ramverk som kan anpassas till en bred uppsättning områden. De betonar att det essentiella med perspektivet är att det undersöker system holistiskt. Ett systemperspektiv är således ett sätt att betrakta system som en komplex sammansättning av många sammanlänkande komponenter som behöver samarbeta för att helheten av systemet ska fungera adekvat.

Ytterligare perspektiv inom systemteori är det kring sociotekniska system, vilket betonar helheten av ett integrerat system i form av relationen mellan tekniska och sociala aspekter och hur dessa komponenter samverkar (Leveson m.fl., 2009). Sociotekniska perspektiv belyser att ett system, såsom en organisation eller ett samhälle innefattar interaktioner mellan teknik och människor – vilka är ömsesidigt beroende (Klein, 2014). Varje ingående del påverkar varandra; teknologin påverkar människors beteende och människors beteende påverkar teknologins funktion. Tekniska system existerar således inte isolerat från mänskligheten, utan är integrerade i sociala, organisatoriska och kulturella strukturer. Larsson m.fl (2010) karaktäriserar dessa system som komplexa där exempel på komplexa sociotekniska system i samhället är kärnkraftverk och flygplatser. Sociotekniska system i vårt moderna samhälle tenderar att öka i komplexitet där dessa komplexa system består av flera delar som är beroende av varandra, vilket innebär att det kan uppstå oväntade interaktioner mellan systemets olika komponenter som inte är uppenbara. Le Coze (2018) pekar på detta samband ytterligare: När olyckor inträffar i komplexa och hög-riskfyllda system såsom inom kärnkraften, handlar det inte bara om tekniska förfaranden utan sådana typer av händelser är bäst förstådda genom den sociotekniska linsen. Eftersom det finns en koppling mellan tekniska aspekter och mänskliga, sociala eller samhälleliga faktorer som påverkar hur systemen fungerar. Exempel på sådana händelser inkluderar katastrofer som Fukushima-olyckan i Japan 2011, där tekniska fel inte endast bottnade i maskinella/tekniska brister utan också berodde på mänskliga beslut och samhälleliga faktorer.

Utifrån sociotekniska aspekter inom systemteori utgör sociotekniska system en integrerad helhet där människor, teknologi och organisatoriska strukturer samverkar för att uppnå gemensamma mål (Malajti m.fl., 2018). Systemen kännetecknas av en hög grad av både social och teknisk komplexitet samt är beroende av sin operativa interna miljö och påverkas även av den externa miljön de är en del av. Olika faktorer i omgivningen, såsom politiska, juridiska, sociala eller tekniska eller miljömässiga förändringar kan ha en betydande inverkan på systemen. Således influeras sociotekniska system av externa faktorer som kan påverka hur både de sociala och tekniska delarna inom systemet fungerar, där mänsklig påverkan ökar komplexiteten. Följaktligen påvisar de teoretiska

resonemangen kring sociotekniska aspekter vikten av att betrakta tekniska system i sin helhet med hänsyn till både tekniska och sociala aspekter. Perspektivet är således en del av att beskriva förhållandet mellan teknik och samhälle, för att generera förståelse för hur dessa två världar samverkar i en komplex synergi.

Sociotekniska perspektiv inom systemteori har traditionellt koncentrerats till arbetssystem och organisatoriska sammanhang inom vilka individer samverkar i syfte att uppnå ett kollektivt mål eller uppgift, exempelvis inom fordons-och koldriftssindustrin (Eason, 2014). Dock kan sociotekniska system vara avsevärt större än enskilda organisationer eller industrier. Cybersäkerhetsrisker är också att betrakta som sociotekniska till sin natur, då dessa inte endast emanerar från tekniska sårbarheter utan också från mänskliga interaktioner (McEvoy & Kowalski, 2019). Sociotekniska aspekter negligeras vanligen i utformningen av och i riskanalyser och hanteringsmetoder inom cybersäkerhet. Det innebär att det existerar ett gap mellan de befintliga perspektiven om sociotekniska system och tillämpningen av dessa inom cybersäkerhet enligt McEvoy & Kowalski (2019). Även Malajti m.fl. (2018) påpekar att sociotekniska perspektiv inom systemteorin applicerade på informations- och cybersäkerhetsområdet är småskaligt och något som fått lite uppmärksamhet. Likaså att sociotekniska perspektiv inom systemteorin bidrar till att skapa förståelse för vikten av att likvärdigt betona och betrakta de sociala, tekniska och miljömässiga dimensionerna av informations- och cybersäkerhet för att uppnå optimal säkerhet.

4.4 Normal accident theory

Charles Perrow var den som initialt utformade teoretiseringar kring ”normala olyckor” som sedermera blivit känt som normal accident theory (NAT). Perrow (1984 s. 3–4) menar att många högriskteknologier och system såsom kemiska industrier, kärnkraftverk, flygsektorn och liknande bär specifika karaktäristika utöver deras giftiga och explosiva egenskaper som gör olyckor i dessa system oundvikliga, till och med normala. Detta i form av hur störningar kan interagera med varandra och hur olika system är sammankopplade. Dessa karaktärsdrag hos systemen kallas *interaktiv komplexitet* och *tät sammankoppling* och ökar risken för olyckor (Perrow, 1984, s. 5–8). Tät sammankoppling innebär att systemets delar är direkt sammankopplade och att ett fel i en del direkt leder till ett fel i en annan del: Varje del av systemet är nära beroende av andra delar vilket gör systemet mycket sårbart för störningar. I tätt sammankopplade system är varje del starkt beroende av varandra och med tanke på systemets egenskaper är flera och oväntade interaktioner av störningar oundvikliga – vilket kan resultera i multipla störningar. Interaktiv komplexitet förklaras som när en serie händelser uppstår i ett system utan förutbestämd ordning och som inte omedelbart är uppenbara eller förståeliga. Det innebär att händelser kan utvecklas på ett oväntat sätt och påverka andra delar av systemet på ett sätt som inte går att förutse – vilket kan generera så kallade systemolyckor. Tätt sammankopplade system som präglas av interaktiv komplexitet besitter eventualiteten att medföra storskaliga olyckor och katastrofer genom att små händelser eller fel sprids

genomgripande över systemet. Det skapar kedjereaktioner av störningar, där dessa beroendeförhållanden inte alltid uppenbara initialt utan först efter en olycka inträffat.

I senare tid beskriver Perrow (2011) att även om åtgärder görs för att förhindra olyckor kommer normala olyckor oundvikligen inträffa i de komplexa och tätt sammankopplade systemen i dagens moderna samhälle. Det kan resultera i den typ av oförutsägbara, kaskadhändelser som sågs vid multikatastrofen i Japan 2011 och olyckan som följde i kärnkraftverket Fukushima. Utifrån NAT uppstår alltså olyckor i tekniska system från incidenter eller lokala fel som sprider sig och stör eller skadar det större systemet, eftersom det i interaktivt komplexa och tätt sammankopplade systemen är svårt att förstå samt kontrollera incidenter och förhindra olyckor (Leveson m.fl., 2009). Shrivastava m.fl. (2009) beskriver att de två systemiska dimensionerna; naturen av interaktioner inom ett system samt graden av koppling mellan dess subsystem är centrala för NAT:s huvudpoäng: Ett fel i teknologiska system som samtidigt är komplexa och tätt kopplade kan under specifika omständigheter leda till systemolyckor. När omständigheterna är rätt kan störningar utlösa andra, som kan interagera med varandra på ett sätt som är svårförståeligt. De komplexa interaktionerna kan i sin tur generera kaskadhändelser hastigt.

Backman (2023) framhäver att NAT är ett perspektiv som klassiskt applicerats inom forskning avseende säkerhet, tekniska system och säkerhetsarbete i högriskmiljöer. Därtill att NA-dynamiken som beskrivits ovan är närvarande när (högrisk)-system har två samtidiga egenskaper: Interaktiv komplexitet och tät koppling mellan systemkomponenterna vilket är karaktärsdrag som existerar i alla system inom cyberdomänen. Vidare menar Backman (2023) att delar och perspektiv från NAT gynnsamt kan användas för att förstå hur störningar i enskilda systemkomponenter i de sociotekniska system som ligger till grund för kritisk infrastruktur, kan resultera i kaskadeffekter och oväntade konsekvenser. Likaså för att förstå hur denna dynamik speglar risker för sidoeffekter sprungna ur offensiva cyberhändelser.

4.5 Operationalisering

I föreliggande uppsats granskas strategier och bedömningar avseende cybersäkerhets-risker genom en integrering av flera teoretiska perspektiv och begrepp. Systemiska risker som koncept är inkluderat för att undersöka huruvida strategier och bedömningar tar hänsyn till komplexiteten och dynamiken i cybersäkerhetsriskerna; om beståndsdelar inom konceptet återfinns och därigenom huruvida cyberriskerna betraktas som en systemisk risk. Det angränsande begreppet riskstyrning betonar vikten av att anamma ett helhetsperspektiv i hantering och styrning av systemiska risker. Genom att lyfta och integrera dynamiska aspekter på riskhantering sprungna ur riskstyrning – belyses vikten av kontinuerlig anpassning och förbättring av riskhanteringsstrategier gällande systemiska risker och i relation till en värld präglad av snabba förändringar. Systemteori erbjuder en övergripande ram för att förstå de komplexa interaktionerna mellan olika

komponenter inom system och hur risker kan spridas genom dessa beroenden. Således erbjuds ett verktyg för att få djupare förståelse för hur enskilda händelser kan få konsekvenser för hela system. Vidare används det sociotekniska systemperspektivet utifrån dess betoning på det ömsesidiga, komplexa samspelet mellan tekniska och sociala aspekter inom system och inkluderas för att analysera hur mänskliga faktorer och tekniska system samverkar inom cybersäkerhet.

NAT är inkluderat utifrån att perspektivet erbjuder teoretiska insikter om komplexa, tätt sammanlänkade system och spridningseffekter. Likaså anses de harmonisera med de övriga teoretiska utgångspunkterna och tillsammans utgöra en sammanhängande ram för att adressera ett systemperspektiv på risker inom cybersäkerhet. De teoretiska utgångspunkterna betraktas även i linje med den tidigare forskning som presenterats gällande beroendeförhållanden, kaskadeffekter, kritisk infrastruktur och hur det tillsammans hänger ihop med cyberriskerna. Sammanfogat formar de en enhetlig ram för att förstå cyberrisker ur ett bredare perspektiv, särskilt med tanke på de sammanlänkade systemen som präglar den digitala arenan. Tillsammans utgör detta en ram för att granska nationella strategidokument med avseende på ett helhetsperspektiv samt på deras förmåga att adressera och hantera komplexiteten och dynamiken i cyberrisklandskapet. Slutligen utgör dessa utgångspunkter tillsammans det analytiska ramverket för uppsatsen.

5 Metod

I följande del presenteras den metod som tillämpats, proceduren kring datainsamling samt den analysprocess som utförts för att bearbeta insamlad empiri. Uppsatsens metod är av kvalitativ karaktär med en deduktiv ansats, där en dokumentanalys i form av en riktad innehållsanalys har genomförts med utgångspunkt att möta uppsatsens syfte och besvara dess frågeställningar.

5.1 Datainsamling, tillvägagångssätt och urval

Som nämnt har Sverige för tiden när uppsatsen skrivs endast en nationell cybersäkerhetsstrategi (NCSS). Initialt avsågs med hänvisning till att den nya NCSS är under utformning – att använda *Slutbetänkande av Cybersäkerhetsutredningen* (SOU: 2021:63) som ytterligare dataunderlag, då utredningen hänvisades till på regeringens webbplats angående den nya strategin. Där beskrevs också att den nya NCSS även syftar till att vara en del av implementeringen av NIS2-direktivet från EU och att utredningen av det skulle publiceras under februari 2024, vilket öppnade tanken för att den kunde bli ett relevant dokument att inkludera. I detta skede hade även den nya samlade nationella strategin mot våldsbejakande extremism och terrorism nyligen publicerats, vilken granskades en övergripande gång. Dokumentet ansågs relevant utifrån att strategin innehåller avsnitt gällande cybersäkerhet, risker och hot samt är förlagd i ett angränsande område till cybersäkerhet och cyberrisker. Således utgjorde NCSS, SOU:n samt den nationella strategin mot våldsbejakande extremism och terrorism det initiala materialurvalet.

När processen kring analys av empirin tog vid gjordes ytterligare sondering gällande data för att uppdatera kring eventuella nya tillgängliga dokument och för att utesluta att den nya NCSS hade publicerats, vilket den inte hade. I detta skede uppdagades att utredningen kring implementeringen av NIS2-direktivet var publicerad, men försenad. Dokumentet granskades och ett konstaterande gjordes att det hade en tydlig juridisk karaktär, därför inte av relevans för uppsatsens syfte. Däremot uppmärksammades det att SOU:n inte längre fanns kvar som ett hänvisat dokument, vilken verkade ha ersatts med utredningen för implementeringen av NIS2-direktivet. Likaså beskrivs inte SOU:n ligga till grund för den nya NCSS. Istället noterades det på regeringens webbplats att: I arbetet med den nya strategin beaktas rekommendationer från Riksrevisionen granskningsrapport ”Regeringens styrning av samhällets informations- och cybersäkerhet RiR 2023:8” samt att Regeringskansliet med stöd av Nationellt cybersäkerhetscenter anordnat workshops för ett 50-tal berörda aktörer, vilket även betraktas i den nya strategin (Regeringskansliet, 2023).

Efter att ha granskat riksrevisionens utredning konstaterades att den är av utredande karaktär gällande regeringens politiska styrning och arbete med samhällets informations- och cybersäkerhet. Således hamna utanför uppsatsen syfte och ansågs därmed inte relevant att inkludera i materialurvalet. Med hänvisning till det som presenteras i bakgrunden

gällande Nationellt cybersäkerhetscenter och dess roll i det nationella arbetet med cybersäkerhet, samt att Regeringen framhäver att workshops med centret är medtaget och beaktat i den nya NCSS – ansågs det aktuellt att inkludera centrets rapporter i dataunderlaget som en ansats till att försöka få ett mer omfångsrikt material som samtidigt kunde ge näring till uppsatsen syfte. Därav är fyra rapporter publicerade av centret en del av det slutgiltiga materialurvalet, då centret vid tidpunkten för slutlig datainsamling endast publicerat fem totalt. Den som exkluderats är en delredovisning av regeringsuppdraget de fått gällande att stärka samverkan med näringslivet och således inte relevant i sammanhanget.

De fyra rapporterna som inkluderats är: *Cybersäkerhet i Sverige 2020: Hot, metoder, brister och beroenden* vilken beskrivs som en produkt av en gemensam bild från de sju myndigheterna gällande cybersäkerhet i Sverige 2020 (NCSC, u.å.b). Rapporten framhålls vara grundad på bedömningar från myndigheter med uppgifter som är centrala för att skydda Sverige mot cyberhot samt att rapporten inte är hemlig, men innehållet är delvis baserat på sekretessbelagd information. Hädanefter benämns rapporten som ”R1”. Andra rapporten *Cybersäkerhet i Sverige 2021: I skuggan av en pandemi 2021* syftar till att presentera lärdomar från covid-19-pandemins påverkan på Sveriges cybersäkerhet och att lämna rekommendationer gällande förberedelser inom cybersäkerhetsområdet inför en ny stor kris (NCSC, u.å.c). Hädanefter benämnd som ”R2”. Den tredje rapporten *Cybersäkerhet i Sverige 2022 del 1: Hot, metoder, brister och beroenden* beskrivs likadant som den för 2020, alltså är dessa två snarlika med samma syfte (NCSC, u.å.d). Vidare benämnd som ”R3”. Fjärde rapporten; *Cybersäkerhet i Sverige 2022 del 2: Rekommenderade säkerhetsåtgärder* framhålls som en systerrapport till förgående och ska erbjuda en grund för att ge organisationer förutsättningar att tänka mer på cybersäkert (NCSC, u.å.e). För de som redan tillämpar ett cybersäkerhetsarbete, kan den fungera som checklista där de två rapporterna tillsammans ska ge en god förståelse för ämnet cybersäkerhet. Rekommendationer som sammanställs i den avser att motverka de sårbarheter som lyfts i del 1. Hädanefter benämnd som ”R4”.

Ytterligare ett dokument inkluderas vid sista tidpunkten för datainsamling: *Nationell säkerhetsstrategi* (Statsrådsberedningen, 2017), vilken i skrivande stund är Sveriges enda övergripande säkerhetsstrategi medan en ny är under utarbetning. Strategin inkluderades då den ansågs som ett relevant, kompletterande material till de två andra säkerhetsstrategierna samt utifrån att den behandlar cyberområdet. Gällande omfattningen på de sju dokumenten som inkluderats i materialurvalet, är den nationella säkerhetsstrategin tjugoåtta sidor. De fyra rapporterna från Nationellt cybersäkerhetscenter mellan tjugo och trettiotvå sidor vardera, den nationella strategin mot våldsbejakande extremism och terrorism är på sjuttioen. Och den nationella cybersäkerhetsstratginen är trettiofem sidor.

5.2 Analys av material – riktad innehållsanalys

Analysprocessen i uppsatsen har sin utgångspunkt i en kvalitativ textanalys i form av en dokumentanalys. En dokumentanalys kan ses som en ändamålsenlig metod att tillämpa om syftet är att granska dokument i form av elektroniskt och tryckt textmaterial (Bowen, 2009), vilket går i linje med föreliggande uppsats. Bryman (2018, s. 664) beskriver att statliga myndigheter och organisationer producerar både statistisk information och kvalitativa data i form av olika officiella dokument; policydokument – varifrån dokumenten innehåller användbara data för forskning. Sheard (2022) belyser att forskningsfrågor kan besvaras genom att endast använda redan existerande källor istället för att skapa ny primärdata i studier, och att undersökning av officiella dokument blir allt vanligare i forskning som avser policysfären. Genom att använda offentliga dokument som data i uppsatsen skapas potential för att få insyn i den nationella, officiella hanteringen av cyberrisker och cybersäkerhet. Det i sin tur ger möjlighet att undersöka hur riskerna betraktas i en nationell policykontext. Därtill kan officiella dokument i sammanhanget betraktas som en typ av ”företrädare” för ett nationellt synsätt på cyberrisker.

Dokumentanalysen och analysprocessen har skett i form av en kvalitativ innehållsanalys, vilket är en metod som enligt Bryman (2018, s. 677) är ett adekvat verktyg och tillvägagångssätt för en kvalitativ dokumentanalys. Liknande framhåller Elo & Kyngäs (2008): Att det är ett systematiskt tillvägagångssätt för att antingen beskriva eller kvantifiera fenomen, där innehållsanalysen även möjliggör testning av teoretiska resonemang och frågor. Hsieh & Shannon (2005) beskriver att innehållsanalys är en allmänt använd kvalitativ forskningsteknik, som innebär att tolka innehåll i textdata med målet att generera förståelse och kunskap för det ämne som studeras. Det finns olika varianter av kvalitativ innehållsanalys. Den som appliceras och används i föreliggande uppsats är den som benämns *riktad innehållsanalys*, varvid den analysprocess och tematisering som sker därinom är inspirerad av tidigare forskning inom ämnesområdet (Hsieh & Shannon, 2005). Därtill utgår den från teoretiska resonemang och är således deduktiv i sin ansats, vilket sammantaget innebär att befintliga teorier och tidigare forskning används för att styra kodning och analys av data (Elo & Kyngäs 2007; Hsieh & Shannon, 2005; Kibiswa, 2019). Teorier och tidigare forskning som används i den riktade innehållsanalysen vägleder sedan resultatdiskussionen.

Hsieh & Shannon (2005) menar att en riktad innehållsanalys är lämplig när det finns befintlig teori eller tidigare forskning om ett fenomen som är ofullständig eller skulle gynnas av ytterligare beskrivning. Likaså anses den deduktiva, riktade innehållsanalysen användbar för att testa relevansen av teorin/de teorierna som vägleder studien, eller för att utvidga tillämpningen av dessa till andra sammanhang än där de initialt applicerats (Elo & Kyngäs 2007; Kibiswa, 2019). På samma sätt är metoden ändamålsenlig om en utformad hypotes skall testas. Förda resonemang kring en deduktiv, riktad innehållsanalys skapar relevans för ett sådant tillvägagångssätt i föreliggande uppsats: Som tidigare nämnt i teorikapitlet är inte systemteoretiska, sociotekniska aspekter och

normal accident theory, perspektiv som är särskilt utvidgade eller vanligt applicerade i en kontext kring cybersäkerhet och cybersäkerhetsrisker, även fast exempelvis Malajti m.fl. (2018) och Luiijf m.fl. (2013) menar att systemförståelse såväl som ett dynamiskt förhållningssätt är viktigt i utformningen av strategier för cybersäkerhet. Således blir metoden användbar för att utvidga tillämpningen av dessa teoretiska perspektiv till andra sammanhang än där de främst appliceras. Och trots att det inte är en tydlig hypotes som ska testas i uppsatsen, är syftet med den att undersöka huruvida myndighetsdokumenten speglar en systemförståelse för cyberriskerna; därigenom testa teoretiska resonemang och frågor. Likaså är tidigare forskningen på området å ena sidan bred och spretig. Å andra sidan smal, sett till studier kring hur nationell myndighetspolitik betraktar cyberrisker, speciellt utifrån dimensionerna som är i fokus för uppsatsen. Därtill kan det genom tidigare forskning som presenteras, anses att cyberrisker och dess potentiella konsekvenser är fenomen vilka skulle gynnas av ytterligare beskrivning. Hsieh & Shannon (2005) belyser att resultaten av en riktad innehållsanalys vanligen syftar till att ifrågasätta eller stödja de teorier som använts som utgångspunkt i studien, för att i slutändan generera ny kompletterande kunskap inom området. Avsikten i föreliggande uppsats är dock inte att styrka eller avfärda de teoretiska utgångspunkterna, snarare se hur väl de kan användas i en kontext kring cybersäkerhetsrisker och policy.

Den initiala fasen i en innehållsanalys innebär att bestämma analysenhet, alltså den grundläggande enhet som väljs för analys (Elo & Kyngäs 2007; Kibiswa, 2019). I detta fall; myndighetsdokument. De textuella enheter som följaktligen analyseras är delar av texten som väljs ut för närmare analys i syfte att förstå och tolka innehållet i texten (Kibiswa, 2019). Textuella enheter kan variera i storlek och kan bestå av enstaka ord, fraser, meningar eller hela stycken som kommunicerar relevant information för studiens syfte och frågeställningar. Alltså specifika delar av texten som utgör fokus för analys och tolkning. Nästa del i analysprocessen innebär att skaffa sig en uppfattning av datan och få känsla för dess helhet i syfte att fördjupa sig i materialet (Elo & Kyngäs 2007).

Inom ett riktat tillvägagångssätt initieras analysen med teoretiska resonemang och relevanta aspekter från tidigare forskning, vilket är det som vägleder för utformning av koder och styr analysprocessen (Hsieh & Shannon, 2012). Med hjälp av befintlig teori och/eller tidigare forskning identifieras nyckelbegrepp eller enheter som bildar kodningskategorier. Kategorierna ska vara relevanta för forskningsfrågorna och syftet med studien och kan brytas ner i subkategorier (Hsieh & Shannon, 2012; Kibiswa, 2019). Därefter bestäms operativa definitioner för varje kategori med hjälp av teoretiska utgångspunkter och/ eller tidigare forskning. Två olika strategier existerar inom den riktade innehållsanalysen, där följande är den som används i uppsatsen. Först undersöks materialet och alla textpassager som upplevs relevanta utifrån teori och tidigare forskning, markeras. Därefter kodas alla markerade passager med de förbestämda koderna.

I en riktad innehållsanalys används alltså teori och tidigare forskning som utgångspunkt för analys och för att utveckla kodningsschemat, vilket görs innan datan analyseras där

kodningsschemat är en översättningsenhet som organiserar datan i kategorier (Hsieh & Shannon, 2012). Parallellt med kodnings- och analysprocessen kan ytterligare koder utvecklas och det initiala kodningsschemat revideras utifrån vad som upptäcks i materialet. Likväl kan en strikt strukturerad kodningsmatris och tillvägagångssätt användas vid riktade innehållsanalyser, där användning av en strukturerad matris innebär att endast välja de aspekter i datan som passar in i kodningsschemat (Elo & Kyngäs, 2008), vilket är det tillvägagångssätt som valts för uppsatsen. Det kan också benämnas som testning av kategorier, begrepp och teoretiska modeller. Tillvägagångssättet anses därigenom relevant samt vara passande givet uppsatsens syfte, frågeställningar och yttre ramar.

Analysprocessen initierades genom att ett kodningsschema upprättades där kodningskategorier, subkategorier och operationella definitioner skapades med utgångspunkt i uppsatsens tidigare forskning samt den teoretiska referensramen. I åtanke fanns att kategorierna skulle vara relevanta för forskningsfrågorna och uppsatsens syfte. Likaså att kodningskategorierna och subkategorier skulle täcka så mycket som möjligt inom de olika teoretiska perspektiven samt inkludera begrepp och aspekter från tidigare forskning som inte är lika tydliga i den teoretiska ramen. Kodningsschemat i uppsatsen är inspirerat av det från Kibiswa (2019): Se appendix 1: Kodningsschema, för förklaring av kodningskategorier, subkategorier, de operationella definitionerna samt kodningskategoriernas förankring i teori och tidigare forskning.

Nästa steg i processen innebar fördjupning i datamaterialet vilket innefattade att granska dokumenten och markera textpassager (textuella enheter), där textavsnitt markerades som relaterade till kodningskategorierna och subkategorierna. Därefter granskades dokumenten igen för att kodas utefter de förbestämda kodningskategoriena, där alla textpassager som markerats tilldelades en numerisk kod från kodningsschemat och utifrån de operationella definitionerna till varje kodningskategori. Textpassager som markerades skulle alltså motsvara en operationell definition och en kodningskategori/subkategori, vilket innebär att en textpassage teoretiskt sett kunde få flera koder om den passade in på mer än en operationell definition eller speglade flera subkategorier inom samma kodningskategori. Nästa steg i processen innebar att lägga in de kodade textpassagerna i en kodningsmatris utifrån dess tilldelade numeriska kod och var textpassagen återfanns. Textpassagerna färgkodades och sorterades efter dokumenttyp samt efter vilken numerisk kod den tilldelas, för att skapa en struktur och få en överblick av datan som skulle analyseras vidare. Därefter och med hänvisning till Assarroudi m.fl. (2018), abstraherades kodningskategorierna från kodningsschemat tillsammans med textpassagerna. Genom att sammanföra koderna med mönster och konceptuella samband som framträtt i empirin under analysprocessen, bildades generiska kategorier. Nedan syns ett komprimerat, exemplifierande utdrag från kodningsmatrisen för de tre säkerhetsstrategierna, i syfte att förtydliga kodnings- och analysprocessen. Notera att siffran i parentes är sidnummer i dokumentet. De andra numeriska koderna är sifferkoden från kodningsschemat.

Teori/tidigare forskning/kodningsschema	NSS	NSMVT	NCSS
Systemiska risker (Blå)	1.1.2, 1.1.4 (3) 1.1.4 (8) 1.1.2 (10) + (18) 1.1.1, 1.1.4 (18) 1.1.1, 1.1.2 (18)	1.1.4,.1.1.5 (5) 1.1.2, 1.1.4 (50) 1.1.1, 1.1.2, 1.1.4 (50) 1.1.4 (51)	1.1.4 (3) 1.1.2, 1.1.3 (3) 1.1.2, 1.1.4 (4) 1.1.2, 1.1.5 (9) 1.1.1, 1.1.5 (9) 1.1.2, 1.1.5 (10) 1.1.1, 1.1.4, 1.1.5 (11) 1.1.4 (29)
Socio-tekniska perspektiv (Lila)			2.3.1 (8) 2.3.1 (18) 2.3.1 (26)
Systemteori (Lila)	2.2.1 (22) 2.2.1 (23)	2.2.1 (60)	
(Spridnings)effekter av cyberrisker/attacker- Konsekvenser för kritisk infrastruktur/samhällsviktig verksamhet, liv/hälsa och miljö. (Tidigare forskning) (Rosa)	6.1.2 (22–23) 6.1.1(23)x2 6.1.1 (22)	6.1.1 (7) 6.1.1 (46) 6.1.1 (48) x2 6.1.1 (49) x2 6.1.2 (50) 6.1.2 (56) 6.1.1 (60) 6.1.1 (49)	6.1.2 (4) 6.1.1 (6) 6.1 (6) 6.1.1(6) x2 6.1.1 (7) 6.1.1, 7.1.2 (14) 6.1.1 (18)
NAT (Röd)			5.1.3 (6)

Nationell strategi för samhällets informations-och cybersäkerhet

Kraven på samhällets informations- och cybersäkerhet ökar i allt snabbare takt. Utvecklingen och den förändrade användningen av ny teknik och nya innovationer innebär att hot blir svårare att upptäcka, att riskerna blir mer svårbedömda och att beroenden blir svårare att överskåda. KOD 1.1.2, 1.1.3 (3)

Den tekniska säkerheten behöver fortsatt stärkas samtidigt som hänsyn tas till att det i många fall är den mänskliga faktorn som ligger bakom incidenter eller utnyttjas vid angrepp. Av den anledningen är det viktigt att öka medvetenheten såväl som förmågan hos alla användare av IT-system och att skapa förutsättningar för utvecklingen av en säkerhetskultur i hela samhället. KOD 2.3.1(8) socio-tekniska perspektiv.

Säkring av funktionaliteten och säkerheten hos industriella informations- och styrsystem utgör en mycket viktig del i såväl det förebyggande arbetet som i hanteringen vid störningar i centrala samhällsfunktionaliteter som el- och dricksvattenförsörjning. Även störningar inom områden som transportsystem, industriell produktion och sjukvård är exempel där förebyggande arbete är viktigt. KOD 7.1.1 (18)

Beroenden och kopplingar mellan olika tekniska system är en sårbarhetsfaktor i sig genom att störningar kan få konsekvenser som är svåra att förutse och hantera. KOD 5.1.3(6)

5.3 Etiska överväganden

Utöver de grundläggande och universella principerna kring god forskningssed som alltid ska respekteras samt att beakta de etiska riktlinjerna kring samhällsforskning generellt (Bryman, 2018, s. 166, 170), anses inte uppsatsen innefatta några svårare etiska överväganden. Detta i avseendet att den inte medför rent forskningsetiska problematiska överväganden gällande hur deltagare i studien kan påverkas, utifrån att datan inte inbegriper undersökningsdeltagare eller uppgiftslämnare. Istället används officiella,

redan publicerade dokument från myndigheter som empiriskt material. Morgan (2022) framhåller att använda redan existerande dokument som data, vanligen framkallar färre etiska problem i jämförelse med att använda andra kvalitativa metoder. Eftersom offentliga dokument är tillgängliga för alla att granska, vilket de som publicerat dokumenten är medvetna om. Likväl har en utgångspunkt genomgående under uppsatsen gång självklart varit att anamma de generella regler, uppförandekrav och förhållningssätt som Vetenskapsrådet (2017) upprättat för all typ av forskning. Att göra utförliga och tydliga redovisningar av resultat såväl som tillvägagångssätt i en studie, är en viktig del för att upprätthålla god etik (Forsberg & Wengström, 2016, s. 132). Därav har ansträngningar gjorts kontinuerligt för att i så stor utsträckning som möjligt redogöra för uppsatsens tillvägagångssätt på ett tydligt sätt.

6 Resultat

Resultatavsnittet är uppdelat i två delar. Första delen avser dokument från Nationellt cybersäkerhetscenter följt av de tre nationella säkerhetsstrategierna. Uppdelning är gjord med hänvisning till att rapporterna och strategierna är två olika typer av policydokument. Dokumenten från cybercentret är att betrakta som myndighetsrapporter, och en gemensam bedömning av cybersäkerheten i Sverige från myndigheterna som ingår i centret (NCSC, u.å.b). Säkerhetsstrategierna å andra sidan är dokument och skrivelser från regeringen, där skrivelser är meddelande från regeringen till riksdagen gällande hur en viss fråga betraktas eller gällande hur arbetet är förlagt inom ett visst politikområde (Regeringen, u.å.). Vidare presenteras resultatet utifrån de generiska kategorierna som utarbetats under analysprocessen. Även genom att visa frekvensen av kodningskategorier/subkategorier i datan och genom att ge beskrivande exempel, med hänvisning till tillvägagångssätt inom den riktade innehållsanalysen från Hsieh & Shanno (2005). De fyra rapporterna från Nationellt cybersäkerhetscenter kommer som nämnt fortsatt hänvisas till som: R1, R2, R3 och R4. Gällande andra delen av resultatet kommer de tre säkerhetsstrategierna hänvisas till som följande. *Nationell säkerhetsstrategi* (Statsrådsberedningen, 2017): NSS, *Nationell strategi mot våldsbejakande extremism och terrorism – förebygga, förhindra, skydda och hantera* (Skr. 2023/24:56): NSMVT, och *Nationell strategi för samhällets informations- och cybersäkerhet* (Skr. 2016/17:213): NCSS.

6.1 Rapporter från Nationellt cybersäkerhetscenter

6.1.1 Teknikens utveckling och beroendets paradox

I tre av de fyra rapporterna från NCSC diskuteras cyberdomänen och dess relaterade risker i systemiska termer. Totalt sett kunde många textpassager från rapporterna kodas under kodningskategorier och subkategorier sprungna ur perspektiv på systemiska risker. Framför allt i R1, där passager kodades flest gånger till sådana subkategorier. Liknande noteras även i R3 då textpassager kodades näst flest gånger till subkategorier inom systemiska perspektiv. Utifrån kodningen framkommer det att rapporterna främst lyfter beståndsdelar kopplade till subkategorierna *1.1.3 Teknologisk progression/hastig utveckling/digitalisering* samt *1.1.2 Beroendeförhållanden*, då flest textpassager kodades under dessa subkategorier: Tio respektive sex gånger. Det som uppmärksammas i detta avseende är att R1 och R3 flertalet gånger framhäver den snabba digitaliseringen och teknologiska utvecklingen som en tydlig drivkraft för förändring i samhället, och hur det direkt har ett samband till cybersäkerhet. Resonemangen i rapporterna vittnar om att dessa förfaranden är centrala faktorer för cybersäkerhetsrisker.

Resonemang kring beroendeförhållanden samt hur det relaterar till cybersäkerhet och angrepp förkommer i alla tre rapporter, särskilt i de två liknande rapporterna; R1 och R3. Betoning görs på att det digitala samhället har genererat sårbarheter och beroenden, i form av att den högteknologiska och digitala transformationen tillsammans med ett uppkopplat

samhälle har skapat beroenden av kontinuerligt fungerande IT-och kommunikations-system vilket löper genom samhällets olika delar. Beroendet sträcker sig från kritiska samhällssystem till applikationer som används av den enskilde individen. I R3 beskrivs beroendeförhållandet därutöver genom det uppkopplade samhällets beroende av elektronisk kommunikation och uppkoppling, där konsekvensen blir att förmågan att leverera el samt upprätthålla kommunikationer är digitaliserad, på så sätt sårbar för samma svagheter och utsatt för liknande cyberrisker som övrig digitaliserad verksamhet. Ett resonemang i R1 förhåller sig till detta ytterligare:

> ”Sårbarheter i det uppkopplade samhället är sällan eller aldrig lokala företeelser. Introduktionen av nya tjänster och teknik sker i en takt som innebär att sårbarheterna ökar och att konsekvenserna av cyberangrepp blir svåröverblickbara”. (R1, NCSC, u.å.b, s. 24)

Utifrån citatet hörsammas aspekten kring att konsekvenserna av ett angrepp kan bli gränsöverskridande, således att cyberriskerna besitter sådan systemisk egenskap. I R1 och R2 återfinns unisona resonemang kring att komplexa beroenden och beroendeförhållanden i vårt digitaliserade samhälle gör att konsekvenserna av cyberangrepp blir svåröverblickbara. Kodning till subkategorin *1.1.4 Gräns/systemöverskidade* förekom totalt tre gånger och då i R1 och R2. I samma kontext förekom kodning till subkategorin *1.1.1 Osäkra/komplexa/tvetydiga* tre gånger totalt och i samma rapporter. Sammantaget vittnar det om en adressering av komplexiteten i cyberriskerna, beroendeförhållanden samt att sårbarheter och incidenter relaterade till cyberrisker är gränsöverskridande fenomen. Dock benämns cyberrelaterade risker och angrepp inte uttryckligen som gränsöverskridande. Inte heller som osäkra och/eller tvetydiga, utan antydningar uppfattas. En subkategori inom systemiska perspektiv på cyberrisker som inte uppfattades och därav inte kodats i någon rapport var: *1.1.5 föränderliga i tid/rum*, vilket relaterar till den dynamiska aspekten av systemiska cyberrisker. Systemiska perspektiv på riskerna inom cyberdomänen existerar, men några beståndsdelar därinom hörsammas inte i rapporterna. Därutöver förläggs betoningen på digitaliseringen och dess relation till cybersäkerhetsrisker.

6.1.2 Sammanlagda hot och samspel mellan teknik/människa i cybersäkerhet

Förekomsten av systemteoretiska perspektiv återfinns i tre av rapporterna; R1, R3 samt R4, där samtliga innehåller resonemang som anspelar på interaktionen mellan teknik/människa och hur det avspeglas i cybersäkerheten. Totalt sett gjordes flest kodningar (femton gånger) till subkategorin *2.3.1 Interaktion mellan teknik och människor*, alltså till socio-tekniska aspekter. Diskussioner mer riktade mot systemteori och som således föll under kodningskategorin *2.2 Systemberoende/sammanlänkning av risker* och subkategorin *2.2.1 Systemberoende inom cybersäkerhet* var färre; totalt nio gånger förekom sådan kodning. Resonemang avseende samspelet mellan människa och teknik i cybersäkerheten uppfattas genomgående i form av att det diskuteras inom ramen för tillvägagångssätt och metoder för cyberangrepp, initial åtkomst till system/information samt vilka sårbarheter angripare vanligen utnyttjar. Mycket fokus är

förlagt på angreppssätt i rapporterna över lag, där presentationen av dessa vittnar om interaktionen mellan teknik och människa och hur det influerar cyberriskerna, sårbarheten och möjligheten till att genomföra angrepp. Exempelvis lösenordsattacker, nätfiske (phishing), riktat nätfiske (spearphishing); angrepp via e-post, vattenhålsattacker (placerad skadlig kod på en hemsida). Metoder för åtkomst som presenteras i R1 och R3 är behäftade runt att utnyttja mänskliga faktorer, där phishing och spearphishing lyfts fram som tydligt framgångsrika i sammanhanget, eftersom de i stor utsträckning beskrivs utnyttja mänskliga egenskaper såsom nyfikenhet.

Tre av de fyra rapporterna diskuterar även sårbarheter som existerar relaterade till hantering av och brister i autentisering och behörigheter i olika IT-system inom verksamheter. I R1 och R3 lyfts att en femtedel av de allvarliga IT-incidenterna som rapporterats under 2019 till MSB av statliga myndigheter, bedöms ha sin grund i handhavandefel. Dock uppmärksammades inga konkreta resonemang kring hur samspelet mellan teknik och människa influerar cybersäkerhetsrisker i rapporterna, och inga uttryck existerar heller kring att cybersäkerhet är ett sociotekniskt system. Följaktligen förekom ingen kodning till subkategorin *2.3.2 Komplexitet och dynamik i socio-tekniska system* i någon av rapporterna. Således uppfattades inga diskussioner kring social och teknisk komplexitet i cybersäkerhetsrisker och inte heller kring hur cybersäkerhet/riskers interna miljö påverkas av externa faktorer, exempelvis politiska/juridiska eller miljömässiga förändringar. Inte heller huruvida det följaktligen influerar sårbarheter eller cyberriskerna i sin helhet.

I rapporterna diskuteras aspekter kring sammanlänkning av risker, vilket framträder genom kodning till subkategorin *2.2.1 Systemberoende inom cybersäkerhet*. Diskussioner som syns i detta avseende förkommer i R1 och R3 och rör den existerande samhällsutmaningen gällande att molntjänster är koncentrerade till ett fåtal leverantörer, vilket innebär att hotaktörer kan slå ut flera samhällskritiska system samtidigt om de får tillgång till miljön. Därigenom blir de sammanlagda konsekvenserna för samhället av ett angrepp större, jämfört med konsekvensen av ett angrepp mot ett enskilt system. Ytterligare hörsammas sammanlänkning av riskerna utifrån att R1 samt R3 adresserar att hotbilden mot en molntjänst blir den sammanlagda hotbilden mot alla som använder tjänsten – därav behöver problematiken kring överförda hotbilder hanteras. En av rapporterna (R4) skildrar därutöver att informationssystem vanligtvis exponerar ett flertal tjänster mot de nätverk det är anslutet till, och ju fler tjänster som är tillgängliga desto fler möjliga sårbarheter. Ytterligare kopplingar till systemberoenden ses genom resonemang i R4 gällande verksamheters IT-miljöer: Om någon del i ett nätverk eller dess stödresurser slutar fungera, föreligger en stor risk för allvarliga störningar i hela verksamhetens IT-miljö. Sammantaget existerar alltså systemteoretiska resonemang i tre av rapporterna. Dock förekom inte kodningskategorin *2.1.1 Emergens* och subkategorin *2.1.1 Interaktion mellan systemkomponenter* inom ramen för systemteori, i någon av rapporterna. Inga textavsnitt uppfattades således diskutera emergens, eller hur fristående delar inom ett cybersäkerhetssystem börjar påverka varandra och således skapar oväntade händelser.

Inga resonemang uppfattades heller kring att olyckor eller risker uppstår när systemets komponenter interagerar med varandra på sätt som inte var förutsägbara utifrån deras individuella egenskaper.

6.1.3 Kontinuerligt utvecklingsarbete

Samtliga rapporter vittnar om dynamiska aspekter gällande cybersäkerhetsrisker och sårbarheter, i avseendet att bemöta dessa. Resonemang vilka relaterade till riskstyrning och dess perspektiv kring ett dynamiskt förhållningssätt i hantering av systemiska risker, återfinns i samtliga rapporter. Kodning till subkategorin *3.1.1 Adaptivitet/kontinuerligt lärande*, förekom nio gånger. Adressering av behovet kring ett adaptivt förhållningssätt i cybersäkerheten uppfattas i samtliga rapporter genom diskussioner kring betydelsen av ett dynamiskt säkerhetsarbete i relation till cyberdomänen. I två av rapporterna (R1 och R3) återfinns därutöver resonemang kring att säkerhetshotet från cybermiljön varierar över tid – därför är planering och genomförandet av säkerhetsarbetet i sammanhanget inte en engångsföreteelse vars resultat är statiskt, utan en dynamisk process som inkluderar kontinuerlig uppföljning och utvärdering. Följande citat är två likadana textpassager som kodades två gånger till subkategorin *3.1.1 Adaptivitet/kontinuerligt lärande*, i R1 och R3.

> ”Takten i den tekniska utvecklingen är hög och det upptäcks kontinuerligt nya sårbarheter som sedan åtgärdas. Det pågår således en ständig kapplöpning mellan medel och motmedel. Därför krävs det ett konstant utvecklingsarbete för att upprätthålla en förmåga till avancerade cyberoperationer”. (R1, NCSC, u.å.b. s. 11; R3, NCSC, u.å.c. s. 9)

Genom citatet uppfattas en viss adressering av den dynamiska karaktären i cybersäkerhetsriskerna, och hur arbetet mot att bemöta det således behöver vara adaptivt och kontinuerligt. I rapporterna återfanns inga textavsnitt som diskuterade vikten av ett holistiskt tillvägagångssätt och ett helhetsperspektiv i riskstyrningen för att hantera systemiska cyberrisker. Inte heller några diskussioner kring behovet att hantera dem utifrån deras komplexa/sammanlänkade natur, därför förekom ingen kodning till subkategorin *3.1.2 Holistiskt tillvägagångssätt och helhetsperspektiv* i någon av rapporterna.

6.1.4 Cybersäkerhetsrisker och cyberattackers samhällspåverkan

Tre av de fyra rapporterna (R1, R3 och R4) adresserar relationen mellan cyberangrepp och påverkan på samhället. Kodning till subkategorin *6.1.1 Effekter/konsekvenser på kritisk infrastruktur/samhällsviktig verksamhet* förekom totalt åtta gånger och majoriteten av dessa i R3; fem gånger. Således är en observation att kodning förekom fler gånger till effekter på samhällsviktig verksamhet/kritisk infrastruktur i R3 jämfört med den liknande rapporten R1, där samma kodningskategori förekom tre gånger totalt – vilket vittnar om ett större fokus på dessa aspekter i den senare rapporten. I R1 förekommer diskussion gällande att bland de målen som utsätts för cyberangrepp, återfinns verksamheter vilka är centrala för samhällets grundläggande funktioner. Övriga diskussioner förhåller sig till förmågan att leverera el och att upprätthålla kommunikationer som är avhängda på digitalisering. Hörsammande görs också kring att påverkan på elsystemet skulle medföra

omfattande samhällskonsekvenser. I R3 återfinns resonemang kring cyberangrepps påverkan i en kontext kring hotaktörer, där samhällskritisk infrastruktur framhålls som mål för främmande makt. Ytterligare resonemang som uppfattas rör sig kring att stora delar av den samhällsviktiga verksamheten är uppkopplad. Detta exemplifieras genom vattenreningsverk och elproducenter, vilka har inbyggda industriella informations- och styrsystem som vanligen är uppkopplade mot internet. Styrsystemen framhålls ålderstigna och tillgängliga på avstånd— därav bär de sårbarheter som kan utnyttjas. Härigenom görs adresseringar gällande cyberangrepps eventuella effekter på samhällsviktig verksamhet och kritisk infrastruktur samt dessa entiteters centrala roll för samhället.

En iakttagelse i sammanhanget rör ett resonemang i R3 i en kontext kring angrepp mot mjukvaruleverantörer. En illustrering av sådant angrepp görs genom attacken mot detaljvaruhandeln Coops kassasystem; attacken beskrivs medfört att butikerna tvingades stänga i varierande längd med stora ekonomiska följder som konsekvens. Dock diskuteras inte i termer av effekter och påverkan på samhället och enskilda individer, utan endast som en ekonomisk konsekvens för koncernen. Vidare förekom resonemang kring cyberattackers/cybersäkerhetsriskers eventuella påverkan på människors liv och/eller hälsa samt diskussioner kring attackers påverkan på miljön, färre gånger än de kring samhällsviktig verksamhet och kritisk infrastruktur. Sammanlagt förekom kodning till subkategorin *6.1.2 Effekter/konsekvenser på liv/hälsa/miljö* endast två gånger för samtliga rapporter, en gång i R1 och en gång i R3. Diskussionerna i detta avseende förekommer i en kontext kring det uppkopplade samhällets beroende av elektricitet och elektronisk kommunikation samt runt en exemplifiering av cyberangreppet mot Ukrainas elnät 2015. Följande citat återfinns i båda rapporterna och är den enda textpassage som kodades till nämnd subkategori:

> ”Förutom de omedelbara konsekvenserna av omfattande strömavbrott gällande människors liv och hälsa, så skulle väldigt många system som är beroende av fungerande it upphöra att fungera. Det som tidigare upplevdes som en smärre olägenhet skulle idag leda till betydande problem på flera nivåer i samhället”. (R1, NCSC, u.å.b. s. 24; R3, NCSC, u.å.d. s. 25)

Här hörsammas att ett elavbrott kan leda till konsekvenser på hälsa och liv. I sammanhanget och indirekt sammankopplas detta till cyberangrepp mot elsektorn – således adresseras en spridningseffekt av en attack och dimensionen kring människors liv och välmående vid sådan händelse. Dock uttrycks inte spridningseffekten explicit. Trots att citatet placerades under subkategorin *6.1.2 Effekter/konsekvenser på liv/hälsa/miljö,* framkommer inga resonemang kring påverkan på miljön. Detta avser samtliga rapporter; inga diskussioner eller resonemang förekommer kring cyberriskerna och attackers eventuella påverkan på miljön, i något avseende.

Ytterligare diskussioner förekommer kring påverkan på samhället i R3, varvid sådan kunde kodas till kategorin *7.1 Kaskadeffekter* och subkategorin *7.1.1 Potentiella kaskadeffekter av cyberattacker inom KI/SVV:* ”Påverkan på elsystemet och leveransen av el skulle ge kaskadeffekter på samhällskritiska system och samhället i stort” (R3, NCSC, u.å.d, s. 25). Textpassager som benämner kaskadeffekter återfanns endast denna

gång. Alltså förekom kodning till subkategorin. 7*.1.1 Potentiella kaskadeffekter av cyberattacker inom KI/SVV* endast en gång sammanlagt. Ordet kaskadeffekter eller kaskad förekom inte heller i andra sammanhang utanför citatet eller kontexten kring samhällsviktig verksamhet/kritisk infrastruktur, i någon av rapporterna. Sammantaget är fokus förlagt på elsektorn inom samhällsviktig verksamhet/kritisk infrastruktur och dess sårbarheter för angrepp i rapporterna. Andra delar av samhällsviktig infrastruktur, såsom hälso-och sjukvårdssektorn, diskuteras inte någon gång i rapporterna. Däremot nämns sjukvårdssektorn i R2, då den avser lärdomar från covid-19, dock förekommer inga resonemang gällande effekter/konsekvenser på liv och hälsa i sammanhanget.

6.1.5 Avstånd, latens och oanade konsekvenser i cyberrisker

Resonemang som anspelade på komponenter inom normal accident theory, högrisk-teknologier och systemolyckor var få i samtliga rapporter. Kodning till sådana resonemang gjordes sammantaget fyra gånger; en gång i respektive rapport och till subkategorin *5.1.3 Oväntade händelser och latenta beroendeförhållanden.* Resonemang som förkommer i avseendet är desamma i R1 och R3: Att konsekvenser av allvarliga IT-incidenter inte alltid uppstår eller är uppenbara i direkt anslutning till händelsen, utan kan uppkomma över tid. Det anspelar på eventuella oväntade effekter av cyberattacker, samt hur incidenter/störningar i ett system kan sprida sig på sätt som inte är förutsägbara. I övriga rapporter adresseras oväntade och latenta dimensioner av cyberangrepp i form av diskussioner kring att konsekvenserna av ett intrång kan upptäckas och bli märkbara lång tid efter angreppet. Resterande subkategorier sprungna ur NAT: *5.1.1 Interaktiv komplexitet och tät sammankoppling* och *5.1.2 Kedjereaktioner av störningar* samt kodning till dessa, förekom inte i någon av rapporterna. Således uppfattades inga diskussioner som anspelade på interaktiv komplexitet och tät sammankoppling mellan systemkomponenter inom cybersäkerhetssystem, och hur det relaterar till förekomsten av systemolyckor. Inte heller hur cybersäkerhetssystems delar är starkt beroende av varandra och hur störningar i en del kan sprida sig och påverka andra delar, och hur det ökar sårbarheten för storskaliga störningar. Inga resonemang uppfattades heller kring hur små incidenter/störningar kan utlösa kedjereaktioner av störningar och hur dessa kan eskalera till systemolyckor inom cybersfären.

Tre av fyra rapporter vittnar om att det existerar en dimension kring okonventionella gränser i cyberrisker. Kodning till subkategorin *8.1.1 Distans i cyberrisker* gjordes totalt sex gånger, med flest kodningar (tre) i R3. I de snarlika rapporterna R1 och R3 förekommer diskussioner kring att samhällsviktig infrastruktur har industriella informations- och styrsystem som vanligen är uppkopplade mot internet, vilket gör dessa tillgängliga på distans. I dessa lyfts även en exemplifiering från verkligheten och ett angrepp, där internetexponerade frysar i en livsmedelsbutik var åtkomliga relaterat till undermålig lösenordshantering. Det i sin tur möjliggjorde reglering av temperatur samt avstängning av frysarna på distans. I R2 förs resonemang kring att kriminella aktörer inom cybersfären besitter få geografiska begränsningar för sin verksamhet, där angrepp

kan utföras hemifrån. Således uppfattas en adressering kring cyberriskers/attackers karaktär av att inte besitta konventionella gränser, där hot och attacker kan utföras från geografiskt avlägsna platser utan fysisk närvaro.

En observation är att mycket av den kodade empirin är av samma karaktär för de likartade rapporterna R1 och R3, utifrån att många textpassager som kodades var identiska eller snarlika. Specifikt textpassager som kodats till systemiska perspektiv, systemteoretiska perspektiv och textpassager som anspelade åt kategorier inom dynamiskt förhållningssätt till cybersäkerhetsriskerna, trots att det skiljer två år mellan rapporterna. Ytterligare notering är att en kodningskategori och subkategori inte förekom i någon av rapporterna: *4.1 Harmonisering* och *4.1.1 Sammanlänkning med andra nationella säkerhetsstrategier och (internationella) ramverk*, vilket kan anses naturligt då rapporterna inte är av typen nationella säkerhetsstrategier. Ytterligare observation är att rapporterna har ett förhållandevis starkt fokus på aktörer som har förmågor och som utför cyberangrepp och andra insteg i vår digitala infrastruktur, och i samma kontext uppfattas mycket av innehållet stationerat kring presentationer av metoder för angrepp.

6.2 Nationella säkerhetsstrategier

6.2.1 Ökande beroenden och digitaliseringens komplexitet

Precis som i rapporterna från Nationellt cybersäkerhetscenter är de systemiska perspektiven på cyberdomänen framträdande i de tre nationella säkerhetsstrategierna. Samtliga strategier adresserar aspekter som återspeglar systemiska beståndsdelar och sammantaget kodades många textpassager (näst flest totalt) i strategierna under kodningskategorier/subkategorier sprungna ur perspektiv på systemiska risker. Det med en jämn fördelning mellan NS och NSMVT, sex respektive fyra gånger. Mer framträdande var det i NCSS, där totalt åtta kodningar förekom till systemiska perspektiv. Utifrån kodningsprocessen blir det tydligt att strategierna sammantaget främst diskuterar beståndsdelar som rör subkategorierna *1.1.3 Teknologisk progression/hastig utveckling/digitalisering* och *1.1.2 Beroendeförhållanden*, eftersom majoriteten av kodning gjordes till dessa subkategorier; totalt elva respektive nio gånger. Notera att det är ett resultat som framträdde även i rapporterna från Nationellt cybersäkerhetscenter. I detta sammanhang framkommer det av strategierna att den ökade digitaliseringen har haft avgörande betydelse för samhället samt att det existerar tydliga säkerhetsutmaningar som följer med det. I NSMVT framhålls att den ökade digitaliseringen och snabba teknikutvecklingen medfört att informations- och cybersäkerhet har utvecklats till en fråga om nationell och internationell säkerhet. I NCSS återfinns resonemang kring att digitaliseringen påverkar i stort sett alla delar samhället, vilket medför möjligheter men också risker där digitaliseringen skapat nya möjligheter och samtidigt nya konfliktytor och sårbarheter. Varvid informations- och cybersäkerhet har vidgats från en avgränsad teknisk angelägenhet till att numer vara en fråga med relevans för fred, säkerhet och global utveckling. Resonemang i samtliga strategier vittnar om att processerna kring den

digitala evolutionen är centrala katalysatorer för cybersäkerhetsrisker. Likaså framkommer det i samtliga strategier att den teknologiska utvecklingen och digitaliseringen har skapat ömsesidiga och komplexa beroenden, där betoning görs på beroendet av IT-system inom olika centrala samhällsfunktioner och hur dessa förfaranden tillsammans genererar sårbarheter. Adresseringar och resonemang kring beroende-förhållanden och hur det relaterar till cybersäkerhetsrisker existerar således i samtliga strategier.

Ytterligare resonemang som återfinns i NCSS avser att samhällets behov av informations- och cybersäkerhet ökar och att den teknologiska förändringen innebär att hot blir svårare att upptäcka, riskerna mer svårbedömda och att beroenden blir svårare att överskåda. Sådana resonemang förekommer även i NSS. Härigenom syns en adressering av komplexiteten i cybersäkerhetsriskerna samt hur det har en relation till beroendeförhållanden som existerar i samhället. I NCSS förekommer därutöver beskrivning kring informationssäkerhetens komplexitet, gränsöverskridande karaktär och snabba utvecklingstakt, vilket anspelar på cyberriskerna som komplexa och gränsöverskridande. Därutöver hörsammas att flöden av tjänster och produkter sker i flera led, varvid bristande informationssäkerhet kan få följdverkningar långt utanför den egna verksamhetens gränser. I dessa sammanhang framträder det systemiska perspektivet kring cybersäkerhetsriskerna som system- och gränsöverskridande. Varvid kodning till subkategorin *1.1.4 Gräns/systemöverskridande* förekom totalt fem gånger, med majoriteten (fyra gånger) i NCSS, en gång i NSS och ingen i NSMVT.

Kodning till subkategorin *1.1.1 Osäkra/komplexa/tvetydiga* förekom totalt fem gånger, fördelat på samtliga strategier där diskussioner främst avser informationssäkerhetens komplexitet, digitaliseringens medförande av komplexa beroenden och att riskerna således blir mer svårbedömda. Dock uppmärksammades inga resonemang som konkret beskrev att cybersäkerhetsriskerna är *osäkra* eller *tvetydiga.* En annan beståndsdel inom systemiska perspektiv på cybersäkerhetsriskerna som inte uppfattas i någon av de tre strategierna, var den som återfinns i subkategorin; *1.1.5 Föränderliga i tid/rum,* då kodning till denna inte förekom alls. Således uppfattades inga resonemang kring den dynamiska aspekten i riskerna vilket är ett utfall som även sågs avseende de fyra rapporterna. Perspektiv kring hur systemiska riskerna är inom cyberdomänen existerar i strategierna, men somliga beståndsdelar därinom adresseras ej. Ytterligare iakttagelse är att det även i strategierna likt rapporterna, finns en tydlig betoning på teknologisk progression och dess relation till cybersfären, risker och sårbarheter därinom.

6.2.2 Hot mot och kopplingar mellan system och mänskliga faktorn

Samtliga strategier adresserar i någon mån systemteoretiska aspekter, men i olika grad och tappning. Förekomsten av kodning till kodningskategorin *2.2 Systemberoende /sammanlänkning av risker* och subkategorin *2.1. 1 Systemberoende inom cybersäkerhet* återfanns endast i två av rapporterna: I NSS och NSMVT där kodning förekom två respektive en gång. Diskussioner som framträder i detta avseende i NSS är i en kontext

kring hot mot elförsörjningen och transportsektorn (inte cyberhot specifikt utan antagonistiska generellt), där det framkommer att samhället är uppbyggd på integrerade system av vital infrastruktur. Det i sin tur genererar komplexa utmaningar i flera led. Elförsörjningen lyfts som en central komponent i samhället, där störningar snabbt kan ge konsekvenser inom andra verksamheter, såsom informations- och kommunikationsteknologin samt transportsystemet. Således hörsammas att sårbarheter eller attacker mot en del av systemet kan spridas och påverka andra delar av systemet kring vital infrastruktur. I NSMTV kodades endast en textpassage till systemteoretiska aspekter och då till subkategorin *2.1.1 Systemberoende inom cybersäkerhet*, vilken var: ”Förmågan att hantera systemhotande cyberangrepp ska vara en självklar del i beredskapen för att kunna hantera situationen under och efter ett attentat” (Skr.2023/24:56 s. 60). Citatet återfinns i kontextuella resonemang gällande myndigheters beredskap för att hantera nya typer av attentat och hot samt stärkt förmåga att hantera cyberhot. Här syns en form av adressering gällande att cyberangrepp kan ge effekter/konsekvenser på hela (samhälls-)system. Dock förekommer ingen förklaring till vad systemhotande innebär i sammanhanget, och ingen utvidgad diskussion syns därefter. Ingen kodning till ovanstående kategori förekom i NCSS, eftersom inga resonemang uppfattades som speglade systemberoenden. Ingen kodning förekom i någon av strategierna till kodningskategorin *2.1 Emergens* eller subkategorin *2.1.1 Interaktion mellan systemkomponenter*. Alltså uppfattas inga textavsnitt som diskuterade emergens, eller hur fristående delar inom ett cybersäkerhetssystem börjar påverka varandra och således skapar oväntade händelser. Inga resonemang uppfattades heller kring att olyckor eller risker uppstår när systemets komponenter interagerar med varandra på sätt som inte var förutsägbara utifrån deras individuella egenskaper. Detta resultat sågs även i rapporterna, således förekom inga resonemang som anspelade på emergens i något av de sju dokumenten.

Gällande sociotekniska dimensioner framträder sådana endast i NCSS, där kodning till kodningskategorin *2.3 Socio-tekniska aspekter av cybersäkerhet* och subkategorin *2.3.1 Interaktion mellan teknik och människor* förekom sammantaget tre gånger. Det som framkommer i detta avseende är diskussioner kring att den tekniska säkerheten behöver stärkas ytterligare och samtidigt behöver hänsyn tas till att den mänskliga faktorn i många fall är grunden bakom incidenter eller det som utnyttjas vid angrepp. Ytterligare resonemang återfinns angående att störningar kan ha sin grund i misstag vid handhavande, alternativt bero på tekniska/maskinella fel eller antagonistiska aktiviteter. Därigenom hörsammas interaktionen mellan teknik och människa i cybersäkerheten och dess ingående sårbarheter och risker. Dessa sociotekniska aspekter och att mänskliga faktorer utnyttjas vid angrepp, var något som framträdde även i rapporterna från NCSC. Dock benämns inte cybersäkerhet och dess risker uttryckligen som ett sociotekniskt system i något dokument. En socioteknisk benämning ses dock i ett annat sammanhang i NCSS: I en kontext kring högre utbildning, forskning och utveckling framhålls att utvecklingen av självstyrande bilar och intelligenta städer aktualiserar både

sociotekniska, juridiska och etiska frågor med direkt anknytning till informations- och cybersäkerhet.

Följaktligen förekom ingen kodning i NCSS till aspekter som kunde härledas till subkategorin *2.3.2 Komplexitet och dynamik i socio-tekniska system.* Inga diskussioner eller resonemang uppfattades som belyste graden av teknisk och social komplexitet inom sociotekniska system eller inom cybersäkerheten. Inga textpassager återfanns heller som anspelade på hur dessa systems interna miljö påverkas av externa faktorer såsom politiska/juridiska/miljömässiga förändringar. Inte heller hur det influerar sårbarheter eller cybersäkerheten överlag. Utifrån kodningsprocessen framkommer inget vittnande om sociotekniska perspektiv på cybersäkerheten och dess associerade risker i de två andra strategierna, utifrån att ingen kodning förekom till kodningskategorin *2.3 Socio-tekniska aspekter av cybersäkerhet* eller subkoderna *2.3.1 Interaktion mellan teknik och människor* eller *2.3.2 Komplexitet och dynamik i socio-tekniska system.* Ett uteblivet perspektiv på komplexitet och dynamik i sociotekniska system framträdde också inom rapporterna, vilket således blir en ytterligare gemensam nämnare dokumenten emellan – gällande avsaknad av vissa systemteoretiska aspekter.

Resonemang som anspelar på komponenter inom normal accident theory, högriskteknologier och systemolyckor är ytterst få i samtliga strategier. Kodning till kategorier sprungna ur NAT förekom endast en gång sammanlagt och då i NCSS, till subkategorin *5.1.3 Oväntade händelser och latenta beroendeförhållande.* Resonemanget som förekommer berör att kopplingar och beroenden mellan olika tekniska system är en sårbarhetsfaktor, relaterat till att störningar kan få konsekvenser som är svåra att förutse. Det anspelar på eventuella oväntade effekter av cyberattacker, samt hur incidenter/störningar i ett system kan sprida sig på sätt som inte är förutsägbara. Resterande subkategorier relaterade till beståndsdelar inom NAT: *5.1.1 Interaktiv komplexitet och tät sammankoppling* och *5.1.2 Kedjereaktioner av störningar* samt kodning till dessa, förekom inte i någon av strategierna. Således uppfattades inga diskussioner som anspelade på interaktiv komplexitet och tät sammankoppling mellan systemkomponenter inom cybersäkerhetssystem, och hur det relaterar till förekomsten av systemolyckor. Detta är något som även framkommer i rapporterna; en avsaknad av aspekter som rör interaktiv komplexitet, tät sammankoppling och kedjereaktioner av störningar.

6.2.3 Uppföljning och kontinuerlig anpassning

Samtliga strategier adresserar en dynamisk aspekt avseende hanteringen av cybersäkerhet, där strategierna pekar på behovet av kontinuerlig anpassning till föränderliga hotmiljöer och det tekniska landskapet för att säkerställa effektivitet inom informations- och cybersäkerhetsområdet. Totalt förekom kodning till kodningskategorin *3.1 Dynamisk riskstyrning för hantering av (systemiska) cyberrisker* och subkategorin *3.1.1 Adaptivitet/kontinuerligt lärande* nio gånger, med jämn fördelning mellan strategierna. I NSS framkommer att det krävs fortlöpande arbete med att minska

sårbarheter för att kunna bemöta utmaningarna inom informations- och cybersäkerhetsområdet. I NSMVT förekommer resonemang kring att åstadkommandet av effektivt skydd för samhällsviktig verksamhet i hela hotskalan, kräver kontinuerlig analys och kunskapsbyggande kring föreliggande hot, sårbarheter och risker. Således hörsammas en viss grad av behovet kring anpassning till föränderliga hotlandskap och nya insikter om risker för att hantera cyberrelaterade sådana.

I NCSS framkommer det att regelverk och policy behöver förnyas oftare mot bakgrund av omvärldsförändringar och den teknologiska utvecklingen vilket påverkar säkerhetskraven. Det vittnar om att säkerhetshotet från cybermiljön varierar över tid, och i någon mån om att dynamisk styrning av cybersäkerhetsrisker krävs. Därutöver syns resonemang kring kontinuerligt lärande utifrån beskrivningen att en viktig komponent i det förebyggande arbetet av cybersäkerhetsrisker består av it-incidentrapportering, vilket möjliggör ett kontinuerligt lärande av inträffade händelser. Ytterligare anspelningar på dynamisk riskstyrning ses genom resonemang kring att säkerhetsutmaningarna i sammanhanget inte kan lösas en gång för alla; teknik- och hotutvecklingen innebär att informations- och cybersäkerhetsområdet förändras samt utvecklas i snabb takt. Därav måste strategin vara flexibel och kunna anpassas till de snabba omvärldsförändringarna – därför inte tidsatt och behöver uppdateras vid behov, där avsikten att genomföra en första uppdatering 2018 i samband med genomförandet av NIS-direktivet i svensk rätt. Härigenom erkänns dynamiken i cybersäkerhetshoten till viss del och i samma andetag att strategin behöver vara ett levande dokument, som kan kräva revidering relaterat till föränderlig risk- och hotbild.

Kodning till subkategorin *3.1.2 Holistiskt tillvägagångssätt och helhetsperspektiv* förekom endast en gång för samtliga strategier; i NCSS och i ett sammanhang kring en samlad ansats i arbetet med informations- och cybersäkerhet. Följande är den enda textpassage som kodades. ”För att informationshantering och IT-användning i samhället ska kunna utvecklas på ett tryggt och säkert sätt krävs att alla aktörer har en helhetssyn på informationssäkerhet” (Skr.2016/17:213, s. 9). Härigenom syns en viss adressering av vikten kring ett helhetsperspektiv i riskstyrningen för att hantera (systemiska) cybersäkerhetsrisker. Dock finns ingen förklaring av vad helhetssyn på informationssäkerhet innebär, inga resonemang uppfattades heller kring att ett helhetsperspektiv inkluderar breda dimensioner av cyberriskerna, eller om behovet att identifiera/bedöma/hantera riskerna utifrån deras komplexa/sammanlänkade natur. Värt att notera är att kodning till *3.1.2 Holistiskt tillvägagångssätt och helhetsperspektiv* endast förekom denna gång för samtliga sju dokument.

6.2.4 Hot, risker och sårbarheter inom kritisk infrastruktur och konsekvenser av angrepp

Resonemang gällande kritisk infrastruktur och samhällsviktig verksamhet inom cybersäkerhetsområdet är något som framträder i samtliga strategier, där relationen mellan cyberangrepp, antagonistiska hot och påverkan på samhälle adresseras. Flest antal kodningar totalt gjordes till kodningskategorin riktad mot samhällsviktig verksamhet och kritisk infrastruktur: Kodning till subkategorin *6.1.1 Effekter/konsekvenser på kritisk infrastruktur/samhällsviktig verksamhet* förekom sammanlagt sjutton gånger, med flest kodningar i NSMVT (nio) följt av NCSS, åtta gånger. I NSS framkommer det i sammanhang att det föreligger hot mot energiförsörjningen, transporter och infrastruktur samt att störningar i elförsörjningen kan medföra svåra påfrestningar på samhället. Värt att notera är att resonemanget återfinns i en kontext kring våldsbejakande extremism/terrorism, inte specifikt inom cybersäkerhet och digitala risker. Vidare förekommer resonemang kring att om kritisk infrastruktur och tillhörande informations- och kommunikationssystem skadas, kan det resultera i allvarliga konsekvenser för hela samhällets funktionalitet. Härvid adresseras relationen mellan hot mot samhällsviktig infrastruktur och infrastrukturens betydelse för samhällets funktionalitet, samt hur det förhåller sig till antagonistiska angrepp. Likaså framträder ett resonemang kring spridningseffekter vid störningar av infrastruktur, utan explicit uttryck för det. Dock nämns inte cyberattacker specifikt i sammanhanget eller som en specifik risk i avseendet.

I de två andra strategierna framkommer ytterligare resonemang kring relationen mellan cyberdomänen och dess påverkan på samhället och kritisk infrastruktur. I NSMVT görs adresseringar krig att kritisk infrastruktur behöver skyddas varvid skyddet behöver anpassas utifrån hotet: Hotet från terrorism är prioriterat, men skyddet av kritisk infrastruktur ska omfatta alla relevanta hot. Ytterligare framkommer det att en konsekvens av digitaliseringens progression är den ökade sårbarheten i samhällets infrastruktur och att cyberbrott förekommer regelbundet därinom, samt att svagheter i skyddet för samhällsviktig verksamhet utnyttjas i syfte att destabilisera samhället. Hörsammande görs kring att flera cyberangrepp fått stora samhälleliga konsekvenser även i Sverige de senaste åren, där vikten av att verksamheter säkerställer en fullgod informations- och cybersäkerhet poängteras. Vilka typer av samhälleliga konsekvenser som avses beskrivs dock inte. I en kontext kring cyberangrepp förekommer ytterligare diskussioner gällande att teknikutvecklingen medfört att infrastruktur inom elförsörjningen, elektronisk kommunikation och annan samhällsviktig verksamhet såsom: Sjukhus/vårdinrättningar, dricksvattenförsörjning, fängelse och informationsförsörjning, blivit föremål för cyberangrepp i större utsträckning än tidigare. Således hörsammas sambandet mellan cyberangrepp och dess påverkan på samhället där olika samhällskritiska verksamheter lyfts i sammanhanget, vilket är en skillnad gentemot rapporterna som inte benämner exempelvis sjukvårdssektorn eller anstalter.

Vidare återfinns resonemang gällande spridningseffekter inom infrastruktur i en kontext kring stärkt skydd av kritisk infrastruktur och rådsrekommendationer från EU samt CER-direktivet:

> ”Ett antal särskilt prioriterade sektorer pekas ut i rådsrekommendationen – energi, digital infrastruktur, transport och rymden. Dessutom betonas särskilt kritisk infrastruktur som har gränsöverskridande betydelse och där störningar skulle få stor negativ inverkan på flera medlemsstater” (NSMVT, Skr.2023/24:56, s .49).

Genom citatet kan en adressering av eventuella spridningseffekter vid störningar i samhällsviktiga sektorer uppfattas. Dock återfinns resonemanget i en kontext kring rekommendation av EU och implementeringen av CER-direktivet i Sverige vilket beskrivs ha för avsikt att stärka förmågan hos kritiska entiteter som tillhandahåller samhällsviktiga tjänster att förebygga, motstå och hantera störningar/avbrott, oavsett om dessa föranletts av exempelvis terroristattacker, naturolyckor, pandemier eller andra allvarliga händelser. Alltså inte i ett sammanhang kring cyberattacker specifikt och det är till ett EU-direktiv som citatet syftar. Övriga diskussioner gällande samhällsviktig verksamhet och kritisk infrastruktur förhåller sig till samhällets avhängighet på internet, vilket syns i resonemang i NCSS: Samhällets kritiska infrastruktur är i hög grad integrerat med internet och därav kan angrepp/incidenter inom infrastrukturen resultera i allvarliga konsekvenser för Sveriges säkerhet. Ytterligare framhålls att många verksamheter är beroende av fungerande digitala informations- och styrsystem, exempelvis eldistribution, vattenförsörjning, transportinfrastruktur och sjukhusutrustning. Hörsammande görs kring att hot- och riskskalan inom det informationsteknologiska området har en bred spännvidd; från mindre omfattande risker för den enskilde individen, till riktade angrepp mot vitala delar av samhällets funktionalitet.

Vidare syns diskussioner i NCSS angående vikten av att säkerställa funktionaliteten i centrala samhällsfunktioner, såsom inom el- och dricksvattenförsörjning. Störningar inom transportsystem, produktion och sjukvård framhålls som exempel där förebyggande arbete är viktigt. Resonemangen i NCSS vittnar om en adressering kring cyberattackers eventuella påverkan på samhällsviktig verksamhet och kritisk infrastruktur, samt vikten av att skydda sådan infrastruktur. Likaså hörsammas den höga graden av digitalisering inom kritisk infrastruktur och dess medförande sårbarheter för cyberattacker. Trots det uppfattades inga tydliga uttryck för spridningseffekter av cyberattacker, inte heller inom ramen för samhällsviktig verksamhet/kritisk infrastruktur. Det som observeras i sammanhanget är: ”Angrepp mot svenskt näringsliv kan få långtgående konsekvenser för enskilda företag såväl som för hela värdekedjor, och därmed hota svenska arbetstillfällen” (NCSS, Skr.2016/17:213, s. 6). Citatet vittnar om spridningseffekter av ett angrepp, men värt att notera är att angreppen här avser dem mot privata sektorn och en slags spridningseffekt inom värdekedjor.

Resonemang kring cybersäkerhetsriskers eventuella påverkan på människors liv och/eller hälsa samt diskussioner kring attackers påverkan på miljön, förekom betydligt färre gånger än de kring samhällsviktig verksamhet och kritisk infrastruktur. Detta är ett

resultat som även ses gällande rapporterna. Sammanlagt förekom kodning till subkategorin *6.1.2 Effekter/konsekvenser på liv/hälsa/miljö* endast fyra gånger i strategierna; en gång vardera i NSS och NSMTV samt två gånger i NCSS. Resonemang som förekommer i NSS avser att störningar och avbrott i försörjningen av el, bränsle och värme kan utmynna i allvarliga konsekvenser, såväl för människors liv och hälsa som för samhällets funktionalitet. Härvid hörsammas en spridningseffekt av en risk som kan påverka människors liv och hälsa, men resonemanget återfinns i ett sammanhang kring terrorism/våldsbejakande extremism och hot mot energiförsörjningen. Inte konkret gällande cyberhot. I NSMVT förekommer följande resonemang: ”Kommunerna ansvarar för räddningstjänst avseende räddningsinsatser vid olyckor och överhängande fara för olyckor för att hindra och begränsa skador på människor, egendom eller miljön” (NSMVT, Skr.2023/24:56, s. 56). Citatet återfinns i en kontext kring kemiska olyckor, ingripande, behov av taktisk förmåga för snabba insatser och hantering av situationen under och efter attentatet; attentat från den våldsbejakande miljön eller sådant som klassas som terrorattentat – inte endast cyberattentat.

Det enda resonemang som återfinns avseende effekter på liv/hälsa/miljö i NCSS, är att strategin i sig har sin utgångspunkt i målen för Sveriges säkerhet: Att värna befolkningens liv och hälsa, liksom samhällets funktionalitet. Utöver detta förekommer inga andra resonemang eller liknande som anspelar på dimensionen kring människors liv/hälsa i sammanhanget. Endast NSS adresserar denna relation genom att störningar och avbrott i försörjningen av el/bränsle/värme kan resultera i allvarliga konsekvenser för människors liv och hälsa, dock benämns det inte i sammanhanget kring cyberattacker specifikt utan kring samhällsviktig verksamhet generellt. Därutöver uppfattades inga resonemang kring cyberattackers eventuella påverkan på miljön vilket gäller samtliga strategier: Inga diskussioner eller resonemang som anspelar på cyberriskernas och attackers eventuella påverkan på miljön uppfattades i något avseende. Notera att detsamma förekom i rapporterna – således är potentiell miljömässig påverkan av cybersäkerhetsriskerna inget som adresseras i något av de sju dokument som analyserats.

En observation i sammanhanget är att även om kodningar till *6.1.1 Effekter/konsekvenser på kritisk infrastruktur/samhällsviktig verksamhet* förekom nästan lika många gånger i NSMVT och NCSS, är textpassagerna som urskilts av olika karaktär: NSMVT har ett större fokus på att skydda samhällsviktig infrastruktur över lag, jämfört med NCSS. Likaså hörsammas sårbarheter och angrepp mot infrastrukturen mer, vilket kan tänkas ha sin delvisa förklaring i att NSMVT är nyligen publicerad och NCSS är i skrivande stund sju år gammal. Ytterligare iakttagelse är att strategierna tydligast framhäver elsektorn inom kritisk infrastruktur, men att två av rapporterna (NSMVT och NCSS) en gång vardera hörsammar andra samhällsviktiga verksamheter också. Detta resultat ses ha ett samband med det för rapporterna, vilka främst har fokus på elsektorn och inte benämner exempelvis sjukvårdssektorn. Därutöver förekom ingen kodning till kodningskategorin *7.1 Kaskadeffekter* och subkategorin *7.1.1 Potentiella kaskadeffekter av cyberattacker inom KI/SVV* i någon av säkerhetsstrategierna. Således uppfattades inga textpassager som

diskuterade eller anspelade på cybersäkerhetsriskernas relation till eventuella kaskadeffekter inom kritisk infrastruktur och samhällsviktig verksamhet. Ordet kaskadeffekter eller kaskad förekom inte heller i andra sammanhang utanför kontexten kring samhällsviktig verksamhet/kritisk infrastruktur, i någon av strategierna. Liknande förfarande sågs även i rapporterna, då kodning till kategorin endast förekom en gång sammanlagt och övriga resonemang avseende kaskadeffekter återfanns inte heller.

6.2.5 Harmonisering med andra säkerhetsstrategier och ramverk

Diskussioner kring andra ramverk och säkerhetsstrategier samt kopplingen mellan dessa, förekommer i samtliga strategier. Kodning till kodningskategorin *4.1 Harmonisering* och subkategorin *4.1.1 Sammanlänkning med andra nationella säkerhetsstrategier och (internationella)ramverk* förekom totalt nio gånger. Majoriteten (fem gånger) förekom i NSMVT. Presentationer av EU-direktivet gällande åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet) och direktivets roll, återfinns i NSS. Därtill lyfts att en nationell strategi för informations- och cybersäkerhet utarbetas (strategin som är inkluderad i föreliggande analys). Liknande samhörighet reflekteras i NCSS, där hänvisningar görs till NSS. Vidare beskrivs NIS-direktivet och att ett slutbetänkande finns kring dess nationella implementering, där NIS-direktivet ställer krav på säkerhet i nätverk och informationssystem och omfattar leverantörer av samhällsviktiga tjänster/vissa digitala tjänster. I NSMVT beskrivs att det nya CER-direktivet från Europaparlamentet syftar till att öka motståndskraften hos både privata och offentliga aktörer, behöriga myndigheter och i unionen som helhet: Genomförandet av CER-direktivet ska bidra till att stärka förmågan att hantera antagonistiska hot. Vidare lyfts att det nya NIS2-direktivet från EU adresserar den ökande digitala hotbilden mot unionen samt de ökande beroendena mellan sektorer och över landsgränser. Därutöver syns ett resonemang kring att genomförandet av NIS2- och CER-direktiven i Sverige, ihop med den nya NCSS ska bidra till att stärka samhällets förmåga att hantera antagonistiska hot. Härigenom adresseras samhörigheten mellan NCSS och andra nationella säkerhetsstrategier samt internationella ramverk för skydd av kritisk infrastruktur och samhällsviktig verksamhet.

En notering är att ingen kodning förekom till kodningskategorin *8.1 Okonventionella gränser* och subkategorin *8.1.1 Distans i cyberrisker.* Alltså uppfattades inga textpassager i någon av strategierna som diskuterade cyberriskers/attackers karaktär av att inte besitta konventionella gränser i termer av att hot och attacker kan utföras från geografiskt avlägsna platser utan fysisk närvaro. Ytterligare iakttagelse är att samtliga strategier betonar vikten av samverkan mellan myndigheter och andra aktörer som en grundläggande förutsättning för att effektivt hantera antagonistiska hot: I NSMVT poängteras att samverkan och samordning på lokal, regional och nationell nivå krävs för att bemöta hotet från terrorism och våldbejakande extremism. Liknande resonemang återfinns i NCSS; informations- och cybersäkerhetsfrågor är ett gemensamt ansvar, där ingen ensam kan lösa säkerhetsutmaningarna, varvid informationssäkerhetens

komplexitet, gränsöverskridande karaktär och utvecklingstakt kräver effektiv samverkan. Därutöver äger och driver privata aktörer stora delar av den samhällsviktiga verksamheten, vilket kräver god samverkan för att uppnå ett adekvat skydd. Således adresseras samverkan inom och mellan privat och offentlig sektor som en viktig faktor för att adekvat bemöta cybersäkerhetsriskerna.

7 Diskussion

Följande diskussionsavsnitt är uppdelat i två delar: Första delen avser en diskussion vilken grundas i uppsatsens resultat med anknytning till uppsatsens syfte, frågeställningar, tidigare forskning samt teoretiska referensram. Primärt avser första rubriken: *Systemförståelse av cyberrisker* svara upp mot syftet, rubrik två: *Spridningsrisker inom system och kaskadeffekter av cyberattacker*, tre: *Kritisk infrastruktur och samhällsviktig verksamhet inom cybersäkerhetsrisker* och fyra: *Cyberattackernas påverkan på liv, hälsa och miljö* mot frågeställningarna. Femte rubriken*: Dynamiskt förhållningssätt och helhetsperspektiv på cyberrisker* svarar även den mot syftet. Därefter följer en metoddiskussion som innehåller reflektioner kring tillvägagångssätt och de metodval som tillämpats i uppsatsen.

7.1 Resultatdiskussion

7.1.1 Systemförståelse av cyberrisker

De systemiska perspektiven på cyberdomänen och dess associerade risker har framhävts som en central dimension i förståelsen av cyberriskerna och dess potentiella omfattning. Precis som Welburn & Strong (2022) beskriver behöver cyberrelaterade incidenter betraktas inom ramen för systemiska risker, för att öka förståelsen av dess möjliga allvarliga konsekvenser. Resultatet visar att strategierna och bedömningarna som granskats framhäver systemiska aspekter på riskerna inom cyberdomänen, men att vissa beståndsdelar därinom saknas alternativt är mindre framträdande. Att cybersäkerhets-riskerna besitter en dimension av att vara föränderliga i tid och rum, alltså dynamiska i sin natur – är en sådan. Riskerna diskuteras inte heller som komplexa, osäkra eller tvetydiga uttryckligen, i stället görs antydningar som speglar komplexiteten. Den dynamiska aspekten i cybersäkerhetsriskerna relaterar till att systemiska risker är föränderliga i sin utveckling över tid och icke-linjära i sina orsak-verkan-samband, där effekterna är stokastiska (Schweizer, 2019; van Asselt & Renn, 2011; Renn, 2021). Renn m.fl. (2022) menar att systemiska risker och dess effekter vanligen är oförutsägbara, vilket gör att riskerna bär hög osäkerhet och är tvetydiga, som i sin tur har en relation till riskernas starka komplexitet. Dessa perspektiv är inget som tydligt framträder i resultatet vilket kan ses som en utmaning utifrån att Schweizer (2019) menar att dimensionen kring riskernas höga komplexitet är något som behöver hörsammas gällande systemiska risker. Att dessa element av cybersäkerhetsriskerna inte uppmärksammas fullskaligt kan således ses som en problematisk avsaknad utifrån att adressera den breda komplexiteten som existerar i riskerna.

Något som framträder tydligt i resultatet är systemiska aspekter som relaterar till teknologisk progression och beroendeförhållanden. Den hastiga teknologiska utvecklingen och digitaliseringen med den, framhålls som en drivkraft för viktiga samhällsförändringar men också som katalysatorer för cyberrelaterade risker. Resultatet vittnar om att dessa förfaranden är centrala faktorer för sårbarheter inom cyberdomänen

generellt, och att det existerar tydliga säkerhetsutmaningar som följer med det. Det går i linje med det Renn (2021) & Renn m.fl, (2022) skriver gällande att systemiska risker delvis är resultatet av de hastiga och djupgående ekonomiska/sociala/tekniska förändringarna i dagens moderna samhälle, där specifikt den teknologiska progressionen har föranlett potentiella hot såsom cyberattacker. I sammanhanget framkommer det även i resultatet att det pågår en ständig kapplöpning mellan medel och motmedel inom cybersäkerhet, relaterat till att den tekniska utvecklingen är hög och att det kontinuerligt upptäcks nya sårbarheter som utnyttjas. Sammantaget skapar detta tanken kring att kapplöpningen förmodligen kommer fortgå i takt med att den teknologiska progressionen fortgår. Följaktligen vittnar det om diskrepansen som existerar i sammanhanget; hoten och riskerna löper snabbare än åtgärder som inte hinner med i samma tempo. Det för tankarna vidare till huruvida tillämpningen och progressionen av exempelvis artificiell intelligens (AI) i samhällets alla delar, endast är ytterligare en katalysator i sammanhanget, men som också kan vara ett motmedel som kan minska risker i cybersfären.

Återkommande i resultatet är att den kraftiga teknologiska progressionen och digitaliseringen skapat ömsesidiga och komplexa beroendeförhållanden, där betoning görs på beroendet av IT-system inom olika centrala samhällsfunktioner. Likaså på hur dessa förfaranden tillsammans genererar sårbarheter som relaterar till cybersäkerhetrisker och cyberangrepp. Det i sin tur speglar dimensioner kring beroendeförhållanden inom systemiska (cyber)risker och det Renn m.fl. (2011) understryker kring att risker med systemisk karaktär är inbäddade i de större samhällsprocesserna samt är integrerade i våra centrala samhällssystem. Således verkar det råda en medvetenhet i strategierna och rapporterna kring systemiska beståndsdelar som avser beroendeförhållanden, hur dessa löper inom centrala samhällsfunktioner samt hur det förhåller sig till i cyberriskerna och sårbarheter.

En systemförståelse i sammanhanget innebär också att ytterligare beroendeförhållanden uppmärksammas tillsammans med andra systemteoretiska aspekter. Betydelsen av detta pekar Sparf (2009) på inom systemteori: System är beroende av alla sina ingående enheter vilket betyder att om en enhet utsätts för en risk och slås ur funktion, riskerar resterande delar i systemet att sättas ur funktion. Sådana teoretiska resonemang kring systemberoenden framträder delvis i resultatet, men inte i full utsträckning. Av resultatet att döma skildras cybersäkerhetsrisker som systemöverskridande fenomen och resonemang återfinns gällande riskerna och dess konsekvensers gränsöverskridande karaktär, men djupare än så går inte diskussionerna. Det som syns gällande systemberoenden korrelerar med det Renn m.fl. (2022) poängterar kring att riskerna kännetecknas av att dess konsekvenser kan sträcka sig bortom det ursprungliga systemet. Andra systemteoretiska aspekter som lyser med sin frånvaro i såväl strategierna som rapporterna är de som rör emergens, vilket enligt Larsson m.fl. (2010) är en central aspekt i sammanhanget: Ett systems komponenter interagerar med varandra och påverkar varandra på sätt som inte är förutsägbara utifrån deras individuella egenskaper, där

olyckor är ett exempel på emergenta fenomen. Det centrala perspektivet uppfattas inte existera utifrån de resultat som framkommit.

Återkommande i resultatet är sociotekniska aspekter på cybersäkerheten. Framförallt i de mer operativa synsätten på cybersäkerhetsrisker, vilket representeras i de fyra rapporterna från NCSC. Leveson m.fl (2009) menar att ett sociotekniskt perspektiv belyser helheten av ett integrerat system i form av samspelet mellan tekniska och sociala aspekter, vilket är något som återspeglas i resultatet utifrån att samspelet mellan teknik/människa i cybersäkerhet är tydligt framträdande. Främst i rapporterna men benämns även i NCSS angående att störningar kan ha sin grund i handhavandefel, och att hänsyn behöver tas till den mänskliga faktorn i incidenter samt att mänskliga egenskaper vanligen utnyttjas vid angrepp. Tillvägagångssätt och metoder inom cyberangrepp som framkommer i resultatet är det som tydligt anspelar på relationen mellan teknik och människa och hur dessa samexisterar i cybersäkerheten. Det går i linje med teoretiseringar från McEvoy & Kowalski (2019) som menar att cybersäkerhetsrisker är att betrakta som sociotekniska till sin natur, då riskerna inte endast emanerar från tekniska sårbarheter utan också från mänskliga interaktioner. Ett intressant resultat är att de sociotekniska dimensionerna som rör komplexitet och dynamik i sociotekniska system, är frånvarande i såväl rapporterna som strategierna. Det McEvoy & Kowalski (2019) belyser kring att cybersäkerhetsrisker likt andra sociotekniska system påverkas av den externa miljön de är en del av, såsom politiska/juridiska/sociala och/eller miljömässiga faktorer vilka kan ha betydande inverkan på systemet, är inget som framkommer i resultatet. Alltså verkar det inte vara ett perspektiv som beaktas; hur komplexiteten i denna process inom systemet influerar risker och sårbarheter. Detta sammantaget både speglar och motsäger det som McEvoy & Kowalski (2019) samt Malajti m.fl. (2018) påpekar gällande att sociotekniska aspekter vanligen ignoreras i hanteringsmetoder inom cybersäkerhet: Å ena sidan råder uppmärksamhet kring att både tekniska och mänskliga aspekter är en del av cybersäkerheten och att teknik och människa samspelar i riskerna, där exempelvis mänskliga faktorer utnyttjas vid angrepp genom tekniken. Å andra sidan återfinns inte hela det sociotekniska spektrumet; den höga graden av både teknisk och social komplexitet samt dynamiken inom det sociotekniska systemet hörsammas inte i vare sig strategierna eller rapporterna.

7.1.2 Spridningsrisker inom system och kaskadeffekter av cyberattacker

Sparf (2009) poängterar att system är nära sammankopplade med varandra. Det är även ett perspektiv som återfinns inom normal accident theory (NAT), där Perrow (1984, s. 5–8) menar att många av våra högrisk-teknologier och system besitter karaktärsdrag i form av *interaktiv komplexitet* och *tät sammankoppling.* Sådana teoretiska perspektiv är inget som framträder i strategierna eller bedömningar som granskats, även om andra beståndsdelar inom NAT framträder. Exempelvis att konsekvenser av allvarliga IT-incidenter inte alltid uppstår eller är uppenbara i direkt anslutning till händelsen – alltså att cyberrisker har en dimension av latenta beroendeförhållanden där oväntade effekter

av cyberattacker kan uppkomma över tid. Genom resultatet framkommer det att aspekter som rör interaktiv komplexitet och tät sammankoppling, inte är systemförhållanden som betänks inom ramen för cybersäkerhetsrisker eller cyberattacker. Likaså återfinns inga resonemang kring att karaktärsdragen även har en samhörighet till kedjeeffekter inom system, där små incidenter kan utlösa kedjereaktioner av störningar och hur dessa kan eskalera till storskaliga händelser och systemolyckor. Det i sin tur kan ses som problematiskt då Shrivastava m.fl. (2009) framhäver att när omständigheterna är rätt i komplexa system, kan störningar utlösas som interagerar med varandra på ett sätt som är svårförståeligt. Dessa komplexa interaktioner kan i sin tur generera kaskadhändelser, i tätt sammankopplade system. Att resultatet pekar på att de flesta beståndsdelar inom NAT är frånvarande är ytterligare intressant utifrån Backmans (2023) resonemang om att NA-dynamiken är karaktärsdrag som existerar i majoriteten av systemen inom cyberdomänen. Möjligen även problematiskt i ljuset av att NAT enligt Backman (2023) gynnsamt kan användas för att förstå hur störningar i de sociotekniska systemen som ligger till grund för exempelvis kritisk infrastruktur kan resultera i kaskadeffekter, och för att förstå hur denna dynamik speglar risker för sidoeffekter sprungna ur antagonistiska cyberhändelser. Eftersom cyberrisker och hotet från cybermiljön tillsammans med riskernas samhörighet till komplexa beroenden genomgående positioneras som framstående, kan det anses anmärkningsvärt att NA-dynamiken och framförallt perspektivet kring cyberattackernas potential att resultera i kaskadeffekter och systemolyckor, är så pass frånvarande.

Kaskadeffekter är alltså ett småskaligt perspektiv i resultatet. Trots att överväganden och bedömningar framträder angående risken för kaskadeffekter till följd av cyberattacker, är de entaliga: Det nämns att påverkan på elsystemet och leveransen av el skulle ge kaskadeffekter på samhällskritiska system och samhället i stort, men inga andra bedömningar kring kaskadeffekter existerar, varken i eller utanför en kontext kring samhällsviktiga verksamheter/kritisk infrastruktur. Likaså uppmärksammas inte heller den bredare samhällspåverkan som kaskadeffekter kan ha, såsom deras potentiella inverkan på liv, hälsa och miljö och inga ytterligare resonemang kring vad ”kaskadeffekter på samhället i stort” de facto innebär återfinns. Det uppfattas intressant, då tidigare forskning från Pescaroli & Alexander (2015) samt Alexander (2018) understryker att kaskadeffekter är starkt kopplad till systems sårbarheter snarare än till hoten enskilt; om sårbarheterna är utbredda eller inte hanteras korrekt i systemet kan även mindre händelser generera kaskadeffekter. Likaså understryks att kritisk infrastruktur ofta är kanalen genom vilken kaskadeffekter sprids. Detta blir av vikt i sammanhanget utifrån att det i resultatet framkommer att den teknologiska progressionen och digitaliseringen har skapat komplexa beroendeförhållanden samt beroenden av konstant leverans av elektricitet. Därutöver att system inom olika centrala samhällsfunktioner är avhängda på digitalisering och elberoende, vilket sammantaget skapat sammanlänkade sårbarheter som dessutom utnyttjas. Därigenom kan det anses anmärkningsvärt att bedömningar kring kaskadeffekter inte framträder tydligare i resultatet, då sårbarheterna framförs som

utbredda och sammankopplade och eftersom risker från cybermiljön genomgående framhävs ha en samhörighet till sårbarheterna som den teknologiska progressionen och digitaliseringen genererat. Att kaskadeffekter inte är mer framträdande i strategier och bedömningar kan därutöver ses gå i linje med det Welburn & Strong (2022) benämner kring att cyberrisker behöver betraktas som systemiska cyberrisker, relaterat till cyberattackers potentiella kaskadeffekter. Likaså kan det uppfattas ha ett samband till det Welburn & Strong (2022) poängterar gällande att cyberattackernas utbredda konsekvenser och kedjereaktioner är undermåligt förstådda.

7.1.3 Kritisk infrastruktur och samhällsviktig verksamhet inom cyber-säkerhetsrisker

Återkommande i resultatet är att samhällsviktig verksamhet och kritisk infrastruktur positioneras som mål för cyberattacker. Framträdande är därutöver att sårbarheter existerar inom samhällskritiska verksamheter, med tydlig relation till digitaliseringen – vilket utnyttjas i antagonistiskt syfte och för att destabilisera samhället. Likaså adresseras relationen mellan cyberangrepp, antagonistiska hot och påverkan på samhället där skyddet av kritisk infrastruktur framhålls som centralt. Vidare framkommer det att stora delar av den samhällsviktiga verksamheten är digitaliserad och således sårbar för cyberangrepp. Detta är något som tydligt går i linje med det Atkins & Lawson (2020), Rulleau (2023) & Palleti m.fl. (2021) påpekar: Att verksamheter inom kritisk infrastruktur blir alltmer digitaliserade och att IT-komponenterna i digitaliserade system ofta är sårbara för attacker då de har funktioner som kan utnyttjas, därav att det är centralt att skydda sektorer inom kritisk infrastruktur eftersom de är frekventa mål för cyberattacker. Detta är korrelerade resonemang som återfinns i resultatet och ett förhållningssätt som framträder i strategierna och bedömningen gällande cyberattacker mot samhällsviktig verksamhet och kritisk infrastruktur. Således syns en tyngdpunkt på samhällets kritiska infrastruktur, vikten av att skydda den samt att cyberangrepp de facto är en reell risk som kan destabilisera samhället genom angrepp på infrastrukturen.

Ytterligare aspekt i sammanhanget är att det i resultatet förekommer perspektiv gällande distans i cyberrisker och attacker. Det som framkommer är de okonventionella gränserna i cyberrisker och att samhällsviktig infrastruktur har industriella informations- och styrsystem som är uppkopplade mot internet, vilket gör dessa tillgängliga för åtkomst på distans. Det uppkommer även exemplifiering på detta genom verkliga attacker som skett på distans (exempelvis attacken mot Ukrainas elnät 2015), vilket korrelerar med det Albahar (2017) lyfter kring vikten av att skydda kritisk infrastruktur mot cyberhändelser: Cybersfären inte har inga konventionella gränser och således kan cyberattacker utföras från långa avstånd och kräver inte fysisk närvaro. Likaså anspelar det på den systemiska beståndsdelen inom komplexa systemiska (cyber-)risker, som Renn m.fl (2022) belyser kring deras okonventionella natur och att kritisk infrastruktur är prototyper för systemrisker eftersom riskerna påverkar system som samhället är beroende av. Distansen i cyberriskerna är dock inget som problematiseras ytterligarare i rapporterna. En differens

framträder även i avseende kring distansen, utifrån att strategierna inte förhåller sig till dimensionen av att attacker mot samhällsviktig verksamhet och kritisk infrastruktur kan utföras på distans.

Övriga förhållningssätt i strategierna och bedömningarna avseende cyberattacker mot samhällsviktig verksamhet och kritisk infrastruktur, relaterat till det som framträder tydligast i resultatet: Att påverkan på elsystemet skulle medföra omfattande samhällskonsekvenser, utifrån att elsektorn utöver att vara en kritisk infrastruktur bär beroenden till annan kritisk/samhällsviktig infrastruktur samt till mångt och mycket är digitaliserad. I ljuset av detta framträder även ett starkare fokus på elsektorn inom samhällskritisk verksamhet och dess sårbarheter för cyberangrepp – i förhållande till annan kritisk infrastruktur, framför allt i rapporterna. Andra delar av vår samhällsviktiga infrastruktur såsom hälso- och sjukvårdssektorn och cyberangrepp därinom lyfts inte i någon rapport. Det överensstämmer inte helt med resultatet avseende strategierna, vilka benämner exempelvis sjukhus/vårdinrättningar, dricksvattenförsörjning och fängelser. Likväl får elsektorn större fokus sammantaget betraktat. Det är ett intressant resultat utifrån att Bernard m.fl. (2020) poängterar att hälsosektorn utgör ett betydande mål för cyberangrepp bland nationell kritisk infrastruktur, på grund av dess centralitet för samhället. Trots det understrykes att sjukvårdssektorn får mindre uppmärksamhet än annan kritisk infrastruktur, vilket är något som korrelerar med resultatet som framkommit här.

Vidare leder det återigen in på avsaknaden av bedömningar gällande kaskadeffekter och perspektiv på NA-dynamiken inom cybersäkerhetsriskerna. Där exempelvis Cutter (2018) betonar att kaskadeffekter och deras allvarliga konsekvenser oftast kan härledas till den kritiska infrastrukturen som har en avgörande roll för samhällets funktion. Att den samhällsviktiga verksamheten genomgående i resultatet positioneras som sårbar blir därav anmärkningsvärt. Likaså i ljuset av att Cutter (2018) understryker att det sociala funktionella beroendet på den kritiska infrastrukturen är resultatet av upparbetade sårbarheter hos det moderna samhället, där teknologin är tätt integrerad och sammanlänkad vilket i sin tur gör lätt skapar störningar och avbrott. Förefaller detta i ett sammanhang kring kritisk infrastruktur vilken är en kanal för kaskadeffekter, blir det desto tydligare att det är problematiskt att sjukvårdssektorn inte får lika starkt fokus som annan samhällsviktig verksamhet. Likaså blir det bekymmersamt att kaskadeffekter relaterat till den tätt sammankopplade teknologin inom samhällsviktig infrastruktur är ett perspektiv som lämnar mer att önska inom strategierna och bedömningarna. Ytterligare relaterat till att Bernard m.fl. (2020) framhåller att den potentiella attackytan är omfattande i hälso- och sjukvårdssektorn utifrån dess komplexitet i form av teknologiska beroenden och sociotekniska karaktärsdrag.

7.1.4 Cyberattackernas påverkan på liv, hälsa och miljö

Utifrån ovanstående diskussion framkommer det att samhällsviktig verksamhet och kritisk infrastruktur samt dess relation till cybersäkerhetsrisker är framträdande

dimensioner. Det som inte framträder lika tydligt i resultatet är relationen mellan cyberattacker och dess eventuella påverkan på liv, hälsa och miljö, i stället är den mycket sparsam. Beskrivningar av den relationen som förekommer i resultatet avser att störningar och avbrott i försörjningen av el/bränsle/värme kan resultera i allvarliga konsekvenser för människors liv och hälsa. Det framkommer dock inte i ett konkret sammanhang runt cyberattacker specifikt, men anspelas på indirekt. Likaså är resonemangen kring relationen inte djupare än så – vad skulle ett avbrott i elnätet få för konkreta, indirekta effekter? Och vilka de allvarliga konsekvenser är som kan påverka människors liv och hälsa, framgår inte. Dessa förfaranden kan betraktas som anmärkningsvärda, specifikt i relation till det tidigare lyfts i uppsatsen genom Eddy & Perlroth (2020): 2020 utsattes ett sjukhus i Tyskland för en cyberattack som stängde av vitala digitala resurser på sjukhuset, där ett dödsfall betraktas ha orsakats av försenad behandling till följd av attacken. Men även lika starkt i ljuset av det Bernard m.fl. (2020) understryker kring att störningar i tekniska system i sjukvårdsnätverk kan resultera i betydande destabiliserande samhällskonsekvenser och leda till förlust av liv, samt att angrepp mot medicintekniska enheter har skett historiskt. Och fastän förlust av liv inte ännu varit direkt kopplad till en attack mot en medicinteknisk enhet, gör hastigheten av dess tillämpning i kombination med bristen på säkerhetregleringar på institutionell nivå både individer och verksamheter i sammanhanget sårbara. Det i sin tur kan sammanfogas med det som lyfts angående distans och okonventionella gränser i cyberattacker, framförallt till det Albahar (2017) belyser kring att cybersfären inte har några konventionella gränser och således kan cyberattacker utföras på distans utan fysisk närvaro, därav bli lika dödliga som konventionella angrepp. Kombineras dessa perspektiv blir avsaknaden av att tydligt hörsamma relationen mellan cyberattacker och dess eventuella påverkan på människors liv och hälsa alarmerande, ytterligare eftersom det i NCSS nämns att sjukhusutrustning är beroende av fungerande digitala informations- och styrsystem som framhålls sårbara. Det för tankarna till att cyberangrepp de facto kan leda till påtagliga och skrämmande konsekvenser för människors hälsa och liv, i många tänkbara scenarion där sådana förfaranden dessutom kan ske i det dolda. Därav vara ett perspektiv som behöver existera i bedömningar gällande cyberriskernas potentiella sekundära effekter och angreppens potential i att påverka människors hälsa samt leda till förlust av liv.

I resultatet framträder även en avsaknad av miljömässiga dimensioner i form av cyberriskernas relation till eventuell påverkan på miljön. Den relationen speglas endast en gång i resultatet utifrån sambandet mellan antagonistiska attacker och kemiska olyckor – där insatser vid dessa behöver begränsa skador på människor, egendom och miljö. Därutöver framträder inga relationella aspekter på miljön och cyberattacker. Det är ett intressant resultat utifrån att den miljömässiga dimensionen även i den tidigare forskningen och i uppsatsens övriga litterära underlag, är betydligt mer frånvarande än andra aspekter som avser konsekvenser av cyberattacker och dess påverkan på samhället. Detta kan ses i linje med att Burk & Kallberg (2016) beskriver att fastän skyddet av kritisk infrastruktur generellt sett är en nationell prioritet, är lite fokus förlagt på att bedöma eller

ta hänsyn till de eventuella konsekvenserna på människor och miljön om cybersäkerheten brister. Trots att hänsyn tas till samhällspåverkan i rapporterna och strategierna, ses inte full hänsyn tas till påverkan på människor och miljön. Detta blir ytterligare intressant utifrån att det som nämnt existerar röster kring att cyberattacker mot lantbrukare och attacker som påverkar livsmedelssäkerheten, numera är en reell risk. Tanken kring att det finns potential för att cyberattacker leder till påverkan på miljö och/eller kringliggande områden, exempelvis hota livsmedelsäkerheten, är således inte orimlig längre. Sammantaget genererar dessa resultat i uppfattningen att miljöperspektivet och sammanhörande områden är oerhört småskaliga i det kontextuella cybersäkerhetsområdet. Således vara något som behöver mer uppmärksamhet för att betrakta cyberriskernas omfattning och samhällspåverkan i breda termer, där det förefaller genom analysen av strategierna och rapporterna att allvaret i cybersäkerhetsriskerna inte är fullständigt förstådda.

7.1.5 Dynamiskt förhållningssätt och helhetsperspektiv på cyberrisker

När det kommer till ett dynamiskt förhållningssätt gällande systemiska (cyber-)risker och styrningen av dessa, pekar resultatet på behovet av kontinuerlig anpassning till föränderliga hotmiljöer och det tekniska landskapet för att säkerställa effektivitet inom informations- och cybersäkerhetsområdet. Därutöver att policys behöver förnyas oftare mot bakgrunden av omvärldsförändringar och den teknologiska utvecklingen, givet att det påverkar säkerhetskraven. Det överensstämmer med perspektiven på styrning av systemiska risker, vilken behöver vara adaptiv för att adekvat hantera dessa komplexa och föränderliga risker (Renn m.fl., 2022; Renn m.fl., 2011). Enligt Renn m.fl. (2011) innefattar riskstyrning också en dynamisk styrningsprocess som inbegriper kontinuerligt lärande samt justering vid nya insikter. Ett sådant förhållningssätt framträder delvis i resultatet utifrån att säkerhetsutmaningarna i sammanhanget inte kan lösas en gång för alla; teknik- och hotutvecklingen innebär att informations- och cybersäkerhetsområdet förändras och utvecklas i snabb takt. Därav måste strategier ha en flexibilitet och kunna anpassas till omvärldsförändringarna. Det är ett tankeväckande resultat eftersom Sveriges NCSS publicerades år 2017 och beskrivs inte vara tidsatt, utan ska uppdateras vid behov med en första gång 2018 i samband med implementeringen av NIS-direktivet. Precis som Riksrevisionen (2023) poängterar har det inte skett några förändringar eller korrigeringar i strategin, utöver kompletteringen 2018 (som avsåg NIS-direktivets rättsliga aspekter). I skrivande stund är den nya NCSS inte publicerad och som nämnt har den varit under utarbetning sedan hösten 2023. Med tanke på den återkommande bilden som framträder i resultatet, där teknikutvecklingen och digitaliseringen fortsätter att accelerera och där sårbarheter ständigt upptäcks – är det anmärkningsvärt att inga övriga anpassningar eller tydliga förändringar har gjorts i strategin de senaste sju åren. Detta tyder inte fullt ut på ett dynamiskt förhållningssätt till riskstyrningen, vilket är avgörande för att effektivt hantera komplexa, systemiska cyberrisker (Renn m.fl., 2022; Renn m.fl., 2011). Riskstyrningen i avseendet behöver därutöver vara adaptiv i relation till föränderliga förhållanden och nya insikter om risker. Det som framkommer i detta avseende i resultatet

är att en viktig komponent i det förebyggande arbetet av cybersäkerhetsrisker består av it-incidentrapportering, vilket möjliggör ett kontinuerligt lärande av inträffade händelser. Med sådan kontinuerlig, nyvunnen kännedom kan kritik återigen riktas mot att strategin inte uppdaterats utförligare eller tidigare, och att riskstyrningen i sammanhanget inte inneburit tydliga adaptiva förhållningssätt till förbättringar.

Vidare framkommer det i resultatet att säker utveckling av informationshantering och IT-användning i samhället, kräver att alla aktörer har en helhetssyn på informationssäkerhet. Dynamiska aspekter och helhetsperspektiv inom hanteringen och styrningen av cybersäkerhetsrisker, uppfattas alltså i någon mån i resultatet. Likväl förs tankarna till att det djupgående dynamiska och adaptiva förhållningssätt som krävs för en adekvat styrning av systemiska cyberrisker inte speglas fullt i dokumenten. Panda & Bower (2020) betonar att tillvägagångssätt för hantering av cyberrelaterade risker kräver ett helhetsinriktat synsätt som tar hänsyn till hela samhället och komplexiteten i riskerna. Ett sådant helhetinriktat synsätt där hänsyn till alla dimensioner inom samhället tas, förekommer inte i full utsträckning i dokumenten – exempelvis utifrån att miljömässiga perspektiv lyser med sin frånvaro. Detta kan vidare ses i ljuset av att Panda & Bower (2020) understryker vikten av att förstå att cyberrisker kan resultera i allvarliga händelser utifrån potentiella kaskadeffekter som cyberattacker kan medföra. Dimensionen kring cyberriskernas vidd ihop med potentiella kaskadeffekter har tidigare i diskussionen lyfts som tunna perspektiv i resultatet, vilket blir en ytterligare svaghet avseende ett adekvat helhetsperspektiv inom styrningen av cyberriskerna.

Vidare kan ovanstående resonemang sammankopplas till det Luiijf m.fl. (2013) påpekar kring att NCSS vanligen saknar ett dynamiskt förhållningssätt i avseendet att hantera teknologiska hot relaterade till cybersfären. Trots att forskningen av Luiijf m.fl. (2013) är över tio år gammal, speglar resultatet som framkommit här att deras resultat fortfarande är relevant och att det finns mer att önska kring ett dynamiskt förhållningssätt till cybersäkerhetsriskerna. Resultatet motsäger dock det Luiijf m.fl. (2013) indikerar kring en svag adressering av sambandet mellan NCSS och andra nationella säkerhetsstrategier, internationella ramverk och direktiv för skydd av kritisk infrastruktur. Tvärtom visar resultatet en tydlig harmonisering och sammanlänkning mellan NCSS, andra nationella säkerhetsstrategier och internationella ramverk för skydd av kritisk infrastruktur, vilket är en viktig aspekt för att effektivt hantera cybersäkerhetshot enligt Luiijf m.fl. (2013). Av allt att döma av det som framkommit i resultatet tillsammans med diskussionen av det och de politiska reglagen som skett på internationell nivå avseende cybersäkerhetsområdet, föreligger höga förhoppningar på den nya NCSS.

Slutligen är det utifrån resultatet tydligt att samverkan mellan myndigheter och andra aktörer, är en grundläggande förutsättning för att effektivt hantera antagonistiska hot. Därutöver att informations- och cybersäkerhetsfrågor är ett gemensamt ansvar, där ingen ensam kan lösa säkerhetsutmaningarna: Informationssäkerhetens komplexitet, gränsöverskridande karaktär och utvecklingstakt kräver effektiv samverkan. Det

framkommer även att privata aktörer både äger och driver stora delar av den samhällsviktiga verksamheten, vilket gör en stark samverkan ytterligare viktigt för att uppnå ett adekvat skydd. Således återkommer samverkan inom och mellan privat och offentlig sektor som en betydelsefull faktor för att bemöta cybersäkerhetsriskerna, vilket kan ses korrelera med att exempelvis van Asselt & Renn (2011) menar att systemiska risker inte kan hanteras av enskilda aktörer eller delar av samhället. Istället krävs en bred samordnad strategi som involverar olika samhällsaktörer och sektorer.

7.2 Metoddiskussion

Det kvalitativa tillvägagångssättet ihop med en innehållsanalys av dokument har inneburit goda möjligheter att frambringa ett resultat utifrån uppsatsen syfte och frågeställningar. Användningen av dokument som dataunderlag anses ändamålsenligt för uppsatsen syfte såväl som frågeställningar, med förbehåll för att vissa nackdelar och utmaningar kommer med sådant tillvägagångssätt. Att undersöka frågor rörande cybersäkerhet och risker därinom har tydliga begränsningar, eftersom dessa frågor ofta hamnar inom ramen för sekretessbelagd information. Det är något som Craig m.fl. (2022) poängterar gällande studier i ämnet och analyser av NCSS (likt föreliggande uppsats): Mycket av den statliga verksamheten inom cybersäkerhetområdet är och kommer förbli hemlig, vilket utgör ett hinder för empiri och forskning på området. Vidare framförs att forskning på NCSS inte kan bedöma sådan hemlig information, men erbjuder likväl ett sätt att förstå hur stater och myndigheter betraktar och hanterar cybersäkerhetsområdet – åtminstone offentligt. Det går i linje med det Nationellt cybersäkerhetscenter (u.å.b) lyfter kring att deras offentliga rapporter (som är ett dataunderlag i uppsatsen) delvis är grundade på sekretessbelagd information.

Precis som Bryman (2018, s. 674) poängterar kring studier som använder dokument som data, reflekterar inte sådan empiri hela verkligheten, vilket det råder medvetenhet kring och något som behöver understrykas i sammanhanget. Strategidokument och rapporter kan å ena sidan betraktas som representationer av den verksamhetsverklighet där dokumenten ingår (Bryman, 2018, s. 674). Å andra sidan kan dokumenten inte anses spegla hela verkligheten. I detta fall inte hela verkligheten kring hur cybersäkerhetscentrat eller regeringen betraktar cyberriskerna, dokumenten i sammanhanget bör istället ses som ett fönster som genererar inblick i verksamheterna. I uppsatsens kontext innebär det att avsaknaden av perspektiv och aspekter som identifierats i dokumenten, presenterats i resultatet och som vidare diskuteras, möjligen är sådant som återfinns i andra delar av verksamheterna och som inte uttrycks i dokumenten av olika skäl. Emellertid kan frågan gällande huruvida dataunderlag speglar hela verkligheten av det som studeras, anses föreligga även i andra tillvägagångssätt och inom all typ av forskning. Det hade likväl varit såväl intressant som önskvärt att tillämpa ett tillvägagångssätt i uppsatsen som innefattade en triangulering, och då i form av att kombinera datainsamlingsmetoder och källor snarare än att kombinera kvalitativ och kvantitativa tillvägagångssätt (Bryman, 2018, s. 468, 764). Företrädesvis hade intervjuer med personer som besitter expertis och

som arbetar operativt med frågor rörande cybersäkerhetsrisker varit ett lämpligt sådant. Detta för att komplettera dataunderlaget och för att kunna söka ytterligare svar på hur cyberrisker betraktas och huruvida dess systemiska karaktär betänks inom policydomäner såväl som inom mer operativ verksamhet. Det hade möjligen kunnat ge en mer omfångsrik bild av ämnet, givet uppsatsens syfte och frågeställningar. Trots resonemang rörande dokument som källa och studier av cybersäkerhetsfrågor med dess dimension kring sekretess, anses datainsamlingsmetoden som använts vara den som lämpat sig bäst för uppsatsen – utifrån rådande förutsättningar och tidsramar men även givet dess syfte.

Det kvalitativa tillvägagångssättet har upplevts adekvat under uppsatsens gång. Syftet och frågeställningarna i uppsatsen anses svåra att bemöta genom ett kvantitativt tillvägagångssätt som vanligen tillämpar insamling av numeriska data, användning av statistik och med en strävan efter kvantifierbara resultat (Bryman, 2018, s. 198–199, 223). Istället har en kvalitativ metod tillåtit användningen av deskriptiva dataunderlag som ger förklaringar och detaljer av det ämne som studeras (Bryman, 2018, 479). Det har möjliggjort att möta studiens syfte och besvara dess frågeställning genom att undersöka dokument som kunde stödja förståelsen för hur cybersäkerhetsriskerna betraktas i en policykontext. Likaså har användningen en av kvalitativ innehållsanalys upplevts ändamålsenligt i sammanhanget för att på ett systematiskt sätt kunna analysera och beskriva det fenomen som undersökts i uppsatsen (Elo & Kyngäs, 2008). Vidare gjordes valet att tillämpa ett deduktivt tillvägagångssätt och således genomföra en riktad innehållsanalys. Detta grundat på att en riktad innehållsanalys ansågs passande utifrån uppsatsens tydliga teoretiska nedslag ihop med syftet, och eftersom ett riktat tillvägagångssätt möjliggjorde att testa teoretiska ståndpunkter i andra sammanhang än de vanligtvis appliceras (Kibiswa, 2019; Elo & Kyngäs 2007). Likaså medför en deduktiv ansats att teorin tillåts vara överordnad i förhållningssättet till materialet och därigenom låta teoretiska resonemang vägleda bearbetning av data (Bryman, 2018, s.49–50; Hsieh & Shannon, 2012). Det är ett angreppssätt som ansågs relevant under uppsatsens gång och såhär i efterhand, utifrån att det möjliggjorde att testa främst systemteoretiska perspektiv i en kontext kring cybersäkerhetsrisker – vilka som nämnt inte är lika framträdande i detta forskningsområde. Nämnas bör att andra tillvägagångssätt betänktes, främst en induktiv innehållsanalys. Valet av en riktad innehållsanalys över en konventionell grundar sig på dess förmåga att vara teoretiskt förankrad och möjliggöra en djupgående analys av specifika aspekter inom cybersäkerhetsriskerna. Det tillät en djupare undersökning av teoretiska koncept som är relevanta för att undersöka systemförståelsen av cyberrisker inom nationell myndighetspolitik, vilket en konventionell metod inte ansågs kunna erbjuda i samma utsträckning.

Även om den riktade innehållsanalysen och dess deduktiva ansats anses adekvat behöver dess tillkortakommanden belysas. Användningen av den deduktiva, riktade innehållsanalysen lämnar utrymme för frågor kring hur ett sådant tillvägagångssätt påverkat resultatet och analysen, således även slutsatserna i uppsatsen. Hsieh & Shannon (2012) belyser att det finns vissa inneboende element som kan ses som utmanande inom

användningen av en riktad innehållsanalys. Det har att göra med att den som använder metoden närmar sig sin data med en bias grundad i den teoretiska ramen som styr forskningen, vilket kan påverka hur data och resultat tolkas. Dessa förfaranden råder det medvetenhet kring, varför det i uppsatsen har strävats efter transparens. Vidare utmaning som upplevts i sammanhanget relaterar till att även om tillvägagångssätten inom en riktad innehållsanalys är tämligen strikta, lämnas utrymme för tolkning i kontexten. Detta uppmärksammades under kodningsprocessen av datan, då det upplevdes utmanande att förhålla sig strikt konsekvent i kodningen. Alltså att vara konsekvent i bedömningen om textpassager överensstämde eller inte med de olika operationella definitionerna i kodningsschemat, vilket var det som vägledde kodningsprocessen. Det genererar reflektionen att en testning av kodningschemat kunde utförts, för att underlätta den slutliga kodningsprocessen samt för att på förhand upptäcka att de operationella definitionerna i somliga fall var lika varandra och därav eventuellt kunnat sammanfogats i kodningschemat.

Frågan om tillförlitligheten i uppsatsen, dess reliabilitet, handlar om huruvida resultatet skulle bli detsamma om samma tillvägagångssätt genomfördes igen och således om den kan replikeras (Bryman, 2018. S. 72). Förmodligen skulle inte resultatet bli detsamma om tillvägagångssättet genomförs av en annan individ, även om transparens och beskrivning av tillvägagångssätt finns i uppsatsen. Detta då någon annans lins på såväl teorierna som materialet antagligen skulle generera annan tolkning av både teori och empiri, därav även ett annat resultat, analys och slutsatser. Således är det svårt att exakt och utförligt värdera tillförlitligheten i sammanhanget, vilket även Bryman (2018, s. 72, 465) lyfter som en existerande och problematisk aspekt i många kvalitativa studier. Möjligt att tänka är att en kvantitativ ansats hade kunnat ökat tillförlitligheten eftersom användning av numeriska data och statistiska resultat förmodligen genererat mindre subjektiv påverkan. Gällande validiteten som generellt avser huruvida studieresultat kan överföras till andra sammanhang, kan föreliggande uppsats likt många andra kvalitativa studier kritiseras för att inte ha generaliserbara resultat (Bryman, 2018, s. 465, 484). Emellertid har avsikten med uppsatsen inte varit att frambringa generaliserbara resultat, snarare generera djup till det ämne uppsatsen är förlagd i: Hur cybersäkerhetsrisker betraktas inom en nationell policykontext. Likväl torde specifikt extern validitet som avser hur väl studieresultat kan generaliseras till andra kontexter (Bryman, 2018, s. 465–466), vara något som kan knytas till föreliggande uppsats. Detta utifrån att Bryman (2018, s. 485) beskriver att resultat i kvalitativa studier kan ses överförbara i termer av att vara generaliserbara till teori, och inte till populationer. Istället är det den teoretiska förankringen och resonemanget som är avgörande för att bedöma huruvida resultaten kan generaliseras. Om de teoretiska slutsatserna som dras från den kvalitativa datan är motiverade samt stöds av tidigare forskning och teoretiska utgångspunkter, kan resultaten bedömas som generaliserbara. I fallet med föreliggande uppsats har tidigare forskning, teoretiska utgångspunkter och resultat genomgående reflekterat varandra, vilket påvisas främst i uppsatsens resultatdiskussion men även i tillämpad analysmetod. Enligt Bryman (2018, s. 485)

innebär det att resultaten kan anses ha överförbarhet alternativt relevans för andra sammanhang, även om de inte är mätbara och statistiskt representativa på det sätt som krävs för kvantitativa studier.

8 Slutsatser och framtida forskning

Avsikten med uppsatsen har varit att undersöka huruvida strategier och bedömningar för cybersäkerhet inom policysfären adresserar den komplexa karaktären av cyberrisker. Detta i termer av att identifiera om en systemförståelse för cyberriskerna existerar, inklusive riskernas potential att orsaka kaskadeffekter och därigenom urskilja om strategierna och bedömningarna speglar en helhetsförståelse av cyberriskerna. Med avstamp i systemteoretiska utgångspunkter tillsammans med tidigare forskning, har sju olika policydokument analyserats för att möta uppsatsens syfte. I följande avsnitt presenteras slutsatser utifrån uppsatsen syfte och frågeställningar, där varje stycke behandlar en frågeställning vardera med start från första frågeställningen och framåt. Avslutningsvis framförs förslag på framtida forskningsämnen som relaterar till det som uppkommit under uppsatsprocessen.

8.1 Slutsatser

Uppsatsens resultat tillsammans med tidigare forskning och teoretiska utgångspunkter har påvisat att det finns luckor i synsättet på relationen mellan cyberattacker och dess eventuella påverkan liv, hälsa och miljö. Inslag finns kring att cyberattacker kan påverka och skapa avbrott i samhällsviktig verksamhet och hur det kan leda till allvarliga konsekvenser för människors hälsa och liv. Trots det lyser djupare förståelse för denna relation och konkreta resonemang avseende effekterna på hälsa och liv till följd av cyberattacker med sin frånvaro. Likaså är det ett småskaligt perspektiv på cyberriskernas konsekvenser jämfört med andra dimensioner av riskbilden. Det kan uppfattas problematiskt med tanke på att cyberhoten blir alltmer framträdande, vilket framkommer tydligt i resultatet. Särskilt i ljuset av att hotet är framträdande i en kontext kring kritisk infrastruktur såväl som mot medicinsktekniska enheter inom sjukvården vilka även är implanterade i patienter. Tidigare attacker som lyfts såväl som tidigare forskning som pekar på att attacker har drabbat sjukhus och hur det genererat effekter på människors välmående och liv, är talande för att cybersäkerheten inte bara är en teknisk fråga utan en fråga som i samtiden även berör människors hälsa och liv i värsta fall. Därutöver är det desto tydligare att relationen mellan cyberattacker och dess eventuella påverkan på miljön och kringliggande områden, varken beskrivs direkt eller indirekt. Vare sig i regeringsdokumenten eller i de mer operativa från Nationellt cybersäkerhetscenter.

Strategierna och rapporterna som har granskats har ett förhållandevis stort fokus på cybersäkerhetsriskeras stationering inom samhällsviktig verksamhet och kritisk infrastruktur, där bedömningarna vittnar om att dessa centrala samhällssektorer är framstående mål för cyberattacker. Sårbarheterna som uppkommer till följd av ökade beroenden, teknologisk progression och digitalisering framhålls som betydande faktorer i sammanhanget eftersom samhällskritisk infrastruktur utöver att vara sårbar för attacker, dessutom i stor utsträckning är avhängd på digitalisering. Det öppnar även upp för attacker och åtkomst på distans. Olika delar av den samhällsviktiga infrastrukturen bär

även beroenden av varandra, vilket skapar sammanlänkade sårbarheter och i sin tur en ytterligare komplex riskbild. Kritisk infrastruktur framhålls som centralt för samhällets funktionalitet och tydligt som något skyddsvärt i sammanhanget. Emellertid speglas en diskrepans i fokus mellan olika sektorer, där elsektorn framhävs mer än andra kritiska sektorer såsom hälso- och sjukvårdssektorn. Detta trots att sjukvårdssektorn utgör betydande mål för cyberattacker och har en omfattande attackyta, vilket sammantaget är något som växer fram genom resultatet och tidigare forskning.

Framträdande är att dokumenten som granskats har en märkbar frånvaro av överväganden och bedömningar kring risken för kaskadeffekter till följd av cyberattacker, med undantag för övervägandet gällande potentiella kaskadeffekter kopplat till elsystemet och dess potentiella inverkan på samhället i stort. Den allmänna bristen på resonemang kring kaskadeffekter som process tillsammans med andra relaterade dynamiska beståndsdelar inom systemperspektivet, väcker frågor kring hur väl cyberriskerna förstås utifrån dess potential att resultera i omfattande konsekvenser. Speciellt utifrån cyberdomänens komplexa och sammankopplade karaktär samt i ljuset av att cyberdomänen och dess risker är cementerade i alla våra centrala samhällsfunktioner där kaskadeffekter vanligen kanaliseras. Sammanfattningsvis skildras en systemförståelse av cyberriskerna i policydokumenten, vilket framkommit genom resultatet och den teoretiska diskussionen. Vissa aspekter av den systemiska dynamiken verkar dock vara frånvarande, vilket hindrar att en fullständig förståelse för cyberrisker och deras potentiellt allvarliga konsekvenser kan anses vara fullt uppnådd. Men som tidigare lyft är policydokumenten förhoppningsvis inte talande för hela verkligheten kring att bedöma, hantera och styra dessa komplexa risker i vårt digitala landskap.

8.2 Framtida forskning

Det finns flera framtida forskningsområden som hade varit intressanta att utforska baserat på resultaten och slutsatser som framkommit här. Med tanke på cybersäkerhetriskernas potential i att påverka människor hälsa samt leda till förlust av liv, hade dessa aspekter av cybersäkerheten varit av värde att titta närmare på framöver. Ytterligare intressant område att beforska och som framträtt småskaligt, är det som tydligt fokuserar på dimensionen kring cyberattackers påverkan på miljön och livsmedelssäkerhetens sårbarhet för cyberrisker. Vidare uppslag skulle vara att använda liknande forskningsfrågor som i föreliggande uppsats, men att då använda en annan datainsamlingsmetod. Exempelvis genomföra en intervjustudie med aktörer och/eller experter som arbetar operativt med dessa cybersäkerhetsfrågor. Alternativt studera hur frågorna i sammanhanget betraktas i en kontext kring exempelvis risk- och sårbarhetsanalyser och kontinuitetshantering. Även om sådana ämnen kan ha sekretessbelagda dimensioner, är det värt att utforska för att få en mer holistisk bild av hur cyberrisker betraktas i policydomäner.

Ett annat uppslag som hade varit intressant utifrån att samverkan framkommer som en viktig faktor för att hantera cybersäkerhetsrisker, är att studera samverkan mellan privata och offentliga aktörer. Detta för att se hur det influerar cybersäkerhetsriskerna relaterat till blandat aktörskap i ägandet och drivandet av kritisk infrastruktur, och i ljuset av att kritisk infrastruktur framkommit som en stark kanal för cyberrelaterade risker. Därutöver hade det varit intressant att studera den nya nationella strategin för samhällets informations- och cybersäkerhet när den publiceras.

9 Referensförteckning

Atkins, S., & Lawson, C. (2021). An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure. *Public Administration Review*, *81*(5), 847-861. https://doi-org.ezproxy.ub.gu.se/10.1111/puar.13322

Assarroudi, A., Heshmati Nabavi, F., Armat, M. R., Ebadi, A. & Vaismoradi, M. (2018). Directed qualitative content analysis: the description and elaboration of its underpinning methods and data analysis process. Journal of Research in Nursing, 23(1), 42–55. https://doi-org.ezproxy.ub.gu.se/10.1177/1744987117741667

Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of Cyber Policy*, *3*(2), 258-283. https://doi-org.ezproxy.ub.gu.se/10.1080/23738871.2018.1520271

Backman, S. (2023). Normal cyber accidents. *Journal of Cyber Policy*, *8*(1), 114–130. https://doi-org.ezproxy.ub.gu.se/10.1177/0018726709339117

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *Geneva Papers on Risk and Insurance. Issues and Practice*, *40*(1), 131-158.

Bernard, R., Bowsher, G., & Sullivan, R. (2020). Cyber security and the unexplored threat to global health: a call for global norms. *Global Security (Abingdon, England)*, *5*(1), 134-141. https://doi.org/10.1080/23779497.2020.1865182

Boréus, K. & Bergström, G. (2018). Textens mening och makt: metodbok i samhällsvetenskaplig text- och diskursanalys (4 uppl.). Studentlitteratur.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative research journal*, *9*(2), 27-40. https://doi.org/10.3316/QRJ0902027

Bryman, A. (2018). *Samhällsvetenskapliga metoder* (3 uppl.). Liber.

Burk, R. A., & Kallberg, J. (2016). Cyber Defense as a part of Hazard Mitigation: Comparing High Hazard Potential Dam Safety Programs in the United States and Sweden. *Journal of Homeland Security and Emergency Management*, *13*(1), 77-94. https://doi.org/10.1515/jhsem-2015-0047

Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2023). Rushing for security: a document analysis on the sources and effects of time pressure on organizational cybersecurity. *Information and Computer Security*, *31*(4), 504-526. https://doi.org/10.1108/ICS-01-2021-0013

Craig, A. J. S., Johnson, R. A. I., & Gallop, M. (2022). Building cybersecurity capacity: a framework of analysis for national cybersecurity strategies. *Journal of Cyber Policy*, *7*(3), 375-398 https://doi-org.ezproxy.ub.gu.se/10.1080/23738871.2023.2178318

Dinicu, A., Oancea, R., & Bârsan, G. (2021). The Multidimensional Impact on Society of Cyber Attacks Targeting the Energy Critical Infrastructure Sector. *Land Forces Academy Review*, *26*(4), 406–417.

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Cutter, S. L. (2018). Compound, Cascading, or Complex Disasters: What's in a Name? *Environment : Science and Policy for Sustainable Development*, *60*(6), 16–25

Eddy, M. & Perlroth, N. (2020, 18 september). *Cyber Attack Suspected in German Woman's Death.* The New York Times. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

Eason, K. (2014). Afterword: The past, present and future of sociotechnical systems theory. *Applied Ergonomics*, *45*(2), 213–220. https://doi.org/10.1016/j.apergo.2013.09.017

Elo, S. & Kyngäs, H. (2008). The qualitative content analysis process. Jo*urnal of Advanced Nursing 62(1),* 107–115

European Union Agency For Network and Information Security. (2017). *ENISA overview of cybersecurity and related terminology.* https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

Forsberg, C., & Wengström, Y. (2016). *Att göra systematiska litteraturstudier: värdering, analys och presentation av omvårdnadsforskning* (4. rev. utg.). Natur Kultur Akademisk.

Försvarsdepartementet. (2020). Regeringsbeslut Fö2019/01330: *Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter.* https://www.regeringen.se/globalassets/regeringen/dokument/forsvarsdepartementet/regeringsbeslut/uppdrag-om-fordjupad-samverkan-inom-cybersakerhetsomradet-genom-ett-nationellt-cybersakerhetscenter.pdf

Górka Marek. (2018). The Cybersecurity Strategy of the Visegrad Group Countries. *Politics in Central Europe*, *14*(2), 75–98. https://doi.org/10.2478/pce-2018-0010

Hsieh, H.-F., & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research*, *15*(9), 1277–1288. https://doi-org.ezproxy.ub.gu.se/10.1177/1049732305276687

International Telecommunication Union. (u.å.). *Definition of cybersecurity*. Hämtad 24-02-21, från https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

International risk governance center. (2018). *IRGC GUIDELINES FOR THE GOVERNANCE OF SYSTEMIC RISKS: In systems and organisations In the context of transitions.* https://irgc.org/risk-governance/systemic-risks/guidelines-governance-systemic-risks-context-transitions/

Johansson, J. & Hassel, H (2016). Beroendes betydelse i det sammankopplade samhället. I S. Baez Ullberg & P. Becker (Red.) *Katastrofriskreducering - perspektiv, praktik, potential.* (1 uppl., ss. 293-315). Studentlitteratur.

Kaufman, G. G., & Scott, K. E. (2003). What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It? *The Independent Review (Oakland, Calif.)*, *7*(3), 371–391. https://www.jstor.org/stable/24562449

Kibiswa, N. K., PhD. (2019). Directed Qualitative Content Analysis (DQlCA): A Tool for Conflict Analysis. *The Qualitative Report*.

Klein, L. (2014). What do we actually mean by 'sociotechnical'? On values, boundaries and the problems of language. *Applied Ergonomics*, *45*(2), 137–142. https://doi.org/10.1016/j.apergo.2013.03.027

Kumar, V. S., Prasad, J., & Samikannu, R. (2018). A critical review of cyber security and cyber terrorism – threats to critical infrastructure in the energy sector. *International Journal of Critical Infrastructures*, *14*(2), 101-119.

Larsson, P., Dekker, S. W. A., & Tingvall, C. (2010). The need for a systems theory approach to road safety. *Safety Science*, *48*(9), 1167–1174. https://doi.org/10.1016/j.ssci.2009.10.006

Leveson, N., Dulac, N., Marais, K., & Carroll, J. (2009). Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems. *Organization Studies*, *30*(2–3), 227–249. https://doi-org.ezproxy.ub.gu.se/10.1177/0170840608101478

Le Coze, J.-C. (2018). An essay: Societal safety and the global1, 2, 3. *Safety Science*, *110*, 23–30 https://doi.org/10.1016/j.ssci.2017.09.008

Lindsten, P-O. (2024, 4 april). Nästa mål för cyberattacker: Sveriges bönder. *Dagens Industri.* https://www.di.se/nyheter/nasta-mal-for-cyberattacker-sveriges-bonder/

McEvoy, T. R., & Kowalski, S. J. (2019). Deriving Cyber Security Risks from Human and Organizational Factors – A Socio-technical Approach. *Complex Systems Informatics and Modeling Quarterly*, (18), 47–64.

Morgan, H. (2022). Conducting a Qualitative Document Analysis. *Qualitative Report*, *27*(1), 64–77.

Myndigheten för samhällsskydd och beredskap (2024, 9 februari). *Nationellt center för cybersäkerhet.* https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/samhallets-arbete-for-okad-cybersakerhet/nationellt-center-for-cybersakerhet-ncsc/

Myndigheten för samhällsskydd och beredskap. (2024, 9 februari). *Cyberhot.* https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/risker-och-sarbarheter-inom-cybersakerhet-och-cyberfysiska-system/hot-och-metoder-inom-cybersakerhet/cyberhot/

Mittermaier, E., Granholm, N. & Veibäck, E. (2020). *Perspektiv på pandemin: Inledande analys och diskussion av beredskapsfrågor i ljuset av coronakrisen 2020.* Totalförsvarets forskningsinstitut (FOI). rådet. https://www.foi.se/rest-api/report/FOI-R--4992--SE

Nationellt cybersäkerhetscenter. (u.å.a). *Vårt uppdrag.* Hämtad 24-02-22, från: https://www.ncsc.se/om-centret/vart-uppdrag

Nationellt cybersäkerhetscenter. (u.å.b). *2020 Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden.* https://www.msb.se/contentassets/fe72c449466e4017bd76787762ab9dc5/rapport-cybersakerhet-i-sverige-2020--hot-metoder-brister-och-beroenden.pdf

Nationellt cybersäkerhetscenter. (u.å.c). *2021 Cybersäkerhet i Sverige – i skuggan av en pandemi.* https://www.msb.se/siteassets/block/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cybercenter/cybersakerhet-i-sverige--i-skuggan-av-en-pandemi-2021.pdf

Nationellt cybersäkerhetscenter. (u.å.d). *Cybersäkerhet i Sverige 2022. Del 1: Hot, metoder, brister och beroenden.* https://www.ncsc.se/siteassets/publikationer/ncsc-rappor-1-cybersakerhet-i-sverige-2022-hot-metoder-brister-och-beroenden.pdf

Nationellt cybersäkerhetscenter. (u.å.e) .*Cybersäkerhet i Sverige 2022 Del 2: Rekommenderade säkerhetsåtgärder.* https://www.ncsc.se/siteassets/publikationer/ncsc-rapport-2-cybersakerhet-i-sverige-2022-rekommenderade-sakerhetsatgarder.pdf

Olsen, O. E., Kruke, B. I., & Hovden, J. (2007). Societal Safety: Concept, Borders and Dilemmas. *Journal of Contingencies and Crisis Management*, *15*(2), 69–79. https://doi-org.ezproxy.ub.gu.se/10.1111/j.1468-5973.2007.00509.x

Panda, A., & Bower, A. (2020). Cyber security and the disaster resilience framework. *International Journal of Disaster Resilience in the Built Environment*, *11*(4), 507–518. https://doi-org.bibproxy.kau.se/10.1016/j.ssmqr.2022.100166

Perrow, C. (1984) Normal accidents: *Living with high-risk technologies.* Basic Books.

Perrow, C. (2011). Fukushima and the inevitability of accidents. *Bulletin of the Atomic Scientists, 67*(6), 44-52. https://doi.org/10.1177/0096340211426395

Regeringskansliet. (u.å.). *Skrivelse*. Hämtad 24-05-03, från: https://www.regeringen.se/rattsliga-dokument/skrivelse/

Regeringens skrivelse 2016/17:213. *Nationell strategi för samhällets informations-och cybersäkerhet.* https://www.regeringen.se/rattsliga-dokument/skrivelse/2017/06/skr.-201617213

Regeringens skrivelse 2023/24:56. *Nationell strategi mot våldsbejakande extremism och terrorism – förebygga, förhindra, skydda och hantera.* https://www.regeringen.se/rattsliga-dokument/skrivelse/2024/01/skr.-20232456

Regeringskansliet (2023, 3 november). Nationell strategi för samhällets informations- och cybersäkerhet.

https://www.regeringen.se/regeringens-politik/krisberedskap/nationell-strategi-for-samhallets-informations--och-cybersakerhet

Renn, O., Klinke, A., & van Asselt, M. (2011). Coping with Complexity, Uncertainty and Ambiguity in Risk Governance: A Synthesis. *Ambio*, *40*(2), 231–246.

Renn, O., Lucas, K., Haas, A., & Jaeger, C. (2019). Things are different today: the challenge of global systemic risks. *Journal of Risk Research*, *22*(4), 401–415. https://doi.org/10.1080/13669877.2017.1409252

Renn, O. (2021). New challenges for risk analysis: Systemic risks. *Journal of Risk Research, 24*(1), 127-133. https://doi-org.ezproxy.ub.gu.se/10.1080/13669877.2020.1779787

Renn, O., Laubichler, M., Lucas, K., Kröger, W., Schanze, J., Scholz, R. W., & Schweizer, P. (2022). Systemic Risks from Different Perspectives. *Risk Analysis: An International Journal*, *42*(9), 1902–1920. https://doi-org.ezproxy.ub.gu.se/10.1111/risa.13657

Riksrevisionen. (2023, 13 april). *Regeringens styrning av samhällets informations- och cybersäkerhet − både brådskande och viktig (RiR 2023:8).* https://www.riksrevisionen.se/download/18.4aeb2da8187b22973fb2828/1682339418438/RiR_2023_8_rapport.pdf

Schweizer, P., & Renn, O. (2019). Governance of systemic risks for disaster prevention and mitigation. *Disaster Prevention and Management*, *28*(6), 862-874. DOI: 10.1108/DPM-09-2019-0282

Schweizer, P.-J. (2021). Systemic risks - concepts and challenges for risk governance. *Journal of Risk Research*, *24*(1), 78–93. https://doi.org/10.1080/13669877.2019.1687574

Scholz, R. W. (2017). Digital threat and Vulnerability management: The SVIDT method. *Sustainability (Basel, Switzerland)*, *9*(4), 554. https://doi.org/10.3390/su9040554

Shaked, H., Schechter, C., & Fullan, M. (2017). Definitions and Development of Systems Thinking. *In Systems Thinking for School Leaders* (pp. 9–22). Switzerland: Springer International Publishing AG.

Sheard, L. (2022). Telling a story or reporting the facts? Interpretation and description in the qualitative analysis of applied health research data: A documentary analysis of peer review reports. *SSM - Qualitative Research in Health*, *2*. https://doi-org.bibproxy.kau.se/10.1016/j.ssmqr.2022.100166

Shrivastava, S., Sonpar, K., & Pazzaglia, F. (2009). Normal Accident Theory versus High Reliability Theory: A resolution and call for an open systems view of accidents. *Human Relations (New York)*, *62*(9), 1357–1390. https://doi-org.ezproxy.ub.gu.se/10.1177/0018726709339117

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*, 105143. https://doi.org/10.1016/j.ssci.2020.105143

Sonnsjö, H. & Mobjörk, M. (2013). Om indirekta, komplexa och oönskade händelser: Att analysera risker med stor osäkerhet. Totalförsvarets forskningsinstitut. https://www.foi.se/rest-api/report/FOI-R--3649--SE

Sparf, J. (2009). Risk ur ett systemteoretiskt perspektiv. I A. Olofsson & S. Öhman (Red.), *Risker i det moderna samhället: Samhällsvetenskapliga perspektiv. Omvårdnadens grunder: Hälsa och ohälsa* (1 uppl., ss. 103–118). Studentlitteratur.

Statsrådsberedningen. (2017). *Nationell säkerhetsstrategi.* https://www.socialdemokraterna.se/download/18.6a46455216c3d0f447e7134/1568881617947/nationell-sakerhetsstrategi.pdf

Säkerhetspolisen. (2022, 1 juli). *Cybersäkerhet.* https://sakerhetspolisen.se/verksamheten/cybersakerhet.html

Tarhan, K. (2022). Historical Development of Cybersecurity Studies: A Literature Review and Its Place in Security Studies; *Strategic Review, (15),* 393-414.

Van Asselt, M. & Renn, O. (2011). Risk governance. *Journal of Risk Research, 14*(4), 431-449. https://doi.org/10.1080/13669877.2011.553730

Vetenskapsrådet. (2017). *God forskningssed.* https://www.vr.se/analys/rapporter/vara-rapporter/2017-08-29-god-forskningssed.html

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Welburn, J. W., & Strong, A. M. (2022). Systemic Cyber Risk and Aggregate Impacts. *Risk Analysis*, *42*(8), 1606–1622. https://doi-org.ezproxy.ub.gu.se/10.1111/risa.13715

Zajko, M. (2015). Canada's cyber security and the changing threat landscape. *Critical Studies on Security*, *3*(2), 147–161. https://doi.org/10.1080/21624887.2015.1071165

Appendix 1. Kodningsschema

Teori/Tidigare forskning	**Kodningskategori**	**Subkategori/Subkod**	**Operationell definition**	***Koder i texten***
1. Systemiska risker	1.1 Komplexitet och dynamik i cyberrelaterade risker	1.1.1 Osäkra/komplexa/tvetydliga 1.1.2 Beroendeförhållanden 1.1.3 Teknologisk progression/hastig utveckling/digitalisering 1.1.4 Gräns/systemöverskidade 1.1.5 Föränderliga i tid/rum	Textavsnitt som beskriver/relaterar till den övergripande beskrivningen/ karaktären och den dynamiska karaktären hos cyberrisker. Inklusive diskussioner om osäkerheten och komplexiteten hos dessa (systemiska) risker samt beroendeförhållanden i system/cyberrisker.	1.1.1–5
2. Systemteoretiska perspektiv	2.1 Emergens	2.1.1 Interaktion mellan systemkomponenter	Textavsnitt som belyser emergens och hur fristående delar inom ett system börjar påverka varandra och skapar oväntade händelser. Exempel: hur olyckor eller risker uppstår när systemets komponenter interagerar med varandra på sätt som inte var förutsägbara utifrån deras individuella egenskaper.	2.1-1
	2.2 Systemberoende /sammanlänkning av risker	2.2.1 Systemberoende inom cybersäkerhet	Textavsnitt som diskuterar hur system inom cybersäkerhet är beroende av alla sina enheter och hur en enskild enhets utsatthet för en cyberrisk kan få konsekvenser för hela systemet. Inklusive analyser av hur sårbarheter eller attacker mot en del av cybersäkerhetssystemet kan spridas och påverka andra delar av systemet.	2.2.1
	2.3 Socio-tekniska aspekter av cybersäkerhet	2.3.1 Interaktion mellan teknik och människor	Textavsnitt som diskuterar hur teknik och människor ömsesidigt påverkar varandra inom socio-tekniska system (cybersäkerhet/cyberrisker). Exempel:	2.3.1

Teori/Tidigare forskning	**Kodningskategori**	**Subkategori/Subkod**	**Operationell definition**	***Koder i texten***
			Hur teknologins funktion påverkas av mänskligt beteende och vice versa, samt hur detta påverkar cybersäkerhet.	
		2.3.2 Komplexitet och dynamik i socio-tekniska system	Textavsnitt som belyser graden av både social och teknisk komplexitet i socio-tekniska system (cyberrisker). Inklusive diskussioner om hur systemets (cybersäkerhet/risker) interna miljö påverkas av externa faktorer: Ex politiska/juridiska förändringar, och hur det infulerar/bidra till sårbarhet för cyberrisker/hantering av cyberrisker:	2.3.2
3. Riskstyrning och tidigare forskning från Luiijf m.fl. (2013).	3.1 Dynamisk riskstyrning för hantering av (systemiska) cyberrisker	3.1.1 Adaptivitet/kontinuerligt lärande	Textavsnitt som diskuterar behovet av adaptiva /dynamiska strategier för cyberrisker. Inklusive av hur riskstyrning bör vara dynamisk och kunna anpassa sig till föränderliga hotlandskap och nya insikter om risker inom cyberrymden. Diskussioner av att integrera lärande och anpassning/hanteringen för att effektivt hantera den snabba utvecklingen av cybersäkerhetshot. Avsnitt som beskriver och erkänner och dynamiken i cybersäkerhetshoten och som belyser att strategierna måste vara levande dokument som kan behöva revidering.	3.1.1
		3.1.2 Holistiskt tillvägagångssätt och helhetsperspektiv	Textavsnitt som belyser vikten av ett holistiskt tillvägagångssätt och ett helhetsperspektiv i riskstyrningen för att hantera *systemiska* cyberrisker, innefattade helhetsperspektiv och	3.1.2

Teori/Tidigare forskning	**Kodningskategori**	**Subkategori/Subkod**	**Operationell definition**	***Koder i texten***
			breda dimensioner av riskerna. Inklusive diskussioner om behovet att identifiera/bedöma/hantera riskerna utifrån deras komplexa/sammanlänkade natur.	
4. Tidigare forskning från Luiijf m.fl. (2013).	4.1 Harmonisering	4.1.1 Sammanlänkning med andra nationella säkerhetsstrategier och (internationella) ramverk	Textavsnitt som diskuterar sambandet mellan NCSS andra nationella säkerhetsstrategier och strategier för skydd av kritisk infrastruktur samt andra internationella ramverk kring detsamma.	4.1.1
5. Normal Accident Thoery (NAT)	5.1 Högrisk-teknologier och systemolyckor	5.1.1 Interaktiv komplexitet och tät sammankoppling	Textavsnitt som speglar komplex interaktivitet och tät sammankoppling mellan systemkomponenter inom cybersäkerhetssystem, och hur dessa relaterar till förekomsten systemolyckor. Inklusive hur systems delar är starkt beroende av varandra.	5.1.1
		5.1.2 Kedjereaktioner av störningar	Textpassager som fokuserar på hur små incidenter/störningar inom cybersäkerhetssystem kan utlösa kedjereaktioner av störningar och hur dessa kan eskalera till systemolyckor inom cybersfären.	5.1.2
		5.1.3 Oväntade händelser och latenta beroendeförhållanden	Textpassager som diskuterar osäkerheter och oväntade effekter av cyberattacker. Inklusive hur incidenter/störningar i ett system kan sprida sig och interagera med andra delar av systemet på sätt som inte är förutsebara.	5.1.3

Teori/Tidigare forskning	**Kodningskategori**	**Subkategori/Subkod**	**Operationell definition**	***Koder i texten***
6. Tidigare forsking; Bernard m.fl (2020); Rulleau (2023); Palleti m.fl (2021 Panda & Bower (2020)	6.1 (Spridnings)effekter av cyberattacker och cybersäkerhetsrisker	6.1.1 Effekter/konsekvenser på kritisk infrastruktur/samhällsviktig verksamhet	Textpassager som diskuterar cyberattacker och cyberriskers påverkan/konsekvenser för samhällsviktig verksamhet och kritisk infrastruktur. Inklusive vikten av att skydda kritisk infrastruktur, samt dess roll i samhällets funktion och graden av digitalisering inom kritisk infrastruktur och dess sårbarhet för cyberattacker.	6.1.1
		6.1.2 Effekter/konsekvenser på liv/hälsa/miljö	Textpassager som diskuterar cyberattackers/cybersäkerhetsriskers eventuella påverkan på människors liv och/eller hälsa. Inklusive passages som diskuterar attackers påverkan/effekter/konsekvenser på miljön eller samhället.	6.1.2
7.Tidigare forskning: Pescaroli & Alexander (2015); Alexander (2018); Cutter (2018); Rulleau (2023); Panda & Bower (2020)	7.1 Kaskadeffekter	7.1.1 Potentiella kaskadeffekter av cyberattacker inom KI/SVV	Textpassager som diskuterar cybersäkerhetsriskernas relation till eventuella kaskadeffekter, specifikt inom kritisk infrastruktur och samhällsviktig varsamhet.	7.1.1
8. Systemiska risker och tidigare forskning från Albahar (2017)	8.1 Okonventionella gränser	8.1.1 Distans i cyberrisker	Textpassager som diskuterar cyberriskers/attackers karaktär av att inte besitta konventionella gränser/vara transnationella i sin natur. Inklusive att hot och attacker kan utföras från geografiskt avlägsna platser utan fysisk närvaro.	8.1.1

I tabellen: Teoretiskt perspektiv/tidigare forskning som använts/relaterar till kodningskategorin (1:a kolumnen), kodningskategorier och deras kod (2:a kolumnen), under/subkategorier och deras kod (3:e kolumnen), vad varje huvudkod/subkod innebär och hur de kan identifieras i texten (definition) och kriterier för att identifiera ett textavsnitt (4:e kolumnen). Den sista kolumnen visar den numeriska koden som tilldelas en textpassage för att visa vilken kategori/subkategori den tillhör.