Nordiska cybersäkerhetsstrategier

En jämförande studie av de nordiska ländernas nationella cybersäkerhetsstrategier

Avhandling pro gradu
Fakulteten för samhällsvetenskaper och ekonomi
Offentlig förvaltning
Åbo Akademi

Christian Jämsén, 1801005
Handledare: Nina Tynkkynen
Våren 2021

ÅBO AKADEMI – FAKULTETEN FÖR SAMHÄLLSVETENSKAPER OCH EKONOMI

Ämne: Offentlig förvaltning
Författare: Christian Jämsén
Arbetets titel: Nordiska cybersäkerhetsstrategier - en jämförande studie av de nordiska ländernas nationella cybersäkerhetsstrategier
Handledare: Nina Tynkkynen
Under det senaste decenniet har allt mer uppmärksamhet fästs vid nationell informations- och cybersäkerhet. Såväl inom EU som globalt har en stor mängd stater under de senaste tio åren antagit olika lagar och strategier för att bättre kunna svara på de nya hot som en allt mer teknik- och nätbaserad omvärld utsätter det moderna samhället för. Även de nordiska länderna har sedan över 10 år tillbaka utverkat sina första cybersäkerhetsstrategier och uppdaterat dem efter hand som behov uppstått. Syftet med studien är att analysera hur de fem nordiska ländernas cybersäkerhetsstrategier skiljer sig åt och hur skillnaderna formuleras och tar sig uttryck i tyngdpunkter och målsättningar. Vidare är syftet att granska hur strategierna anknyter till det valda teoretiska ramverket och hur väl strategierna tagit viktiga avväganden och frågeställningar i beaktande, som anses höra till välavvägda och välformulerade nationella cybersäkerhetsstrategier. Kontexten för studien är nordisk. Studiens design är jämförande och utnyttjar tematisk innehållsanalys för att jämföra de nordiska nationella cybersäkerhetsstrategierna med varandra. Källmaterialet utgörs av de fem nordiska ländernas offentligt tillgängliga och senaste nationella cybersäkerhetsstrategier. Redan en första snabb genomläsning av strategierna ger för handen att det förekommer skillnader mellan strategierna. De tydligaste skillnaderna handlar om utformning och de sätt som strategierna är skrivna på. De synligaste och mest övergripande skillnaderna i strategierna förekommer antagligen just på grund av de olika nationella utgångslägena och de olika läsargrupper man velat nå med publikationerna. Detta i sin tur kan antas ha påverkat betoningen av olika helheter i strategierna. Några få centrala frågor har inte alls berörts i tre av de totalt fem studerade strategierna. Trots skillnaderna, verkar de nordiska ländernas cybersäkerhetsstrategier vara mer lika än de är olika. I regel har alla strategierna tämligen väl, bortsett några få undantag, tagit ställning till de frågor som enligt de valda teoretiska ramverken bör tas i beaktande, för att uppnå en välavvägd och välformulerad nationell cybersäkerhetsstrategi.
Nyckelord: cyber, cybersäkerhet, informationssäkerhet, datasäkerhet, cybersäkerhetsstrategi, strategi, nationell säkerhet, nationell cybersäkerhet, tematisk innehållsanalys, jämförande design.

Datum: 2.5.2021	Sidoantal: 83

Innehållsförteckning

Tabellförteckning

Figurförteckning

1 Inledning

> Känslan av trygghet har också rubbats med nya digitala metoder. Vare sig det gäller riksdagen eller uppgifter om personers hälsa, ger ordet ”dataintrång” ett alltför harmlöst intryck. Cyberattackerna hotar säkerheten, de är attacker mot individer, attacker mot hela samhällsordningen. Vi måste kunna avvärja dem bättre, även internationellt.
>
> Republikens president Sauli Niinistö, nyåsrstal 2021(Niinistö 2021)

Under det senaste decenniet har allt mer uppmärksamhet fästs vid informations- och cybersäkerhet. Såväl inom EU som globalt har en stor mängd stater under de senaste tio åren antagit olika lagar och strategier för att bättre kunna svara på de nya hot som en allt mer teknik- och nätbaserad omvärld utsätter det moderna samhället för. För att effektivt kunna stå emot nätvärldens skadliga händelser måste samhället öka sin resiliens, definiera nya sätt att reagera och motverka de skadliga händelser, som den nya tekniken för med sig samt att hitta nya samarbetsformer såväl mellan myndigheter som med den privata sektorn. Nationella cybersäkerhetsstrategier har under de senaste 10 åren etablerat sig som sedvanliga styrredskap i försöket att svara på de nya utmaningarna en allt mer sammanlänkad nätinfrastruktur fört med sig. Trots att de nationella strategierna i regel lyfter fram liknande frågor, förekommer det fortfarande en betydande variation vad gäller nationella prioriteringar, betoningar och konceptualisering av utmaningarna (Cordey & Dewar 2019). Vidare verkar det förekomma en betydande skillnad mellan vad som förstås med de olika begreppen som är kopplade till ”cyber” i största allmänhet och ”cybersäkerhet” i synnerhet.

De fem nordiska länderna har länge gjort nära samarbete, har liknande samhällen, kultur och lagstiftning. Trots detta förekommer det även skillnader mellan de nordiska länderna. Island, Danmark och Norge är Nato medlemmar medan Finland och Sverige inte är det. Danmark, Sverige och Finland är EU medlemmar medan Norge och Island inte är det. Norge och Island tillhör den Europeiska ekonomiska gemenskapen. Alla de nordiska länderna har publicerat nationella cybersäkerhetsstrategier. Strategierna ska ge riktning åt ländernas insatser inom området och erbjuda en samlad syn på hur de nordiska samhällena ska möta de utmaningar den nya sammankopplade tekniken fört med sig.

En snabb genomläsning av strategierna ger för handen det i dessa förekommer en hel del likheter men även olikheter. En del av olikheterna beror direkt på strategiernas struktur och

utformning samt vilka målgrupper vart och ett land velat tilltala. Andra olikheter beror antagligen på den nationella betoning länderna velat ge de enskilda frågorna. Mot denna bakgrund är det intressant att närmare se på vilka skillnaderna mellan de olika nordiska cybersäkerhetsstrategierna är och hur väl de tagit centrala frågor och avvägningar i beaktande.

1.1 Nationell säkerhet och nya utmaningar

I dagens högteknologiska värld är det få saker som inte är uppkopplade till Internet på ett eller annat sätt. Det gäller såväl hemelektronik som flygplan, fabriksanläggningar, elnät och vattenförsörjning. En del funktioner och service är mindre och en del mer avgörande för ett fungerande modernt samhälle. I närhistorien finns det redan gott om exempel på att det är möjligt att bryta sig in i och ta kontroll över diverse hemelektronik, flygplan och nationella elnät. Två allvarligare exempel är från år 2015 och 2016 då troligen ryska aktörer lyckades bryta sig in ukrainska elkraftverk och avbryta elproduktionen (Schneier 2013; The Wired 2016; BBC News 2017). Det senare fallet genomfördes med ett skadeprogram som kallas CrashOverride och som klassats som ett militärt cybervapen (Schneier 2013).

Den första cyberattacken som bevisligen men indirekt dödat en människa inträffade i september år 2020 då ett sjukhus i Düsseldorf utsattes för ett utpressningsskadeprogram som satte sjukhusets kritiska digitala resurser ur bruk. Dödsfallet anses vara en olycklig och icke planerad bieffekt av cyberangreppet, men visar på vår digitaliserade omgivnings svagheter på ett skrämmande sätt (Helsingin Sanomat 2021). År 2017 utsattes den globala logistikjätten A.P. Møller-Maersk för en omfattande cyberattack, närmare bestämt ett stort angrepp av skadeprogrammet NotPetya som förlamade så gott som hela det globala bolagets verksamhet och krävde omfattande rengörings- och återinstallationsåtgärder på företagets IT-infrastruktur. Attacken på Maersk tros vara ett misstag, där Møller-Maersk blivit ett olyckligt sidooffer, i en räcka cyberoperationer som kunnat spåras till konflikten mellan Ukraina och Ryssland (The Wired 2018). I december år 2020 uppdagades ett stort dataintrång riktat mot centrala myndigheter och ministerier i USA. Dataintrånget tros allmänt vara en underrättelseoperation utförd av Ryssland (Helsingin Sanomat 2020a). Iran har varit skådeplatsen för omfattande cyberoperationer. Den mest kända är antagligen fallet från 2010 då skadeprogrammet Stuxnet lyckades förstöra den iranska urananrikningsanläggningen Natanz anrikningscentrifugar.

Operationen antas allmänt ha varit utförd av Israel och USA som en operation avsedd att förhindra och försvåra Irans väg till att bli en atomvapenmakt (Blakemore 2012a; Haaretz 2019). Även i Finland har en rad allvarliga cyberangrepp skett. Under år 2020 uppdagades ett dataintrång i Psykoterapiföretaget Vastaamos patientdatabas som följdes av en rad utpressningsförsök av såväl företaget som patienterna, vars data läkt (Helsingin Sanomat 2020b). I slutet av 2020 uppdagades ett dataintrång i den finska riksdagens e-post omgivning, som misstänks vara spioneri (Yle 2021).

Angrep över nätet kan även vara politiskt kopplade och används som verktyg vid sidan av t.ex. politisk aktivism eller traditionell krigföring (DeNardis 2014). Presidentvalen i USA år 2016 var till exempel mål för många sorters cyberoperationer (BBC News 2016; Reuters 2018). Den finska skyddspolisen lyfte i sin årsredovisning från år 2020 fram att tyngdpunkten på underrättelseverksamhet och spioneri klart har övergått till digitala omgivningar (SUPO 2020). Vidare lyfter den finska polisen i sin verksamhetsberättelse från år 2020 fram att cyberbrottsligheten i sina olika former markant har ökat under granskningsperioden (POHA 2021). I sin hotbildsutvärdering från oktober 2020 lyfte det federala regeringsdepartementet Departement for Homeland Security (DHS) fram statligt kopplade cyberhot, cyberkriminalitet och cyberbetonade påverkningsförsök för att undergräva den amerikanska demokratin som verkliga och möjliga hotbilder (Department for Homeland Security 2020).

Från ett säkerhetsperspektiv ger cybermiljön möjligheter till nya asymmetriska påverkningsmöjligheter och hot i en allt högre grad (Limnéll, Majewski & Salminen 2014). Med en proportionellt sett liten insats är det möjligt att göra stor skada. Med asymmetriska påverkningsmöjligheter och hot menas att en aktör använder sig av okonventionella medel för att uppnå sitt mål. Strategin går ut på att åstadkomma största möjliga hoteffekt med minsta möjliga insats (Försvarshögskolan 2020; Wedin). Asymmetriska strategier används ofta av aktörer som resursmässigt är underlägsna sin motståndare. Som exempel kan nämnas terroristiska gärningar statsstyrda hybridoperationer eller klart styrda och målinriktade försök till informationspåverkan (Harris 2014). Stater är allt mer oroade över att terroristgrupper utvecklar en förmåga att attackera kritisk infrastruktur i cybermiljön och på så sätt skapa allmän oro (Awan 2012). Cybermiljön har även öppnat dörrarna för hybridstrategier där asymmetriska påverkningsmöjligheter och hot används vid sidan av konventionella d.v.s.

symmetriska militära strategier. USA till exempel har redan länge integrerat sin traditionella militära operativa verksamhet med nyare cybermetoder. De nya metoderna användes för första gången fullskaligt i kriget mot Irak år 2003 till år 2011. Till den nya militära strategin hörde bland annat att genomföra olika sorters cyberattacker som t.ex. dataintrång och aktiv digital underrättelseverksamhet, för att stöda den militära verksamheten i området (Harris 2014).

Ju mer informationsresurser finns uppkopplade till nätet desto lättare, billigare och således lönsammare blir det för stater och kriminella att utveckla färdigheter för att genomföra olika sorters skadliga cyberoperationer. I det moderna samhället är nationell och ekonomisk säkerhet samt yttrandefrihet mycket långt beroende av hur säker cybermiljön i sin helhet är. En stats förmåga att säkra cybermiljön är en förutsättning för dess förmåga att idka global handel, att sköta grundläggande statliga uppgifter, även militär verksamhet inkluderat (DeNardis 2014).

1.2 Syfte och frågeställning

Syftet med studien är att analysera hur de fem nordiska ländernas cybersäkerhetsstrategier skiljer sig åt och hur skillnaderna formuleras och tar sig uttryck i tyngdpunkter, målsättningar och samarbetsformer samt hur dessa anknyter till det valda teoretiska ramverket. Ramverket baserar sig på de ”tre perspektiven”, ”fem mandaten” och ”fem dilemmana” presenterade i *National cyber security framework manual* (Klimburg 2012) och kan anses vara triviala för en välavvägd nationell cybersäkerhetsstrategi (se nedan kapitel 3).

En första genomläsning av strategierna ger redan för handen att förekommer skillnader mellan strategierna. De första och tydligaste skillnaderna handlar om utformning och sätt som de olika strategierna är skrivna på. Redan denna observation ger för handen att de olika strategierna betonar olika saker. Trots det första intrycket om skillnader, är hypotesen i denna studie att de nordiska ländernas cybersäkerhetsstrategier är mer lika än de är olika. På grund av sitt kulturella förflutna, sitt beroende av omvärlden och geografiska läge har de fem nordiska länderna mer gemensamt än saker som skiljer dem åt. Från denna utgångspunkt torde skillnaderna i strategierna sist och slutligen vara tämligen små och främst bero på de enskilda ländernas egna lägen och utvecklingsnivå i frågan om cybersäkerhet.

De centrala frågorna som studien försöker svara på är följande:

1. Hurdana skillnader förekommer det i hur de olika strategierna betonar det statliga, nationella och internationella perspektiven (de tre perspektiven)?
2. Hurdana skillnader förekommer det i hur de olika strategierna betonar de fem huvudsakliga mandaten (militära cyberfrågor, cyberbrottsbekämpning, underrättelseverksamhet, skyddande av kritisk infrastruktur och nationell krisberedskap, cyberdiplomati och förvaltning av Internet) och de tre tvärgående mandaten (skydd och utbyte av information, koordinering och forskning)?
3. Hurdana skillnader förekommer det i hur de olika strategierna betonar cybersäkerhetens fem dilemman (åsiktsfrihet mot politisk stabilitet, ekonomisk stimulans mot mot högre säkerhet, dataskydd mot utbyte av information, modernisering av infrastruktur mot skydd av kritisk infrastruktur, privat sektor mot den offentliga sektorn)?
4. Hur väl tar de nordiska strategierna ställning till de centrala element (perspektiven, mandaten och dilemmanen) som enligt Hatahway & Klimburg, Luiijf & Healey och Klimburg & Healey (Klimburg 2012) utgör kärnan till välformulerade och välavvägda cybersäkerhetsstrategier?

Studien granskar och jämför de fem nordiska ländernas senaste cybersäkerhetsstrategier. Strategierna har utgivits mellan åren 2015-2019 och således begränsas studien till de nämnda åren. Studien tar inte heller i beaktande olika nationella kompletterande strategier eller styrdokument som t.ex. Norges internationella cybersäkerhetsstrategi (ICSS_NO 2017) eller Sveriges handlingsplan för cybersäkerhet för åren 2019-2022 (MSB 2019).

1.3 Tidigare forskning

Det förekommer en begränsad mängd forskning, studier och texter kring cybersäkerhet i allmänhet och cybersäkerhetsstrategier i synnerhet, om hur den utformats och uppfattats i nationell kontext genom tid. I detta kapitel lyfts endast de för denna studie centralaste studierna och deras betoningar gällande cybersäkerhet och cybersäkerhetsstrategier fram.

I *Strategier för informasjonssikkerhet - En komparativ studie av strategiarbeidet i Norge, USA, Australia og EU* ges en översikt i hur cybersäkerhetsstrategier utformats i de undersökta områdena och hur de påverkat säkerhetsarbetet. Studien är en av de första komparativa studier gällande nationella informationssäkerhetsstrategier. Studien slutsats var att de olika nationella strategier betonar olika saker, nivåer och problem. I USA har säkerhetsutmaningarna setts som federala medan de i Norge mer setts som sektorsmässiga. Den sektorsmässiga fragmenterade ansvarssplittringen ser studien som något problematiskt i en helhet där samverkan och koordinering är viktigt (Gulichsen, Hoff, Sørli, Hagen & Nystuen 2003). Johnsen (2015) har granskat hur den norska cybersäkerhetsstrategin jämför sig med övriga EU-länders strategier och USA. Studien hävdar att det trots den norska strategins omfattning, finns områden som kräver uppmärksamhet. Strategin borde bättre positionera sig till övriga nationella strategier och de hotbilder som lyfts fram i dem. Vidare borde begreppsdefinitioner ses över för att bättre sammanjämka den norska strategin med övriga strategier och på detta sätt lägga grunden för ett djupare internationellt samarbete. Studien låter förstå att sammanjämkande av de mentala modellerna som strategierna vill kommunicera, bygger grunden för en gemensam förståelse som i sin tur är grunden för ett djupare internationellt samarbete. Studien argumenterar även för en omdefinition av begreppet cybersäkerhet för att bättre ta i beaktande fysiska säkerhetsaspekter och hot (Johnsen 2015).

I studien *Nineteen National Cyber Security Strategies* jämförs 19 länders nationella cybersäkerhetsstrategier med varandra. Studien pekar såväl på gemensamma nämnare som svagheter i strategierna. Syftet med studien har varit att hjälpa länderna att utforma bättre och mer välformulerade cybersäkerhetsstrategier. Studien hittade i jämförelsen fyra olika utgångspunkter för utvecklandet av strategier. De tre huvudsakliga utgångspunkterna var 1) ekonomi 2) nationell säkerhet och 3) militärt försvar. Vidare pekar studien på samma begreppsliga svagheter i strategierna som Gulichsen m.fl. gjort tidigare. Studien hävdar i likhet med den tidigare norska studien att begreppsliga olikheter i strategierna hänger samman med vad som förstås med cybersäkerhet och således även det internationella samarbetet kring temat. Begreppsförvirring kan leda till missförstånd såväl internationellt som nationellt (Luiijf, Besseling & Graaf 2013).

I studien *Protection of critical infrastructure in national cyber security strategies* granskas hur skydd av kritisk infrastruktur behandlats i cybersäkerhetsstrategierna. Studien har i sin helhet granskat 86 olika strategier med målet att hitta likheter för att kunna uppnå globalt konsensus vad beträffar förståelse och skydd av kritisk infrastruktur i cybersäkerhetskontexten. Studien stöder sig till stora delar på Luiijf, Besseling och De Graafs (2013) tidigare artikel, men påpekar samtidigt att de tidigare studierna inte lyckats komma fram med egentliga och användbara komparativa redskap för att studera nationella cybersäkerhetsstrategier. För studien utvecklades en egen komparationsmetodik (Izycki & Colli 2019).

I artikeln *Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy* har 54 staters cybersäkerhetsstrategier kartlagts i en litteraturöversikt. Syftet med studien har varit att bättre förstå utvecklandet av nämnda strategier som ett politiskt fenomen. Studien har genom deskriptiv kodning sökt svar på motiv bakom utvecklandet av nationella cybersäkerhetsstrategier. Studien lyckade hitta tre huvudmotiv: 1) nationell säkerhet, 2) lagstiftningsmässiga behov och 3) politiska motiv. Enligt studien är cybersäkerhetsmotiv faktorer som leder till formulerandet av en nationell cybersäkerhetsvision och innehåller förutbestämda förhållanden, antaganden och bakgrunder som i slutändan leder till unika formuleringar i cybersäkerhetsstrategierna (Azmi, Tibben & Win 2016).

Studien *Cyber Security Strategies - An Overview* är en överblicksartikel som jämför ett antal olika cybersäkerhetsstrategier med varandra. Enligt studien är en nationell cybersäkerhetsstrategi ett verktyg för att uppnå ett gemensamt definierat nationellt mål. Strategin ska inte alltså betraktas som ett självändamål i sig. Utvecklandet av en nationell cybersäkerhetsstrategi är en utmanande uppgift som kräver betydlig koordinering mellan olika samhälleliga aktörer. Studien hävdar att trots strategierna olikheter, har de visat sig vara effektiva redskap för stater att hantera cyberrelaterade risker och hot (Martin 2015).

The Evolution of German Cybersecurity Strategy granskar processen bakom Tysklands cybersäkerhetsstrategis utformning genom två och ett halvt decennium. Enligt studien har den tyska cybersäkerhetsstrategin utvecklats från en preventiv civil strategi till en omfattande

helhet som inkluderar strategiska militära aspekter. Studien lyfter fram att trots den omfattande utvecklingen, saknar den tyska strategin fortfarande klara strategiska principer och prioriteringar (Schallbruch & Skierka 2018).

I *National Cyberdefense Policy Snapshots* granskas hur nationella cybersäkerhetspolicyer korsar cyberförsvarspolicyer genom att jämföra åtta olika länder med varandra. Meningen med publikationen är att erbjuda en större förståelse för hur cybersäkerhetspolicyer hänger samman med nationella säkerhetspolicyer. Publikationen lyfter fram problematiken kring cybermiljöns begreppsdefinitioner och de därtill hörande utmaningarna som även tangeras i denna uppsats. Studien hävdar att det trots likheterna mellan cybersäkerhetens och cyberförsvarets olika nationella strategier förekommer grundläggande skillnader och prioriteringar mellan de olika områdena (Cordey & Dewar 2019).

I *Cybersecurity in the EU: Threats, frameworks and future perspectives* granskas cybersäkerhetsfältet ur ett EU-perspektiv. Studien lyfter fram utmaningar med gemensamma begreppsdefinitioner inom EU-kontexten och granskar de cyberrelaterade hot som format EU:s cybersäkerhetsstrategi. Studien granskar även de utmaningar EU:s medlemsstater står inför, då det gäller att formulera gemensam cybersäkerhetspolicyer på unionsnivå och relatera dessa till EU:s bredare globala kontext. Största utmaningarna inom EU utgörs av medlemsländernas väldigt olika ingångsnivåer vad beträffar teknisk utveckling och cybersäkerhet samt en bred oenighet kring EU:s vidare säkerhets- och försvarsambitioner. Studien konstaterar även att Nato:s operativa och strategiska överlägsenhet i frågor som som berör säkerhet och försvar, är utmaningar som även avspeglas på EU nivå (Giantas & Liaropoulos 2019). Nato:s Cooperative Cyber Defence Centre of Excellence (CCDCOE) har i publikationen *National cyber security framework manual* lyft fram olika teoretiska ramverk som hjälper till att förstå den nationella cybersäkerhetens olika nivåer och utmaningar inom den offentliga policyformuleringens kontext. De olika delstudierna i publikationen tar upp områden och frågor som måste tas i beaktande då nationella cybersäkerhetsstrategier utformas. Manualen fungerar som en handbok och målar upp den nationella cybersäkerhetens ramar för de nationer som funderar på att utforma eller revidera sina nationella cybersäkerhetsstrategier (Klimburg 2012).

1.4 Källor

De fem nordiska ländernas färskaste cybersäkerhetsstrategier utgör källmaterialet för denna studie. I detta kapitel kommer de nordiska ländernas cybersäkerhetsstrategier och deras utveckling i korthet att presenteras.

Utvecklingen inom de fem länderna har skett i lite olika takt, vilket betyder att en del länder redan hunnit förnya sina strategier en eller flera gånger. Alla ländernas strategier förutom den isländska strategien finns tillgängliga som fullständiga tryck på engelska och på respektive nationalspråk. Islands strategi finns som helhet publicerad endast på isländska. En sammanfattad version finns att tillgå på engelska.

Redan en ytlig granskning av strategierna ger för handen att det förekommer skillnader mellan dem såväl i betoningar som övrig utformning. I denna studie har de nordiska ländernas engelskspråkiga versioner studerats och jämförts med varandra.

1.4.1 Finland

Finlands första cybersäkerhetsstrategi godkändes år 2013 och ersattes med en ny uppdaterad strategi år 2019. Enligt 2013 års strategi är statsmaktens centrala uppgifter att sörja för säkerheten i samhället. Vidare måste de samhällskritiska funktionerna kunna garanteras i alla situationer. Strategin lyfter fram att Finland i egenskap av ett informationssamhälle är beroende av att datanäten och datasystemen fungerar. Finland är mycket sårbart för störningar som riktas mot denna grundläggande infrastruktur. I strategin fastslås centrala verksamhetsmål, med vilkas hjälp nya cybersäkerhetsutmaningar kan bemötas. Strategin hänvisar till Finland säkerhetsstrategi från år 2012 och de principer som där fastställts för tryggandet av kritiska funktioner i Finland. De kritiska funktionerna är den statliga ledningen, internationell verksamhet, den nationella försvarsförmågan och den inre säkerheten, centrala funktioner för ekonomi, central nationell infrastruktur, befolkningens utkomstskydd och handlingsförmåga samt mental kristålighet. I strategin skildras en vision, en handlingsmodell och strategiska riktlinjer för cybersäkerheten. Strategin åtföljs av ett åtgärdsprogram som innehåller de praktiska åtgärder som förvaltningsområdena och aktörerna har beredningsansvar ansvarar för (NCSS FI 2013). Cybersäkerhetsstrategin från år 2013 lade

grunden för den nya strategin år 2019. Den förnyade strategin stöder sig på de allmänna principer som styrde 2013 års strategi. Strategin förnyades på grund av det förändrade läget såväl i den internationella som den nationella omgivningen. Enligt den nya strategin är Finlands målsättning fortfarande att vara ett av de främsta länder inom området för cybersäkerhet. Den förnyade cybersäkerhetsstrategin stöder sig även på den år 2017 förnyade säkerhetsstrategin. I cybersäkerhetsstrategin har även EU:s cybersäkerhetsstrategi tagits i beaktande. Den nya strategin står som grund för ett nytt nationellt utvecklingsprogram inom området för cybersäkerhet. (NCSS FI 2019)

1.4.2 Sverige

Sverige godkände sin första formella nationella strategi för samhällets informations- och cybersäkerhet är 2017. Den nationella strategin för samhällets informations- och cybersäkerhet är ett uttryck för den svenska regeringens övergripande prioriteringar och syftar till att utgöra en plattform för Sveriges fortsatta utvecklingsarbete inom området. Huvudsyftena med strategin är att bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet samt att höja medvetenheten och kunskapen i hela samhället. Enligt strategin ska de strategiska lösningarna utvecklas genom internationell samverkan och dialog kring förebyggande åtgärder, både inom EU och i andra internationella organ. Strategin ser ett strukturerat och riskbaserat arbete med informations- och cybersäkerhet som en viktig förutsättning för vidare digitalisering av samhället, svensk tillväxt och konkurrenskraft, och en nödvändighet för att näringslivet ska kunna utveckla och tillhandahålla konkurrenskraftiga varor och tjänster.

Huvudsyftet med strategin är att bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet samt att höja medvetenheten och kunskapen i hela samhället. Strategin omfattar därmed hela samhället, det vill säga statliga myndigheter, kommuner och landsting, företag, organisationer och privatpersoner. Strategin för samhällets informations- och cybersäkerhet har sin utgångspunkt i målen för Sveriges säkerhet: att värna befolkningens liv och hälsa, samhällets funktionalitet, samt förmågan att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter. Den svenska informations- och cybersäkerhetsstrategin anknyter till såväl

till regeringens säkerhets- och digitaliseringsstrategier. Den nationella säkerhetsstrategin anger att Sverige aktivt ska värna nationella intressen och försvara dem närhelst de riskerar att undermineras, inklusive mot de hot och risker som finns på det informationsteknologiska området. Digitaliseringsstrategin anger att förutsättningarna i Sverige ska vara de bästa för alla att på ett säkert sätt ta del av, ta ansvar för samt ha tillit till det digitala samhället. (NCSS SE 2016)

1.4.3 Norge

Den år 2018 publicerade norska cybersäkerhetsstrategin är den fjärde i rad. Norges första nationella strategi för digital säkerhet publicerades redan år 2003. Norge var således ett av de första länderna i världen som utarbetat en nationell strategi inom området. I takt med att hotbilderna förändrats och verksamhetsomgivningen utvecklats, har strategin tidigare reviderats år 2007 och år 2012. Den nyaste strategin syfte är möta de utmaningar som följs av en snabb och konsekvent digitalisering av det norska samhället. Vidareutvecklingen av tidigare nationella strategierna baseras på behovet av ett stärkt samarbete mellan offentlig och privat, civilt och militärt samt internationellt. Enligt strategin måste det vara säkert att använda digitala tjänster. Privatpersoner och företag måste ha förtroende för den nationella säkerheten, individuell välfärd och att demokratiska rättigheter skyddas i ett digitaliserat samhälle. Strategins främsta målgrupp är såväl myndigheter som företag inom den offentliga och den privata sektorn, inklusive de norska kommunerna. Strategin ska också sörja för att individer erbjuds nödvändig kunskap och riskförståelse för att kunna använda modern teknik på ett säkert sätt. Ansvaret för nationell digital säkerhet är fördelat på ett antal olika statliga myndigheter. Myndigheterna kan inte själva lösa alla utmaningar cybermiljön för med sig. Kritiska samhällsfunktioner och övriga nationella entiteter är beroende av digitala infrastrukturer som ständigt ökar i omfattning och komplexitet. Långa och komplexa digitala värdekedjor, som spänner sig över flera sektorer och nationella gränser, är en verklig utmaning vid bedömning av digital sårbarhet. De digitala säkerhetsutmaningarna måste lösas genom särskild tonvikt på samarbete och partnerskap mellan relevanta aktörer såväl nationellt som internationellt. Utmaningarna måste lösas tillsammans och över invanda sektorsgränser, så att alla intressenters säkerhetsbehov beaktas (NCSS NO 2017). Norge har även en skild

internationell cybersäkerhetsstrategi, som lägger speciell vikt på den internationella aspekten (ICSS_NO 2017). Den internationella strategins viktigaste punkter finns upptagna i den norska cybersäkerhetsstrategin från år 2017.

1.4.4 Danmark

Danmark presenterade sin första cybersäkerhetsstrategi år 2014. Med strategin tog den danska regeringen ett viktigt steg mot att stärka det allmänna förtroende till att Danmark är ett säkert land som även tryggar den digitala omgivningen (Centre for Cybersecurity, DK 2015). Målet med den första strategin var i allmänhet att skapa en grundnivå för nationell cybersäkerhet och i synnerhet att öka medvetenheten kring cybersäkerheten i samhället. Den senaste strategin utgavs år 2018. Strategin lyfter fram att förtroende för säkerheten av digitala lösningar är avgörande för en fortsatt digital utveckling av det danska samhället. De digitala lösningarna som välfärden och samhället bygger på måste vara skyddade mot utomstående cyberhot. I och med den nya strategin ämnade den danska regeringen öka ambitionsnivån på insatserna inom området för cybersäkerhet. I strategin understryks det att hotet från skadliga cyberattacker inte helt kan elimineras, men att den danska regeringen genom den nya strategin försöker trygga att det danska samhället även i fortsättning kan dra nytta av de tekniska och ekonomiska möjligheter som cybermiljön erbjuder. Strategin identifierar en rad olika samhällskritiska funktioner och konsekvenser sammanhängande med allvarliga cyberhot. Inom alla samhällskritiska sektorer som energi, transport, telekommunikation, ekonomi, hälsa och sjöfart måste ansträngningarna ökas för att en godtagbar cybersäkerhetsnivå kan uppnås i Danmark. Ökad resiliensen i samhället ses som en komplex men viktig utmaning. Enligt den danska strategin är en störningsfri drift av kritisk digital infrastruktur en förutsättning för att det moderna samhället ska kunna fungera. Otillräckliga säkerhetsåtgärder och procedurer i den digitala infrastrukturen kan innebära betydande konsekvenser för samhället. Moderna cyberhot påverkar alla delar av samhället. Konsekvenserna kan variera men i de allvarligaste fallen kan statlig säkerhet eller samhällets funktionsförmåga vara allvarligt hotat. I extrema fall kan förluster av människoliv komma på fråga. Ett lyft av den nationella cybersäkerheten är allas ansvar. Den danska strategin lyfter fram tre markörer i strategin som ska visa vägen

för de kommande fyra åren (2018-2021): 1) en trygg vardag för individer och företag 2) Ökad kompetens 3) Klarare ansvar och riskbaserat säkerhetsarbete. (NCSS DK 2017)

1.4.5 Island

Det isländska inrikesministeriet utsåg år 2013 en arbetsgrupp vars uppgift var att utveckla en nationell strategi för cybersäkerhet. Den isländska cybersäkerhetsstrategin publicerades år 2015. Enligt strategin ska Island ha en Internetkultur som är sund, främjar mänskliga rättigheter, skyddar individer samt respekterar ekonomiskt frihet, välstånd och utveckling. Cybersäkerhet bör vara en av de viktigaste hörnstenarna i isländskt ekonomiskt välstånd. Den isländska cybersäkerheten ska enligt strategin vila på en grund av sofistikerad medvetenhet om säkerhetsfrågor och relevant lagstiftning. Samtidigt måste Island ha förutsättningar att ta itu med cyberbrottslighet, svara på cyberhot och vidta åtgärder för att förhindra spionage och missbruk av personlig och kommersiell information. De viktigaste målen i strategin är att Island nationellt ska kunna motstå cyberhot, ha ökad resiliens, ha uppdaterad och relevant lagstiftning och kunna bekämpa cyberbrottslighet. Vidare är målsättningen att öka samarbetet inom sfären för cybersäkerhet såväl nationellt som internationellt. Den isländska cybersäkerhetsstrategin har kopplats samman med den nationella isländska säkerhetsstrategin. (NCSS IS 2015).

2 Cybersäkerhet, strategier och förvaltning av cybermiljön

2.1 Om ”cyber” och ”cybersäkerhet”

Den omgivning som sammankopplar världen via ett digitalt nätverk har i modern kontext kommit att kallas för ”cybermiljön” eller ”cyberomgivningen”, på engelska ”cyberspace”. Cybermiljön är fortfarande en relativt ny, komplex, mångdimensionell och outforskad arena och försöken att konceptualisera termer som ”cybermiljö” och ”cybersäkerhet” pågår fortfarande (Giantas & Liaropoulos 2019).

Termen ”cyber” har använts i ett antal olika kontexter sedan mitten på 1800-talet, men har sitt ursprung i forngrekiskan. Från och med 1940-talet blev termen ”Cybernetik” allmänt känd genom Norbert Wiener. Wiener använde begreppet ”cybernetik” för att beteckna vetenskapen om kontroll och kommunikation mellan det biologiska (djur) och det icke-biologiska (maskiner) (Lehto 2015; Azmi & Kautsarina 2019). Under 1990-talet vann termen ”cyberrymd” fotfäste i den akademiska kontexten (Azmi & Kautsarina 2019).

Gemensamt för alla moderna definitioner är att de på ett eller annat sätt kopplar ihop den digitala världen med den fysiska värld vi lever i. ”Cyber” i modern kontext syftar starkt på den abstrakta och alternativa digitala verkligheten som uppstått och möjliggjorts av Internet och datorer sammanlänkade med varandra samt med den fysiska verklighet människan lever i (Blakemore 2012a; IGF 2018; Azmi & Kautsarina 2019). ”Rymd” i detta sammanhang kan definieras som en virtuell miljö där mänsklig aktivitet möts. Cyberrymden kan i sin enkelhet beskrivas som Internet i sin helhet medräknat all global media och alla digitala kommunikationskanaler. Internet är cyberrymdens ryggrad via vilken mänsklig verksamhet sammanlänkas med datasystem ägda av enskilda individer, företag, övriga organisationer och stater (Blakemore 2012a).

Trots att prefixet ”cyber” i dagens läge används rätt allmänt, förekommer det skillnader i vad som förstås med begreppet ”cyber” i allmänhet och ”cybersäkerhet” i synnerhet (Azmi & Kautsarina 2019). Användningen av ordet ”cyber” har sakta vunnit mark under de senaste

decennierna inom ramen för det som kanske mer traditionellt kallats för informations- eller datasäkerhet. Informationssäkerhet har traditionellt syftat till konfidentialitet, riktighet och tillgänglighet då det gäller data och informationsteknik (Azmi & Kautsarina 2019). I dagens kontext verkar den traditionella definitionen av informationssäkerhet alltför snäv för att beskriva den sammanlänkade digitala helheten av möjligheter och hot som det moderna samhället befinner sig i just nu.

Många stater definierar vad just de menar med begreppet ”cyber” in sina nationella cybersäkerhetsstrategier (Lehto 2015). Fastän många aktörer, däribland enskilda EU-medlemsstater, har definierat och konceptualiserat cyber-relaterade termer utifrån sina egna utgångspunkter, förekommer det inte någon enhetlig definition, gemensam delad förståelse eller vision på EU-nivå (Giantas & Liaropoulos 2019).

I den finska ordlistan över cybersäkerhet definieras cybermiljön som en verksamhetsmiljö sammansatt av en eller flera digitala datasystem (Sanastokeskus TSK ry 2018). Cybermiljön (cyberspace) består av tre helheter 1) entiteter 2) interaktion 3) tillgångar. Entiteterna objekt (maskiner, individer, organisationer, stater) som är sammanlänkade med varandra genom cybermiljön. Eftersom entiteterna är sammanlänkade till varandra sker det även interaktion mellan dem. Tillgångar är något värdefullt oberoende om de är virtuella (digitala) eller befinner sig på gränsen mellan den virtuella och det fysiska (Azmi & Kautsarina 2019). Cybermiljön har definierats som bestående av digitala informations- och kommunikationssystem och otaliga nätverk sammankopplade med varandra och bildande en enhetlig infrastruktur. Cybermiljön består enligt definitionen av informations- och kommunikationsteknik, information och människan (Jansson & Sihvonen).

Till skillnad från land, hav och luft är cybermiljön ett av människan konstruerat utrymme med komponenter som ändrar över tid. Klimburg och Mirtl (2012) konceptualiserar cybermiljön som en miljö med fyra självständiga och distinkta lager av aktivitet. *Det fysiska lagret* inkluderar all hårdvara som t.ex. datorer, satelliter, sensorer, lagringsmedia och övrig teknisk utrustning. *Det logiska lagret* består av kod inkluderande programvara och protokoll som hör till programvaran. *Det innehållsmässiga lagret* består av alla information som skapats, fångats upp, lagrats och provocerats inom cybermiljön. Information i detta sammanhang kan förstås

som kunskap om objekt som fakta, händelser, saker, processer och idéer. Det innehållsmässiga lagret innehåller information som lätt kan läsas och förstås av människan. *Det sociala lagret* består av alla människor som använder och formar cybermiljön. Det sociala lagret inkluderar såväl stater, organisationer som enskilda individer (Klimburg & Mirtl 2012).

Eftersom dagens sammanlänkade digitala teknik så starkt är sammankopplat med den fysiska värld vi lever och således även påverkar vår fysiska liv, är vi tvungna att fästa allt mer uppmärksamhet vid cybermiljöns säkerhet och de hot som cybermiljön för med sig. Händelser i cybermiljön kan han långt gående påföljder i den fysiska verklighet vi lever i. Cybersäkerheten har kommit att bli en allt viktigare del av våra liv (Limnéll, Majewski & Salminen 2014).

Den traditionella definitionen av cybersäkerhet har kritiserats för att inte i tillräcklig grad ta i beaktande termen ”säkerhet”, här synonymt med engelskan ”safety”. Speciell uppmärksamhet har fästs vida att cybersäkerheten även omfattar motarbetande av incidenter som skulle kunna leda till avsiktlig eller oavsiktlig död, skada, förstörelse av egendom eller miljö (Johnsen 2015).

I denna studie används begreppet cybermiljö synonymt med engelskans ”cyberspace”. Denna studie definierar begreppet ”cybermiljö” i likhet med Klimburg och Mirtl som en av människan konstruerad omgivning med komponenter som ändrar över tid bestående av ett fysiskt lager, ett logiskt lager, ett innehållsmässigt lager och ett socialt lager. Vidare förekommer det interaktion mellan entiteterna i dessa lager.

Med cybersäkerhet förstås i denna studie de åtgärder som samhället i sin helhet på olika nivåer, tar för att skydda sig från yttre hot som förekommer i cybermiljön och som starkt är sammankopplade med samhällets förmåga att motstå och uthärda dessa hot samt trygga en fortsatt existens och var och ens grundläggande behov.

2.2 Om strategibegreppet

Ordet strategi härstammar ursprungligen från grekiskans *stratos* (armé) och *-ag* (att leda) och har en militär sammankoppling (Ansoff 1984; Juuti & Luoma 2009). Inom traditionell militär teori är strategins uppgift att vinna kriget (Kamensky 2008). De tidigaste och mest kända

strategiska verken är Sun Tzus *Krigets konst* skriven ca. 400 f.Kr. (Tzu 1982) och Carl von Clausewitz *Om kriget,* utgiven under medlet av 1800-talet (Clausewitz von 1997). För von Clausewitz innebar strategin en lära där man genom att granska och iaktta egna och andras agerande kan vinna fördelar på stridsfältet (Näsi & Aunola 2001).

Den moderna strategiforskningen hänger långt ihop med organisationsteori och hur organisationer väljer och uppnår sina mål. Strategikonceptet med koppling till organisationsteorierna har traditionellt fokuserat på företag och den privata sektorn (Laamanen et al. 2005). Även om det moderna strategibegreppet genom sitt förflutna starkt är kopplat till den privata sektorn, används begreppet aktivt även inom den offentliga sektorn. Den största skillnaden mellan den privata och den offentliga sektorn hittas i avsaknaden av konkurrensperspektiv hos de offentliga aktörerna (Juuti & Luoma 2009). Den offentliga sektorns uppgift att skapa samhälleligt mervärde (Public Value) (Virtanen & Stenvall 2019). Detta mervärde kan delvis skapas genom strategier med formulerade målsättningar.

Strategin är ett verktyg med vars hjälp företaget kan anpassa sig till omgivningens förändringar samt forma och välja sin omgivning (Kamensky 2008). Strategin är därför en förlängning av en entitets uppdrag och bildar således en bro mellan organisationen och dess miljö (Bryson 2018). Strategin visar organisationens riktning i ett långt perspektiv och är receptet till organisationens framgång. Strategin erbjuder ett sätt för organisationen att utnyttja sina resurser i en verksamhetsomgivning som förändras (Ansoff 1984; Juuti & Luoma 2009; Bryson 2018). Strategin kan vidare ses som en källa till konkurrensfördelar och överlägsenhet samtidigt som den kan erbjuda ett sätt att fylla marknadens och intressenternas förväntningar (Juuti & Luoma 2009). Strategin kan hjälpa till att svara på frågorna hur organisationen kan välja rätt och ny riktning för verksamheten och hur den kan använda sig av de befintliga resurserna för att uppnå de önskade målen.

Strategin, speciellt inom den offentliga sektorn, kan definieras som ett arrangemang för entiteten att uppnå sitt uppdrag (d.v.s. göra det den finns till för), uppfylla förväntningarna, skapa offentligt mervärde (Bryson 2018) samt att svara på förändringar i omgivningen (Ansoff 1984). Strategins grundläggande uppgift är att bidra till medveten styrning av verksamheten istället för ett mållöst drivande (Vanhala, Laukkanen & Koskinen 2002). En

strategilös verksamhet kan innebära spontanitet, överraskningar och inkonsekvens (Juuti & Luoma 2009).

Strategiskt ledarskap är verksamhet som definierar konkreta målsättningar och riktning för verksamheten på ett långvarigt och målinriktat sätt. Strategin i sig självt är den formulerade planen och således en del av det strategiska ledarskapet (Santalainen 2008). Med offentligt strategiskt ledarskap menas verksamhet som ger riktning åt den offentliga verksamheten (Virtanen & Stenvall 2019).

Strategisk planering kan definieras som en deliberativ och disciplinerad ansträngning, en process, vars mål är att att producera fundamentala beslut och verksamhet som formar och vägleder vad en entitet är, vad den gör och varför den gör det. Strategisk planering inom den offentliga sektorn kan vara till fördel inom en rad olika perspektiv. Genom strategisk planering kan man bland annat öka effektiviteten hos offentliga organisationer eller bredare samhälleliga system. Strategisk planering kan hjälpa till att öka koordineringen av verksamhet och frågor över organisatoriska eller hävdvunna gränser, öka resiliensen, anpassa sig till förändringar i omgivningen eller att tackla breda samhälleliga frågor (Bryson 2010, 2018).

2.3 Om nationella cybersäkerhetsstrategier

Traditionellt har den privata sektorn haft en stort ansvar i att bekämpa olika hot i cybermiljön samtidigt som varje individ ytterst varit ansvarig för sig själv och sina egna handlingar (DeNardis 2014). Utformandet av cybersäkerhetspolicyer är sällan enbart en statsangelägenhet. I många länder har icke-statliga aktörer haft en betydande roll i utformandet av nationella cybersäkerhetsstrategier (Klimburg & Healey 2012). Stater har ofta tagit på sig ett speciellt ansvar i att säkra kritisk infrastruktur och erbjuda olika sorters lösningar för detta ändamål bl.a. genom att grunda cybersäkerhetsmyndigheter och erbjuda annan relevant service (DeNardis 2014).

Invanda distinktioner mellan 1) inhemskt och internationellt 2) mellan politikområden 3) mellan offentligt, privat och den tredje sektorn har suddats ut. Inom flera områden har nationell suveränitet överförts till multinationella bolag, internationella organisationer och allianser (Bryson 2018). Suddigheten av de traditionellt invanda gränserna innebär att ingen

organisation eller institution har full kontroll eller ett klart mandat att agera i cybermiljön. Den ökade oklarheten i jurisdiktion och mandat kräver att såväl det offentliga som tredje sektorn tänker, agerar och lär sig strategiska modeller (Bryson 2018).

Utformandet av nationella säkerhetsstrategier är ett relativt nytt fenomen. Största delen av säkerhetsstrategierna kan spåras tillbaka till slutet av 1990- och början av 2000-talen, men även äldre undantag förekommer (Lindström & Luiijf 2012). Många nationella säkerhetsstrategier har haft eller består fortfarande av element som helt eller delvis även behandlar cyberdimensionen. På grund av den snabba tekniska utvecklingen och de nya hot som cybermiljön fört med sig har allt fler stater utvecklat självständiga cybersäkerhetsstrategier för att bättre kunna svara på de nya hot som står inför dörren (Lindström & Luiijf 2012; Jansson & Sihvonen). Under de senaste tio åren har många stater börjat se cybermiljön som en strategisk dimension där statlig närvaro är nödvändig, inte minst för att trygga enskilda staters trovärdighet (Limnéll, Majewski & Salminen 2014).

De nationella cybersäkerhetsstrategierna kan ses som formulerade nationella åtgärdsplaner, som baserar sig på nationella visioner om att uppnå en mängd målsättningar, som i sin tur bidrar till en ökad skärhet i cybermiljön (Luiijf, Besseling & Graaf 2013). Enligt en annan syn borde en nationell cybersäkerhetsstrategi definiera målsättningar och medel, vem som ansvara för arbetet och kostnader samt eventuellt hur åtgärderna ska finansieras (Gulichsen et al. 2003). Cybersäkerhetsstrategier kan se som planer som beskriver nationernas centralaste målsättningar inom området. En nationell cybersäkerhetsstrategi är ett verktyg för att förbättra resiliensen av nationella informationsinfrastrukturer och digital service. Strategin är verktyg på hög nivå och antar ett uppifrån-ned (top-down) perspektiv på styrningen av den nationella cybersäkerheten. Den nationella strategin fastställer nationella målsättningar och prioriteringar (ENISA 2012).

Gemensamt med många cybersäkerhetsstrategier, oberoende definitionsskillnader, är att de ser cybersäkerhet som något fundamentalt för att skydda statliga hemligheter, möjliggöra nationellt försvar och att försvara kritisk infrastruktur som genomtränger det moderna samhället och den moderna ekonomin (Lehto 2015). Vidare innefattar likheterna bland annat betoningen av tväradministrativa åtgärder, förebyggande arbetet och resiliens mot hot,

internationellt samarbete, utveckling av lagstiftning samt forsknings- och utvecklingssamarbete (Limnéll, Majewski & Salminen 2014). De nationella cybersäkerhetsstrategierna är effektiva endast ifall de klart och tydligt definierar ramarna för styrning (governance) (Martin 2015).

En effektiv cybersäkerhetsstrategi försöker balansera accepterade normer i ett land med de möjligheter som Internet och cybermiljön erbjuder. Internet kan ses som en disruptiv teknik som omdefinierat många normer rörande militära frågor, allmän ordning och säkerhet, näringsliv och civilsamhället. Samhället måste balansera upp dessa hot med de möjligheter den digitala miljön erbjuder som t.ex. öppenhet och tillgänglighet av information, handel och nya tjänster. Medan en strikt säkerhetspolicy säkerställer stabilitet, kan det samtidigt minska de potentiella fördelarna tekniken för med sig (Limnéll, Majewski & Salminen 2014; Azmi, Tibben & Win 2016).

De nationella strategierna ser olika ut till såväl innehåll som utformning. Skillnaderna kan bero på historiska, kulturella, organisatoriska, politiska eller andra faktorer. Strategiernas utformning och struktur kan skilja sig åt beroende på vem man vill nå t.ex. en bred allmänhet, kritiska infrastrukturoperatörer eller politiker. En viktig faktor att beakta är att få allmänheten medveten om cybersäkerhet. En fallgrop i många strategier är att de inte är klart riktade och således inte klart preciserar vem de vill nå. De nöjer sig med att på ett allmänt plan konstatera att alla aktörer i samhället är ansvarig för sin egen säkerhet, utan vidare att gå in på detaljer om ansvar och mer detaljerade åtgärdsförslag (Lindström & Luiijf 2012).

2.4 Om förvaltning och ansvar i cybermiljön

I sin helhet är ansvaret och administrationen i cybermiljön starkt fragmenterad. Ett stort ansvar läggs på den enskilda individen, privata serviceleverantörer och de aktörer som upprätthåller nätverksinfrastruktur. Trotts detta har det globala samarbetet för att administrera, utveckla och koordinera de olika aspekterna av cybermiljön, åtminstone vad gäller de stora frågorna och gemensamma övergripande standarder, anförtrotts en rad olika internationella organisationer. Av historiska skäl och på grund av cybermiljöns natur finns det en stor mängd olika typers aktörer och organ som deltar i förvaltandet och utvecklandet av omgivningen. Samarbetet mellan det offentliga och privata är starkt. Aktörerna består av enskilda stater,

överstatliga organisationer fungerande under FN som t.ex. *International Telekommunication Union* (ITU) eller *Internet Governance Forum* (IGF) eller av oberoende organisationer som *Internet Corporation of Assigned Names and Numbers* (ICANN), *The World Wide Webb Consortium* (W3C), *The World Wide Webb foundation*.

Förvaltningen av cybermiljön kan grovt delas in i teknisk förvaltning och policyformulering (Klimburg & Mirtl 2012; DeNardis 2014). Förvaltningen av cybermiljön är inte ett monolitiskt system som styrs av en eller ett fåtal aktörer. Förvaltningen och den optativa verksamheten i anknytning därtill består av fler skikt breda helheter som till exempel utveckling av gemensamma standarder, cybersäkerhet och internationella konventioner och forum för samarbete. Den primära uppgiften för förvaltningen av Internet inkluderar planeringen och administrationen över den centrala teknologier som krävs för att Internet ska fungera. Den tekniska arkitekturen inkluderar lager på lager av system, kod, tekniska standarder och kritisk infrastruktur utan vilka den mänskliga användningen av Internet skulle vara omöjligt. Förvaltningen av Internet är splittrad och verkställs i stora drag genom tekniska arkitekturbeslut, privata företags policyer, internationella organisationer, internationella fördrag samt nationell lagstiftning och policyer (DeNardis 2014)

Tabell 1: Förvaltningsaktörer i cybermiljön
Källa: Luiijf och Healey 2012

Nivå	Aktörer
Statliga	Regeringar, statliga myndigheter, övriga offentliga aktörer, militär, kommunala organisationer
Nationella/samhälleliga	Operatörer och tjänsteproducenter av kritisk infrastruktur, IKT-tjänsteproducenter, industri och den privata sektorn, vetenskap och forskning, producenter och leverantörer av säkerhetsinfrastruktur, befolkningen
Internationella	Multinationella organ (t.ex. EU, G8, Världsbanken, Europol, Interpol, ITU), intresseorganisationer (t.ex. ICANN, IGF), standardiseringsorganisationer (ISO), centrala internationella infrastruktur och serviceleverantörer.

Fast förvaltningen av Internet inte direkt och explicit åligger stater, har många stater ändå tagit ansvar över en mängd förvaltningsmässiga uppgifter som till exempel åtgärder för att skydda minderåriga, att införa upphovsrättslagar och överlag reglera vad som är tillåtet och inte tillåtet i nätet (DeNardis 2014). De nya hot cybermiljön fört med sig har även lett till att en rad överstatliga överenskommelser har introducerats (Council of Europe 2001; Awan 2012).

Cybermiljön är en omgivning inom vilken stater opererar och kan påverka, men som de inte kan kontrollera (Ekstedt, Parkhouse & Clemente 2012). Definitionen av gränser och jurisdiktion i cybermiljön är föremål för ett flertal tolkningar. Då en del hävdar att cybermiljön borde fortsätta vara gränsfri hävdar andra att cybermiljön är en förlängning på nationell suveränitet (Azmi, Tibben & Win 2016). Det har debatterats om vems ansvar det är att kontrollera cybermiljön och organisera cybersäkerheten. En del förespråkar en fri cybermiljö där var och en utan restriktioner får skapa skapa och fritt publicera innehåll. Förespråkarna för en fri cybermiljö argumenterar emot att cybermiljön skulle ägas eller kontrolleras av privata företag eller stater, eftersom det skulle begränsa friheten. Andra synsätt lyfter fram att cybermiljön i sig, oberoende hur liberal synen än är, inte ens i sin friaste form kan anses vara en helt fri och oreglerad domän. Enligt detta synsätt regleras cybermiljön av program, system och koder. Den eller de som kan bidra och har tillgång till koderna är de som de facto har makten i cybermiljön. Koderna kan vara positiva och demokratiska eller negativa och bidra till att skapa totalitär kontroll (Blakemore 2012b).

Frågor rörande förvaltning och säkerhet av cybermiljön har vid ett flertal tillfällen lyfts fram. De centralaste debattinitiativen omfattas av det så kallade Montevideo uttalandet och Parisinitiativet. I Montevideo uttalandet efterlystes starkare insatser för att övervinna de utmaningar som förvaltningen av Internet står inför och förespråkade starkt utvecklandet av modeller där representerar för olika intressegrupper kan vara med och påverka och där förhållandet mellan stater och övriga aktörer är mer jämlikt (ICANN 2013). Parisinitiativet efterlyste en ram för regleringen av Internet och bekämpning av cyberattacker, hatretorik och övriga cyberhot. Enligt Parisinitiativet kan cybersäkerhetsnormer fungera som en mekanism mellan statliga och icke statliga aktörer att komma överens om vad som är ansvarsfullt

beteende, i en miljö där lagstiftningen alltid hänger efter den tekniska utvecklingen (IGF 2018).

3 Teori och metod

3.1 De tre teoretiska ramverken

Den teoretiska ramen för denna studie utgörs av en helhet bestående av tre olika ramverk gällande nationell cybersäkerhet, som formulerats i *National cyber security framework manual.* Dessa tre helheter försöker konceptualisera den komplexa helhet en cybersäkerhetsstrategi består av och är (Klimburg 2012). Att utarbeta en omfattande cybersäkerhetsstrategi kräver att olika frågor och ämnen med olika utgångspunkter som t.ex. ekonomi, politik, kultur och internationella relationer lyfts fram och balanseras mot moderna starkt cyberrelaterade frågor som idéer om öppenhet och fria informationsflöden. På grund av att cyberomgivningen omfattar ett stort antal väldigt olika centrala aktörer på ett antal olika nivåer, krävs också att cybersäkerhetsstrategierna har tillräckligt samhällelig representation (Azmi, Tibben & Win 2016). De tre teoretiska ramverken försöker erbjuda ett teoretisk perspektiv som hjälper till att formulera en nationell cybersäkerhetsstrategi och beakta svåra motsättningar. De tre ramverken kan direkt appliceras på olika nivåer av policyutveckling och lyfter fram centrala företeelser och frågor en nationell cybersäkerhetsstrategi borde ta ställning till på ett eller annat plan (Klimburg 2012). De teoretiska ramverken ska dock inte ses som absoluta kategoriseringar, som en bra och utförlig cybersäkerhetsstrategi måste innehålla för att uppnå sitt syfte. Snarare ska de teoretiska ramverken ses som frågor varje nation, som upprättar en cybersäkerhetsstrategi, måste ta ställning till. Från detta betraktelsesätt är det alltså inte fruktbart att räkna förekomsten av varje enskild kategori i strategierna. Snarare ger förekomsten, frekvensen eller avsaknaden av kategorin information ifrall en stat begrundat frågan och möjligen i vilken grad frågan betonats i den enskilda cybersäkerhetsstrategin. Det finns inget enskilt rätt sätt att bygga upp en nationell cybersäkerhetsstrategi på. Varje enskild stat tar ställning till de frågor och omständigheter som berör just dem, men de teoretiska ramverken kan hjälpa till med att förstå och definiera de

centralaste och komplexa helheter som är förknippade med nationell cybersäkerhet (Klimburg 2012).

Det första ramverket lyfter fram motsättningar mellan nationell säkerhet å ena sidan och friheter och rättigheter å andra sidan genom de så kallade ”fem dilemmana”. De ”tre perspektiven” kopplar ihop nationell cybersäkerhet med public policy-modeller och försöker förklara hur staten genom sin cybersäkerhetsstrategi ser på sin omgivning och de aktörer som är nära sammankopplade med ämnet. Slutligen erbjuder ”de fem mandaten” en ram genom vilken nationell säkerhet traditionellt har granskats.

3.1.1 Den nationella cybersäkerhetens fem dilemman

Nationell cybersäkerhet är inte ett självändamål i sig, utan snarare en balansgång mellan skydd mot risker å ena sidan och öppenhet och frihet å andra sidan. För att kunna balansera mellan risker och möjligheter måste de nationella cybersäkerhetssträvandena ta ställning till hur de hanterar de dilemman som uppstår mellan säkerhet å ena sidan och fri- och möjligheter å andra sidan. En ogynnsam balans kan ha såväl ekonomiska som social följdverkningar (Hathaway & Klimburg 2012).

Den nationella cybersäkerhetens fem dilemman är:

1. ekonomisk stimulans mot förhöjd nationell säkerhet,
2. modernisering av infrastruktur mot skydd av kritisk infrastruktur,
3. den privata sektorn mot den offentliga sektorn,
4. dataskydd mot utbyte av information,
5. yttrandefrihet mot politisk stabilitet.

Stater som funderar på att öka den nationell cybersäkerheten måste ta i beaktande den alternativa påverkan höjd säkerhet kan föra med sig i på ekonomiska möjligheter att utnyttja nätet och dess digitala möjligheter. En till toppen vriden säkerhet ger inte utrymme för ekonomisk frihet och innovationer i någon vidare bemärkelse och omvänt en digital miljö med utrymme för frihet och självförverkligande kommer ofta med låg säkerhet. Stater tampas hela tiden med problemet i att utnyttja de digitala möjligheter nätet för med sig samtidigt som

de tvingas ta ställning till skydd av immateriell egendom, dataskydd, skydd av kritisk infrastruktur och nationellt försvar. Många stater som USA eller Sverige och överstatliga organisationer som t.ex. EU har egna digitaliseringsstrategier som utlovar hög digital utveckling. Digitaliseringsstrategierna har ofta en del gemensamt som att de strävar till digitala innovationer, höghastighets fibernät, modernisering av kritisk infrastruktur, som möjliggör kommunikation genom nätet och ökade satsningar på forskning och produktutveckling som ska bidra till ekonomisk tillväxt. Samtidigt som moderniseringarna för med sig möjligheter, kan dessa möjligheterna komma på bekostnad av nationell säkerhet. Vid utvecklandet av nationella cybersäkerhetsstrategier gäller det att hitta en passlig balans mellan dessa två aspekter (Hathaway & Klimburg 2012).

Ett av de mer framstående motsatserna som starkt hänger samman med det ekonomisk tillväxt och nationell säkerhet är frågan om modernisering av infrastruktur mot ett starkare skydd av kritisk infrastruktur. Precis som övriga företag, söker även de som driver nationellt kritisk infrastruktur ständigt effektivitet i verksamheten genom t.ex. billigare och mer tillgängliga tekniska komponenter. Den nya tekniken tillåter tillverkning av massproducerade och allt billigare komponenter och programlösningar, som ofta medför högre tillgänglighet och lönsamhet, men som samtidigt medför nya säkerhetsrisker. En stor del av den service som kan klassas som kritisk infrastruktur (som t.ex. vatten och elförsörjning, teleoperatörer m.m.) består helt eller delvis av privata bolag med syfte att skapa vinst till sina aktieägare, vilket i första hand betyder att bolagen granskar sin verksamhet från ett lönsamhetsperspektiv. Bolagets lönsamhet på kort sikt kan innebära stora nationella säkerhetsrisker på lång sikt. Stater måste i sina nationella cybersäkerhetsstrategier balansera dessa två olika intressen mot varandra och avgöra hur lönsamhet och modernisering av kritisk infrastruktur kan möjliggöras utan alltför stora risker för den nationella säkerheten (Hathaway & Klimburg 2012).

Den privata sektorn spelar en avgörande roll inom teknik- och cybersäkerhetsbranschen. Det är den privata sektorn som står för merparten av nya tekniska innovationer, service, tillverkning av komponenter och programvara som behövs för att digitalisering överhuvudtaget är möjligt. Den privata sektorn står även för en stor del av de cyber- och informationssäkerhetslösningarna som finns till förfogande. Som ovan nämnts ansvarar även privata aktörer för en stor del av den nationella kritiska infrastrukturen. Stater har ett stort

intresse att skydda och samarbeta med privata aktörer som är centrala för den nationella säkerheten. Sättet och medlen som används eller kan användas för samarbete är omdebatterade. Samtidigt förekommer det en hel del intressekonflikter mellan det offentliga och det privata, som inte alltid är helt enkla att lösa från ett nationellt perspektiv. Sätt att påverka eller samarbeta med den privata sektorn kan innebära allt från påtvingande lagstiftning, till skattelättnader, grundande av samarbetsforum för informationsutbyte till erbjudande av direkt tekniska cybersäkerhetslösningar för nationellt kritisk infrastruktur (Hathaway & Klimburg 2012).

En centralt dilemma i dagen informationssamhälle är det ekonomiska värdet på personuppgifter, utbyte och fritt flöde av information mot starkare dataskydd och medborgarnas rätt till sin egen information. En stor del av Internetekonomin bygger i dagens läge på tillsynes gratis tjänster som de facto finansieras genom insamling, anrikning, profilering och till slut försäljning av personuppgifter eller annan information. Informationen i sig har blivit en handelsvara. Enda sedan 1980-talet har allt mer uppmärksamhet fästs vid högre dataskydd av personuppgifter och i dagens läge är området t.ex. inom EU starkt reglerat. Utöver detta finns det ett stort behov att utväxla information av en eller annan orsak, oberoende om det är frågan om statlig säkerhet eller med ekonomiska fördelar. Nationell lagstiftning är nödvändigtvis inte tillräckligt utvecklad för att kunna erbjuda medborgarna dataskydd och samtidigt möjliggöra utbyte av information för att motverka olika cyberrelaterade nationella hot (Hathaway & Klimburg 2012).

Internet har i dagens läge utvecklats till ett centralt medium for yttrande av åsikter, opinionsbildning och en plattform som kan användas för att utveckla demokratistödjande deliberativa mekanismer och innovationer. Speciellt för medborgare i mer auktoritativa stater har nätet erbjudit en kanal för oppositionen och oliktänkare, som inte alltid setts med blida ögon av de makthavande. Speciellt i auktoritativa regimer finns det ambitioner på att starkt reglera utbudet av tjänster som erbjuds medborgarna. Då nätet ger nya möjligheter för åsiktsyttring och mobilisering av opinion erbjuder det även myndigheterna en outsinlig och lättillgänglig plattform för övervakning och i värsta fall förtryck av grundläggande fri- och rättigheter (Hathaway & Klimburg 2012). Samtidigt som yttrandefriheten kan vara något centralt att främja och försvara kan det medföra besvär för stater, eftersom det kan används

som ett verktyg för att öka den politiska medvetenheten och mobilisera stora massor. Yttrandefriheten innebär givetvis också att information av kriminell karaktär måste accepteras närvara. Olika säkerhetsåtgärder som att blockera, filtrera, förbjuda eller övervaka informationsflödet måste vara noggrant övervägda eftersom de kan utgöra ett hot mot grundläggande rättigheter och friheter (Ekstedt, Parkhouse & Clemente 2012). Utan välfungerande och tydlig lagstiftning kan gränserna lätt töjas ut. Nya tekniska innovationer gör det allt lättare att samla in, anrika och modifiera data på ett sätt som gör att frågor beträffande dataskydd är högst aktuella idag (Hathaway & Klimburg 2012).

3.1.2 Tre perspektiv på cybersäkerhet

Staterna måste i sina cybersäkerhetsstrategier ta ställning till hur strategierna förhåller till sig och betonar tre centrala perspektiv. Dessa perspektiv är 1) *det statliga*, 2) *det nationella* (eller *det samhälleliga*) och 3) d*et internationella* (Hathaway & Klimburg 2012). Grunden till denna indelning är hämtade från public policy teoribildningen som granskar hur policyer implementeras genom tre modeller: i statskontexten (Whole of Government, WoG), i nationskontexten (Whole of Nation, WoN) eller i systemkontexten (Whole of System, WoS). WoG betonar samarbetet över gränserna inom statsförvaltningen, WoN betonar samarbetet inom nationen med såväl privata aktörer som med organisationer. WoS betonar ett globalt systemomspännande samarbete (Klimburg & Healey 2012).

Tabell 2: Matris över policyimplementeringsperspektiv.

Källa: Klimburg och Healey 2012

	Whole of Government	Whole of Nation	Whole of System
Synonymer	Förenade staten, Nätverkande staten	Hela samhället	Hela unionen, hela alliansen eller koalitionen
Relaterade koncept	”3D Approach” (diplomati, utveckling, och försvar)	Omfattande betraktelsesätt	”3C Approach” (koherent, koordinerat och kompletterande)
Aktörer	Staten Centralförvaltningen Lokalförvaltningen	Serviceproducenter IKT/säkerhetsspecialister Civilsamhället/det akademiska	Diplomater Parter inom Internetförvaltningen Industri/Vetenskapliga/ Tekniska arbetsgrupper
Huvudarbetsmetod	koordinering	Samverkan (cooperation)	Samarbete (collaboration)

Det statliga perspektivet i cybersäkerhetskontexten handlar i all enkelhet om att samordna de offentliga, främst statliga aktörer och resurser kring nationella cybersäkerhetsfrågor. Det statliga perspektivet innefattar en bred rad olika förvaltningsområden och cybersäkerhetsmandat som t.ex. militära cyberfrågor, cyberbrottsbekämpning, ekonomiska frågor och diplomati eller utrikespolitiska frågor. Många av de statliga cybersäkerhetsärendena överlappar en rad olika förvaltningssektorer, -nivåer och myndigheter. Alla de olika aktörerna tolkar utmaningarna och utvecklingsbehoven från sina egna perspektiv, ifall det inte förekommer samordning över sektorsgränserna. Ett av de viktigaste uppgifterna, utgående från det statliga perspektivet, är att sörja för koordinering över förvaltningsgränserna (Klimburg & Healey 2012). Ansvar och uppgifter som tangerar den statliga cybersäkerheten är ofta uppdelade på många olika förvaltningsområden, avdelningar och statliga myndigheter (Hathaway & Klimburg 2012). Det ligger i och för sig i ärendets natur eftersom ämnet är så brett omfattande. Denna splittring är förståelig men leder

samtidigt till stora utmaningar då det gäller samordningen av av cybersäkerhetsverksamheten mellan de olika statliga aktörerna. Kort sagt är hela den övertäckande statliga cybersäkerheten allas sak men ingens ansvar. För att uppnå bättre samordning finns en del metoder och modeller att tillgå (Hathaway & Klimburg 2012). En modell är t.ex. att centralisera helhetsledarskapet av cybersäkerhetsfrågor på en myndighet eller att på ett eller annat sätt förbättra förutsättningarna för koordinering och samarbete över myndighetsgränserna.

Inte minst på grund av cybermiljöns starkt internationella natur finns det ett ständigt behov för internationellt samarbete. Internationella cybersäkerhetsfrågor är inte endast en angelägenhet för mellanstatlig aktivitet, utan involverar i högsta grad även icke statliga aktörer (Klimburg & Healey 2012). Den internationella perspektivet finns närvarande i så gott som alla cybersäkerhetsstrategier. Cybermiljön i sig själv är global och intressefrämjande inom ramen för nationell cybersäkerhet kräver internationellt samarbete. Eftersom cybermiljöns förvaltningsmodell är splittrad och många av aktörerna inom området är privata företag eller oberoende organisationer, sker en stor del av det internationella samarbetet utanför den traditionella statliga ramen. På grund av detta är det av stor vikt för en stat att lyckas komma överens om eller utse en enda ledande aktör som överser och koordinerar det internationella samarbetet (Hathaway & Klimburg 2012). Cybersäkerhetens komplexa internationella dimension har inte alltid och i alla sammanhang varit helt klar. Fast perspektivet nog till vissa delar beaktats i äldre cybersäkerhetsstrategier är det först på senare tid som intresset för perspektivet ökat. Det internationella perspektivet inom cybersäkerhetsfrågor handlar inte enbart som ”simpla” internationella och utrikespolitiska frågor som kan skötas genom utrikesministerierna. Snarare är det frågan om en mängd olika perspektiv och mandat med vitt skilda intressen och behov som måste sammanjämkas genom olika samarbetsprocesser mellan en bred rad olika aktörer såväl statliga som icke-statliga (Klimburg & Healey 2012).

Inkluderandet av de civila och privata sektorerna är viktiga för att uppnå en tillfredsställande nationell cybersäkerhetsnivå. Den privata sektorn är mycket långt den som utvecklar kod, bygger program och som levererar digitala tjänster. Det är också denna sektor som upprätthåller en stor del av samhällets nätverksinfrastruktur. Mycket av den samhällskritiska infrastrukturen drivs och ägs av privata aktörer (Klimburg & Healey 2012). Engagemanget och samarbetet med säkerhetsentreprenörer och företag som opererar kritisk infrastruktur har

traditionellt ansetts vara kritiskt för den nationella säkerheten. På grund av att antalet icke-statliga aktörer relevanta för den nationella cybersäkerheten stadigt ökat under åren, har många stater valt att utforma samhällsomfattande cybersäkerhetsstrategier. Grunden för det nationella samarbetet kan antingen basera sig på tvingande lagstiftning eller på mer fritt samarbete. En samhällsomfattande cybersäkerhetsstrategi försöker utöka säkerhetssamarbetet till ett brett spektrum, för den nationella cybersäkerheten relevanta, icke-statliga aktörer inom samhället. På grund av att ett tillräckligt omfattande på tvingande lagstiftning uppbyggd samarbete knappast är möjligt inom moderna demokratiska stater, betonas istället olika samarbetsstrategier i många nationella cybersäkerhetsstrategier (Hathaway & Klimburg 2012). Den nationella perspektivets främsta syfte är att ta i beaktande och utveckla samarbetsmodeller för att inkludera dessa icke statliga aktörer i det nationella cybersäkerhetsarbetet. Utformningen av de enskilda samarbetsformerna och betoningarna varierar och är beroende av de enskilda nationella politiska systemen, kulturen och invanda samarbetsformerna (Klimburg & Healey 2012).

3.1.3 Den nationella cybersäkerhetens mandat

Nationell cybersäkerhet som övergripande ämne innefattar, som ovan redan framkommit, ett brett spektrum infallsvinklar och betraktelsesätt. Nationella cybersäkerhetsstrategier kan granskas utifrån hur de betonar och lyfter fram fem distinkta perspektiv eller *mandat.* De fem mandaten överlappar varandra i verkligheten men samtidigt betraktas dessa mandat inom den nationella statliga kontexten som separata intresse- och verksamhetsområden. Mandaten berör såväl statliga som icke-statliga aktörer (Klimburg & Mirtl 2012). De fem mandaten delas in enligt följande (Hathaway & Klimburg 2012):

1. militära cyberfrågor,
2. cyberbrottsbekämpning,
3. underrättelseverksamhet,
4. skyddande av kritisk infrastruktur och nationell krisberedskap,
5. cyberdiplomati och förvaltning av Internet.

Militära cyberfrågor betonar verksamhet som har att göra med att försvara nationella militära nätverk och kritisk infrastruktur, att utveckla förmåga till cyberbaserad krigföring, att utveckla cybermetoder för taktisk traditionell krigföring och strategisk cyberkrigföring (Hathaway & Klimburg 2012). På organisationsnivå måste militären kunna skydda sina egna operativa nätverk och tekniska resurser från utomstående hot. På nationell nivå måste militären utveckla taktisk och operativ cyberkapacitet för att kunna försvara nationen mot militära cyberhot samt för militär krigföring (Klimburg & Healey 2012).

Cyberbrottsbekämpningsfrågor kan innefatta utvecklandet av en bred rad olika förmågor inom en rad olika domäner. Detta kan inkludera allt från utvecklandet av polisens kompetens och resurser till lagstiftning och internationellt samarbete inom ramen för cyberbrottsbekämpning (Hathaway & Klimburg 2012). Eftersom en stor del av de cybersäkerhetsincidenter som sker på nätet även i de flesta fall kan klassas som brott, finns det en stark koppling mellan cyberbrottsbekämpningen och cybersäkerheten.

Underrättelseverksamhet i cybermiljön kan vara svår att upptäcka och ofta används samma verktyg och program för att genomföra underrättelseoperationer som cyberbrott. Många stater använder sig även av kriminella grupperingar utan direkt statlig koppling för att genomföra underrättelseoperationer. Cyberunderrättelseverksamheten är i högsta grad internationell till sin natur vilket medfört att stater är tvungna att utveckla utrikespolitiska reaktions- och attributionsmekanismer (Hathaway & Klimburg 2012). Underrättelseverksamheten koncentrerar sig först och främst på förebyggande verksamhet då det gäller nationella säkerhets- eller militära hot. Målet är att hålla sig uppdaterad om underliggande hotande händelser, aktörer, planer, tekniker och motiv oberoende om det är frågan om aktivism, statssäkerhetsfrågor, militära hot, enskilda men potentiellt farliga aktörer eller terrorism (Klimburg & Healey 2012).

Skyddande av kritisk infrastruktur och nationell krisberedskap handlar om hur de olika aktörerna som upprätthåller och opererar kritisk infrastruktur (som t.ex. vattenförsörjning, elnätverk, finansiella tjänster m.m.) engageras i det nationella arbetet för en ökad cybersäkerhet. På grund av att cybermiljön omfattar och berör kritiska funktioner genom så gott som hel samhället är det av största vikt att den nationella krisberedskapen utökas med

cyberdimensionen. Detta innebär såväl utvecklandet av institutionella strukturer som sörjer för samarbetet mellan det statliga och det icke-statliga aktörer, utvecklandet av stabila kriskommunikationsnätverk och relevant lagstiftning inom området (Hathaway & Klimburg 2012).

Cyberdiplomati handlar om hur den moderna staten och statliga diplomatin förhåller sig till den nya kontext cybermiljön har infört i mellanstatligt agerande. Delvis handlar det om multilaterala förhållanden och om hur staten förhåller sig till och utvecklar sitt samarbete inom den internationella kontexten för förvaltningen av cybermiljön och delvis om bilaterala förhållanden om hur stater ”beter sig” i cyberomgivningen samt hur de byter, behandlar, samlar in, utvärderar och presenterar information inom den traditionella internationella kontexten (Hathaway & Klimburg 2012). Inom mandatet behandlas även frågor som har att göra med internationella proaktiva arrangemang, harmoniserade förebyggande åtgärder och aktiv internationellt bistånd då det gäller cyberfrågor (Klimburg & Healey 2012).

De ovan presenterade fem mandaten kan vidare kopplas ihop med tre identifierade tvärgående mandat som är: skyddande och utbyte av information, koordinering samt forskning, utveckling och utbildning (Klimburg & Healey 2012). För att bättre representera det innehåll som finns upptaget i de fem nordiska ländernas cybersäkerhetsstrategier har tvärmandatet ”forskning” utökats med ”kompetensutveckling” så att klassen i sin helhet heter ”forskning och kompetensutveckling” inom ramen för denna studie.

Normativt borde de fem mandaten betraktas och koordineras som en holistisk helhet för att garantera ett möjligast omfattande nationellt cybersäkerhetsperspektiv. Realiteten är dock att vart och ett av mandaten utvecklas utifrån sina egna villkor, prioriteringar och principer. Detta innebär att det nationella cybersäkerhetsfältet är splittrat (Klimburg & Mirtl 2012).

En oförståelse för de olika mandaten och deras kopplingar kan leda till konfliktfyllda lagstiftningsmässiga krav och behov och friktioner mellan cybersäkerhetsfunktioner, myndigheter och organisationer (Klimburg & Healey 2012). Från detta perspektiv är mandaten centrala utgångspunkter vid utformandet av cybersäkerhetsstrategier.

3.2 Metod och analys av materialet

3.2.1 Forskningsdesign och forskningsstrategi

Studien bygger på jämförande forskningsdesign och mer exakt är det frågan om en jämförande flerfallstudie. Ett tillämpningsområde för jämförande forskningsdesign är då man vill jämföra nationer, samhällssystem, organisationer eller kommuner med varandra (Bryman 2012; Denk 2012). Jämförande design kan användas antingen med kvantitativ eller kvalitativ forskningsstrategi. En jämförande flerfallsstudie bygger på att två eller fler fallstudier samtidigt genomförs (Campbell 2010; Bryman 2012). Målet är att hitta kontraster, likheter och mönster mellan fallen (Campbell 2010; Esser & Vliegenthart 2017). Den komparativa designens fördel är att den erbjuder en möjlighet att skilja på karaktäristiken hos två eller fler fall och således erbjuda en språngbräda för djupare teoretisk reflektion om kontrasterande fynd (Campbell 2010; Bryman 2012). Den jämförande studien kräver att källmaterialet bearbetas på ett sätt som gör det jämförbart (Metsämuuronen 2008; Tjora 2010; Bryman 2012; Denk 2012).

Studiens forskningsstrategi är kvalitativ till sin natur och tillämpar deduktiv eller teoribaserad kvalitativ innehållsanalys. Kvalitativ innehållsanalys är en metod för att systematiskt och objektivt kunna beskriva och kvantifiera fenomen (Elo & Kyngäs 2008). Källmaterialet har analyserats och kategoriserats utifrån teoretiska klasser för att lättare kunna göra jämförelser, generaliseringar och dra slutsatser mellan de olika fallen. Kvalitativ innehållsanalys lämpar sig för ett stort urval olika typer källor däribland dokument, avtal, transkriberingar m.m. (Hsieh & Shannon 2005; Marvasti 2019). Genom innehållsanalys är det möjligt att objektivt och systematiskt analysera dokument och göra resultaten testbara, vilket ger resultaten tillförlitlighet (Tuomi & Sarajärvi 2002; Marvasti 2019). I den teoribaserade innehållsanalysen formas en analysstomme eller matris som baserar sig på vald teori och det studerade innehållet kodas i enlighet med denna (Tuomi & Sarajärvi 2002; Hsieh & Shannon 2005). Den kvalitativa innehållsanalysen kan använda sig av såväl kvalitativa som kvantitativa metoder eller så kallade blandade metoder (mixed methods) (Marvasti 2019; Schreier, Stamann, Janssen, Dahl & Whittal 2019) och det kan vidare vara svårt att göra en klar skillnad mellan strikt kvalitativ och kvantitativ textanalys (Lindgren 2011).

Kvantifieringen av kvalitativt material kan erbjuda nya perspektiv på det studerade fenomenet och hjälpa till med att skapa överblick över ett stort eller komplext kvalitativt material. (Tuomi & Sarajärvi 2002; Harboe 2013; Schreier et al. 2019). Då det kvalitativa materialet kvantifierats är det möjligt att mäta omfattning, frekvens och förekomst d.v.s. hur mycket utrymme det ägnas åt de enskilda studerade enheterna i texten (Harboe 2013).

Den kvalitativa innehållsanalytiska processen går i korthet ut på att formulera forskningsfrågorna, samla in materialet och till slut systematiskt koda och analysera materialet (Hsieh & Shannon 2005; Marvasti 2019).

3.2.2 Datainsamling, -bearbetning och analys

De fem nordiska ländernas cybersäkerhetsstrategier finns fritt tillgängliga på nätet. Strategierna hittas på respektive nationalspråk via relevanta nationella myndighetssidor och även på engelska via Europeiska unionens cybersäkerhetsmyndighets (ENISA) portal (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map). Finlands nyaste strategi finns inte publicerad på ENISA:s webbplats, utan är tillgänglig via Säkerhetskommitténs webbsida (https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/). I studien har de nordiska ländernas engelskspråkiga versioner av cybersäkerhetsstrategierna analyserats och jämförts. Islands nationella cybersäkerhetsstrategi finns endast publicerad som ett sammandrag på engelska, men den engelskspråkiga versionen innehåller de centralaste delarna som möjliggör att den inkluderas i studien.

För att jämförelsen ska ha relevans måst även underlaget vara jämförbart utifrån den tids- och rumsmässiga aspekten (Denk 2012; Esser & Vliegenthart 2017). Underlaget består av de fem nordiska ländernas nyaste och ikraft varande cybersäkerhetsstrategier, för att ge en så bra jämförbarhet som möjligt då det gäller den tids- och rumsmässiga aspekten. Den äldsta strategin är från år 2015 och den nyaste från år 2019.

Studiens källmaterial har kodats och bearbetats med hjälp av programvara för kvalitativ forskning (CAQDAS-verktyg). Verktyget gör det dels lätt att analysera själva texterna,

kvantifiera förekomsten av kategorier för ytterligare observationer och jämföra källorna med varandra. Programmet hjälper till med systematiseringen av kodningsarbetet (Tjora 2010).

Innehållet har kategoriserats och kodats enligt de fem dilemmanen, tre perspektiven samt de fem mandaten i enlighet med tabell 3 nedan.

Tabell 3: De teoretiska ramverken för nationella cybersäkerhetsstrategier.
Källa: Klimburg (2012)

Teoretisk ram	Kategori
Perspektiven	Internationell
Perspektiven	Nationell
Perspektiven	Statlig
Dilemman	Dataskydd mot utbyte av information
Dilemman	Ekonomisk stimulans mot högre säkerhet
Dilemman	Privat sektor mot offentlig sektor
Dilemman	Åsiktsfrihet mot politisk stabilitet
De fem mandaten	Cyberbrottsbekämpning
De fem mandaten	Cyberdiplomati och förvaltning av Internet
De fem mandaten	Militära cyberfrågor
De fem mandaten	Skydd av kritisk infrastruktur och nationell krisberedskap
De fem mandaten	Underrättelseverksamhet
De fem mandaten (tvärmandat)	Forskning & Kompetensutveckling
De fem mandaten (tvärmandat)	koordinering
De fem mandaten (tvärmandat)	Skydd och utbyte av information

Klassificering och tolkning av kvalitativt material är till viss del beroende av den som utför själva arbetet. Vidare kan det förekomma fel eller inexaktheter i klassificeringen beroende på en eller annan orsak. Då det gäller kvalitativ tolkande forskning kan det inte i positivistisk mening förekomma fullständig neutralitet (Tjora 2010). För att öka reliabiliteten i studien och

minska risken för direkt felklassificering och inexakthet har klassificeringen av de fem cybersäkerhetsstrategierna upprepats tre separata gånger med minst två veckor mellan gångerna. Meningen med de tre klassificeringsrundorna var att få en tämligen stor säkerhet om att all relevant text är klassificerad och att den är rätt klassificerad i enlighet med kategorierna.

I praktiken har analysen av strategierna gjorts så att texterna har lästs skilt för sig i analysverktyget. Under varje genomläsning har stycken, meningar eller ställen i texten som klart anspelar på någon av de använda kategorierna markerats och kategoriserats. Ifall ett stycke eller en mening innehållit syftningar till fler än en kategori har det ifrågavarande stycket markerats med alla identifierade kategorier. Av detta följer att samma ställe kan hittas under flera kategorier i jämförelsen. Om texten till exempel i samma stycke eller mening syftar till att fästa uppmärksamhet vid dataskyddsfrågor så att det gynnar den ekonomiska tillväxten och investeringsattraktiviteten har det ifrågavarande stycket klassats under dilemmat ”dataskydd mot utbytet av information” och ”ekonomisk stimulans mot högre säkerhet”. Citatet från den isländska strategin nedan ger ett exempel på hur ett stycke kategoriserats i fler en en kategori enligt föregående exempel.

> As the Internet is international, it is important that Iceland’s legislation should be compatible with that of its neighbours as far as possible. Legislation must ensure personal data safety and serve as a basis to create an attractive environment for IT-companies to operate and develop in (NCSS IS 2015).

Strategierna är uppbyggda på strukturerade på olika sätt. De danska, norska och isländska strategierna har först en inledande och förklarande textdel som åtföljs av konkreta och mer detaljerade åtgärdspunkter. Den svenska strategin består av långa förklarande textstycken med de huvudsakliga målsättningarna och underordnade verksamhetsmål upptagna i punktform under vart och ett tema. I den svenska strategins förklarande text kan det förekomma ställen som klart och tydligt betonar eller understryker någon viss åtgärd eller målsättning och på så sätt ger mer vikt åt den. Den finska strategin är relativt kort och koncist och består av förklarande bastext med strategiska linjedragningar och huvudsakliga verksamhetsmål integrerade i själva texten. De noggrannare och mer exakta finska åtgärderna finns upptagna i ett skilt åtgärdsprogram.

Tolkningen av innehållet i strategierna är inte helt entydigt och enkelt. De olika utformningarna och uppbyggnaderna av strategitexterna har gjort det jämförande arbetet utmanande och ställvis svårt. Skillnaderna i strategierna utformning har gjort det nödvändigt att välja sätt på vilket markeringarna och klassificeringen i texterna görs. Strävan har varit har att undvika direkta dubbelmarkeringar, men att ändå få fram det relevanta betoningarna i texterna speciellt gällande saker som understrukits med speciell kraft. Ifall en målsättning först har tagits upp i den förklarande delen av texten och exakt samma sak ännu upptagits som detaljerad verksamhetsmål har omnämnandet endast klassificerats en gång för att inte klassificera exakt samma sak fler gånger. Om den förklarande delen däremot har understrukit något särskilt starkt kan detta ha markerats, trots omnämnandet i verksamhetsmålet, för att få fram den extra starka betoningen på frågan.

Som resultat av kodningen har materialet kvantifierats och identifierats för kontextualisering, vidare innehållsanalys och jämförelse. På basen av kodningen har även en komparationsmatris skapats. På grund av att strategierna är olika till utformning, omfattning och innehåll är det inte möjligt att direkt jämföra det kvantifierade materialet från en strategi med en annan. Däremot kan det kvantifierade materialets olika klasser ses representera betoningar i de enskilda strategierna och därmed kan resultatet användas för att jämföra de olika kategoriernas inbördes förhållande inom en strategi, för att på så sätt få fram nationella betoningar. Helheten av betoningarna i en strategi kan sedan i sin tur jämföras med betoningarna i en annan strategi. Analysen tar vara på såväl innehåll, betoningar som förekomst av kategorier i strategierna.

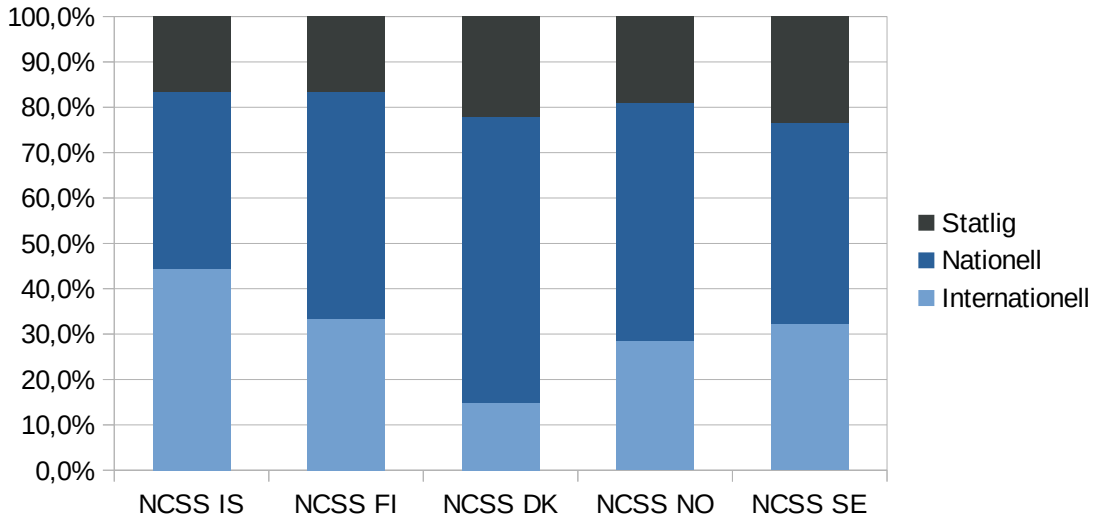
4 Nordiska cybersäkerhetsperspektiv

4.1 Allmän överblick över perspektiven i de studerade strategierna

I det stora hela verkar det inte finnas väldigt stora och avgörande skillnader i hur de olika nordiska länderna betonar de olika perspektiven i sina cybersäkerhetsstrategier. Alla fem länder har beaktat såväl det statliga, det nationella som det internationella perspektivet, men skillnaderna i hur de olika perspektiven finns upptagna i strategierna varierar från land till land. De finska, norska och svenska strategierna är närmast varandra då det gäller betoningar på perspektiven. Störst skillnad förekommer i den isländska och den danska strategin i jämförelse. Figur 1 nedan visar de interna betoningarna av de tre perspektiven i de studerade strategierna. Av de nordiska länderna betonar Island starkast Danmark svagast det internationella perspektivet, medan Norge, Sverige och Finland lagt ungefär lika stor vikt på det internationella. Det statliga perspektivet betonas klart minst i den isländska strategin och mest i den svenska. Det nationella perspektivet är relativt jämnstarkt i alla strategier, men framkommer klart starkast i den danska och svagast i den isländska strategin.

Noggrannare utvärdering om likheter och skillnader angående de tre perspektiven hittas i respektive underkapitel.

Figur 1: Betoningar på cybersäkerhetsperspektiv i de nordiska cybersäkerhetsstrategierna.



Som det framgår från tabell 4 nedan förekommer de tre perspektiven internationellt, nationellt, och statligt i alla de studerade strategierna. Rött anger lägsta betoning, gul högsta, x anger ifall perspektivet återfinns i strategin. Perspektiven betonas dock olika i de olika strategierna. En överblick ger för handen att de finska, norska och svenska strategierna är mest lika vid betoning av perspektiven. Gemensamt är att de lägger högsta betoning på det nationella och lägsta betoning på det statliga perspektivet. Den isländska och danska strategin skiljer sig åt i det att Island betonar det internationella högst och Danmark lägst. Alla strategier verkar identifiera problem och frågor som på ett eller annat sätt är förknippade med det nationella utvecklingsbehovet och betona perspektiven i enlighet med det.

Tabell 4: Komparationsmatris över förekomst och betoning av de tre perspektiven i cybersäkerhetsstrategierna.

Kategori	NCSS IS	NCSS FI	NCSS DK	NCSS NO	NCSS SE
Internationell	x	x	x	x	x
Nationell	x	x	x	x	x
Statlig	x	x	x	x	x

Gemensamt för alla strategier är att det beaktar det nationella perspektivet relativt sett starkt. Den isländska strategin är den ända som har en klart mindre betoning på det nationella till fördel för det internationella perspektivet. Denna skillnad kan tänkas bero på Islands läge mitt

i Atlanten mellan två kontinenter, lilla storlek och starka beroende till andra länder. De svenska, norska och finska strategierna betonar det nationella perspektivet relativt sett ungefär lika starkt, dock så att Sveriges betoning är svagast och Norges klart starkast av dessa tre. Den danska strategin har klart starkast betoning på det nationella perspektivet av alla studerade strategier.

Skillnaderna mellan strategierna då det gäller det statliga perspektivet är tillsynes inte stora, men finns närvarande. Gemensamt för alla är att det statliga perspektivet genomgående är av mindre betydelse i jämförelse med det nationella eller internationella perspektiven. Som ovan framkommit betonas det statliga perspektivet klart minst i den isländska strategin och tillsynes mest i den svenska strategin. Mycket av de föreslagna åtgärderna eller verksamhetsmålen som tas upp i svenska strategin kan tolkas riktade till offentliga myndigheter. Den svenska strategin är inte helt klar på alla punkter i hur och till vem någon åtgärd specifikt ska riktas och lämnar således en del till läsaren att tolka.

4.2 Det statliga perspektivet

Den isländska strategin betonar det statliga perspektivet svagast. Den isländska cybersäkerhetsstrategin har egentligen bara två punkter som explicit kan hänföras till det statliga perspektivet. I strategin ses cybersäkerheten främst som en samhällelig eller nationell angelägenhet med global spännvidd (NCSS IS 2015).

Den finska strategin betonar det statliga perspektivet jämförelsevis svagare än det nationella och internationella, men perspektivet är ändå inte utan betydelse för strategin. Tvärtom försöker strategin lyfta fram särskilt viktiga områden där myndigheternas förutsättningar för samarbete och koordinering över förvaltningsgränserna är av stor vikt. Den finska strategin lyfter speciellt fram att utvecklandet av den nationella cybersäkerheten förutsätter kompetenskrav och samarbetsskyldighet för den offentliga förvaltningen. Strategin poängterar även explicit att stödet, resurserna och verktygen som handhas av ansvariga myndigheter ska förstärkas (NCSS FI 2019).

Danmarks betoning på det statliga i strategin är ganska långt i linje med de övriga nordiska länderna. Den danska strategin understryker att myndigheterna har ett sektorsvist fördelat och

således fragmenterat ansvar då det gäller utvecklandet av den nationella cybersäkerheten i Danmark. Det sektorsvisa ansvaret kräver samordning mellan de statliga myndigheterna (NCSS DK 2017).

Betoningen på det statliga perspektivet i den norska strategin är ungefär på samma nivå som i den danska strategin. Liksom den danska strategin lyfter även den norska fram att ansvaret för cybersäkerheten på nationell nivå är splittrad mellan olika förvaltningssektorer och att samordning behövs (NCSS NO 2017).

Den svenska betoningen på det statliga perspektivet verkar ligga på samma nivå som Finlands och Norges i förhållande till de övriga perspektiven i strategierna. Den svenska strategin liksom många andra strategier erkänner att myndighetsfältet är splittrat. I den svenska strategin lyfts ökat samarbetet och förbättrad koordinering mellan myndigheterna fram som en central målsättning för att minska fragmentering och öka säkerhetsarbetets effektivitet. Den svenska strategin nämner att uppmärksamhet måste fästas på olika offentliga förvaltningsnivåer. Vidare lägger den svenska strategin en tämligen stark och specifik vikt vid ökad myndighetstillsyn för att förbättra den nationella cybersäkerheten. Den svenska strategin tar även specifikt ställning till att myndigheternas upphandlingsexpertis måste uppmärksammas för att garantera att upphandlingen av IKT-varor och -tjänster i tillräcklig grad beaktar cybersäkerhet (NCSS SE 2016).

Gemensamt för alla strategier, då det gäller det statliga perspektivet, är att de erkänner att myndighetsansvaret är splittrat. Som en följd efterlyser alla strategierna mer koordinering och samarbete mellan de statliga myndigheterna för att få klarhet i den rådande situationen och för att på ett effektivare sätt utveckla den nationella cybersäkerheten (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017; NCSS NO 2017; NCSS FI 2019) . Den danska och den svenska strategin tar speciellt ställning till att arbetet för att förbättra de kommunernas och regionala förvaltningens förmåga att svara på cybersäkerhetsfrågor måste stärkas och utvecklas och riktar således även klara åtgärder till de övriga förvaltningsmässiga nivåerna (NCSS SE 2016; NCSS DK 2017)

Då det specifikt gäller satsningar på myndighetsverksamhet nämns såväl polisen, de nationella säkerhetstjänsterna som försvaret. Omnämnanden i strategierna angående

strategiska satsningar som gäller specifika myndigheter har tolkats höra till det statlig perspektivet, eftersom ingen annan än staten kan påverka deras verksamhetsförutsättningar.

I strategierna handlar det statliga perspektivet mycket om att förbättra enskilda myndigheters, främst polisens försvarsmaktens eller säkerhetstjänstens, förmåga att utföra sina uppdrag relaterade i till cyberomgivningen. Strategierna har en del gemensamt, men verkar speciellt på denna punkt betona målsättningar som utgår från vart och ett lands situation som de just nu befinner sig i. Till exempel förnyades den finska underrättelselagstiftningen år 2019 och två nya underrättelselagar trädde i kraft. I och med de nya lagarna fick Skyddspolisen och Försvarsmakten bredare och uppdaterade befogenheter till underrättelseverksamhet i cybermiljön (Helsingin Sanomat 2019). Den finska cybersäkerhetsstrategin hänvisar till de nya befogenheter och efterlyser mer samarbete mellan ansvariga myndigheter (NCSS FI 2019). Just denna målsättning hänger starkt ihop med den nationella situationen. I likhet med den finska strategin understryker även den danska utvecklandet av underrättelseförmågor inom den danska försvarsmakten (NCSS DK 2017).

Alla strategier lägger vikt vid att förstärka polisens förmåga att bekämpa och förebygga cyberbrott. I strategierna nämns bland annat att polisen måste garanteras tillräckliga resurser och förutsättningar för att effektivt kunna bekämpa cyberbrott (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017; NCSS NO 2017; NCSS FI 2019). Den norska strategin understryker att polisen även i fortsättningen måste åtnjuta allmänhetens förtroende och tillit i att lösa och bekämpa cyberbrott på ett effektivt och ansvarsfullt sätt (NCSS NO 2017).

4.3 Det nationella perspektivet

Det nationella perspektivet finns närvarande i alla strategier med lite olika styrka. Betoningar på det nationella perspektivet i den isländska strategin är lägst av alla de nordiska länderna. Trots att antalet markeringar på det nationella perspektivet är relativt sätt lägst i jämförelse, betyder det inte att perspektivet skulle vara utan betydelse för den isländska strategin. Tvärtom understryker den isländska strategin vikten av att involvera ett brett lager aktörer från olika delar av samhället för att på så vis kunna nå en ökad cybersäkerhetsnivå (NCSS IS 2015). Den finska strategin betonar relativt sett det nationella perspektivet starkast i den interna jämförelsen av de olika perspektiven i strategin. Över hälften av de strategiska målen

har på ett eller annat sätt att göra med övergripande nationella målsättningar (NCSS FI 2019). Den danska strategin har en relativt sett mycket stark betoning på det nationella perspektivet och starkast av alla de jämförda strategierna. Som det uttrycks i strategin ”har den danska regeringen satt upp en ambitiös plan för att höja den danska nationella cybersäkerhetsnivån” (NCSS DK 2017). Den svenska betoningen på det nationella perspektivet är relativt sett starkast i jämförelse med de övriga perspektiven i strategin. Den svenska strategin uttrycker explicit att åtgärderna och strategins perspektiv omfattar hela den nationella domänen (NCSS SE 2016). Den norska strategin betonar det nationella perspektivet relativt sett starkast av de tre perspektiven i den interna jämförelsen. Nivån av nationell betoning är nära den finska strategins betoning (NCSS NO 2017).

Linjedragningar angående nationell utbildning och kompetensfrämjande verksamhet finns allmänt med i strategierna. Genom att utbilda människor och öka på den nationella kompetensen då det gäller cybersäkerhet minskar de nationella cybersäkerhetsriskerna.

Strategierna lyfter fram centrala teman inom de nationella sfären som handlar om att cybersäkerhet är en gemensam nationell angelägenhet där var och en i samhället bär sitt eget ansvar. Andra centrala teman som återfinns i alla studerade strategier är förstärkta nationella resurser, ökad nationell koordinering, mer och bättre skydd av den kritiska infrastrukturen och utbildning och kompetensutveckling. Det nationella perspektivet främsta målsättningar verkar hänga samman med skyddandet av kritisk infrastruktur, som mycket långt upprätthålls och drivs av privata aktörer. Alla strategier understryker även att cybersäkerhet är en mycket komplex fråga, speciellt då det gäller den samhällskritiska infrastrukturen och att det inom cybersäkerhetsfältet verkar en rad olika aktörer. En splittrad cybersäkerhetssektor kräver nya former av samarbete för att lyckas i utvecklingen av den nationella cybersäkerheten (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017; NCSS NO 2017; NCSS FI 2019).

4.4 Det internationella perspektivet

Som det i introduktionen redan framkommit sker en stor del av Internets administration, standardiseringsarbetet och utveckling i diverse internationella icke-statliga organisationer. För att kunna medverka i och påverka detta arbete krävs nationellt engagemang och klart uttalade målsättningar med en internationell dimension.

Det internationella perspektivet finns närvarande i alla de studerade strategierna, men med varierande styrka och betoningar. Den isländska, finska, norska och svenska strategierna lyfter klart fram att den nationella cybersäkerheten bäst kan påverkas i en internationell kontext genom samarbete i centrala internationella organisationer och institutioner som t.ex. EU, FN, OSSE , OECD (NCSS IS 2015; NCSS SE 2016; NCSS NO 2017; NCSS FI 2019). Den finska strategin är tydlig i att det internationella samarbete är en förutsättning för att höja den nationella cybersäkerhetsnivån. Den finska strategin positionerar på ett klart och tydligt sätt den finska nationella cybersäkerheten i en bredare utrikes- och säkerhetspolitisk kontext. Den finska strategin binds smidigt ihop med Finlands utrikespolitiska linjedragningar så väl som med EU:s gemensamma utrikes- och säkerhetspolitik. Denna positionering skiljer sig från de övriga strategierna. (NCSS FI 2019). Den svenska strategin understryker utvecklandet av internationellt samarbete för att minska på sårbarheten och öka på den nationella resiliensen (NCSS SE 2016). Medan den norska strategin gör gällande att de norska myndigheterna enligt strategin ska främja och påverka internationellt cybersäkerhetssamarbete, avtal beträffande statligt agerande i cyberomgivningen och cyberbrottsbekämpning på internationella arenor och forum (NCSS NO 2017).

Gemensamma teman som tre av de fem jämförda strategierna fäster uppmärksamhet vid är främjande och värnande om grundläggande rättigheter, friheter och demokratiska värderingar i de olika internationella sammanhangen där cybersäkerhets utvecklas eller behandlas. De viktigaste aspekterna gällande mänskliga rättigheter i en cyberkontext är yttrandefrihet, åsiktsfrihet och rätt till integritet. Den finska, norska och svenska strategin uttrycker alla klart att länderna ska arbeta för att mänskliga rättigheter och -friheter även respekteras i cybermiljön, att cybermiljön ska vara fri, stabil, tillgänglig och universell (NCSS FI 2013; NCSS SE 2016; NCSS NO 2017). Den finska strategin accepterar inte försök till att begränsa Internets frihet och öppenhet eller fundamentala mänskliga rättigheter (NCSS FI 2019). Den norska strategin understryker att det internationella samarbetet ska ske i samarbetet med näringslivet, den akademiska gemenskapen och övriga delar av civilsamhället. Vidare ska de norska myndigheterna sörja för en effektiv koordinering mellan de norska myndigheter som deltar i det internationella arbetet (NCSS NO 2017). Sverige strävar enligt den svenska strategin till att aktivt ta del i de internationella diskussioner och processer vars mål ligger i att

förbygga konflikter och arbeta för internationell konsensus beträffande standarder om ansvarsfullt statligt agerande i cyberomgivningen (NCSS SE 2016). De danska och den isländska strategierna tar inte ställning till grundläggande värderingar i samband med internationellt samarbete och ländernas internationella målsättningar (NCSS IS 2015; NCSS DK 2017).

Vidare ses internationellt samarbete som viktigt och i många strategier kopplas samarbetet ihop med nationella säkerhetsfrågor. Den isländska strategin lägger stark vikt på försvarsmässiga aspekter av internationellt samarbete. Strategin slår fast att grunden för den isländska säkerheten och försvaret ligger i samarbetet med Nato, de nordiska länderna och USA (NCSS IS 2015). Den finska strategin kopplar på ett klart och tydligt sätt samman den finska cybersäkerheten med EU:s allmänna utrikes och säkerhetspolitik. Den nationella cybersäkerheten kopplas vidare starkt ihop med nationella säkerhetssamarbeten Finland deltar i (NCSS FI 2019).

Lagstiftningsfrågor och myndighetssamarbete är något som lyfts fram i många av strategierna. De finska och svenska strategierna vill utveckla cyberbrottsbekämpningen i en internationell kontext (NCSS SE 2016; NCSS FI 2019). Mer allmänt talar alla strategier för mer fördjupat internationellt myndighetssamarbete (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017; NCSS NO 2017; NCSS FI 2019).

En del av strategierna tangerar de ekonomiska möjligheter ett lyckat cybersäkerhetsarbete kan för med sig och kopplingen till den internationella kontexten. Den svenska liksom den isländska och danska strategierna betonar den internationella aspekten i att skapa konkurrensfördelar och ekonomiska möjligheter (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017). Den finska strategin tangerar även ämnet, men inte lika starkt som de tre föregående gör (NCSS FI 2019). Den norska strategin tar tillsynes inte ställning till möjliga konkurrensfördelar och konkurrensaspekter i ett internationellt perspektiv. Den norska strategin efterlyser på ett allmänt plan ett starkare internationellt samarbete för att höja den nationella cybersäkerheten (NCSS NO 2017).

5 Nordiska cybersäkerhetsdilemman

5.1 Allmän överblick över dilemmana i de studerade strategierna

Som det framgår ur tabell 5 nedan förekommer det en del övergripande skillnader i hur de olika strategierna beaktat och betonat cybersäkerhetens fem dilemman. Rött anger lägsta betoning, gul högsta, x anger ifall perspektivet återfinns i strategin. Det förekommer skillnader i såväl innehåll som i själva betoningen och hur omfattande strategierna tagit dessa i beaktande. En överblick ger för det första för handen att de finska och norska strategierna inte alls tagit ställning till frågan om dataskydd mot utbyte av information. Den danska strategin har inte behandlat frågan om åsiktsfrihet mot politisk stabilitet. På dessa punkter har de nämnda strategierna inte tagit ställning till några av de centrala frågorna som enligt det teoretiska ramen anses höra till välavvägda cybersäkerhetsstrategier.

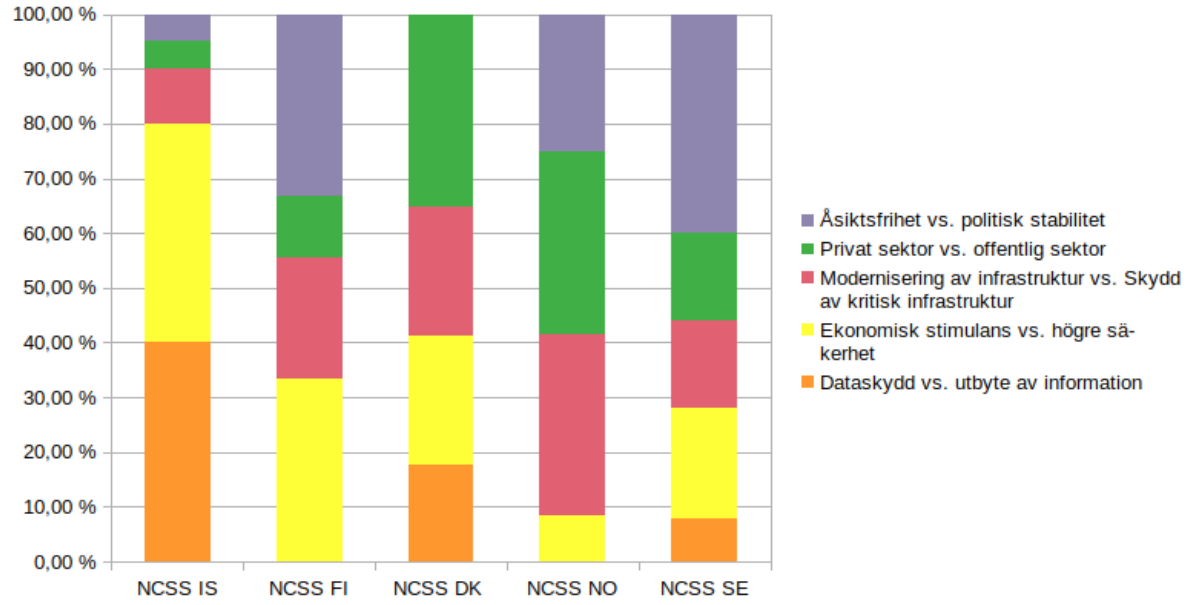
Tabell 5: Komparationsmatris över förekomst och betoning av de fem dilemmana i cybersäkerhetsstrategierna.

Kategori	NCSS IS	NCSS FI	NCSS DK	NCSS NO	NCSS SE
Dataskydd mot utbyte av information	x		x		x
Ekonomisk stimulans mot högre säkerhet	x	x	x	x	x
Modernisering av infrastruktur mot Skydd av kritisk infrastruktur	x	x	x	x	x
Privat sektor mot offentlig sektor	x	x	x	x	x
Åsiktsfrihet mot politisk stabilitet	x	x		x	x

De isländska, finska och svenska strategierna är lika i det att de relativt sett ger hög betoning på dilemmat ekonomisk stimulans mot högre säkerhet, medan de norska och danska strategierna däremot relativt sett ger högsta betoningar åt dilemmat privat sektor mot offentlig sektor. De finska och isländska strategierna har gemensamt i att de betonar sistnämnda dilemma relativt sett svagast. De svenska och danska strategierna är lika i att de relativt sett betonar dilemmat dataskydd mot utbyte av information lägst. Ifall man bortser från avsaknaden av två dilemman i de finska, danska och norska strategierna så har de studerade strategierna tämligen väl lyckats beakta de olika frågor som hänger i hop med välavvägda

cybersäkerhetsstrategier. Figur 2 nedan visar på de olika dilemmanas inbördes förhållande och vikt i de olika studerade strategierna.

Figur 2: Betoningar på dilemmana i de nordiska cybersäkerhetsstrategierna.



5.2 Åsiktsfrihet mot politisk stabilitet

Dilemmat åsiktsfrihet mot politisk stabilitet nämns i fyra av de fem jämförda strategierna. Temat nämns i Islands, Finlands, Norges och Sveriges strategier. Den isländska strategin betonar dilemmat relativt sett svagast av de förutnämnda fyra strategierna (NCSS IS 2015; NCSS SE 2016; NCSS NO 2017; NCSS FI 2019). Den danska strategin tar inte ställning till dilemmat en enda gång (NCSS DK 2017). De övriga länderna kopplar starkt ihop frågan med internationellt arbetet för cybersäkerhet medan Island närmast verkar se det som intern angelägenhet och målsättning. Gemensamt för det strategier som har behandlat dilemmat är att de ser mänskliga rättigheter, legalitet, öppenhet, tillgänglighet och frihet i cybermiljön som något centralt även i cyberomgivningen och något som förstärker den nationella cybersäkerheten och skapar förtroende för cyberomgivningen bland medborgarna. Den finska strategin understryker explicit att Finland inte accepterar målsättningar som strävar till att begränsa nätets frihet och öppenhet eller de individuella fundamentala rättigheterna och friheterna hos individer (NCSS FI 2019). Dessa aspekter ses som så centrala och

grundläggande för det nationella säkerhetsarbetet att de grundar en central målsättning att arbeta för i den internationella cyberkontexten.

5.3 Ekonomisk stimulans mot högre säkerhet

Dilemmat ekonomisk stimulans mot högre säkerhet omnämns i alla strategier, men med olika omfattning och vikt. Starkast förekommer temat i den isländska strategin och svagast i den norska och då också bara förbigående och indirekt. Island lägger stark betoning på temat. Den norska strategin tangerar ämnet endast ytligt och begränsat (NCSS NO 2017) medan de övriga fyra strategierna har behandlat frågan om ekonomisk stimulans relativt omgående (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017; NCSS FI 2019). De strategier som tagit ställning till dilemmat verkar inte se ekonomisk stimulans mot högre säkerhet som direkta motsättningar. Snarare ses en högre nationell cybersäkerhet bygga en stabil grogrund och erbjuda nya ekonomiska möjligheter, som är nationerna till nytta i en global kontext. De nordiska strategierna lyfter fram lite olika aspekter gällande vad som borde beaktas för att främja ekonomisk stimulans, men gemensamt är att alla klart har en strävan att försöka utveckla en nationella konkurrenskraften i en internationell kontext. Cybersäkerheten är en grundpelare till det isländska ekonomiska välståndet och vilar på sofistikerad medvetenhet om säkerhetsfrågor och riktig lagstiftning. Den isländska strategin betonar dilemmat speciellt starkt och understryker att en cybersäker digital miljö i framtiden är en värdefull exportprodukt. Utvecklandet av den isländska digitala miljön bidrar med högre säkerhet och gör den på så sätt mer konkurrenskraftig i den internationella kontexten och en stark exportprodukt. Islands förmåga att bekämpa cyberbrottslighet är en nödvändig förutsättning för att Island ska kunna dra full nytta av de sociala och ekonomiska möjligheter Internet erbjuder (NCSS IS 2015). Även den danska strategin gör en stark och den svenska en något svagare koppling mellan cybersäkerhet och konkurrensfördelar. De svenska och danska strategierna gör gällande att företagen kan dra stor nytta av den digitala ekonomin och att säkerheten direkt påverkar de ekonomiska aspekterna (NCSS SE 2016; NCSS DK 2017). Den finska strategin beaktar temat, men positionerar sig ganska försiktigt till att skapa konkurrensfördelar och utnyttja cybersäkerheten som en konkurrensfördel. Privata företags

konkurrensfördelar uppnås enligt strategin genom ett standardiserat säkerhetsarbete och utvecklande av produkter med inbyggd säkerhet (NCSS FI 2019).

5.4 Dataskydd mot utbyte av information

Dilemmat dataskydd mot utbyte av information betonas inte alls i de finska och den norska strategierna, svagt i den svenska, medelmåttigt i den danska och starkast i den isländska strategin.

Den isländska strategin identifierar relativt tydligt svåra frågor som hänger ihop med detta dilemmat. Den danska strategin lyfter fram frågor angående dataetiska överväganden och behovet av en mer omgående dataskyddsstrategi. Den danska strategin lyfter fram en målsättning som är förknippat med dilemmat ifråga, nämligen att införa en ”Tech-ambassadör” till vars uppgifter bland annat skulle höra främjandet dataskyddsfrågor gentemot stora globala teknologibolag (NCSS DK 2017). Den svenska strategins betoning på dilemmat är rätt allmänt, med några få omnämnanden som är väldigt allmänna (NCSS SE 2016). Den isländska strategin lyfter starkt fram att missbruket av personlig information ska förhindras och dataskyddet bör stärkas. Å ena sidan kräver en förhöjd cybersäkerhet mer omfattande övervakning av de digitala miljöerna samtidigt som skyddet av personuppgifter måste kunna garanteras (NCSS IS 2015). Dessa två målsättningar är svårförenliga och kräver noggranna överväganden. Fastän t.ex. den isländska strategin tydligast av alla har lyft fram centrala element som hänger ihop med dilemmat, kan dilemmat snarare karaktäriseras som vidrört än som utförligt behandlat i alla de strategier som tangerat frågan.

Ingen av de förutnämnda strategierna berör egentligen problematiken kring dataskydd och förhöjd nationell cybersäkerhet. Jämförelsen ger för handen att dilemmat nog vidrörts i en del strategier, medan andra överlag inte beaktat det. Behandlingen av problemen i anknytning till dilemmat är ytligt i alla strategier som beaktat det, även i den isländska som behandlat ämnet mest omgående.

5.5 Modernisering av infrastruktur mot skydd av kritisk infrastruktur

Alla jämförda strategier har behandlat dilemmat modernisering av infrastruktur mot skydd av kritisk infrastruktur på ett eller annat sätt (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017; NCSS NO 2017; NCSS FI 2019). Tydligast har frågor i anknytning med dilemmat behandlats i den norska och isländska strategierna (NCSS IS 2015; NCSS NO 2017). I den isländska strategin fästs uppmärksamhet speciellt vid planering av lösningar som berör den kritiska infrastrukturer (NCSS IS 2015). Den norska strategin har relativt sett en stark och omfattande betoning på frågan. Den norska strategin uppmärksammar problematiken kring ny teknik, komplexa omgivningar och att det finns ett ständigt behov av att minska kostnaderna och och öka tillgången på kompetens (NCSS NO 2017). De olika intressena är klart identifierade i den norska strategin. Dessa intressen kan vara svårförenliga och lätt skapa målsättningar som är i konflikt med varandra. Den finska strategin fäster speciell uppmärksamhet vid kravhanteringen och kraven som riktas till säkerhetskritisk service (NCSS FI 2019). Den danska strategin vill identifiera och kartlägga kritisk infrastruktur med syfte att rikta åtgärder och modernisera den kritiska infrastrukturen (NCSS DK 2017). Den svenska strategin tangera i sig inte själva problematiken kring att modernisera mot att öka säkerheten, men strategin tar på fler ställen upp att mycket grundläggande funktioner borde utvecklas eller förnyas så att de erbjuder mer säkra omgivningar (NCSS SE 2016).

Speciellt den norska och även i någon mån den isländska strategin ser inte modernisering som en motsats mot skydd, utan snarare som en förutsättning för att bättre kunna skydda den kritiska infrastrukturen. God planering och robusta pålitliga lösningar ökar den kritiska infrastrukturens säkerhet och skydd (NCSS IS 2015; NCSS NO 2017).

5.6 Den privata sektorn mot den offentliga sektorn

Synpunkter på dilemmat ”den privata sektorn mot den offentliga sektorn” finns beaktade i alla de studerade strategierna. Betoningarna mellan strategierna varierar. Dilemmat har relativt sett lägst betoning i de isländska och finska strategierna högst i de danska och norska strategierna (NCSS IS 2015; NCSS DK 2017; NCSS NO 2017; NCSS FI 2019). Den finska

strategin nämner inte specifikt problematiken kring den privata och offentliga sektorn. Strategin känner dock igen att det förekommer olika aktörer inom samhället som påverkar och bidrar till den nationella cybersäkerheten och lyfter fram att allas insatser krävs. Själva problematiken tangeras dock inte och på denna punkt skiljer sig den finska strategin från de övriga strategierna (NCSS FI 2019).

Ett tämligen genomgående tema gällande problematiken i alla strategier är att den offentliga sektorn inte ensam klarar av de utmaningar som samhällena står inför. De privata aktörernas bidrag och engagemang behövs för att kunna utveckla den nationella cybersäkerheten. Nya sätt att samarbeta behövs över de invanda gränserna. Olika förslag till samarbetsarenor och sätt tas upp i den isländska, danska och norska strategierna. Utbyte av information ses som speciellt viktigt i detta sammanhang och hindren för utbyte borde röjas så långt som möjligt.

Alla andra strategier, inkluderat den isländska, känner igen och har behandlat problematiken mer ingående. De strategier som tangerar dilemmat understryker att cyberomgivningen är en komplex helhet med en rad olika aktörer representerande en rad olika branscher och sektorer. Myndigheterna kan inte själva lösa utmaningarna som är förknippade med nationell cybersäkerhet (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017; NCSS NO 2017). Speciellt fäster de danska och norska strategierna uppmärksamhet vid att en stor del av den kritiska infrastrukturen ägs och opereras av privata aktörer (NCSS SE 2016; NCSS DK 2017; NCSS NO 2017). Vidare understryker den norska strategin att en stor del av de beslut som berör utveckling och säkerhet i cyberomgivningen görs av kommersiella eller icke-statliga organisationer. Ur ett internationellt perspektiv görs besluten utanför de traditionella mellanstatliga arenorna (NCSS NO 2017). Då det gäller målsättningar för att utveckla samarbete eller det identifierade förhållandet har strategierna olika utgångspunkter. Den isländska strategin föreslår inrättandet av ett cybersäkerhetsforum för att öka koordinering och samarbete mellan offentligt och privat (NCSS IS 2015). De danska och norska strategierna eftersträvar ett stärkt cybersäkerhetssamarbetet mellan privat och offentligt. Strategierna nämner en rad åtgärder som t.ex. olika samarbetsformer, informationsutbyte, dialoger, partnerskap och kunskapsutbyte (NCSS SE 2016; NCSS DK 2017; NCSS NO 2017). Den svenska strategin skiljer sig något från de övriga strategierna. Till skillnad från de andra nämns inte utvecklingsåtgärder som syftar på jämbördiga samarbetsformer eller partnerskap.

Den svenska strategin understryker däremot på många punkter starkare myndighetstillsyn, riktat mot privata aktörer (NCSS SE 2016). I och för sig nämns även myndighetstillsyn i den norska strategin som ett redskap för ökad cybersäkerhet. I den norska strategin verkar tillsynen dock vara ett redskap bland andra som inte ges speciellt utrymme i den norska strategin. Den norska strategin ser att myndigheterna har en viktig roll som lagstiftare, facilitatorer och tillsynsparter (NCSS NO 2017). De övriga strategierna betonar däremot mer samarbete än ökad tillsyn. Tillsyn kan kanske ses som motsatsen till partnerskap, eftersom det grundar sig på förpliktande säkerhetsbestämmelser och övervakning och sätter således aktörerna i olika position i förhållande till varandra. Den finska strategin behandlar inte specifikt problematiken kring den privata och offentliga sektorn (NCSS FI 2019).

Gemensamt för alla strategier verkar vara att de ser cybersäkerheten som allas ansvar. Som en del av detta ansvar ska var och en sörja och ansvara för sin egen säkerhet och på detta sätt bidra till en ökad nationell säkerhet.

6 Nordiska cybersäkerhetsmandat

6.1 Allmän överblick över cybersäkerhetsmandaten i de studerade strategierna

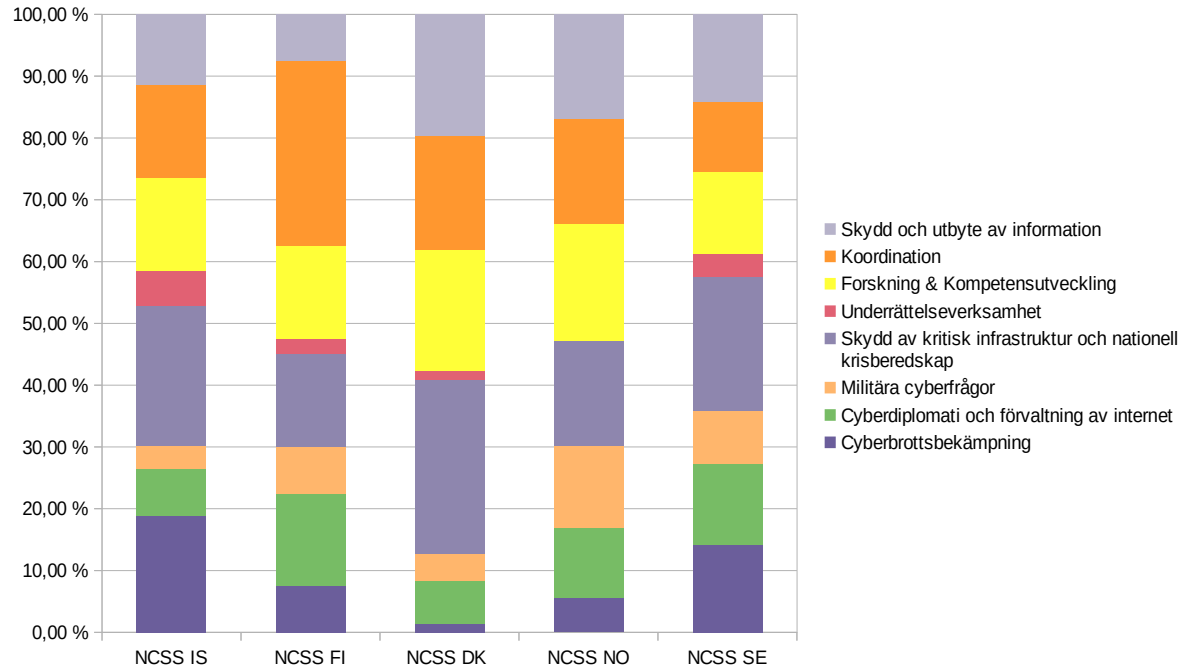
Som det framgår ur tabell 6 nedan förekommer det en del övergripande skillnader i hur de olika strategierna beaktat och betonat cybersäkerhetens fem mandat och de tre tvärmandaten. Rött anger lägsta betoning, gul högsta, x anger ifall perspektivet återfinns i strategin. En snabb överblick ger för handen att alla mandat finns beaktade i alla förutom en strategi. Den enda större avvikelsen i strategierna verkar vara att den norska strategin inte beaktar mandatet underrättelseverksamhet. Dock ät betoningen även i de övriga strategierna gällande underrättelseverksamhet relativt sett låg. Gemensamt för de isländska, danska och svenska strategierna är att alla lägger starkast betoning på mandatet skydd av kritisk infrastruktur och nationell krisberedskap. Den finska strategin lägger stark betoning på koordinering och den norska på forskning.

Tabell 6: Komparationsmatris över förekomst och betoning av mandaten i de nordiska cybersäkerhetsstrategierna.

Kategori	NCSS IS	NCSS FI	NCSS DK	NCSS NO	NCSS SE
Cyberbrottsbekämpning	x	x	x	x	x
Cyberdiplomati och förvaltning av internet	x	x	x	x	x
Militära cyberfrågor	x	x	x	x	x
Skydd av kritisk infrastruktur och nationell krisberedskap	x	x	x	x	x
Underrättelseverksamhet	x	x	x		x
Forskning	x	x	x	x	x
Koordination	x	x	x	x	x
Skydd och utbyte av information	x	x	x	x	x

Figur 3 nedan synliggör de olika mandatens inbördes förhållande och styrka i de studerade strategierna. En överblick ger för handen att alla strategier fäster högst vikt vid skydd av kritisk infrastruktur och nationell krisberedskap, forskning, koordinering samt skydd och utbyte av information.

Figur 3: Betoning av mandaten i de nordiska cybersäkerhetsstrategierna.



6.2 Cyberbrottsbekämpning

Mandatet cyberbrottsbekämpning har behandlats i alla strategier. Mandatet har i de olika strategierna betonats med olika styrka. Starkast är området tangerat i den isländska strategin och svagast i den danska. Den danska strategin nämner mandatet med en punkt (NCSS DK 2017). Som redan tidigare framkommit kopplar den isländska strategin effektiv ihop cyberbrottsbekämpning med möjligheten till att skapa gynnsamma ekonomiska konkurrensfördelar. Målet är delvis att höja den isländska nationella cybersäkerheten men även att göra den isländska cyberomgivningen så oattraktiv som möjligt för kriminella aktörer (NCSS IS 2015). De isländska, norska, svenska och finska strategierna lyfter fram vikten av internationellt samarbete inom området (NCSS IS 2015; NCSS SE 2016; NCSS NO 2017; NCSS FI 2019). Alla strategier talar på ett eller annat sätt för att öka polisens förutsättningar att bekämpa cyberbrottslighet. Den svenska strategin förespråkar speciellt förebyggande verksamhet inom området (NCSS SE 2016). De finska, isländska och svenska strategierna lyfter fram utvecklandet av lagstiftning så att den bättre svarar på de nya utmaningarna (NCSS IS 2015; NCSS SE 2016, 2016). Den isländska strategin understryker att Islands

cyberbrottsbekämpning och lagstiftning ska vara på samma nivå som de övriga nordiska ländernas (NCSS IS 2015). Detta indikerar på att lagstiftningen av en eller annan orsak inte uppleva vara på samma nivå som de övriga nordiska ländernas, då det gäller effektiv cyberbrottsbekämpning. Någon vidare utvärdering om lagstiftningens effektivitet eller nivå finn inte i den isländska strategin. Den lagstiftningsmässiga aspekten är inte framträdande i den danska eller den norska strategin. De finska, norska och svenska strategierna fäster uppmärksamhet vid förebyggande brottsbekämpningsarbete (NCSS SE 2016; NCSS NO 2017; NCSS FI 2019), något som inte uttryckligen förekommer i de övriga strategierna. Den norska strategin verkar i jämförelse vara tydligast och precisast då det gäller formulerade målsättningar för mandatet. Allmänt taget har mandatet beaktats i relativt väl i alla strategier förutom den danska.

6.3 Cyberdiplomati och förvaltning av Internet

Mandatet cyberdiplomati och förvaltning av Internet beaktas i alla de studerade strategierna De nordiska ländernas strategier verkar i regel ha lyft fram relevanta och aktuella frågor som relaterar till mandatet. Starkast betonas det i den finska strategin och svagast i den danska. Gemensamt för alla strategier är att de lyfter fram vikten av mandatet och det internationella samarbete för den nationella cybersäkerheten. Alla strategier eftersträvar generellt sett ett ökat internationellt samarbete och alla strategier omnämner de viktigaste organisationerna och arenorna där cybersäkerhetsarbete görs som t.ex. FN, Nato, EU, OECD, OSCE (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017; NCSS NO 2017; NCSS FI 2019). Den svenska strategin nämner specifikt de för Internets förvaltning centrala organisationerna som ICANN, IETF, ITU och IGF (NCSS SE 2016) och den finska lyfter fram internationellt samarbetet på såväl den politiska som den tekniska nivån, vilket kan tolkas syfta på just förutnämnda centrala organisationer (NCSS FI 2019). Skillnader förekommer i vad som lyfts fram som viktigt och vilka åtgärder som ska tas. De isländska, finska, norska och svenska strategierna understryker vikten med att påverka de nationella målsättningarna inom ramen för de befintliga internationella forumen och arenorna som existerar. De viktigaste målen för dessa strategier är en säkrare cybermiljö som beaktar de grundläggande demokratiska värderingarna och mänskliga rättigheterna (NCSS IS 2015; NCSS SE 2016; NCSS NO 2017; NCSS FI

2019). Såväl den norska, danska som isländska strategin fäster uppmärksamhet vid koordinering och samordning mellan de parter som representerar länderna på de internationella arenorna (NCSS IS 2015, 2015; NCSS NO 2017). Speciellt betonas detta i den danska strategin (NCSS DK 2017). Den svenska och den finska strategin lyfter skilt fram utvecklandet av diplomatiska och politiska mekanismer för att verifiera, peka ut och utkräva ansvar samt motåtgärder som kan användas då en nation utsätts för cyberangrepp (NCSS SE 2016; NCSS FI 2019). Den danska strategin är den enda som klart och tydligt lägger ambitioner på att förstärka koordineringen och insatserna på den diplomatiska arenan genom att utnämna en ”tech-ambassadör” och en ny cyberkoordinatorstjänst vid det danska utrikesministeriet. Syftet med den nya koordinatorn är att på så sätt höja på den internationella representationen och samarbetet. (NCSS DK 2017). De svenska, norska och finska strategierna lägger specifikt vikt vid nordiskt regionalt samarbete (NCSS SE 2016; NCSS NO 2017; NCSS FI 2019).

6.4 Militära cyberfrågor

Militära cyberfrågor lyfts starkast fram i de svenska och norska strategierna, men mandatet har beaktas i alla strategier. Svagast är betoning i den isländska strategin. Den isländska strategin understryker snarare olika aspekter gällande försvarssamarbete än direkt satsningar på militära cyberförmågor och speciellt nämns samarbetsparter som Nato och USA i detta sammanhang. Den isländska strategin understryker att samarbetet med Nato inom cyberområdet kommer att fördjupas och att Nato gjort gällande att även cyberattacker kan klassificeras hörande under Nato-fördragets 5:e artikel (NCSS IS 2015). På samma sätt understryker även den norska strategin att kan en cyberangrepp betraktas som en ”väpnad attack” som kan utlösa en nations rätt till självförsvar (NCSS NO 2017). Dessa konstaterande kan ses som direkta försvarsmässiga och tydliga markering inom cyberdomänen, något som inte återfinns i de tre övriga strategierna. Att detta inte nämns i de övriga strategierna betyder inte direkt att det inte skulle utarbetas eller utvecklas försvarsmässiga motåtgärder. Däremot berättar det något om viljan att klart och tydligt signalera dessa frågor utåt.

De norska och danska strategierna talar explicit om utvecklandet om direkta cyberoperativa försvarsförmågor (NCSS DK 2017; NCSS NO 2017). Även de svenska och den finska

strategierna vill utveckla det nationella cyberförsvaret, men är inte lika explicita i sina uttryck (NCSS SE 2016; NCSS FI 2019). Den svenska strategin gör dock klart för sig att Sverige ska ha ett utvecklat cyberförsvar för att kunna möta och hantera angrepp från kvalificerade motståndare i cyberrymden (NCSS SE 2016). De finska och danska strategierna vill båda utveckla den militära cyberunderrättelseverksamheten (NCSS DK 2017; NCSS FI 2019). Förövrigt verkar den finska strategin ganska sparsam i sina uttalanden om utvecklandet av militära cyberförmågor.

Gemensamt för alla verkar vara viljan att utveckla ett trovärdig cyberförsvarsförmåga som ger nationerna nationell handlingsfrihet och en trovärdig handlingsförmåga även i cybermiljön. Klarast på denna punkt är den danska, norska och svenska strategierna. Den norska strategin vill fördjupa samarbetet mellan civilsamhället och militären för att bättre kunna svara på utmaningarna genom vad de kallar för totalförsvarsmodellen. Strategin understryker att försvarssektorn är beroende av civil digital infrastrukturer och tjänster (NCSS NO 2017). Danmark har en något liknande mekanism med sitt så kallade försvarsavtal som engagerar ett bredare lager aktörer än enbart militären kring försvarsfrågor (NCSS DK 2017). Den svenska strategin riktar i första hand sina cyberförsvarsinsatser för att skydda kritisk infrastruktur (NCSS SE 2016).

6.5 Skydd av kritisk infrastruktur och nationell krisberedskap

Skydd av kritisk infrastruktur och nationell krisberedskap är rikligt representerat i alla strategier. Variationer mellan de interna betoningarna i strategierna förekommer. De isländska, danska och svenska strategierna betonar mandatet starkast (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017). Den danska strategin betonar mandatet starkast i jämförelse av dessa tre strategier (NCSS DK 2017). Alla strategier uttrycker på ett eller annat sätt att stödåtgärder måste riktas till de aktörer som upprätthåller kritisk infrastruktur för att garantera en hållbar utveckling (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017; NCSS NO 2017; NCSS FI 2019). Den isländska strategin är aningen otydlig då det gäller strategiska verksamhetsmål riktade mot den kritiska infrastrukturen. Den isländska målsättningen är att öka resiliensen på isländsk infrastruktur och informationssystem, så att resiliensen är jämförbar med de övriga

nordiska ländernas. Detta uttalande antyder på att resiliensnivån är på en lägre nivå eller icke jämförbar med de övriga nordiska ländernas (NCSS IS 2015). Den svenska strategin kommer med få konkreta nationella verksamhetsmål och förlitar sig snarare på att säkerhetsarbetet gällande den kritiska infrastrukturen implementeras genom Europeiska unionens direktiv om säkerhet i nät- och informationssystem (NIS-direktivet) (NCSS SE 2016). De danska, isländska och norska strategierna lyfter fram behovet av att utvecklingsarbetet med riskbedömning inom cybersäkerhetsområdet (NCSS IS 2015; NCSS DK 2017; NCSS NO 2017). De svenska och finska strategierna lyfter fram att särskilt kritiska verksamheter ska stödas med satsningar på speciell teknisk detekterings- och varningslösningar som staten sörjer för (NCSS SE 2016; NCSS FI 2019). Förbättrad cybersäkerhet inom den offentliga administrationen förespråkas särskilt i den danska, isländska och finska strategierna (NCSS IS 2015; NCSS DK 2017; NCSS FI 2019). Den norska och svenska strategin efterlyser beredskapsövningar riktade till aktörer med kritisk digital infrastruktur (NCSS SE 2016; NCSS NO 2017).

De finska och den norska strategierna lägger upp som mål att identifiera kritisk infrastruktur och definiera utvecklande åtgärder skyddet av ifrågavarande infrastruktur (NCSS NO 2017; NCSS FI 2019). De danska och svenska strategierna har däremot definierat eller identifierat de sektorer som utvecklande åtgärder bör riktas till. Den danska strategin pekar ut ett antal sektorer vilka kräver speciell uppmärksamhet: energi, transport, telekommunikation, hälsovård och den maritima sektorn (NCSS DK 2017). Den svenska strategin fäster uppmärksamhet vid branscher som eldistribution, vattenförsörjning, transportinfrastruktur, hälso- och sjukvård och industriella verksamheter (NCSS SE 2016).

6.6 Underrättelseverksamhet

Mandatet underrättelseverksamhet nämns i alla strategier förutom den norska. Överlag har mandatet fått en mycket svag betoning i alla de studerade strategierna. Mandaten omnämns bara ett fåtal gånger per strategi (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017; NCSS NO 2017; NCSS FI 2019). Den isländska strategin efterlyser en förmåga att kunna upptäcka och bekämpa spionage, men nämner inget om att utveckla egna cyberunderättelsförmågor (NCSS IS 2015). Behoven kring detta mandat verkar väldigt starkt utgå från var och en nations egna

behov och aktuella läge. De finska, danska och svenska strategierna uttrycker alla en vilja att vidareutveckla de förmågor som redan finns på området och fördjupa myndighetssamarbetet kring frågan (NCSS SE 2016; NCSS DK 2017; NCSS FI 2019). Målet är överlag att utveckla och trygga den nationella säkerheten genom att utveckla den nationella cyberunderrättelseverksamheten.

6.7 Forskning

Tvärmandatet forskning har som ovan redan nämnts, utvidgats och innefattar även betoningar på allmän kompetensutveckling inom cybersäkerhetsområdet. Alla strategier nämner ambitioner och strävanden i samband med mandatet forskning (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017; NCSS NO 2017; NCSS FI 2019). Starkast finns detta tvärmandat närvarande i den norska strategin (NCSS NO 2017). Då det gäller den nationella kompetensutvecklingen har alla strategier klart uttryckta önskemål om att den allmänna cybersäkerhetskompetensen i samhället borde ökas. Alla strategierna förespråkar stansningar på området. Hur detta ska förverkligas och vart insatserna ska riktas varierar från strategi till strategi. En del av målsättningarna i strategierna är bättre avgränsade och riktade andra. Speciellt sådana mål som allmänt riktar sig till hela samhället på bred front kan vara svåra att förverkliga på grund av att de saknar klara målgrupper och avgränsningar. Alla strategier innehåller uttalanden gällande utvecklandet av kompetenser som inte är tydligt avgränsade och riktade (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017; NCSS NO 2017; NCSS FI 2019). Den isländska strategin vill till exempel att kunskapsbasen hos individer, den offentliga förvaltningen och företagen (NCSS IS 2015)och den finska att var och en har tillräckliga kunskaper för att säkert kunna använda sig av den digitala miljön (NCSS FI 2019).

Många av strategierna efterlyser utvecklandet av läroplaner och utbildningsprogram på olika skolstadier så att de bättre beaktar samhällets kompetensbehov i frågan om cybersäkerhet. Speciellt de danska och finska strategierna är tydliga på att utveckla läroplanerna på de olika stadierna så att de bättre tar cybersäkerheten i beaktande (NCSS DK 2017; NCSS FI 2019). Ämnet forskning tangeras inte i den isländska strategin (NCSS IS 2015). På denna punkt skiljer sig den isländska strategin från alla de andra studerade strategierna. De övriga nordiska strategierna nämner satsningar på forskning inom cybersäkerhetsområdet. Den svenska

strategin ämnar speciellt rikta forskningsinsatser på utvecklingen av säkerhet in industriella styrsystem (NCSS SE 2016). Den danska strategin kopplar även ihop forskning med målet om ökad nationell kompetensutveckling (NCSS DK 2017). De finska, svenska och norska strategierna vill öka övningsverksamhet som ett led i att öka den nationella cybersäkerhetskompetensen (NCSS SE 2016; NCSS NO 2017; NCSS FI 2019).

Den isländska strategin lyfter fram en intressant aspekt gällande utvecklande av gemensam terminologi. Strategin vill att relevant terminologi ska definieras för att underlätta förståelsen för cyberrelaterade fenomen inom samhället (NCSS IS 2015).

De finska och svenska strategierna lyfter fram övningsverksamhet som kompetensfrämjande målsättningar som är eftersträvansvärda (NCSS SE 2016; NCSS FI 2019).

6.8 Koordinering

Eftersom koordinering är ett tvärgående mandat förekommer det omnämnanden i olika sammanhang igenom strategierna. Koordinering betonas internt jämförelsevis starkast i den finska strategin (NCSS FI 2019). Alla strategier identifierar behovet av koordinering av cybersäkerhetsarbetet mellan den offentliga och privata sektorn (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017; NCSS NO 2017; NCSS FI 2019). Alla de nordiska strategierna understryker koordinering och samarbete speciellt mellan den offentliga och privata sektorn och då det gäller den kritiska infrastrukturer. Koordinering och informationsutbyte gällande en bättre nationell lägesbild och uppdagande, hantering av och motåtgärder mot cyberhändelser nämns likaså i alla strategierna (NCSS IS 2015; NCSS SE 2016; NCSS DK 2017; NCSS NO 2017; NCSS FI 2019). De danska, finska och norska strategierna efterlyser starkare koordinering gällande internationell cybersäkerhetsverksamhet (NCSS DK 2017; NCSS NO 2017; NCSS FI 2019). Som redan tidigare nämnts uttrycker den danska strategin ambitioner i att förstärka och utveckla en internationella koordineringen gällande cybersäkerhetsärenden (NCSS DK 2017). Även den finska strategin betonar speciellt koordinering och samarbete inom EU (NCSS FI 2019).

Den finska strategin verkar skilja sig åtminstone på en punk från de övriga strategierna och det är ambitionen att klart centralisera nationella koordineringen av cybersäkerhetsarbetet på

nationell nivå genom inrättande av en ny tjänst till vars ansvar hör den nationella koordineringen (NCSS FI 2019).

6.9 Skydd och utbyte av information

Mandatet skydd och utbyte av information har beaktats i alla strategier. Skydd av information och informationsresurser verkar i strategierna tolkats i bred mening med en rad olika kontexter och åtgärder som lyfts fram. Internationellt samarbetet och informationsutbyte lyfts fram av Island som en viktig förutsättning för att kunna skydda de nationellt viktiga resurserna. Strategin strävar till att skapa förhållanden som tillåter snabbt informationsutbyte mellan involverade parter och relevanta aktörer i syfte att minimera skador, försnabba utredningsprocesser och möjliggöra att hoten kan skötas så smidigt och snabbt som möjligt (NCSS IS 2015). De övriga strategierna fokuserar mer på internt nationellt informationsutbyte och koordineringen kring denna fråga. De finska, danska, norska och svenska strategierna betonar nationella incidenthanteringsmodeller och förstärkande av nationella cybersäkerhetsmyndigheternas roll i detta sammanhang (NCSS SE 2016; NCSS DK 2017; NCSS NO 2017; NCSS FI 2019). Effektiverade incidenthanteringsmodeller fungerar som skyddsmekanismer och knutpunkter för utbyte av relevant information. Gemensamt är att de olika länderna strävar efter att utveckla mekanismer som underlättar informationsutbytet mellan relevanta parter och bidrar till att förbättra den nationella lägesbilden. Alla länder har ambitioner inom området. Informationsdelningen gällande hot, risker och säkerhetsåtgärder möjliggör att skyddet hos enskilda aktörer anpassas på ett effektivt sätt.

De svenska och danska strategierna är aningen mer detaljerad speciellt då det rör sig om enskilda lösningar för att skydda informationen än de övriga strategierna. Den svenska strategin efterlyser satsningar på utveckling av nationella krypteringslösningar och den danska att utveckla säkra kommunikationslösningar för statliga myndigheterna (NCSS SE 2016; NCSS DK 2017).

De isländska och danska strategierna lägger speciell vikt vid dataskydd. Den isländska strategin betonar skyddet av personuppgifter som ett svar på den snabbt utvecklade tekniken (NCSS IS 2015). Den danska strategin vill å sin sida utveckla säkra digitala identiteter så att nyttjandet av nättjänster är och upplevs som tryggt (NCSS DK 2017).

7 Slutsatser

Forskningen kring cybersäkerhet i allmänhet och cybersäkerhetsstrategier i synnerhet är ett relativt nytt område. Detta innebär att förståelsen för vad cybersäkerhet är, hur det ska förstås i en nationell kontext och hur nationer på bästa sätt kan påverka och kanske förbättra den nationella cybersäkerheten är varierande. Meningen med studien har delvis varit öka förståelsen kring nationella cybersäkerhetsstrategier och deras roll som centrala styrdokument för nationell säkerhet och delvis att mer ingående granska hur strategierna via sina formuleringar och betoningar kan lägga vikt på olika saker. Vidare har studien belyst vilka komplexa och viktiga avvägningar och frågeställningar som ligger bakom nationella cybersäkerhetsstrategier och som nationerna på ett eller annat sätt är tvungna att ta ställning till.

Denna studie har gett en fördjupad inblick i och förståelse för hur nationella cybersäkerhetsstrategier kan skilja sig åt och utformas trots att de nationer vars cybersäkerhetsstrategier granskats har mycket gemensamt såväl politiskt, kulturellt som ur ett nationellt säkerhetsperspektiv. Studien har belyst skillnader i betoningar och studerat hur väl de studerade strategierna tagit centrala frågeställningar och avvägningar, som anses avgörande för välavvägda nationella cybersäkerhetsstrategier, i beaktande.

Oberoende skillnaderna i strategierna och de nationsspecifika utgångslägena verkar det i regel som om de studerade strategierna tagit de centrala frågeställningarna och avvägningarna tämligen väl i beaktande. Det förkommer dock märkbara skillnader i betoningar på olika områden mellan de studerade strategierna. Några få teman är inte alls behandlade i tre av de studerade strategierna.

Denna studie har genom tematisk innehållsanalys baserad på de tidigare presenterade teoretiska ramverken, jämfört de studerade strategierna och deras interna betoningar mot varandra, för att komma åt skillnader och likheter. Resultaten är deskriptiva till sin natur. På grund av strategiernas olika struktur, utformning och det faktum att de klart är riktade till olika målgrupper har tolkningen och således även analysen av innehållet ställvis varit utmanande. Alla strategier är inte lika tydliga och precisa i avgränsning och riktande av

åtgärder trots att de tangerar samma saker. Trots många likheter i kommunicerade teman målar var och en strategi upp en bild om målsättningar och åtgärder som tycks anknyta till just det landets utvecklingsskede och behov. Otydligheten i formuleringar och åtgärder eller avsaknaden av viktiga avvägningar kan å sin sida leda till strategierna är till liten eller ingen nytta, då det gäller att hitta en väg till ett säkrare digitalt sammanlänkat samhälle.

7.1 Diskussion

Trots att de nordiska cybersäkerhetsstrategierna innehåller mycket likheter och lyfter fram liknande frågor förekommer det fortfarande en klar variation vad gäller nationella prioriteringar, betoningar och konceptualisering av utmaningar i enlighet med vad Cordey och Dewar (2019) kommit fram till.

Johnsen (2015) och Luiijf, Besseling & Graaf (2013) efterlyste i sina studier att cybersäkerhetsstrategier mer ingående borde ta ställning för att utarbeta gemensamma begreppsdefinitioner inom området för att på detta sätt lägga grunden för ett bättre internationellt samarbete och för att skapa en gemensam nationell förståelse för området. Vidare argumenterade Johnsens studie för en vidaredefinition av begreppet ”cybersäkerhet”. De nordiska strategierna har i största allmänhet tämligen väl definierat vad just de menar med de centralaste begreppen som behandlas i respektive strategier. Island har som enda strategi efterlyst utarbetande av mer precisa och omfattande begreppsdefinitioner. I och för sig har det t.ex. i Finland sedan tidigare, innan den nya strategin trädde i kraft, redan utarbetats en nationell begreppsordlista för cybersäkerhetsområdet (Sanastokeskus TSK ry 2018).

På grund av de olika utformningarna och utgångspunkterna i de jämförda nationella strategierna ser betoningarna olika ut. Målsättningarna och verksamhetsmål i en del av strategierna verkar bristfälligt avgränsade och identifierade för att klart kunna rikta effektiva åtgärder till de målgrupper och områden där verkan skulle vara störst. Allmänna exempel på dylika områden i strategierna är t.ex. kompetensutveckling och skydd av kritisk infrastruktur. Kompetensutveckling strävar till att höja den nationella medvetenheten om cyberrelaterade risker. Den nationella cybersäkerheten kommer inte att höjas ifall nivån på vetskap och kompetens är på låg nivå. För att höja den allmänna kompetensen finns det ett behov av att

integrera cybersäkerhetsaspekter i nationella utbildningsprogram på olika nivåer. Vidare behövs det nationella utbildningsprogram som garanterar att en tillräcklig mängd experter finns att tillgå. Som sista led i den kompetensutvecklande verksamheten borde det nationellt sörjas för att nyckelbeslutsfattare i samhället har tillräckligt med kunskap för att kunna ta övervägda beslut (Luiijf & Healey 2012). Alla strategier nämner ambitioner och strävanden i såväl forskning som allmän kompetensutveckling. Då det gäller den nationella kompetensutvecklingen har alla strategier klart uttryckta önskemål om att den allmänna cybersäkerhetskompetensen i samhället borde ökas. Gemensamt är att alla strategierna talar om en allmän insats. Hur detta ska förverkligas varierar från strategi till strategi. En del av målsättningarna i strategierna är bättre avgränsade och riktade andra. Speciellt sådana mål som allmänt riktar sig till hela samhället på bred front utan noggrannare målgruppsdefinitioner, kan vara svåra att förverkliga på grund av att de saknar en klart avgränsad riktning. Speciellt de isländska, danska, svenska och delvis den norska strategin innehåller uttalanden gällande utvecklandet av kompetenser som inte är tydligt riktade. Många av de studerade strategierna, (även inkluderande en del av de förutnämnda) efterlyser å andra sidan utvecklandet av nationella läroplaner och utbildningsprogram på olika skolstadier, så att de bättre beaktar samhällets kompetensbehov i frågan om cybersäkerhet. Åtgärder som dessa är lätta att genomföra och förverkliga genom att uppdatera de nationella läroplanerna och utnyttja den nationella skolsystemet för implementering. Åtgärder som dessa kan anses väl riktade och avgränsade. Det förekommer inom de studerade strategierna fler liknande exempel där målgrupperna för insatser är otydligt definierade. Den svenska strategin vill t.ex. förbättra säkerheten i industriella styrsystem (sk. SCADA-system), men definierar inte tydligt ifall ambitionen gäller hela det svenska näringslivet eller bara den samhällskritiska infrastrukturen. En klart bättre avgränsning skulle vara att rikta åtgärderna till aktörer, målgrupper eller sektorer där insatserna har mest effekt t.ex. operatörer av den samhällskritiska infrastrukturen.

Lehto (2015) har identifierat att många cybersäkerhetsstrategier har likheter i det att de ser cybersäkerhet som något fundamentalt för att skydda statliga hemligheter, möjliggöra nationellt försvar och att försvara den kritiska infrastrukturen som genomtränger det moderna samhället och den moderna ekonomin. Skydd av kritisk infrastruktur och nationell

krisberedskap handlar om olika operationella och taktiska funktioner som bland annat innefattar övningsverksamhet, motåtgärder, återhämtning och uppföljning av cyberincidenter (Luiijf & Healey 2012). De nordiska cybersäkerhetsstrategiers beaktar alla föregående punkter och är lika i det att de sätter stor vikt vid skyddet av den kritiska infrastrukturen.

Mandatet skydd och utbyte av information har beaktats i alla strategier. Skydd av information och informationsresurser verkar i strategierna tolkats i bred mening med en rad olika kontexter och åtgärder som lyfts fram. Mandatet har sitt huvudfokus att förebygga, reagera och återhämta sig från cyberincidenter den verksamhet som byggs runt dessa funktioner. Informationsutbyte bygger på förtroende mellan en eller flera organisationer. Informationsutbyte bygger på frivillighet och förtroende och ska inte blandas med förpliktande utlämnande av information som baserar sig på lagstiftning och ofta är enkelriktat. Informationsutbyte kan ske nationellt eller internationellt (Luiijf & Healey 2012). Den isländska strategin lyfter relativt starkt fram internationellt informationsutbyte, som en viktig förutsättning för att kunna skydda de nationellt viktiga resurserna medan övriga strategierna mer verkar fokusera på nationell koordinering och informationsutbyte på nationell nivå. Speciellt de finska, danska, norska och svenska strategierna betonar nationella incidenthanteringsmodeller och förstärkande av nationella cybersäkerhetsmyndigheternas roll i detta sammanhang. Effektiverade incidenthanteringsmodeller fungerar samtidigt som skyddsmekanismer och knutpunkter för utbyte av relevant information. Gemensamt är att de olika länderna strävar efter att utveckla mekanismer som underlättar informationsutbytet mellan relevanta parter och bidrar till att förbättra den nationella lägesbilden.

Nationella säkerhetsstrategier borde klargöra och ta ställning till hur stater kommer att agera i internationella kontexter med speciell vikt på proaktiv utrikespolitik. Den internationella dimensionen i sin helhet med ”cyberdiplomati och förvaltning av Internet” medräknat är ett viktigt element inom ramen för en utvecklad och effektiv nationell cybersäkerhet. Förvaltning av Internet och cyberdiplomati handlar delvis om hur utvecklings- och förvaltningsorgan tas i beaktande i en internationell och mycket långt självreglerande miljö och delvis om hur nationerna engagerar sig i och ser på det internationella multi- och bilaterala relationsarbetet inom cyberdomänen. Många nationer har haft svårt att klart definiera och hitta sina mål inom den internationella och förvaltningsmässiga kontexten (Luiijf & Healey 2012). En överblick

av de studerade strategierna ger för handen att frågan om internationell verksamhet samt cyberdiplomati och förvaltning är beaktat i alla strategier. Betydande skillnader mellan strategierna förekommer dock. Den isländska strategin lägger störst vikt och den danska minst vikt vid det internationella perspektivet. Norges, Sveriges och Finlands strategier ligger tämligen nära varandra i den relativa betoningen av det internationella perspektivet. Aningen överraskande är att den danska betoningen på perspektivet är så svagt med tanke på att landet är med i såväl EU som Nato. I och för sig lyfter den danska strategin fram att det internationella arbetet måste förstärkas, men allmänt verkar det som om helhetsvikten av det internationella perspektivet genomgående förblir lågt och otydligt i strategin. Den finska strategin positionerar på ett klart och tydligt sätt den finska nationella cybersäkerheten i en bredare utrikes- och säkerhetspolitisk kontext på ett sätt som verkar skilja sig från de övriga strategierna. Orsaken kan möjligen sökas i Finlands historiska förflutna och geopolitiska läge vid EU:s nordöstra utkant.

Internet har i dagens läge utvecklats till ett centralt medium for yttrande av åsikter, opinionsbildning och en plattform som kunnat användas för att utveckla demokratistödjande deliberativa mekanismer och innovationer. Speciellt för medborgare i mer auktoritativa stater har nätet erbjudit en påverkningskanal för oppositionen och oliktänkare. Eftersom den moderna cyberomgivningen blivit en central plattform för utövande av grundläggande rättigheter, är skyddet av dessa rättigheter och tillgänglighet till Internet centrala frågor för stater som vill skydda och främja dessa rättigheter (Ekstedt, Parkhouse & Clemente 2012). Från detta perspektiv är frågan om ”åsiktsfrihet mot politisk stabilitet” central och något en nationell cybersäkerhetsstrategi borde behandla speciellt med tanke på att dessa frågor starkt även är förknippade med det internationella perspektivet samt mandatet ”cyberdiplomati och förvaltning av Internet”. Inom detta dilemma förekommer det skillnader mellan de nordiska länderna. De norska, finska och svenska strategierna drar alla upp linjer för hur länderna aktivt ska arbeta för och utveckla arbetet kring de grundläggande fri- och rättigheterna även i cybermiljön. Alla förutnämnda länder förbinder sig till att arbeta för ett fritt, öppet, nåbart, tillgängligt och stabilt Internet, där demokratiska principer och mänskliga fri- och rättigheter respekteras. De danska och isländska strategierna tar inte ställning till dessa aspekter, vilket kan ses som avvikande i den nordiska kontexten.

I tidigare forskning har den sektorsvisa ansvarssplittringen då det gäller nationell cybersäkerhet setts som problematisk (Gulichsen et al. 2003). Den sektorsvisa splittringen är antagligen något man inte helt kan komma ifrån. Åtgärder för att minska på utmaningarna som splittringen medför är välkomna. Till skillnad från många andra nationella säkerhetsfrågor är cybersäkerheten ett tema som genomtränger traditionella modeller för organisering och samordning. På grund av detta krävs det aktiva statliga åtgärder som samordnar cybersäkerhetsverksamheten på olika nivåer såväl internationellt som nationellt. Uppgiften att ansvara för koordinationen är ofta hänvisad till någons specifik statligt myndighet. Koordinationsfunktionen har ett antal centrala uppgifter att beakta till vilka bland andra hör utvecklingen och uppdateringen av en nationella cybersäkerhetsstrategin, samordningen av skyddet för kritisk infrastruktur och möjligen upprättandet av samarbetsarenor för privat och offentligt samarbete. Även lagstiftningsarbete skulle kräva samordning men på grund av olika orsaker har många nationer splittrat ansvaret för lagstiftningsarbetet mellan olika förvaltningsområden. Detta kan innebära att myndigheternas skiljande syn på saker kan leda till splittrad lagstiftning (Luiijf & Healey 2012). De nordiska länderna uttrycker i varierande grad ambitioner för att råda bot på ett utmaningen. Alla strategier gör gällande att myndighetsansvaret är splittrat och kräver uppmärksamhet för att få det offentliga samarbetet att fungera friktionsfritt och ändamålsenligt. Något starkare betoning på teman kring ett splittrat ansvar förekommer speciellt i den danska men även i den norska strategin. Den danska strategin är tydlig på med att förstärka sin modell med sektorsvist ansvar sektorsvisa delstrategierna. De olika strategierna tar upp olika åtgärdsförslag och pekar ut olika områden som kräver uppmärksamhet. Till exempel utpekar den svenska och de danska strategierna specifikt att uppmärksamhet ska fästas vid de olika offentliga förvaltningsnivåerna. Denna aspekt är inte lika tydlig i de övriga strategierna. Enligt den finska strategin ökas myndighetskoordineringen genom att centralisera ansvaret till en ny gränsöverskridande funktion inom statsförvaltningen, cybersäkerhetsdirektören, med ansvar att samordna verksamheten och insatserna. Liknande initiativ beträffande en lika klar centralisering av helhetskoordineringen och styrningen verkar inte finnas närvarande i de övriga studerade strategierna. Den danska strategin uttrycker i och för sig ambitioner på att förstärka koordinationen av internationellt verksamhet.

Att skilja på underrättelsefrågor från polisiära eller militära frågor är inte alltid möjligt och ofta är dessa frågor sammanlänkade (Luiijf & Healey 2012). Gemensamt för alla nordiska strategier är att polisens, militärens och underrättelsemyndigheterna omnämns i olika grad.

Militära cyberfrågor kan handla om en bred helhet olika åtgärder och målsättningar, vilka kan skilja sig mellan olika nationer. Militära cyberfrågor kan handla om cyberförsvar där fokuset kan ligga på skyddandet av de militära digitala omgivningarna eller om att utveckla militär operativ cyberkapacitet på olika nivåer och till olika omgivningar (Luiijf & Healey 2012). De svenska, finska och danska strategierna lyfter fram behovet av att utveckla försvarets cyberförmågor och speciellt försvarets underrättelseverksamhet. De olika nationella strategierna verkar betona dessa utvecklingsområden utifrån sina specifika nationella behov och utgångslägen. Den finska strategin fäster stor vikt vid vidareutvecklandet av de underrättelseförmågor det finska försvaret och Skyddspolisen nyligen fått lagenliga befogenheter till, medan den danska strategin fäster uppmärksamhet vid försvarets underrättelseverksamhets analytiska kapacitet och förmågan att utföra cyberoperationer. Genomgående har det militära fått tämligen lite utrymme i den studerade strategierna, även om mandatet är behandlat och givits utrymme. Överlag är omnämnandena gällande mandatet rätt allmänna.

Cyberbrottsbekämpning kan omsätta en bred skala av statliga och internationella organisationer. Vidare kan cyberbrottsbekämpningen omfattas av en rad olika perspektiv, allt från ekonomiska och lagstiftningsmässiga till nationella säkerhetsfrågor (Luiijf & Healey 2012). Speciellt polisens förutsättningar till effektiv cyberbrottsbekämpning betonas genomgående i alla strategier. Vidare har många av de studerade strategierna även identifierat cyberbrottsbekämpningens starkt internationella dimension. Som redan tidigare framkommit kopplar den isländska strategin effektiv ihop cyberbrottsbekämpning med möjligheten att skapa gynnsamma ekonomiska konkurrensfördelar. Den svenska strategin förespråkar speciellt förebyggande verksamhet inom området. Finland, Island och Sverige lyfter fram utvecklandet av lagstiftning så att den bättre svarar på de nya utmaningarna.

Huvudsyfte med underrättelseverksamheten är att samla in, sammanställa och analysera information som sedan kan användas för att motverka eller uppdaga olika cyberhot. Ofta

handlar det om att ytterligare utveckla befintlig verksamhet (Luiijf & Healey 2012). Alla strategier har en genomgående svag betoning på underrättelseverksamhet. I sig behöver inte detta betyda att saken inte får eller har fått uppmärksamhet. Som tidigare framkommit riktar sig åtminstone en del av åtgärderna till att vidareutveckla befintlig verksamhet. Området är i övrigt ett sådant som inte söker offentlig uppmärksamhet i någon större utsträckning, vilket kan vara förklaringen till den relativt sett låga betoningen.

Som Limnéll, Majewski & Salminen (2014) redogjort är Internet en disruptiv teknik som omdefinierar förhållningen till invanda lösningar. Stater måste balansera hot och möjligheter som den digitala miljön fört med sig som mot varandra. Den privata sektorn ansvarar för och driver dessutom en stor del av den samhällskritiska infrastrukturen. Stater som funderar på att öka den nationell cybersäkerheten måste ta i beaktande den alternativa påverkan som höjd säkerhet kan föra med sig i på ekonomiska möjligheter att utnyttja nätet och dess digitala möjligheter. Ett av de mer framstående motsatserna som starkt hänger samman med det ekonomisk tillväxt och nationell säkerhet är frågan om modernisering av infrastruktur mot ett starkare skydd av kritisk infrastruktur (Hathaway & Klimburg 2012). Då det gäller dilemmat skydd och modernisering av kritisk infrastruktur verkar det intressant nog genomgående som om de nordiska strategierna inte ser detta som en motsättning, utan snarare som en målsättning och tillgång som kan erbjuda nationella fördelar. Vidare verkar de nordiska strategierna lägga en tämligen stark vikt vid konkurrensfördelar en höjd nationell cybersäkerhet kan medföra. Den svenska liksom den isländska och danska strategierna betonar relativt sett starkt konkurrensfördelar och ekonomiska möjligheter, medan de övriga strategierna gör det i varierande grad.

Ett betydande dilemma i dagen informationssamhälle är det ekonomiska värdet på personuppgifter, utbyte och fritt flöde av information mot starkare dataskydd och medborgarnas rätt till sin egen information. Att realisera Internetekonomins fulla ekonomiska fördelar är inte möjligt utan ett så stort dataflöde som möjligt. Å andra sidan måste bland annat frågor som är förknippade med dataskydd och nationell säkerhet vägas upp mot det fördelar ett möjligast fritt dataflöde kan innebära. Det förekommer naturliga konflikten mellan medborgarnas förväntningar och regeringens politik för dataskydd och bevarande av integritet gentemot behovet av att dela information med avsikt att öka säkerhet. Företag å sin

sida förlitar sig på konsumenternas och affärspartnernas villighet att överlåta privat information samtidigt som de senare nämnda förväntar sig att den utlämnade informationen förblir privat och hanteras på ett säkert sätt (Hathaway & Klimburg 2012). De finska och norska strategierna har inte alls tagit ställning till frågan om dataskydd mot utbyte av information. De svenska och danska strategierna är lika i att de relativt sett betonar dilemmat dataskydd mot utbyte av information lägst i en relation till de övriga dilemmana i strategierna, men frågan finns dock närvarande i båda strategierna.

På basen av studien verkar det som om strategierna tämligen omfattande har tagit ställning eller på ett eller annat sätt beaktat de centralaste elementen och frågorna som kan anses bilda kärnan för en välavvägd cybersäkerhetsstrategi. Alla strategier har allmänt taget berört de teoretiska ramarna som granskats i denna studie, bortsett några få undantag. De interna betoningarna på de olika områdena skiljer sig åt mellan strategierna. Den största skillnaden, som även påverkar strategierna innehåll, beror på de skiljande strukturerna och utformningarna strategierna har samt på de olika målgrupper de olika länderna försökt nå med strategierna. Fastän de största skillnaderna kan hittas i förutnämnda orsaker förekommer det även klara brister i hur strategierna beaktar centrala frågor och avsaknaden av viktiga avgränsningar i vissa av de studerade strategierna. Vidare förekommer ställvis direkta otydligheter i en del av de studerade strategierna. Bristerna i beaktande av centrala frågor och viktiga avvägningar kan i leda till ad hoc lösningar eller dåligt förberedda ageranden i överraskande situationer. Otydliga eller bristfälligt riktade verksamhetsmål kan å sin sida med stor sannolikhet leda till ineffektiva lösningar och icke avsedda resultat i det nationella cybersäkerhetsarbetet.

Som denna studie påvisat finns det mycket lika men även en del skillnader i de fem nordiska ländernas cybersäkerhetsstrategier. På grund av sitt kulturella förflutna, sitt beroende av omvärlden och geografiska läge verkar det som om de fem nordiska länderna har mer gemensamt än saker som skiljer dem åt. I kommande studier kunde det vara intressant att se på vad dessa skillnader kan bero på. De fem nordiska länderna har länge gjort nära samarbete, har liknande samhällen och lagstiftning. Det förekommer även skillnader mellan de nordiska länderna. Island, Danmark och Norge är Nato medlemmar medan Finland och Sverige är inte det. Danmark, Sverige och Finland är EU medlemmar medan Norge och Island inte är det.

Norge och Island tillhör den Europeiska ekonomiska gemenskapen (EES). Tillhörigheten till de olika gemenskaperna kan vara en möjlig faktor som har påverkat utformningen av cybersäkerhetsstrategierna. Alternativt eller i kombination med förutnämnda faktor kan de enskilda ländernas kulturella, historiska, förvaltningsmässiga, politiska eller säkerhetsrelaterade utgångslägen påverka hur var och en strategi utformats. Det skulle med andra ord vara intressant att se på hur de nationella cybersäkerhetsstrategierna utformats i den nordiska kontexten och vilka betoningar som vart och ett land gjort med beaktande av olika möjliga bakomliggande faktorer. En kommande studie kunde förslagsvis granska ifall strategiernas utformning och betoning påverkas av medlemskap eller icke medlemskap i EU och Nato eller ifall skillnaderna möjligen kan bero på andra till exempel kulturella eller politiska faktorer. En dylik studie skulle kräva omfattande utrymme och noggrann genomgång och operationalisering av olika möjliga bakomliggande faktorer. Det skulle även vara intressant att granska och jämföra hur de olika nordiska cybersäkerhetsstrategierna formuleringar omsatts i praktiken och vilka följder linjedragningarna fått ur ett policyimplementeringsperspektiv.

7.2 Avslutning

Studien jämförde Finlands, Sveriges, Norges, Danmarks och Islands senaste cybersäkerhetsstrategier med varandra. Strategierna har utgivits mellan åren 2015-2019 och således har även studien avgränsats till de nämnda åren. Studien har inte beaktat olika nationella kompletterande strategier som eventuellt existerar (t.ex. Norges internationella cybersäkerhetsstrategi).

Huvudsyftet med studien var att analysera hur de fem nordiska ländernas cybersäkerhetsstrategier skiljer sig åt och hur skillnaderna formuleras och tar sig uttryck i tyngdpunkter, målsättningar, valda handlingsförslag och samarbetsformer och hur dessa anknyter till det valda teoretiska ramverket som baserar sig på de ”tre perspektiven”, ”fem mandaten” och ”fem dilemmana”.

För att avslutningsvis knyta samman studien med de frågor som ställdes i denna studie kan det kort konstateras att de fem studerade nordiska cybersäkerhetsstrategierna har mycket gemensamt, men att det samtidigt förekommer skillnader mellan dem.

De centrala frågorna som ställdes i denna studie ämnade ta reda på hurdana skillnader de förekommer i hur de olika nordiska ländernas cybersäkerhetsstrategier betonar de tre perspektiven, de fem huvudsakliga mandaten och de tre tvärmandaten samt de fem dilemmana. Vidare ämnade studien utreda hur väl strategierna har tagit ställning till de förutnämnda centrala elementen som kan anses utgöra kärnan till en välformulerad och välavvägd cybersäkerhetsstrategi.

Skillnader mellan strategierna förekommer på så gott som alla punkter d.v.s. perspektiven, mandaten och dilemmana samt i sättet de tagit ställning till dessa. Några få frågor har inte berörts i tre av de totalt fem studerade strategierna. Den norska strategin har inte berört frågor kring underrättelseverksamhet eller dataskydd mot utbyte av information och den finska strategin har inte berört dataskydd mot utbyte av information. Den danska strategin har inte berört åsiktsfrihet mot politisk stabilitet.

Likheter mellan strategierna hittas till exempel i att de ser cybersäkerheten huvudsakligen som en nationell angelägenhet, som genomsyrar alla nivåer och aktörer. Med andra ord är den nationella cybersäkerheten allas sak och var och en bär ett ansvar för en höjd nationell säkerhet. Alla strategier identifierar den komplexa och starkt fragmenterade omgivningen som det moderna samhället verkar i och gör gällande att de traditionella och invanda samarbetsmodellerna kräver uppdatering. Speciellt efterlyser strategierna fördjupat samarbete och ökat informationsutbyte mellan den privata och den offentliga sektorn. Den danska strategin betonar speciellt samarbete mellan och utveckling av de identifierade samhällskritiska sektorerna, medan de övriga strategierna är lite mer allmänna på denna punkt.

Gemensamt för alla strategier är att det statliga perspektivet genomgående är av mindre betydelse i jämförelse med det nationella eller internationella perspektiven. En överblick av de tre perspektiven nationellt, internationellt och statligt ger för handen att de finska, norska och svenska strategierna är mest lika. Gemensamt för dessa strategier är att de lägger högsta

betoning på det nationella och lägsta betoning på det statliga perspektivet. Den isländska och danska strategin skiljer sig åt från de tre föregående i det att Island betonar det internationella högst och Danmark lägst. Aningen överraskande är att den danska betoningen på perspektivet är så svagt med tanke på att landet är med i såväl EU som Nato. En plausibel orsak till till att Island relativt sett betonar det nationella perspektivet svagare än de övriga nordiska länderna och internationella perspektivet starkast, kan bero på Islands läge mitt emellan två stora kontinenter, landets lilla storlek och därmed starka beroende av internationella förbindelser då det gäller såväl säkerhet, försvar som handel. Alla strategier verkar identifiera problem och frågor som på ett eller annat sätt är förknippade med det nationella utvecklingsbehoven och betona perspektiven i enlighet med det.

Det förekommer en del skillnader i hur de olika strategierna beaktat och betonat cybersäkerhetens fem dilemman. Skillnader förekommer i såväl innehåll som i själva betoningen och hur omfattande strategierna tagit dessa i beaktande. De isländska, finska och svenska strategierna är lika i det att de ger relativt sett höga betoningar på dilemmat ekonomisk stimulans mot högre säkerhet.

Det förekommer en del övergripande skillnader i hur de olika strategierna beaktat och betonat cybersäkerhetens fem mandat och de därtill hörande tre tvärmandaten. Alla fem huvudmandat och tre tvärmandat finns beaktade i alla förutom en strategi. Den enda större avvikelsen i strategierna verkar vara att den norska strategin inte beaktar mandatet underrättelseverksamhet. Dock är betoningen även i de övriga strategierna gällande underrättelseverksamhet genomgående lågt. Gemensamt för den isländska, danska och svenska strategin är att alla lägger starkast betoning på mandatet skydd av kritisk infrastruktur och nationell krisberedskap. Den finska strategin lägger störst vikt på mandatet koordinering och den norska på mandatet forskning.

Delvis beror skillnaderna direkt på de olika sätt som strategierna är utformade och strukturerade på och delvis på betoningarna i själva innehållet. Skillnaden i struktur och utformning kan beror på många olika faktorer som till exempel på historiska, kulturella, organisatoriska, politiska eller andra faktorer. Skillnaderna kan även bero på att man genom någon specifik struktur eller utformning velat nå en specifik publik. De synligaste och mest

övergripande skillnaderna i strategierna förekommer antagligen just på grund av de olika nationella utgångslägena och de olika läsargrupper man velat nå med publikationerna. Detta i sin tur kan antas ha påverkat betoning av olika saker i strategierna. Ifall man bortser från avsaknaden av två dilemman och ett mandat i de finska, danska och norska strategierna så har de studerade strategierna tämligen väl lyckats beakta de olika frågor som hänger i hop med välavvägda cybersäkerhetsstrategier. Bakomliggande orsaker och förklaringar till vad skillnaderna kan bero på har inte undersökts i denna studie.

Litteratur

Ansoff, H. I. (1984). *Strategisen johtamisen käsikirja*. Helsinki: Kustannusosakeyhtiö Otava.

Awan, I. (2012). Policing the Global Phenomenon of Cyber Terrorism and Extremism. I: *Policing Cyber Hate, Cyber Threats and Cyber Terrorism, edited by Awan I.* London.

Azmi, R. & Kautsarina, K. (2019). *Revisiting Cyber Definition*. https://www.researchgate.net/publication/334989724_Revisiting_Cyber_Definition [2020-10-16].

Azmi, R., Tibben, W. & Win, K. (2016). *Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy*. https://www.researchgate.net/profile/Riza_Azmi/publication/308470260_Motives_behind_Cyber_Security_Strategy_Development_A_Literature_Review_of_National_Cyber_Security_Strategy/links/57e4d4a408ae25aa0208ee66/Motives-behind-Cyber-Security-Strategy-Development-A-Literature-Review-of-National-Cyber-Security-Strategy.pdf [2020-10-16].

BBC News (2016). *US accuses Russia of cyber attacks*. BBC News. https://www.bbc.com/news/election-us-2016-37592684 [2020-11-18].

BBC News (2017). *Ukraine power cut ”was cyber-attack”*. BBC News. https://www.bbc.com/news/technology-38573074 [2020-11-14].

Blakemore, B. (2012a). *Policing Cyber Hate, Cyber Threats and Cyber Terrorism*. London.

Blakemore, B. (2012b). Cyberspace, Cyber Crime and Cyber Terrorism. I: *Policing Cyber Hate, Cyber Threats and Cyber Terrorism, edited by Awan I*. London.

Bryman, A. (2012). *Social research methods*. 4:de uppl. New York.

Bryson, J. M. (2010). The Future of Public and Nonprofit Strategic Planning in the United States. *Public Administration Review*, 70, ss. 255–267.

Bryson, J. M. (2018). *Strategic Planning for Public and Nonprofit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement*. Newark.

Campbell, S. (2010). Comparative Case Study. I: Mills, A., Durepos, G., & Wiebe, E. (red.) *Encyclopedia of Case Study Research*. Thousand Oaks: SAGE Publications, Inc., ss. 175–176.

Centre for Cybersecurity, DK (2015). *The Danish Cyber and Information Security Strategy*.

Clausewitz von, C. (1997). *On War*. Hertfordshire.

Cordey, S. & Dewar, R. S. (2019). *National Cyberdefense Policy Snapshots*. 2:a uppl. Zurich.

Council of Europe (2001). *Convention on Cybercrime*. Council of Europe. No. 185.

DeNardis, L. (2014). *The Global War for Internet Governance*. London.

Denk, T. (2012). *Komparativa analysmetoder*. Lund.

Department for Homeland Security (2020). *Homeland Threat Assessment - October 2020*. https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf [2020-11-14].

Ekstedt, V., Parkhouse, T. & Clemente, D. (2012). Commitments, Mechanisms & Governance. I: *National Cyber Security Framework Manual. Edited by Klimburg A.* Tallinn, ss. 146–190.

Elo, S. & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, 62(1), ss. 107–115, doi:https://doi.org/10.1111/j.1365-2648.2007.04569.x.

ENISA (2012). *National Cyber Security Strategies: An Implementation Guide*. https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide [2020-10-30].
Esser, F. & Vliegenthart, R. (2017). Comparative Research Methods. I: Matthes, J., Davis, C. S., & Potter, R. F. (red.) *The International Encyclopedia of Communication Research Methods*. New Jersey, ss. 1–22.
Försvarshögskolan (2020). *Fakta om asymmetriska hot*. https://www.fhs.se/centrum-for-totalforsvar-och-samhallets-sakerhet/om-centret/organisation/cats/fakta-om-asymmetriska-hot.html [2020-11-14].
Giantas, D. & Liaropoulos, A. (2019). *Cybersecurity in the EU: Threats, frameworks and future perspectives*. https://www.researchgate.net/profile/Riza_Azmi/publication/308470260_Motives_behind_Cyber_Security_Strategy_Development_A_Literature_Review_of_National_Cyber_Security_Strategy/links/57e4d4a408ae25aa0208ee66/Motives-behind-Cyber-Security-Strategy-Development-A-Literature-Review-of-National-Cyber-Security-Strategy.pdf [2020-10-16].
Gulichsen, S., Hoff, E., Sørli, K., Hagen, J. & Nystuen, K. O. (2003). Strategier for informasjonssikkerhet - En komparativ studie av strategiarbeidet i Norge, USA, Australia og EU. *FFI/RAPPORT*, (2003/00271–1), s. 71.
Haaretz (2019). *Dutch intel aided U.S.-Israeli Stuxnet cyberattack on Iran, report reveals*. Haaretz. https://www.haaretz.com/middle-east-news/iran/dutch-intel-aided-u-s-israeli-stuxnet-cyberattack-on-iran-report-reveals-1.7793561 [2020-11-18].
Harboe, T. (2013). *Grundläggande metod: den samhällsvetenskapliga uppsatsen*. Malmö.
Harris, S. (2014). *@ War - The Rise of Cyber Warfare*. London.
Hathaway, M. E. & Klimburg, A. (2012). Preliminary Considerations: On National Cyber Security. I: *National Cyber Security Framework Manual. Edited by Klimburg A.* Tallinn, ss. 1–43.
Helsingin Sanomat (2019). *Tiedustelulait hyväksyttiin: nämä uudet salaiset oikeudet Supo saa, ja näin ne vaikuttavat tavallisen kansalaisen elämään*. Helsingin Sanomat. https://www.hs.fi/politiikka/art-2000006031070.html [2021-02-9].
Helsingin Sanomat (2020a). *Yhdysvallat | Yhdysvaltain hallintoon on tehty tietomurto – lehtitietojen mukaan tekijät olisivat Venäjältä ja vakoilu olisi jatkunut kuukausia*. Helsingin Sanomat. https://www.hs.fi/ulkomaat/art-2000007680443.html [2021-01-3].
Helsingin Sanomat (2020b). *Tietosuoja | Vastaamo: Tietomurtoja saattoi olla kaksi – Toimi näin, jos epäilet tietojasi varastetun tai olet saanut kiristysviestin*. Helsingin Sanomat. https://www.hs.fi/kotimaa/art-2000006698960.html [2021-03-2].
Helsingin Sanomat (2021). *Maailma 2021 | Kauhukuvia tahallisesti tappavista kyberiskuista on maalailtu vuosikymmeniä, mutta tänä vuonna sellainen todella saatetaan nähdä*. Helsingin Sanomat. https://www.hs.fi/ulkomaat/art-2000007713504.html [2021-01-3].
Hsieh, H.-F. & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research*, 15(9), ss. 1277–1288, doi:10.1177/1049732305276687.
ICANN (2013). *Montevideo Statement on the Future of Internet Cooperation*. https://www.icann.org/news/announcement-2013-10-07-en [2020-11-22].

ICSS_NO (2017). *International cyber strategy for Norway*. https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategy_2017.pdf.
IGF (2018). *IGF 2018 Chair's Summary: Thirteenth Meeting of Internet Governance ForumParis, 12-14 November 2018*. https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/6212/1417 [2020-12-22].
Izycki, E. & Colli, R. (2019). *Protection of critical infrastructure in national cyber security strategies*. https://www.researchgate.net/profile/Eduardo_Izycki/publication/335760609_Protection_of_critical_infrastructure_in_national_cyber_security_strategies/links/5d7a3730299bf1cb809a66cf/Protection-of-critical-infrastructure-in-national-cyber-security-strategies.pdf [2020-10-16].
Jansson, S. & Sihvonen, T. Kyberturvallisuus valtiollisena toimintaympäristönä ja siihen kohdistuvat uhkat. *Media & viestintä*, 2018(41), ss. 1–28.
Johnsen, S. (2015). *A Comparative Study of the Norwegian Cyber Security Strategy vs strategies in EU and the US – emerging cybersafety ignored (ESREL 2015 Draft)*. https://www.researchgate.net/profile/S_Johnsen/publication/281857953_A_Comparative_Study_of_the_Norwegian_Cyber_Security_Strategy_vs_strategies_in_EU_and_the_US_-_emerging_cybersafety_ignored_ESREL_2015_Draft/links/55fbd7e708aeba1d9f3a1912/A-Comparative-Study-of-the-Norwegian-Cyber-Security-Strategy-vs-strategies-in-EU-and-the-US-emerging-cybersafety-ignored-ESREL-2015-Draft.pdf [2020-10-16].
Juuti, P. & Luoma, M. (2009). *Strateginen johtaminen - Miten vastata kompleksiseen ja postmodernin ajan haasteisiin*. Keuruu.
Kamensky, M. (2008). *Strateginen johtaminen*. Helsinki.
Klimburg, A. red. (2012). *National cyber security framework manual*. Tallinn.
Klimburg, A. & Healey, J. (2012). Strategic Goals & Stakeholders. I: *National Cyber Security Framework Manual. Edited by Klimburg A.* Tallinn, ss. 66–107.
Klimburg, A. & Mirtl, P. (2012). *Cyberspace and governance - a primer*. Wien: Österreichisches Institut für Internationale Politik / Working Paper 65.
Laamanen, T., Kamensky, M., Kivilahti, T., Kosonen, P., Laine, K. & Lindell, M. (2005). *Strategisen johtamisen käsitteet - englannista suomeksi*. Helsinki.
Lehto, M. (2015). The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies. *International Journal of Cyber Warfare and Terrorism*, 3, ss. 1–18.
Limnéll, J., Majewski, K. & Salminen, M. (2014). *Kyberturvallisuus*. Jyväskylä: Docendo.
Lindgren, S. (2011). Textanalys. I: Fangen, K. & Sellerberg, A.-M. (red.) *Många möjliga metoder*. Lund.
Lindström, G. & Luiijf, E. (2012). Political Aims & Policy Methods. I: *National Cyber Security Framework Manual. Edited by Klimburg A.* Tallinn, ss. 44–65.
Luiijf, E., Besseling, K. & Graaf, P. (2013). Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructure Protection*, 9, ss. 3–31.
Luiijf, E. & Healey, J. (2012). Organisational Structures & Considerations Eric Luiijf, Jason Healey. I: *National Cyber Security Framework Manual. Edited by Klimburg A.* Tallinn, ss. 108–145.

Martin, I. (2015). Cyber Security Strategies - An Overview. *International Journal of Information Security and Cybercrime*, 4(1), ss. 33–40.
Marvasti, A. B. (2019). Qualitative Content Analysis: A Novice's Perspective. *Forum: Qualitative Social Research*, 20(3), ss. 1–14, doi:10.17169/fqs-20.3.3387.
Metsämuuronen, J. (2008). *Laadullisen tutkimuksen perusteet*. Helsinki.
MSB (2019). *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022 : 1 mars 2019*. https://rib.msb.se/filer/pdf/28804.pdf [2020-10-16].
NCSS DK (2017). *Danish Cyber and Information Security Strategy*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategy-for-cyber-and-information-security/@@download_version/8b31862c3e304fceadc0719d18dc3bb3/file_en [2020-10-1].
NCSS FI (2013). *Suomen kyberturvallisuusstrategia 2013*. https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Strategi-fo%CC%88r-cybersa%CC%88kerheten-i-Finland.pdf [2020-09-14].
NCSS FI (2019). *Finland's Cyber Security Strategy 2019*. https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/ [2020-09-9].
NCSS IS (2015). *Icelandic National Cyber Security Strategy 2015–2026, Plan of action 2015–2018. Summary in English of the Icelandic National Cyber Security Strategy approved by the Minister of the Interior in April 2015*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/icelandic-national-cyber-security-strategy/@@download_version/d2ae3c3629894810ab33f7630979eec8/file_en [2020-11-19].
NCSS NO (2017). *National Cyber Security Strategy for Norway*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategy-for-information-security/@@download_version/f201ff6da6eb4101b1ca050e79f53975/file_en [2020-11-19].
NCSS SE (2016). *A national cyber security strategy, Skr. 2016/17:213*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy/@@download_version/54488ef3fa3747f38d2d0040ea06c283/file_en [2020-11-19].
Niinistö, S. (2021). *Republikens president Sauli Niinistös nyårstal den 1 januari 2021*. Presidentti. https://www.presidentti.fi/sv/tal/republikens-president-sauli-niinistos-nyarstal-den-1-januari-2021/ [2021-01-3].
Näsi, J. & Aunola, M. (2001). *Strategisen johtamisen teoria ja käytäntö*. Helsinki.
POHA (2021). *Poliisihallituksen tilinpäätös ja toimintakertomus 2020*. https://poliisi.fi/documents/25235045/27075255/Poliisihallituksen-tilinp%C3%A4%C3%A4t%C3%B6s-ja-toimintakertomus-2020.pdf/da96053f-9f89-23af-a642-fe13838cc5b7/Poliisihallituksen-tilinp%C3%A4%C3%A4t%C3%B6s-ja-toimintakertomus-2020.pdf?t=1616149817573 [2021-03-28].

Reuters (2018). *Cambridge Analytica CEO claims influence on U.S. election, Facebook questioned*. Reuters. https://www.reuters.com/article/us-facebook-cambridge-analytica-idUSKBN1GW1SG [2020-11-18].
Sanastokeskus TSK ry (2018). *Kyberturvallisuuden sanasto*.
Santalainen, T. (2008). *Strateginen ajattelu*. Helsinki.
Schallbruch, M. & Skierka, I. (2018). The Evolution of German Cybersecurity Strategy. I: *Cybersecurity in Germany*. ss. 15–29.
Schneier, B. (2013). *Click here to Kill Everybody - Security and Survival in a Hyper-connected World*. New York.
Schreier, M., Stamann, C., Janssen, M., Dahl, T. & Whittal, A. (2019). Qualitative Content Analysis: Conceptualizations and Challenges in Research Practice—Introduction to the FQS Special Issue ”Qualitative Content Analysis I”. *Qualitative Social Research*, 20(3).
SUPO (2020). *Suojelupoliisin vuosikirja*. https://vuosikirja.supo.fi/etusivu [2021-03-28].
The Wired (2016). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. Wired. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [2020-11-14].
The Wired (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [2020-11-17].
Tjora, A. (2010). *Från nyfikenhet till systematisk kunskap*. Lund.
Tuomi, J. & Sarajärvi, A. (2002). *Laadullinen tutkimus ja sisältöanalyysi*. 2:a uppl. Helsinki.
Tzu, S. (1982). *Sodankäynnin taito*. Vaasa.
Vanhala, S., Laukkanen, M. & Koskinen, A. (2002). *Liiketoiminta ja johtaminen*. Helsinki.
Virtanen, P. & Stenvall, J. (2019). *Julkinen johtaminen*. 2:a uppl. Helsinki.
Wedin, L. Asymmetrisk krigföring – en strategisk utmaning. *Kungl Krigsvetenskapsakademiens Handlingar och Tidskrift*, 2005(4), ss. 108–122.
Yle (2021). *KRP tutkii äärimmäisen harvinaista rikosta: Eduskuntaan kohdistunut tietomurto voi olla vakoilua ja kansanedustajien sähköposteja vaarantunut*. Yle Uutiset. https://yle.fi/uutiset/3-11715912 [2021-03-2].