UiT
NORGES
ARKTISKE
UNIVERSITET

Institutt for samfunnsvitenskap

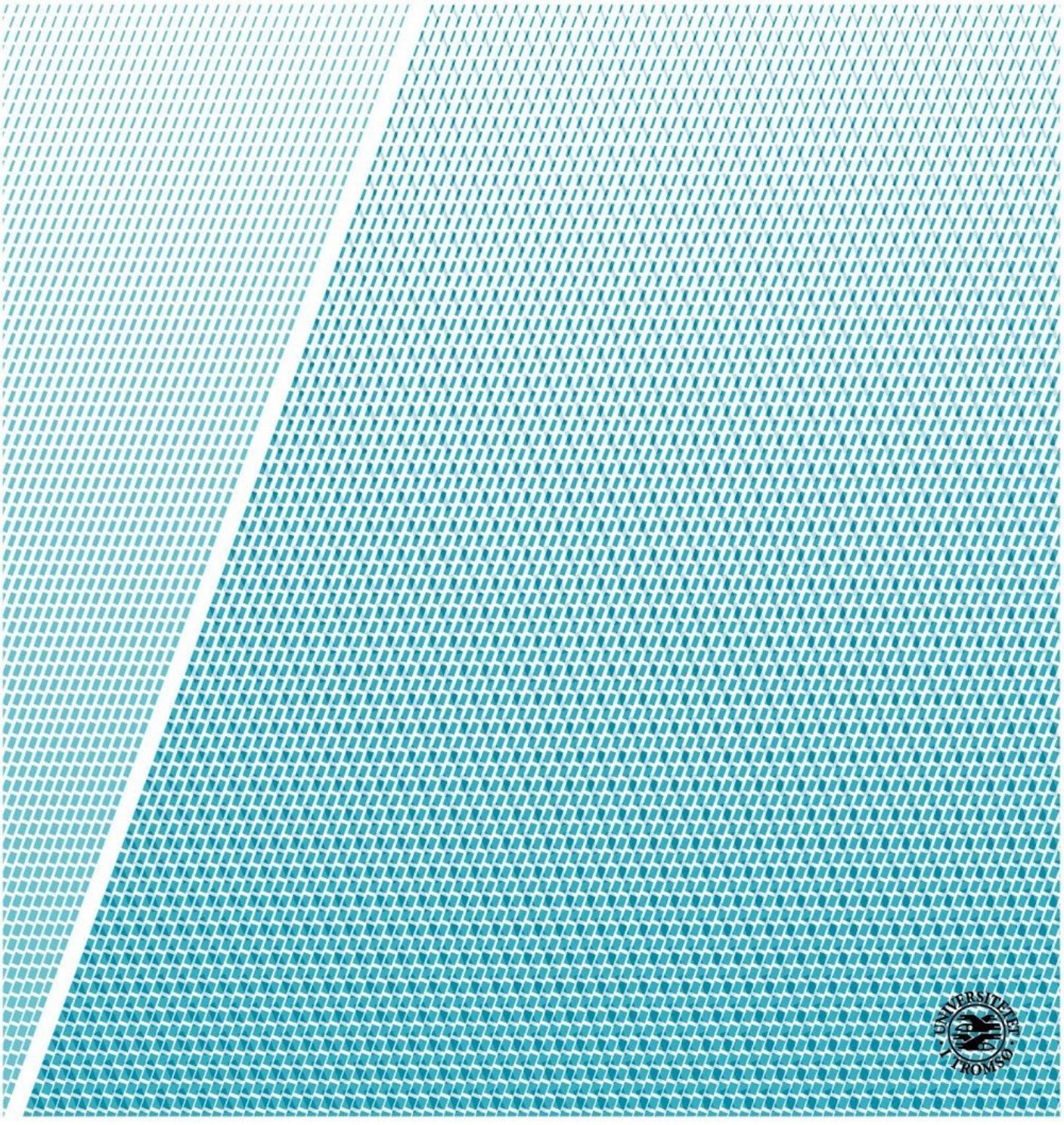
Cybertruslene mot Norge

En analyse av trusselbildet og drivkreftene bak cyber-sikkerhetspolitikken

—

Nora Seel-Bahr

Masteroppgave i Statsvitenskap, mai 2018



Forord

En stor takk rettes til min veileder Tor Christian Dahl-Eriksen for tett oppfølging, gode råd, faglige innsikt og interessante diskusjoner.

Takk til mamma og pappa, Susanne og Jonatan, og Henrik og Elisabeth for all inspirasjon og alle spennende diskusjoner. Det er vanskelig å gi opp med dere rundt meg.

Sist men ikke minst en stor takk til Eirik for at du har lest korrektur og diskutert oppgaven med meg gjennom et helt år, ved siden av din egen krevende jobb. Generelt er jeg takknemlig for at du har holdt ut med meg dette året, kanskje var pendlingen noe mer kjærkommen i de verste stressperiodene mine.

Nora Seel-Bahr

Tromsø, 10. Mai 2018

Sammendrag

Cyberdomenet er grenseløst og bidrar til at hele verden deler kontaktflate, avstandene er korte og teknologien er allment tilgjengelig i store deler av verden. Cyberangrep oppfattes i dag som en av de fremste truslene mot norsk sikkerhet, og feltet muliggjør nye former for angrep med lavere kostnad og enklere midler. Norge er et av verdens mest digitaliserte land, og et storskala angrep mot kritisk digital infrastruktur vil kunne ha enorme konsekvenser. Norges digitale sikkerhet beskrives som lav og muligheten for en styrking av cybersikkerheten utredes per i dag. Det finnes politisk vilje til å utvikle et nytt digitalt grenseforsvar, men hvordan dette kan implementeres er ennå uklart.

Denne studien kartlegger det digitale trusselbildet i Norge, og analyserer drivkreftene bak sikkerhetspolitikken på cyberfeltet, med utgangspunkt i de teoretiske perspektivene realisme, liberalisme og konstruktivisme. Sentralt for oppgaven er hva det digitale trusselbildet består av samt hvordan det presenteres, og dernest hva som former sikkerhetspolitikken på cyberfeltet. Studien benytter en form for policyanalyse med tre analysenivåer (individ, stat og globale omgivelser) og identifiserer drivkrefter bak sikkerhetspolitikken i lys av de teoretiske perspektivene.

Nøkkelord: cybersikkerhet, cyberangrep, sikkerhetspolitikk, utenrikspolitikk, Norge

1. Innledning

1.1 Bakgrunn og problemstilling

I nyere tid har verdens trusselbilde endret seg fra primært tradisjonell krigføring, til en økende risiko for digitale angrep. Såkalte cyberangrep er en form for internetthacking som kan omfatte blant annet spionasje, endring og planting av informasjon og ødeleggelse av digital infrastruktur. Slike angrep, og trusselen om dem, er mye omtalte tema i media, blant annet i forbindelse med Russlands påståtte innblanding i det amerikanske presidentvalget i 2016. Det finnes flere omfattende digitale angrep fra tidligere år, eksempelvis Estland i 2007, Georgia i 2008, Iran i 2010 og Ukraina i 2014. Felles for disse angrepene var store ødeleggelser av den digitale infrastrukturen gjort ved hjelp av hacking og datavirus. Det massive digitale angrepet på Estland ble oppfattet som et russisk angrep, og var rettet mot landets politikere og myndighetspersoners e-poster i tillegg til statlige organers nettsider. Angrepet betegnes som så omfattende at store deler av landet var digitalt ute av drift i flere dager. Angrepet på Irans atomanlegg var et virus kalt Stuxnet som angrep den digitale delen av industrien. Dette angrepet ble gjort for å sabotere Irans atomproduksjon, og hevdes å være et samarbeid mellom Israel og USA.

Norges etterretningstjeneste (heretter E-tjenesten) betegner "trusler i det digitale rommet" som den mest fremtredende trusselen mot nasjonal sikkerhet i 2017 (Fokus 2017), og Nasjonal Sikkerhetsmyndighet (NSM) rapporterer en urovekkende økning i antall digitale angrep mot Norge. Avsenderen bak angrepene kan være vanskelig å ta rede på, samt at cyberangrep åpner for fordekte operasjoner og et bredere aktørbilde som kan variere fra enkeltindivider til grupper og myndigheter (Langø 2011). Likevel portretteres Russland, og med det russiske myndigheter, som den primære trusselaktøren. Det hevdes videre at Norge ikke har gode nok systemer for å oppdage og forhindre slike angrep, hvilket er hvorfor et statlig oppnevnt utvalg (Lysne m.fl. 2016) har utredet den digitale trusselsituasjonen for å vurdere behovet for et eget Digitalt Grenseforsvar. Utvalgets anbefalinger om et styrket digitalt forsvar og opprettelsen av instansen Digitalt Grenseforsvar ble godkjent og vedtatt av daværende Forsvarsminister Ine Eriksen Søreide i oktober 2017 og skal videre utredes

nærmere (Regjeringen 2017). Norge er et av verdens mest avanserte industriland og utstrekningen av vårt digitale nettverk er svært stor. Dette gjør Norge utsatt og gjør risikoen for angrep stor. Det kan fremstå naturlig å ønske og sette i gang ethvert tiltak som vil gjøre befolkningen og nasjonale organer tryggere, men juridisk er cyberfeltet komplisert å manøvrere i. Implementering av et styrket digitalt grenseforsvar vil kunne bety lovendringer med hensyn til personvern, og en vil trolig måtte vurdere å tillate overvåkning av nasjonal internettkommunikasjon. Et slikt mandat ekskluderer straffeforfølgelse av andre lovbrudd enn digital terror fra utlandet (Lysne m.fl. 2016), like fullt er svakere personvern et stort tankekors.

Cyberangrep er et tema som berører en rekke ulike fagfelt, og fra et statsvitenskapelig ståsted er en rekke spørsmål både relevante, betimelige og interessante. Per i dag finnes det begrenset norsk forskning på cyberfeltet, og det meste omhandler juridiske problemstillinger knyttet til personvern og menneskerettigheter, teknologisk forskning på konkrete forbedringer av sikkerheten til digital programvare, eller operative militære tilnærminger og risikoanalyse. Casespesifikke tilnærminger til staters digitale trusler finnes primært om land der store cyberangrep allerede har funnet sted, og er således analyser av historiske tilfeller og ikke utredninger av nåværende situasjon. Denne oppgavens innfallsvinkel og metodiske verktøy er hentet fra Foreign Policy Analysis (forenklet oversatt til policyanalyse), og tar utgangspunkt i en utredelse av den digitale trusselsituasjonen i Norge. Mer konkret er problemstillingen som følger:

Hva består den digitale trusselsituasjonen i Norge av? Hva driver utformingen av den norske sikkerhetspolitikken på cyberfeltet?

Problemstillingens formulering tilsier bruk av kvalitative data, og på grunn av hensynet til at alle benyttede kilder må bestå av åpen og ugradert informasjon er forskningsmetoden dokumentanalyse brukt. For å utrede den digitale trusselsituasjonen er det primært tatt utgangspunkt i årlige rapporter fra E-tjenesten og NSM, kombinert med utvalgte rapporter fra Regjeringen, Forsvarets Forskningsinstitutt (FFI) og Lysne II-utvalget. Problemstillingens andre spørsmål besvares ved å benytte en form for utenrikspolitisk analyse som forklarer hvordan bestemte interne og eksterne faktorer påvirker og former hvilken sikkerhetspolitisk

"policy" et land velger. Disse faktorene er egenskaper ved beslutningstagere; stats- og styringsverket; og globale omgivelser. Hvordan disse faktorene påvirker utformingen av sikkerhetspolitikken diskuteres i lys av tre teorier: realisme, liberalisme og konstruktivisme. De tre perspektivene er brede teoretiske tanketradisjoner som kan kontrasteres i sitt syn på hva som driver atferd, altså hvilke faktorer som former handling og beslutninger. Realismen og liberalismen peker mot at individuell eller statlig atferd er rasjonell men har ulike forklaringer på hva som driver rasjonalitet, mens konstruktivismen mener at atferd er reflekterende og er subjektivt formet av aktørens persepsjon og oppfatning av situasjonen.

Hensikten med oppgaven er å kartlegge Norges cybertrussel-situasjon, og dernest å identifisere hvilke faktorer som påvirker sikkerhetspolitikken på cyberfeltet. Motivasjonen bak valg av problemstilling er mangelen på forskning på området, når det gjelder norske forhold. Etter det jeg har funnet omhandler norske akademiske artikler og masteroppgaver om cybersikkerhet primært risikoen for angrep, herunder risikoanalyser. Dernest finnes det et fåtall oppgaver som dreier seg om operative muligheter for norsk cyberforsvar og eventuelle motangrep. Motivasjonen bak valg av policyanalyse som metode er at dette bidrar til å kartlegge prosessen bak en beslutning og dermed forhåpentligvis skape større forståelse for utfallet. Analysemodellen i kombinasjon med de teoretiske perspektivene søker å vise tre ulike måter å oppfatte situasjonen. Oppgavens begrensninger ligger primært i empirien, grunnet kravet til bruk av offentlig informasjon. Et sentralt problem i den sammenheng er knyttet til hvor mye av informasjonen om cybersikkerhet som publiseres og i hvor stor grad Forsvaret kan være åpne om hele bildet. Det må tas høyde for at Forsvaret ikke kan oppgi all informasjon vedrørende cybertrusler, og at det dermed fremstår som et misforhold mellom oppgitt risiko for angrep og konkrete trusler. I kombinasjon med bruk av konstruktivistisk teori som stiller seg kritiske til nettopp politiske overdrivelser bør denne faktoren tas med i betraktningen.

Oppgaven inneholder, foruten innledningen med et avsnitt om begrepsavklaringer, en teoridel, en metodedel, en empiridel, en diskusjonsdel og til sist en avslutning med noen konkluderende bemerkninger. Teoridelen består av en redegjørelse av sikkerhetspolitisk teori, dernest de teoretiske perspektivene realisme, liberalisme og konstruktivisme. Teoridelen søker å sette en ramme rundt den kommende empiriske dataen. Neste kapittel er metodedelen fordi

dette skal redegjøre for hvordan dataen i empiridelen er innhentet og bearbeidet, samt begrunnelse for dette og forklaring på eventuelle mangler i tilgjengelig empirisk informasjon. Metodedelen inneholder en redegjørelse av metoden som er valgt: policyanalyse, i tillegg til metoden som er brukt for å innhente og bearbeide dataen: dokumentanalyse. Dette er to kvalitative metoder, hvilket det kort redegjøres for. Empiridelen består av all tilgjengelig informasjon om cybersikkerhetspolitikk i Norge som anses nødvendig for å besvare problemstillingen. I analysedelen skal den empiriske dataen og teorien settes sammen og diskuteres opp mot problemstillingen. Dette innebærer at ved hjelp av policymetoden skal teorien gi nye forklaringer til de empiriske dataene. Avslutningen inneholder en kort oppsummering av oppgavens sentrale funn som svar på problemstillingen.

Før alt dette følger en nødvendig begrepsavklaring av noen sentrale begreper med forklaring av de forbehold som er tatt spesifikt for denne oppgaven.

1.2 Begrepsavklaringer

Cybersikkerhet er et tema som byr på mange nye og potensielt ukjente begreper som behøver en forklaring. Det kan være hensiktsmessig å ha noen begreper avklart før teori- og empirikapitlene slik at teksten i disse delene flyter bedre. I det følgende kommer derfor en kort innføring i noen utvalgte begreper som er sentrale for oppgaven, og hvordan begrepene vil brukes spesifikt i denne oppgaven.

Cyber er et begrep som stammer fra ordet cybernetics, eller kybernetikk på norsk. Kybernetikk er et studiefelt som dreier seg om å skape teknologiske kommunikasjons- og kontrollsystemer i maskiner eller sågar roboter. I dag er kybernetikk og begrepet cyber nært forbundet med internett og datateknologi (Oxford Dictionary 2017).

Cybersikkerhet er sikringstiltak på cyberfeltet. Sikkerhet er både tilstanden man er i når man er fri fra fare og trusler, men også prosessen for å nå det punktet gjennom preventive tiltak. For eksempel betyr begrepet cybersikkerhet både det å være trygg i cyberspace, men er også

prosessen gjennom tiltak for datasikkerhet (Internet Live Stats 2017). Cybersikkerhet er både det offentlige og det privates ansvar. Sikring av datasystemer ved å jevnlig oppdatere sikkerhetsprogramvaren er enhvers databrukers ansvar, mens det offentlige er ansvarlige for systemovervåkning, etterretning og koordinering av tiltak (Langø 2011). I denne oppgaven er cybersikkerhet definert som informasjonssikring av digitale trusler mot individer, systemer og samfunnet.

Cyberdomenet, eller *cyberspace*, kan forenklet sies å referere til det digitale rom. Etterretningstjenesten har beskrevet dette som "bredden av digitale løsninger som moderne samfunn baserer seg på innen kommunikasjon, oppbevaring av informasjon og styringssystemer for infrastruktur" (Fokus 2011, s 31). Dette vil si at det både gjelder de fysiske gjenstandene som datamaskin og ledninger, men også de mer abstrakte strukturene som internett (Langø 2011, s. 230). Internett startet som en digital informasjonsdelingskanal og bygget i første rekke opp den nødvendige digitale infrastrukturen (se ordforklaring nedenfor), ble kommersialisert og "allemannseie" med sosiale medier, før det nådde tredje og foreløpig siste fase med mobile nett og nettskyer som får internett til å fremstå som allstedsnærværende (Langø og Sandvik 2013, s. 221-222). Cyberdomenet kan beskrives som en "sammenkobling av informasjonssystemer" og "inkluderer fysiske og virtuelle nettverksenheter, kommunikasjonsinfrastruktur, media og data" (FFI 2013, s 1). Informasjon i cyberdomenet kan ligge både på åpne og lukkede nett, der åpne nettverk er informasjon hvem som helst har tilgang til på internett, mens lukkede nettverk krever egne tillatelser (FFI 2013). Eksempelvis er Forsvarets hemmelige nettbaserte informasjon på Forsvarets egne nettverk, og er ikke tilgjengelig eller søkbar på det allment tilgjengelige internett. Det er likevel teoretisk mulig å komme seg inn i lukkede nettverk.

Digital infrastruktur viser her til de fysiske gjenstander som muliggjør digitale løsninger, som for eksempel ledninger og rutere. I tillegg kan digital infrastruktur også vise til den programvaren de digitale løsningene er avhengige av for å kunne fungere (Meld. St. 37 (2014-2015)), da en datamaskin har tilpasset programvare for alle operasjoner den skal kunne utføre. Dette gjelder alt fra å skrive et Word-dokument til å spille kabal, eller søke etter noe på Google. Virus er kategorisert som digital sabotasje og har muligheten til å totalt ødelegge datamaskinens programvare, slik at den ikke kan brukes (Meld. St. 37 (2014-2015)).

Cybersikkerhet kan både referere til sikkerhetspolitikken på cyberfeltet, og til de digitale barrierer som sikrer informasjon på lukkede nettverk. Politisk cybersikkerhet dreier seg om å hindre trusler mot individer eller organisasjoner, noe som oftest gjelder informasjonssikkerhet, men også systemsikkerhet (Langø og Sandvik 2013, s. 222). Organisasjoner som anser sin informasjon som særlig sensitiv vil typisk ansette egne hackere for å forsøke å hacke sine egne systemer, og dermed teste om det finnes smutthull eller svakheter i sikkerheten (Winterfeld og Andress 2013).

Digital sårbarhet viser her til produktet av (1) de samlede digitale løsningene i Norge og (2) risikoen for angrep. Hvor robuste systemene er vil spille inn på risiko-aspektet. Norge som et av verdens mest avanserte i-land har svært utbredt bruk av digitale løsninger, dette strekker seg fra digitale sykehusjournaler til systemer for strømnett og nettbank. Cyberangrep går ut på å utnytte disse sårbarhetene (Meld. St. 37 (2014-2015); Winterfeld og Andress 2013; Lewis 2002).

Skytjenester er en digital plattform for ekstern lagring av informasjon, som kan tilgjengeliggjøres via internett på en vanlig datamaskin dersom man har koder eller liknende for å få tilgang (Datatilsynet 2017). Et eksempel på en velkjent skytjeneste er Apples iCloud som brukes på blant annet iPhone.

Hacking refererer til prosessen med å trenge inn i lukkede nettverk og dermed tilgjengeliggjøre skjulte informasjonskanaler. En hacker kan komme seg inn i programvaren for så å legge igjen en usynlig, spionerende programvare som observerer og lagrer informasjon (Langø og Sandvik 2013, s. 223). I nyere tid har begrepet *hacktivist* kommet på banen i sammenheng med grupper som Anonymous og WikiLeaks. En hacktivist er en aktivist med et demokratisk mål for øyet, som hacker seg inn i systemer for å publisere hemmelig informasjon som vedkommende mener at burde være åpen for offentligheten. Dette gjelder typisk informasjon myndigheter forsøker å holde skjult. En annen vanlig hacker-metode er å benytte en såkalt *trojaner* (Langø og Sandvik 2013, s. 223). Trojanermetoden kan gå ut på å sende en tilsynelatende uskyldig e-post med beskjed om å laste ned en fil eller trykke på en link, men det som skjer når man gjør dette er at man har

lastet ned et virus eller en spionprogramvare. Et *digitalt virus* har typisk til hensikt å ødelegge datamaskinens programvare, såkalt digital infrastruktur (Langø og Sandvik 2013, s. 224).

Cybervåpen refererer typisk til programvare som kan benyttes til å skaffe seg tilgang til lukket programvare med hensikt å ødelegge den. For eksempel fikk Iran sitt atomanlegg hacket, og deler av kritisk programvare ble ødelagt slik at den ikke kunne fungere som den skulle (Winterfeld og Andress 2013). Cybervåpenet i den sammenheng er programvaren hackeren brukte for å trenge inn i systemet og ødelegge det. En slik operasjon kalles et *cyberangrep*.

Digital sabotasje vil si å "bruke offensive digitale verktøy som har evne til å skade, ødelegge, forstyrre eller undertrykke administrasjons- og ledelsessystemer sivilt eller militært" (Fokus 2016, s 82).

Cyberkrig kan vise til et foreløpig teoretisk scenario der cyberangrep brukes av to stater mot hverandre, altså besvares et cyberangrep med et cyber-motangrep. Dette anses ikke som særlig sannsynlig, og det er bredere teoretisk enighet om at cyberkrig heller vil ha trekk fra *hybrid krigføring* der et initielt cyberangrep er ment å destabilisere kritisk infrastruktur for så å benytte andre mer tradisjonelle metoder for krigføring (Meld. St. 37 (2014-2015) s 11).

Cyberforsvaret er en militær organisasjon i Forsvaret som har ansvar for å beskytte Forsvarets nettverksbaserte systemer fra digitale angrep. Cyberforsvaret jobber med den tekniske delen av cybersikkerhet, mens Etterretningstjenesten jobber med informasjonsinnhenting, overvåkning og forebygging (Forsvaret.no 2017).

En *doktrine* er militærets plan eller rammeverk for hva slags linje de skal følge fremover. En doktrine vil typisk være en slags strategi både i fredstid og dersom konflikt oppstår (Winterfeld og Andress 2013, s. 31). Et typisk doktrine-skille går mellom offensiv eller defensiv strategi, der Norge følger en defensiv strategi med et kun et minimumsforsvar i fredstid (Knutsen 2013). Eksempelvis finnes det to kjente amerikanske doktriner fra den kalde krigen: containment-strategien som gikk ut på å hindre Sovjetunionens ideologiske ekspansjon ved å isolere dem; og deterrence-doktrinen som var en avskrekkingsstrategi. Disse doktrinene la et prinsipielt rammeverk for hvordan sikkerhetspolitiske og militære operasjoner

skulle utføres. Avskrekking er eksempelvis en mer militært offensiv strategi, mens deterrence benyttet flere liberale virkemidler som handel og diplomati (Hook og Spanier 2010). En *cyberdoktrine* er rammeverket for den sikkerhets- og utenrikspolitiske strategiske planen på cyberfeltet (Winterfeld og Andress 2013, s. 31-33).

Dersom en doktrine skal utgjøre et politisk planverk kan det kalles en *policy*. På engelsk skiller man mellom policy, som er en bestemt politisk plan på et felt (Savigny og Marsden 2011, s.89), og politics som refererer til den politiske prosessen med for eksempel valgkamp eller avstemninger over vedtak. På norsk kaller vi i utgangspunktet begge disse aktivitetene for "politikk", hvilket kan skape misforståelser. Derfor er ordet policy benyttet i denne oppgaven i sammenheng med analysen av vår sikkerhetspolitikk på cyberfeltet. Siden ordet policy blir brukt vil begrepet også bøyes eksempelvis til bestemt form på norsk: "policyen", tross at dette verken er korrekt norsk eller engelsk anses det for dette formål som det beste alternativ. Det er vanlig å benytte begrepet utenrikspolitisk analyse, dette referer til policyanalyse og er ment som en oversettelse av analysemetoden Foreign Policy Analysis (FPA) (Fermann 2013, s. 90). Jeg har valgt å ikke bruke begrepet utenrikspolitisk analyse for ikke å skape forvirring rundt forskjellen mellom sikkerhetspolitikk og utenrikspolitikk, som jeg ikke går nærmere inn på.

Et annet begrep som behøver en grundigere avklaring er oppgavens oversettelse av det teoretiske perspektivet *Securitization Theory,* hvilket er et konstruktivistisk perspektiv som tilskrives Københavnerskolen. Begrepet er skapt med bakgrunn i ordet security og derav verbet "to securitize". Security betyr som kjent sikkerhet på norsk, men vi har ikke noen enkel eller naturlig oversettelse for verbet securitization, heller ikke en velkjent teoretisk oversettelse. På dansk kalles det teoretiske tankesettet "sikkerhedsliggjørelse" som kan oppfattes noe tungvint. Det kunne tenkes at sikkerhetiseringsteori eller sikkerhetsliggjøring kunne benyttes, men jeg har likevel valgt å lage en fornorsking av teorinavnet som resulterte i "*securitiseringsteori*", da det ligner mest på det originale navnet. Dette er gjort for å understreke at det dreier seg om en spesifikk teori, av hensyn til originaliteten til teorien, og ikke vanlig bruk av et verb. Det tas likevel forbehold om at heller ikke securitiseringsteori fremstår som det opplagt beste alternativet som begrep.

2. Teori

I dette kapittelet følger en generell redegjørelse av sikkerhetspolitikk fulgt av tre teoretiske perspektiver på sikkerhetspolitikk: realisme, liberalisme og konstruktivisme. Disse perspektivene er valgt på grunn av sine ulike grunntanker: realismen og liberalismen er begge basert på at aktørers handling er rasjonelle, men er uenige i hva som motiverer rasjonelle valg. Konstruktivismen anses her som et reflekterende teoretisk perspektiv og hevder at handling blant annet formes av aktørens identitet. Bakgrunnen for valget av de teoretiske perspektivene er å identifisere flere innfallsvinkler til cybersikkerhet, samt å undersøke ulike drivkrefter som finnes bak Norges sikkerhetspolitiske policy på cyberfeltet. Cybersikkerhet har også skapt en viss debatt om hvorvidt feltet bør anses som sikkerhetspolitisk relevant og i nasjonal interesse eller ikke, og de to perspektivene kan bidra til å vise ulike innfallsvinkler til dette spørsmålet. En utdypende forklaring på hvilke antagelser de teoretiske perspektivene har på cyberfeltet blir gitt i sammenheng med gjennomgangen av realismen, liberalismen og konstruktivismen nedenfor.

Realismen og konstruktivismen er videre valgt for å vise to ulike innfallsvinkler til hvilke temaer som anses som sentrale for sikkerhetspolitikk, hvem som er de sentrale aktørene og hva som er de sentrale drivkreftene bak behovet for sikkerhetspolitiske tiltak. Disse aspektene varierer ut i fra hvilket teoretisk perspektiv det tas utgangspunkt i. Perspektivene viser to ulike utgangspunkt for sikkerhetspolitisk forskning: fra det mer tradisjonelle synet på sikkerhet som finnes i realismen og liberalismen til nyere perspektiver som konvensjonell konstruktivisme.

Med dette som bakgrunn er de primære antagelsene (1) trusselsituasjonen på cyberfeltet kan vurderes objektivt og drives av rasjonelle vurderinger, eller (2) trusselsituasjonen på cyberfeltet er en subjektiv fortolkning og kan være preget av overdrivelse. De primære antagelsene spisses videre med de teoretiske perspektivenes underteorier, særlig neo-realisme og securitiseringsteori, som blir nærmere forklart senere. En nærmere forklaring av disse underteoriene blir gitt i oppgavens teoridel, men de foreløpige antagelsene er at (3) det er i staters rasjonelle interesse å utnytte den anarkiske strukturen i cyberdomenet til sin fordel med

de virkemidler som åpner seg, eller (4) risikoen for cyberangrep er større enn den faktiske trusselen og behovet for cybersikkerhet er dermed overdrevet og bør ikke anses som av nasjonal interesse å sikre.

Kapittelet begynner med en redegjørelse av sikkerhetspolitikk, dernest følger en redegjørelse av de teoretiske perspektivene realisme og konstruktivisme.

2.1 Sikkerhetspolitikk

Begrepet sikkerhetspolitikk er satt sammen av ordene "sikkerhet" og "politikk". Den leksikalske betydningen av ordet sikkerhet gjelder en tilstand med "fravær av uønskede hendelser, eller frihet fra fare og frykt" (SNL Stranden og Rosvold 2015). En bred definisjon av begrepet politikk er "alle sosiale forhold som innebærer makt, styre og autoritet" (Østerud 2014, s 15). Når disse begrepene settes sammen dreier det seg om den politiske prosessen som primært går ut på å sikre landet mot eksistensielle trusler av territorium, interesser og suverenitet. Den norske regjeringens definisjon av sikkerhetspolitikkens hovedmål er "å ivareta Norges suverenitet, territorielle integritet og politiske handlefrihet" (Regjeringen.no 2017).

I fagdisiplinen internasjonal politikk er studiet av sikkerhet i sentrum, og fokuset på sikkerhetspolitisk forskning vokste frem som følge av første verdenskrig. I overgangen til den kalde krigen dreide sikkerhetspolitiske studier seg mer om strategi, og som forskningsfelt ble det kalt strategiske studier helt frem til åttitallet, noe som understreker viktigheten av strategi i en tilstand av vedvarende konflikt (Wæver og Buzan 2016, s. 419). Dette henger sammen med at sikkerhet i internasjonale relasjoner dreier seg om overlevelse og hva som sørger for overlevelse (Collins 2016, s. 1). I denne sammenhengen gjelder ikke dette kun individuell overlevelse, men overlevelse for en rekke ulike faktorer som systemer, ideer og verdier.

Sikkerhetspolitikk som fagfelt har vært i stadig endring hva gjelder de primære fokusområdene. Årsaken er at sikkerhetspolitikken speiler samfunnets opplevde trusler på det

aktuelle tidspunktet, og med tiden har det skjedd en utvidelse av hva som blir ansett som den relevante sikkerhetspolitiske agenda (Wæver og Buzan 2016, s. 418). Som politisk område er sikkerhetspolitikk en del av utenrikspolitikken og er i stor grad overlappende med forsvarspolitikk. Sikkerhetspolitikken søker å forebygge, begrense og håndtere trusler mot rikets territorielle sikkerhet og politiske uavhengighet, herunder å sikre statens eksistens og ivareta statens politiske handlefrihet (Fermann 2013, s 13-14.). Den forsvarspolitiske tilknytningen tydeliggjøres i den tradisjonelle sikkerhetspolitikkens fokus på militære doktriner som toneangivende for fagfeltets forskningsområder, eksempelvis var avskrekkingsstrategien meget sentral i sikkerhetspolitisk tankegang under den kalde krigen (Wæver og Buzan 2016, s. 422).

Et slikt tradisjonelt militært syn på sikkerhetspolitikk finnes hos Holst (1967) som mener at sikkerhetspolitikk er de tiltak og aktiviteter som er ment å skulle influere maktmessige forhold mellom statene, og at staten fører sikkerhetspolitikk for å gardere seg mot at andre stater benytter fysiske tvangsmidler mot dem (Holst 1967, s 21). Dette synet reflekterer sikkerhetspolitikkens fokus på handlingsrom og muligheter som resultat av det eksterne miljøet staten befinner seg i.

Sikkerhetspolitikk har blitt karakterisert som å dreie seg om sikringen av ulike aspekter av nasjonal interesse. En tradisjonell forståelse av dette går ut på at "nasjonal interesse" dreier seg om statlig sikkerhet, mens en utvidet forståelse av sikkerhetspolitikk trekker inn temaer knyttet til individets sikkerhet og sikkerhet for grupper (Hough 2008, s. 6-7), eksempelvis etniske minoriteter. Nasjonal interesse i sikkerhetspolitikk kan oppfattes som ivaretakelsen av de sikkerhetspolitiske hovedmålene som regjeringen har definert innenfor militære, politiske, miljømessige, helsemessige og sosiale områder. På den annen side er saker av nasjonal interesse også gjenstand for politiske kompromiss, hvilket gjør at det som er ønskelig ikke alltid er gjennomførbart i praksis (Huntington 1960, s. 294-295).

Definisjonene av sikkerhetspolitikk er mange, og kretser rundt ord som "trygghet", "trussel" og "sårbarhet" (se f.eks. Collins 2016). Sikkerhet er beskrevet som mangel på trussel om krig, men også en trygghet i, eller forventning om, at dersom krig oppstår vil vi ikke tape (Bellami 1981 i Collins 2016, s. 3). Dette kan overføres til et bredere spekter av emner som ikke bare

innbefatter trussel om krig, men også trussel mot verdier. Sikkerhetspolitikken skal være med på å ivareta landets interesser innad ved å sikre dets posisjon utad. Dette er hvorfor sikkerhetspolitikk i vår globaliserte verden har blitt beskrevet som et felt som eksternaliserer interne interesser, og internaliserer eksterne emner (Collins 2016). Sikkerhetspolitikk er som nevnt ment å reflektere befolkningens behov og ønske om trygghet, og omfatter et bredt spekter av emner der alle har fellestrekket "nasjonal interesse" (Hough 2008, s. 10-11). På sett og vis kan sikkerhetspolitikk sies å reflektere hvilke potensielle trusler befolkningen er mest redde for. I dagens Europa vil dette typisk være terrorisme, for eksempel har Norge etter en rekke europeiske terrortilfeller sikret Karl Johans gate for å forhindre at en lastebil skal kunne kjøres inn i folkemengden (Haugan 2017). Utover terrorisme, som ofte kommer fra ikke-statlige aktører, handler sikkerhetspolitikk typisk om trusler i temaer som militær konflikt og mellomstatlig krig; kultur, identitet og verdier; klima og miljø; og helse (Hough 2008, s. 10; Kveberg og Johnsen 2013, s 14).

På bakgrunn av disse forklaringene er det her tatt utgangspunkt i en definisjon av norsk sikkerhetspolitikk som er hentet fra FFIs rapport “Cyberdomenet, cybermakt og norske interesser” (Kveberg og Johnsen 2013). Sikkerhetspolitikk er "den norske statens evne til å beskytte norske statsborgere mot eksistensielle eller alvorlige trusler, ivareta grunnlaget for velferd, og ivareta statens styreform og territorielle integritet" (Lunde m. fl.. 2008, s. 75, Kveberg og Johnsen 2013, s. 14). Denne definisjonen, og de interesser som ivaretas, utgjør utgangspunktet for hvordan begrepet "nasjonal interesse" er brukt i denne oppgaven.

Som akademisk felt finnes det en rekke fokusområder for sikkerhetspolitikk der ulike teoretiske perspektiver delvis er uenige om hvilke felt som skal være del av sikkerhetspolitikken. Dette fordi sikkerhetspolitikkens innhold ikke er statisk, men følger samfunnet ettersom det endrer seg. Eksempelvis viser nyere sikkerhetspolitisk teori et bredere spekter av fokusområder enn tidligere, og inkluderer blant annet miljøhensyn, terrorisme og digital sårbarhet (Collins 2016, Hough 2008). Satt på spissen kan det sies at tradisjonell sikkerhetspolitikk dreide seg mer om krig, allianseforhold, strategi og militær doktrine (Holst 1967), og mindre om pandemier og ekstremvær (Collins 2016). Dette skillet mellom mer tradisjonell og "nyere" sikkerhetspolitikk reflekteres særlig i ulike perspektivers syn på fagfeltet, og spesielt hva som er relevante emner og hvem som er relevante aktører. Det er

utfordrende å beskrive sikkerhetspolitikk i generelle termer uten å farges av de ulike perspektivene, men det er også nødvendig å gi en kort innføring i emnet. Det er derfor tatt utgangspunkt i at sikkerhetspolitikk som fagfelt har blitt bredere uavhengig av teoretisk perspektiv. Det kan hevdes at det tidligere mer snevre synet på sikkerhetspolitikk skyldes at feltet var dominert av forskere på internasjonale relasjoner (IR) som hovedsakelig fulgte realismens statssentrerte syn på sikkerhetspolitikk. I denne oppgaven vil hovedvekten ligge på sikkerhetspolitikk som fagfelt med et særlig fokus på problemstillingens tema digital sikkerhet.

2.1.1 Cybersikkerhet

Teoretisk er cybersikkerhet delt mellom to skoler: utviderne og tradisjonalistene. Utviderne ser cybersikkerhet som en progressivt naturlig del av sikkerhetspolitikken og sikkerhetspolitisk forskning, mens tradisjonalistene inntar motsatt syn og ser sikkerhetspolitikk primært som tradisjonell mellomstatlig krigføring. Cybersikkerhet ble plassert på agendaen på søttitallet i USA, mens resten av verden fulgte på nittitallet på grunn av økt bruk av internett som åpnet for økt sårbarhet og risiko (Dunn Cavelty 2016, s. 402). Det er forventningen til at sårbarhet og risiko utgjør en så stor fare som gjør at cybersikkerhet aktualiseres som sikkerhetspolitisk problem (Dunn Cavelty 2010). Det er her tatt utgangspunkt i samme definisjon av begrepet cybersikkerhet som er gitt i innledningen: informasjonssikring av digitale trusler mot individer, systemer og samfunnet.

Sikkerhetspolitikk på cyberfeltet foregår primært på feltet informasjonssikring fordi informasjon anses som et maktmiddel i global politikk. Informasjon gir makt over kunnskap, meningsdannelse, ideer og oppfatninger (Dunn Cavelty 2016, s. 401). Selv om etterretning ikke er et nytt interesseområde for sikkerhetspolitikk er feltet mer aktuelt i dag på grunn av mengden av nettbasert informasjon. Dette er mye av grunnen til at cyberfeltet nå beskrives som av stor nasjonal interesse, blant annet på grunn av mengden av personinformasjon hver innbygger legger igjen på internett (Dunn Cavelty 2016, s 401). Slik sett er den nasjonale interessen både grunnet sårbarheten for angrep på kritisk infrastruktur, og trusselen om informasjonsspionasje. Dette gjør at visse skoler taler for en økning av cybersikkerheten, med

mer offensive metoder. På den annen side er det hevdet at det ikke er et proporsjonalt forhold mellom risiko og sannsynlighet på den ene siden, og sårbarhet på den andre, hvilket har åpnet for en kritikk av cybersikkerhet for å planlegge for det verst tenkelige. Den antatt lave sannsynligheten taler imot at cybersikkerhet skal være på dagsorden for nasjonal interesse i sikkerhetspolitikken overhodet (Dunn Cavelty 2016, s. 414).

Cyber-sikkerhetspolitikk er preget av de strategiske valgene mellom en offensiv eller en defensiv linje. Norges militære doktriner har ligget langs en defensiv linje, med fokus på diplomati og et minimumsforsvar i fredstid (Knutsen 2013). Digitale trusler endrer de sikkerhetspolitiske mulighetene og gjør veivalg mellom defensiv og offensiv sikkerhetspolitikk vanskeligere. Suverenitetshevdelse er en sentral del av sikkerhetspolitikken og kan hevdes å være en del av en defensiv linje, mens i cyberdomenet finnes ikke landegrenser og "mesteparten av det er privateid" (Kveberg og Johnsen 2013, s 7). Dette gjør at digitale grenser ikke kan totalsikres fra statens side og dermed svekkes Forsvarets mulighet til å gjennomføre suverenitetshevdelse på lik linje med øvrig sikkerhetspolitikk (Kveberg og Johnsen 2013, s. 7). Det hevdes at dagens krigføring har endret karakter fra et fokus på best ressurser på slagmarken, til å ha best informasjon om slagmarken (Langø 2013, s. 231). Dette skiftet reflekteres ved at cybersikkerhet anses som særlig relevant i dag.

En vanlig sikkerhetspolitisk doktrine fra den kalde krigen er avskrekking (deterrence). Det finnes visse tilhengere av denne doktrinen også i cyber-sikkerhetspolitikk, men den har vist seg vanskelig av en rekke grunner. For en vellykket avskrekking er man avhengig av å overbevise motparten om at man er kapabel og villig til å gjennomføre et stort angrep, hvilket igjen krever en motpart som er åpen om å være motparten. Avskrekking er også avhengig av en måte å måle to parters kapabilitet opp mot hverandre, noe som er svært vanskelig når det gjelder cyber (Dunn Cavelty 2016, s. 413). Videre er risikohåndtering vanskelig på cyberfeltet fordi risikoen er lav mens potensialet for ødeleggelse er høyt, det er dermed nødvendig med en doktrine som tar høyde for at risikoen aldri kan være null. En slik doktrine kan kalles motstandsdyktighet (resillience på engelsk) og går ut på å forme en plan B med strategier for at systemene gjenopprettes raskt etter et angrep. Mostandsdoktrinen aksepterer risiko og planlegger for den (Dunn Cavelty 2016, s. 413).

Da cyberfeltet er preget av usikkerhet taler enkelte for at det bør rettes mer fokus på normbygging og internasjonale lover. Disse punktene er sett på som relevante fokusområder for cybersikkerhet som tar sikte på mindre militært baserte løsninger. I følge Langø (2013) kan cyberfeltet ses både som et stort potensiale, som urealistisk, og som et felt som har fått overdrevent fokus. Langø (2013, s. 229) identifiserer to "skoler" som dominerer cyberfeltet: de som ønsker å ekspandere og de som ønsker å bremse, eller det Langø (2013) kaller revolusjonister og tradisjonalister. En ekspanderende tilnærming ser potensialet for informasjonsmakt i digitale angrep, som igjen vil gi mer makt i militære operasjoner. I dette synet handler det om å utnytte sårbarhet og å skaffe seg makt, og cyberdomenet gir gode muligheter for å gjøre dette effektivt og enkelt. Den bremsende tilnærmingen finnes hos tradisjonalistene som mener at en cyberkrig er urealistisk og mangler empirisk belegg. Dersom cyberkrig defineres som en krig utført utelukkende i "cyberspace" er det nærmest utenkelig (Langø 2013, s. 234). På bakgrunn av dette er det nødvendig å definere hva som her vil anses som cyberkrig. Som beskrevet over kan digitale angrep ta mange former, og hensikten vil trolig ikke primært være å gjennomføre et cyberangrep i seg selv, men snarere et middel for å destabilisere en stat. Et angrep av stor skala kan bidra til å tippe maktbalansen og dermed skape større sårbarhet. Sett på denne måten kan et vellykket cyberangrep brukes som et middel på vei mot målet, heller enn målet i seg selv. I følge tradisjonalistene vil cyberspace endre en stor del av forsvarspolitikken fordi det er vanskelig å forsvare seg mot, men enkelt å angripe andre. Slik sett "favoriserer" cyber-sikkerhetspolitikken generelt på sett og vis angrep som det beste forsvar. Riktig nok hevder de videre, med utgangspunkt i Clausewitz' kriterier for krig (blant annet at krig er voldelig og fysisk og dermed favoriserer landkrig), at slike angrep mangler alle relevante egenskaper for vellykket strategi, og dermed ikke bør anses som sikkerhets- eller forsvarspolitisk relevant (Langø 2013, s. 234).

2.2 Perspektivene

Teoretiske perspektiver er hjelpemidler for å forklare logikken bak en situasjon, hendelse, avgjørelse, atferd eller liknende, og tar ulike utgangspunkt i hva de sentrale forklaringsfaktorene anses å være. I denne oppgaven er det valgt tre teoretiske skoleretninger:

realisme, liberalisme og konstruktivisme. Teoriene er valgt med en tanke om at deres ulike rasjonale kan benyttes for å undersøke hva som driver den sikkerhetspolitiske situasjonen på cyberfeltet i Norge, og gi tre ulike syn på hva sikkerhet er. Det finnes et mylder av teoretiske perspektiver og underteorier i statsvitenskap, og mange er vanskelige å plassere helt rett. Ofte er perspektivene influert av flere teorier som har skapt en slags hybrid. Av hensyn til leservennlighet og verdien av kategorisering har jeg sett meg nødt til å ta noen avgjørelser når det gjelder plasseringen av underperspektivene da disse ikke er opplagte, hvilket vil bli argumentert kort for i gjennomgangen av perspektivene nedenfor.

Det er i denne oppgaven tatt utgangspunkt i et tradisjonelt teoretisk skille mellom rasjonelle og reflekterende perspektiver (Kurki & Wight 2013, s. 24). Rasjonelle teorier er de som tar utgangspunkt i at aktøren handler rasjonelt, og gjelder typisk liberalisme og realisme. Forenklet er liberalismens utgangspunkt at samarbeid er rasjonelt fordi det gir best utfall for aktøren, mens realismen går ut fra at det er strukturen på den internasjonale arena som gir et fåtall av alternative handlinger hvor kun én av dem er rasjonell (Mearsheimer 2013, s. 78). Det reflekterende perspektivet tar utgangspunkt i den konstruktivistiske tradisjonen og avviser teorien om rasjonell atferd. Konstruktivismen mener at forskning ikke bør gå ut fra antagelser og sosialt skapte forståelser av et fenomen eller begrep, men har ideer og subjektiv forståelse i sentrum. På aksen mellom rasjonell og reflekterende er motpolen til strukturell realisme postrukturalisme, som dermed er mer radikalt konstruktivistisk enn den konvensjonelle konstruktivismen som er benyttet i denne oppgaven. Konvensjonell konstruktivisme mener at det eksisterer en objektivt materiell virkelighet: de betviler ikke eksistensen av et fjell, men betydningen av det vil kunne variere. Poststrukturalismens hovedfokus er på dekonstruksjon av språket og et kritisk syn på aksepterte forståelser av begreper (Kurki og Wight 2013, s. 30).

De rasjonelle perspektivene

2.2.1 Klassisk realisme

Den klassiske realismen har sitt opphav i en realisme-tankegang som trekker helt tilbake til antikkens Hellas. Realisme er et paraplybegrep på en av de mest sentrale tanketradisjonene om internasjonale relasjoner, og er trolig den tradisjonen som er mest brukt når det tales om mellomstatlig konflikt (Glaser 2016, Wohlforth 2008). Klassisk realisme er en variant av realismetradisjonen og tar utgangspunkt i at internasjonale relasjoner dreier seg om stater og deres selvhevdelse. Perspektivet bygger blant annet på Thomas Hobbes' Leviathan og Niccolò Machiavellis Fyrsten, som begge omhandler maktsøkende individer med det utgangspunkt at menneskelig natur er slik. De to verkene konkluderer med at en streng og beskyttende stat eller leder er nødvendig for å temme naturtilstanden, da dette er i nasjonal interesse (Lebow 2013, s. 61).

Staten er den eneste relevante aktøren og har som naturtilstand å være makt- og trygghetssøkende fordi menneskelig natur er slik. Den klassiske realismen legger liten vekt på internasjonale normer, institusjoner eller lover som forklaringsfaktor for statlig atferd, men hevder i stedet at det er nasjonal interesse som står i sentrum i staters maktsøken (Glaser 2016, s. 14). Konflikt er uunngåelig og verden kan dermed aldri oppleve en konfliktløs tilstand. Med dette sagt kan konfliktene holdes på et kontrollerbart nivå slik at det ikke utbryter krig, som typisk skyldes at den eksisterende maktbalansen mellom stater er i favør av én stat over en annen. Denne påstanden kalles maktbalanseteorien og er realismens grunntanke når det gjelder mellomstatlig interaksjon. Det eneste som veileder staten i sin interessehevdelse er hva som er i nasjonal interesse, der de primære nasjonale interessene er overlevelse og sikkerhet. Generelt oppnås overlevelse og sikkerhet for realister gjennom militærmakt og en sterk stat, fordi sikkerheten er best når man evner å forsvare seg (Glaser 2016, s. 15). Realisten Hans Morgenthau (1948) mente at et sterkt styre var like viktig for innenrikspolitikk som den globale arena, og at samfunn med sterkt sentralstyre kunne dempe maktsøkende individer og utbrytergrupper som igjen ville skape en fredeligere tilstand. Morgenthau hevdet videre at et svakt styre var grunnen til at det tyske samfunnet bukket

under for nazismen under opptrappingen til andre verdenskrig (Morgenthau 1948 i Lebow 2013, s. 63).

Samarbeid er lavt ansett for klassiske realister, og selv allianseforhold oppfattes som et tveegget sverd (Lebow 2013, s. 62). Likevel kan realister anse allianseforhold som nyttige der det bidrar til å kollektivt redusere kostnadene til forsvar, men de mangler tro på verdien av en avtale. En motpart har alltid mulighet til å lyve og utnytte, hvilket etterlater staten mer sårbar (Glaser 2016, s. 23). Egeninteresse går først i alle tilfeller, og statens største frykt i denne usikre tilstanden er at motparten skal ha mulighet og motiv for angrep (Mearsheimer 2013, s. 79). På tross av dette er det i statens interesse å skape samfunnsmessige bånd som binder sammen felles kultur og interesser fordi dette genererer makt i den forstand at det er lettere å dra i samme retning. Dette er basert på en antagelse om at all form for politikk og menneskelig natur er maktsøkende, mens individer er gruppesøkende (Wohlforth 2008, s. 133). Logikken bak gruppetilhørighet ligger igjen i egoistisk maktsøken og er basert på et rasjonale om at man er mektigere jo flere som står bak en.

Som analyseverktøy forutsetter realismen en rekke faktorer, deriblant en anarkisk verden som består av stater som hver for seg er maktsøkende, og at makt anses både som et mål og som et middel. Realismen forutsetter videre at stater er rasjonelle og at hver enhetlig stat gjør seg opp en mening om hva den rasjonelle handlingen er ut fra egen materiell evne og de usikkerhetene som følger av å ikke vite motpartens motiver (Glaser 2016, s. 14-15). For de klassiske realistene er det menneskelig natur som sørger for rasjonelle handlinger, fordi menneskelig natur er egoistisk og gjør at individer og dermed stater handler i egeninteresse. En vanlig kritikk av realismen gjelder det overdrevne fokuset på staten som enhet, med lite fokus på regimetype, styringsform, eller individuelle egenskaper innad i en stat. Klassisk realisme fokuserer på at det er statens motiv og interesse som leder til maktsøken (Wohlforth 2008, s. 133), mens neo-realismen hevder at dette skyldes det anarkiske systemet, som forklares nærmere i avsnittet om neo-realisme.

Sett i sammenheng med oppgavens problemstilling vil klassisk realisme tale for å anse cyber som et sikkerhetspolitisk problem av nasjonal interesse fordi det er rasjonelt å søke så god sikkerhet som mulig. Dette fordi det er i statens interesse å hindre at andre er teknologisk

overlegne, eller at ens eget forsvar ikke er tilstrekkelig godt. Det er videre ansett som menneskelig natur å være maktsøkende hvilket taler for motpartens utnyttelse av enhver metode, ny eller gammel, for å sikre seg makt.

2.2.2 Neo-realisme

Neo-realisme er en annen variant av realismetradisjonen som kan oppfattes som en videreføring av den klassiske realismen, men med andre primære antagelser. Perspektivet kalles vekselvis strukturell realisme eller neo-realisme og tar utgangspunkt i at strukturen på den globale arena er det som dirigerer statlig atferd, ikke menneskelig natur. Den globale strukturen er anarkisk, og er kjennetegnet av mangelen på et overnasjonalt styrende organ (Mearsheimer 2013, s. 79-80). Før redegjørelsen fortsetter er det nødvendig med en begrepsavklaring: internasjonalt anarki er en betegnelse på at den internasjonale arena mangler overstatlig myndighet, og er ikke en tilstand som forutsetter kaos eller krise (Mearsheimer 2013, s. 79-80). Det hevdes at anarki er det motsatte av hierarki (Mearsheimer 2013, s. 79), men for denne oppgavens formål anses det som unødvendig å legge avgjørende vekt på dette videre. Anarkisk struktur anses her som mangelen på et overnasjonalt styrende organ, og er dermed forenlig med en rangering av staters relative maktforhold.

Med utgangspunkt i klassisk realisme ville menneskelig natur sørget for en evig tilstand av konflikt fordi maktsøken er evigvarende, men neo-realister er uenige i dette pessimistiske synet på naturtilstanden. Neo-realister tillegger ingen vekt på menneskelig natur, men hevder i stedet at den anarkiske strukturen sørger for et selvhjelpssystem der hver stat kompromissløst handler ut fra hva som er det beste alternativet for en selv. Stater er rasjonelle og evner å utarbeide strategier for overlevelse (Mearsheimer 2013, s. 79). Status quo-stater er sikkerhetssøkende snarere enn maktsøkende, og er primært interessert i å ivareta egen selvråderett (Glaser 2016, s 15). På den annen side finnes de mer maktsøkende statene med større globale ambisjoner, som forsøker å skifte maktbalansen i egen favør (Mearsheimer 2013, s. 81). Tross dette skillet har stater vanskelig for å forstå hverandres intensjoner, hvilket skaper konkurranse om makt på materielle størrelser (Glaser 2016, s. 18).

Neo-realister mener at stater er rasjonelle og velger det rasjonelle alternativet i enhver situasjon. Dette innebærer en antagelse om at det alltid finnes én objektivt best mulighet i den anarkiske strukturen. Strukturelle realister har videre pekt på at den anarkiske strukturen globalt kan føre til et såkalt sikkerhetsdilemma (Glaser 2016, s. 21). Sikkerhetsdilemmaet innebærer at stat As forsøk på å øke sin sikkerhet gjør at stat B tolker dette til å bety at sikkerheten er truet og dermed øker sin, hvilket skaper et slags opprustningskappløp basert på usikkerhet og frykt med stort potensiale for konflikt. På tross av dette kan sikkerhetsdilemmaet nyanseres av hegemoni eller gjensidig avskrekking dersom kappløpet når et punkt der den ene har brukt opp sine midler først. Resultatet av dette er at den ene parten står igjen som hegemon i en unipolar maktorden. En annen mulighet er en bipolar maktbalanse der to parter er tilnærmet like sterke. Stabilitet under bipolaritet oppstår gjennom gjensidig avskrekking der begge parter er tilsvarende redde for utfallet av konflikt med hverandre, slik at det er i begges interesse å ikke handle (Glaser 2016, Mearsheimer 2013, Lebow 2013).

Neo-realistene kan deles i to grupper: offensive og defensive realister, der Mearsheimer (offensiv) og Waltz (defensiv) er de mest kjente. Skillet går primært ut på hva de to retningene anser at driver en aktørs handling og hva insentivene er, gitt at målet er makt og/eller posisjon. Makt anses av offensive realister som målet i seg selv fordi makt gir posisjon, mens for defensive realister anses makt som nødvendig for å nå sitt mål: sikkerhet (Glaser 2016, s. 16). For offensive realister er det rasjonelt for stater å søke så mye makt som mulig fordi dette gir strategisk mening for å sikre seg en best mulig plass i verdensordenen. Det er videre begrenset hvor gode muligheter samarbeid gir, på grunn av den anarkiske strukturen legger opp til konkurranse (Glaser 2016, s. 16). Defensive realister mener også at det er rasjonelt å skaffe så god sikkerhet som mulig, men hevder at dette ikke nødvendigvis oppnås ved å ha så mye makt som mulig. Videre anser defensive realister at systemet (anarki) straffer maktsøkende stater med det såkalte sikkerhetsdilemmaet, og mener at gruppetilhørighet er viktigere for å redusere konflikt (Mearsheimer 2013, s. 81).

Med utgangspunkt i en neo-realistisk tankegang er cybersikkerhet særlig relevant. Det kan hevdes at lite er mer anarkisk i sin natur enn cyberspace som ikke eies, drives eller reguleres

av noen samlet instans. Det er dermed svært rasjonelt ut fra et struktur-realistisk perspektiv å utnytte denne anarkiske strukturen med de virkemidler som byr seg til sin fordel. Videre byr strukturen i cyberspace på muligheten til å gjennomføre fordekte operasjoner, eksempelvis kan en stat benytte hackergrupper i befolkningen til å utføre cyberangrep. Det kan dermed vanskelig slås fast at en statssentrert realistisk tankegang ikke kan benyttes på cybersikkerhetsfeltet fordi strukturen i cyberspace muliggjør skjulte operasjoner. Strukturell realisme peker også på at statens kapasitet bør økes på flere områder enn kun militært. Kunnskap om, og kontroll av teknologi, herunder cybersikkerhet, øker statens evne til å hevde seg globalt.

2.2.3 Liberalisme

Liberalismen har røtter tilbake til opplysningstiden og kan knyttes til en rekke åndelige fedre, der Immanuel Kant ofte trekkes frem. Liberalistisk perspektiv er grunnleggende optimistisk om verden og kjennetegnes av et såkalt innside-ut-fokus der det hevdes at intern politikk er det som påvirker det internasjonale samfunn, og ikke omvendt (Morgan 2016, s. 31). Videre hevder liberalister at staters natur er å være samarbeidssøkende, blant annet fordi det lønner seg økonomisk å handle med andre stater. Det internasjonale samfunn er dermed preget av gjensidig avhengighet fremfor gjensidig avskrekking. Også dette perspektivet mener at stater handler ut fra egeninteresse, men at denne interessen er økonomisk vinning som best skapes via samarbeid og dermed at samarbeid er rasjonelt (Morgan 2016, s. 31).

Det liberalistiske perspektiv utvider aktørbildet fra utelukkende stater og inkluderer en rekke andre aktører som blant annet internasjonale organisasjoner, institusjoner, myndigheter og grupper. Klassisk liberalisme anser internasjonale organisasjoner som særlig viktige aktører i IR-forskning fordi de hevder at slike organisasjoner skaper fred (Russett 2013, s. 106-107). Neo-liberalismen er mer statssentrert og fokuserer på institusjonene som et uttrykk for statens egeninteresse (Sterling-Folker 2013, s. 114-115). Visse liberalister hevder også at individuell innflytelse er av betydning i IR-forskning, fordi individer kan ha ulike preferanser som får dem til å jobbe for ulike mål (Moravcsik 2008, s. 236-237). Det er altså individuelle

preferanser i staten som former statlig handling. Slike sosiale interesser på den internasjonale arena blir formet av preferanser, handlingsrom og incentiver (Moravcsik 2008, s. 236-237).

Det politiske systemet innad i et land er det som former statlig handling, slik sett er strukturen i det liberalistiske perspektiv de liberalistiske politiske systemer for handling (Morgan 2016, s 31). Liberalistisk orienterte stater er typisk demokratier og har ulike grader av markedsliberal økonomistyring. Demokratiske stater må forholde seg til en rekke aktører som har rett til å ta del i avgjørelser og politiske prosesser, blant annet befolkningen, parlamentet og ulike samarbeidspartnere. Det kan dermed sies at demokratiet naturlig bremser muligheten til krigføring, og rask reaksjon for trusselhåndtering, fordi avgjørelsen er en lengre prosess og flere har medbestemmelsesrett (Morgan 2016, s. 37).

Når det gjelder sikkerhet mener liberalistene at også dette er best ivaretatt gjennom samarbeid og fellesskap. Økonomisk samhandling skaper felles interesser og gir sterke incentiver for å bevare fred og er dermed en naturlig konfliktdemper (Morgan 2016). Internasjonale organisasjoner, for eksempel FN og IMF (International Monetary Fund), som legger føringer for hvordan staten handler innad og utad er ansett som viktige for å spre de liberale ideene til nye land og på denne måten skape en enda sikrere verden. I slike institusjoner godtar staten å oppgi noe selvråderett til fordel for et mer velfungerende samfunn eller flere handelspartnere. For visse stater er det nødvendig å innføre IMF-policy for å tiltrekke seg internasjonal invest overhodet. Kritisk sett kan det hevdes at institusjonene skaper så sterke incentiver for å være med (og tilsvarende motsatt for å være utenfor) at det i realiteten ikke er frivillig å delta. I tråd med dette kan det hevdes at et så stort frivillig samarbeid mellom liberale stater likevel vil behøve en hegemon som organiserende enhet (Morgan 2016, s. 36).

Teorien om demokratisk fred stammer fra Immanuel Kants bok Perpetual Peace, og er sentral i liberalistisk tankegang. Teorien hevder at demokrati er den beste garanti for fred fordi demokratier ikke går til krig mot hverandre. Det er dermed i alles interesse at alle er demokratier. Teorien trekker frem tre karakteristikker som gjensidig styrker hverandre og skal sørge for fred: demokrati, internasjonale organisasjoner og gjensidig økonomisk avhengighet (Russett 2013, s. 106). Empirisk er det bred støtte for dette argumentet fordi det finnes få eksempler på krig mellom demokratier. Derimot finnes det en rekke eksempler på krig

mellom demokratier og autokratier, noe som tilsier at demokratier ikke nødvendigvis er mer pasifistiske av natur. Imidlertid er ønsket om å spre demokrati og menneskerettigheter videre det som oftest gjør at demokratier involverer seg i krig (Morgan 2016, s. 41). På tross av at det er bred empirisk støtte for teorien om demokratisk fred bør det nevnes at det trolig ikke er likegyldig hvordan variablene defineres. For eksempel er det ikke helt åpenbart hva som anses som et demokrati og det blir ofte tatt utgangspunkt i en demokrati-skala som rangerer graden av demokrati i et land. Elementene i hva som anses som et demokrati vil trolig overlappe i demokrati-indekser men det kan tenkes at utvalgskriteriene kan variere.

Fra et liberalistisk ståsted vil cybersikkerhet være relevant av flere grunner. Cyberdomenet kan sies å ha et usikkert aktørbilde som passer godt med at liberalismen åpner for et bredere sett av aktører, alt fra stater til organisasjoner og grupper. Det rasjonelle for liberalister ligger i statens egeninteresse, særlig ved generering av økonomiske inntekter. Cyberdomenet kan brukes til industrispionasje hvilket vil gi konkurrerende stater økonomiske fortrinn. Det kan videre oppfattes som avskrekkende for potensiell investering dersom et land eller en bedrift ikke har trygge digitale systemer. Et liberalistisk perspektiv vil peke i retning av forsøk på internasjonal normstyring og/eller nasjonale lovverk.

De reflekterende perspektivene

2.2.4 Konstruktivisme

Konstruktivisme er et teoretisk perspektiv som tar utgangspunkt i at den verden vi ser rundt oss skapes av den som ser, altså skapes verdenssynet av den enkeltes observasjon. Verden er todelt mellom den fysiske og den sosiale verden, der konvensjonelle konstruktivister mener at den fysiske verden eksisterer objektivt, mens den sosiale verden skapes av hver enkelt. Den sosiale verden er altså ikke objektiv, men subjektiv og formes gjennom verdier, normer og identiteter og andre sosialt skapte fortolkningsfiltre. Mennesket handler ikke ut ifra sine interesser, men hvordan de *ser* sine interesser (Moses og Knutsen 2012, s. 189). På tross av at konstruktivismen hadde eksistert som samfunnsvitenskapelig tanketradisjon lenge, gjorde den sitt inntok i faget internasjonal politikk som reaksjon på at realismen ikke klarte å forutse eller

forklare slutten på den kalde krigen. Perspektivet var videre uenig i realismens statiske syn på stater og hevdet at interesser endres og identitet formes relasjonelt gjentatte ganger (Fierke 2013, s. 188). I forskning på internasjonale relasjoner (IR) har konstruktivismen bidratt til et bredere sett av analyseenheter og dermed en utvidelse av feltet. Konstruktivismen taler for å anse flere aktører som relevante for IR-forskning og har vist til at globale forhold formes relasjonelt og hendelser er subjektive (Wendt 1995, s. 71-72). Dette har trolig skapt en bredere forståelse av internasjonal politikk som oppfordrer til å stille et bredere sett av spørsmål på IR-feltet.

En konstruktivistisk tilnærming til sikkerhetspolitikk taler for et bredere felt med et utvidet sett av relevante aktører og sikkerhetsanliggender. Likevel er perspektivet kritisk til at stadig nye felt anses som sikkerhetspolitisk relevante basert på retorisk legitimering av risiko og sårbarhet med mindre fokus på reell fare. Perspektivet anser altså det teoretiske feltet sikkerhetspolitikk som bredt, men er kritiske til at nasjonal politisk praksis stadig implementerer nye farer som sikkerhetsanliggender. Konstruktivistisk forskning på sikkerhetspolitikk bør dermed undersøke de aksepterte sannheter om trusler eller fare, og hva disse har sitt grunnlag i. Dette stiller spørsmål ved hvem som får definere hva sikkerhet er og hvilke temaer som er sikkerhetspolitiske. Tradisjonell sikkerhetspolitisk teori handler om militære trusler og sentrerer rundt statlig sikkerhet, mens konstruktivismen taler for en bredere forståelse av trusler og menneskelig sikkerhet (Hough 2008, s. 6). Sosial konstruksjon i sikkerhetspolitikk handler om å mobilisere interesse og å få definert en sak slik man selv ser den, og en videreføring av dette går ut på å forme nye individers oppfatning av saken slik at det viderefører ditt syn (Moses og Knutsen 2012, s. 214; Mabee 2013, s. 81). Makt ligger i evnen til å beskrive en situasjon slik at det oppfattes truende og dermed anses som sikkerhetspolitisk relevant, eller i muligheten til å sette en sak på agendaen. Evnen til meningsdannelse er dermed produktiv makt (Mabee 2013, s. 81).

Noen konstruktivister hevder at ved å skape begreper legitimerer vi eksisterende eller nye ordninger: vi "bekrefter" oppfatninger og institusjonaliserer termer som passer med vår virkelighetsforståelse (Moses og Knutsen 2012, s. 189-190). Sosial konstruksjon går ut på å implementere "sannheter" i samfunnet, og er basert på at de involverte aktørene tror på ideene, ikke hvorvidt de stemmer (Houghton 2007, s. 29). Menings- og definisjonsmakt er

dermed svært viktig. Dette er også hvorfor relasjoner står sentralt i konstruktivismen, og perspektivet hevder at involverte aktører handler basert på persepsjon og overbevisning om denne. Det finnes ikke objektivt truende fenomen eller materielle gjenstander, og selv om en stat har atomvåpen vil statens vurdering av relasjonen til landet være avgjørende for om det anses truende eller ikke (Aguis 2016, s.71). For USA vil det være lite truende dersom Frankrike har atomvåpen, men en helt annen sak dersom Russland eller Iran har det (Houghton 2007, s. 29-30). Relasjoner er en måte å kategorisere verden og gjøre den lettere å forstå eller raskere å tolke, som deretter gir grunnlag for roller eller hierarkisk plassering (Agius 2016, s. 79).

Konstruktivismen anser ideer som det sentrale i internasjonale relasjoner. Ideer, herunder kultur og identitet, er den primære drivkraften i det internasjonale systemet. Identitet er det som former aktørenes relasjon til hverandre, og er fundert i felles aksepterte ideer eller uenighet om disse (Agius 2016). Videre peker konstruktivismen på det sykliske forholdet mellom aktøren og verden: disse påvirker hverandre gjensidig og er det som *skaper* virkeligheten, altså interaksjon, ikke reaksjon. Dette er hvorfor virkeligheten alltid vil være subjektiv, men likevel finnes det en felles virkelighetsforståelse blant aktører som deler ideer, identitet og kultur (Agius 2016, s. 76). Et eksempel er den kalde krigen, som fremstår som en todeling av tilhørighet mellom ideene til vesten og Sovjetunionen. Et annet eksempel er terrorangrepene 9/11, der et fysisk angrep ble beskrevet som et angrep på den vestlige verdens verdier og ideer (Agius 2016, s. 73). Dette peker mot konstruktivismens fokus på retorikk som blir nærmere forklart i avsnittet om securitiseringsteori nedenfor.

Forholdet mellom aktør og struktur i konstruktivismen er basert på en antagelse om at handling er selvregulerende, og et resultat av at aktøren aksepterer ideene som former strukturen (Agius 2016, s. 79). Den viktigste drivkraften bak selvregulering er normer. Eksempelvis er penger og valuta en felles forståelse av at "denne seddelen er verdt 500 kroner i Norge", selv om det ikke nødvendigvis virker rasjonelt at en papirlapp skal være verdt så mye. Rasjonalitet er ikke objektivt for konstruktivister, men perspektivet hevder at enhver handling er rasjonell dersom ditt verdenssyn tilsier at den er rasjonell. Dette kan igjen eksemplifiseres med terrorhandlingene under 9/11 (Agius 2016, s. 73). Normer kan være så sterke at rasjonalitet ikke lenger er tema, og konstruktivister deler normer inn i regulerende

eller konstituerende. Regulerende normer former vår oppførsel i samfunnet, og de konstituerende definerer identitet. Konstruktivisters forklaring på fredstilstand er selvregulerende normer, som igjen er basert på en oppfatning om virkeligheten (Agius 2016, s. 77).

Konstruktivismen hevdes å gå lengre enn realismen i å være strukturalistisk, men mener på sin side at strukturen i det internasjonale samfunn er sosialt skapt og er formet av kunnskap, forståelse og forventninger. Disse skapte strukturene former dernest aktørenes identiteter og oppførsel og er en viktig bakgrunn for "oss og dem"-tankegang. Sosiale strukturer av denne typen eksisterer gjennom praksis og utgjør såkalte effektive normer (Wendt 1995, s. 77). Konstruktivismen avviser realismens tro på forholdet mellom anarkisk struktur og rasjonalitet, og hevder istedet at handling skjer i interaksjon med noe og er preget av faktorer som kultur og egen erfaring. En handling, et individ eller en situasjon kan ikke ses separat fra kontekst, og konteksten former hvilke handlingsalternativer som finnes, ikke rasjonalitet. Dersom det finnes noe i nærheten av rasjonelt for konstruktivistene er dette en funksjon av legitimering gjennom institusjonaliserte normer, da disse former den anarkiske tilstanden (Fierke 2013, s. 190).

Konstruktivismen flytter fokus vekk fra å søke svar på hvorfor noe skjedde, med bakgrunn i at det kan man aldri vite helt sikkert. Eksempelvis vil det være en rekke ankepunkter ved krigen mot terror, men vi kan ikke vite med sikkerhet om George W. Bush virkelig trodde på saken slik den ble lagt frem, eller om det var gjenstand for retorisk legitimering. Språk er sterkt i fokus i konstruktivismen og retningen hevder videre at fordi vi lærer språk gjennom handling kan språket heller ikke ses separat fra handling (Fierke 2013, s. 196-197). Slik sett vil retorikk alltid være et signal om reell handling, og ikke bare en ordvending, fordi vi har lært hva eksempelvis trusler er i praksis.

Ut fra et konstruktivistisk perspektiv er cybersikkerhet en naturlig del av sikkerhetspolitikken som forskningsfelt og potensielt også som politisk felt. Fordi sikkerhet er subjektivt kan det argumenteres for at nær sagt ethvert tema kan være av nasjonal interesse, men cyber er særlig relevant på grunn av konstruktivistenes fokus på individets trygghet. I sammenheng med at vi i Norge har så mye av vårt "liv" på internett kan cybersikkerhet anses som av nasjonal

interesse sikkerhetspolitisk. Én drivkraft bak cybersikkerhet i dette perspektivet er sentrale aktørers evne til å analysere og forstå hva vi til enhver tid anser som mest truende, og deretter sørge for at dette sikres. På den annen side kan det hevdes at fordi det kun er et fåtall av aktører som har tilgang til definisjonsprosessen av sikkerhetspolitiske tema vil det kunne argumenteres for at disse aktørene primært er interessert i å sikre sin egen stilling, og dermed sørge for arbeidsoppgaver til seg selv gjennom å definere et tema som av sikkerhetspolitisk interesse. Videre kan det ut fra et konstruktivistisk syn forventes å finne at det som driver problemet er konstruerte kulturskiller mellom "oss og dem" der vi alltid oppfatter "de andre" som truende, og dermed overdriver risiko.

Sett ut i fra konstruktivistisk tankegang er det sentralt å anta at den sikkerhetspolitiske prosessen på cyberfeltet er drevet av eliter og andre betydningsfulle beslutningstageres ønske om å anse cyber som et sikkerhetspolitisk problem av nasjonal interesse. Drivkraften i prosessen blir dermed i større grad fokusert rundt *at* det er i noens interesse, snarere enn *hvorfor* cyber skulle oppfattes som et eksistensielt truende sikkerhetspolitisk problem.

2.2.5 Securitiseringsteori

> *"Security is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics" (Buzan m. fl. 1998, s 23).*

Securitiseringsteori ble skapt på nittitallet ved Copenhagen Peace Research Institute av sentrale teoretikere som Barry Buzan, Ole Wæver og Jaap de Wilde, som utgjorde den teoretiske retningen Københavnerskolen. Securitization er et begrep som ikke enkelt lar seg oversette til norsk, og det er her tatt utgangspunkt i "securitisering" med definisjonen og de forbehold gitt i innledningen. Securitiseringsteorien er en kritikk av de situasjoner der retoriske virkemidler benyttes for å opphøye politiske områder til høyeste politiske nivå: nemlig eksistensiell trussel. Dersom en sak løftes opp til dette nivået er det i nasjonal interesse at det sikres, hvilket gir et bredt mandat med færre instansers vetorett. Perspektivet anser dermed sikkerhet som et subjektivt fenomen, hvilket gjør at securitiseringsteori her anses som

konstruktivistisk, tross at Københavnerskolen selv kan anses som en uklar blanding mellom neo-realisme, konstruktivisme og postmodernisme (Wæver og Buzan 2016, s. 429). I dette synet kan cybersikkerhet anses som et felt som har blitt securitisert. Dette er problematisk fordi det i visse tilfeller kan innebære endringer i personvernlovgivningen og slik sett kan en securitisering av cyberfeltet tale for et svakere personvern. Når det gjelder forskning på sikkerhetspolitikk ut i fra et securitiseringsteoretisk synspunkt vil dette dreie seg om å forstå den politiske prosessen og strukturen som skal til for å skape et trusselbilde (Balzacq 2010, s. 56). Securitiseringsteorien er dermed både en forklaring på hvordan noe blir til et sikkerhetsanliggende, samtidig som perspektivet inntar en kritisk posisjon til securitisering.

Københavnerskolen er et multisektorielt felt som kritiserer sikkerhetspolitikk for å være for snever og utelukkende statssentrert, og danner isteden fem kategorier av sikkerhetspolitiske sektorer: militær, politisk, økonomisk, miljø og samfunn (Emmers 2016, s. 169). Den sikkerhetspolitiske verden er sammensatt av aktører som kan securitisere et felt, og et såkalt referentobjekt: det som anses som eksistensielt truet dersom det har en legitim overlevelsesrett (Emmers 2016, s 169). Det som trues vil kunne kategoriseres i en av de fem sektorene, og kan variere fra ideologier, identitet, økonomi, og dyre- eller plantearter, til statsapparatet (Buzan m.fl. 1998). Videre deler Københavnerskolen temaer inn i tre kategorier: ikke-politiserte emner; politiserte emner; og securitiserte emner. De ikke-politiserte er emner som ikke behøver statlig handling og ikke er gjenstand for offentlig debatt, de politiserte er gjenstand for politisk dragkamp, og securitiserte emner har behov for umiddelbar krisehåndtering utover statens vanlige håndtering (Emmers 2016, s 170). Securitiseringsteori handler om prosessen fra å være et politisert emne til å bli et securitisert emne. Dette skjer gjennom retoriske grep der en sentral aktør klarer å overbevise sitt publikum om at emnet er et sikkerhetsanliggende (Emmers 2016, s. 171), på samme måte som i konvensjonell konstruktivisme. Et sentralt eksempel er krigen mot terror. Før 9/11 var terrorisme ikke ansett som et statlig anliggende, og var heller ikke definert som krig. Terrorisme ble ansett som en sak på individnivå og noe som var internasjonalt kriminelt fremfor en handling som krevde militær respons. 9/11 kan dermed oppfattes som securitisering av et fenomen som løftet terror opp til et nivå der det var en krig mot terror, med vidtgående mandat (Fierke 2013, s. 199-200).

Securitiseringsteorien er kritisk til at stadig nye emner aksepteres som sikkerhetsanliggender, og hevder at en rekke sikkerhetspolitiske områder har blitt tillagt uproporsjonalt mye vekt fordi det har vært i noens interesse (Buzan m. fl. 1998, s. 24). Perspektivet mener at sikkerhetspolitikk bør handle om reelle trusler og stiller seg spørrende til hvorvidt retoriske grep brukes til å legitimere fenomener som sikkerhetsanliggender. Københavnerskolen følger den konstruktivistiske tankegangen om at ingenting er truende objektivt sett, men at dette vil variere ut fra subjektive vurderinger av situasjonen (Wendt 1995, s. 71-72). Securitiseringsteori understreker fokuset på individets og samfunnets sikkerhet, og er kritiske til utelukkende statssentrert sikkerhetspolitisk forskning. Sikkerhetspolitiske hensyn når det gjelder individet dreier seg om å trygge befolkningen som mennesker, og dermed ivareta hensyn på langt flere områder enn tradisjonell krig.

Sentralt i konstruktivistisk perspektiv er hvilke aktører som har tilgang til definisjonsprosessen, og typisk er dette politiske eliter. Disse innehar mye makt og er sentrale som fokusområde for en analyse da det ligger mye informasjon i hvem som har interesse av at en sak anses som et sikkerhetsanliggende (Houghton 2007, s. 37). Sentralt i denne sammenhengen er det å analysere tekst eller uttalelser og stille spørsmål ved hvem som er det tiltenkte publikum og hvilke språklige virkemidler som er brukt i saken som legges frem (Balzacq 2010, s. 66-67). Definisjonen av en sak er et sentralt fokusområde for Københavnerskolen og deres securitiseringsteori. Teorien hevder at sikkerhet er et subjektivt fenomen, og oppfatningen av hva som anses truende er individuelt og vil variere. Dette kan utnyttes av sentrale aktører og behøver bare formuleres som en trussel for at det skal oppfattes som skremmende (Emmers 2016, s. 172-173; Taureck 2006, s. 56). Resultatet av denne retoriske overdrivelsen er at saken "securitiseres", altså regnes som et sikkerhetsanliggende. Det er dette som gir sikkerhetspolitiske emner en særstilling dersom de anses som å være av nasjonal interesse, og kan føre til at mange hensyn må vike for å sørge for fullgod sikkerhet (Taureck 2006). Med et veldig kritisk blikk kan det hevdes at securitiseringsteori dreier seg om skremselspropaganda som virkemiddel for å sette saker på dagsorden. Evnen til å securitisere en sak ligger hos den politiske eliten som har makt og midler nok (Emmers 2016, s. 171). En bedre måte å løse disse problemene på er å la dem forbli vanlige politiske tema som ikke opphøyes til det sikkerhetspolitiske nivå (Taureck 2006, s. 54-55). Bakgrunnen for

dette er at sikkerhetspolitiske områder har færre begrensninger, da det er i nasjonal interesse å sikre dem (Emmers 2016, s. 171).

Sett i sammenheng med securitiseringsteori vil cybersikkerhet anses som et tema som har blitt "securitisert", altså at retoriske virkemidler som overdrivelser er benyttet for å løfte problemet opp til høyeste sikkerhetsnivå. Forventningene i denne sammenheng er at empirien primært dreier seg rundt risiko og sårbarhet, og mindre om reelle trusler eller faktiske angrep. Det kan videre forventes å finne et bredt forsøk på legitimering av faren, som ikke bare går ut til relevante aktører, men også befolkningen. Empirien forventes å ha ordvendinger som bevisst er valgt for å oppleves skremmende.

3. Metode

I dette kapittelet følger en redegjørelse av forskningsmetoden som er brukt i denne oppgaven. Metoden jeg har valgt er dokumentanalyse, som er en kvalitativ innholdsanalyse, samt en form for policyanalyse. Dette gjør det mulig å analysere sikkerhetspolitikken på cyberfeltet i tillegg til å gi en oversikt over den dokumenterte trusselen knyttet til cybersikkerhet. En dokumentanalyse er en måte å generere informasjon, og er knyttet til innsamlingen av empirisk data. En policyanalyse er en analysemetode som skal brukes for å sette sammen og analysere den empiriske dataen i lys av teorien, og vil benyttes i diskusjonsdelen av oppgaven.

3.1 Dokumentanalyse

En dokumentstudie er en måte å generere og bearbeide tekstdata som allerede er produsert. Dokumentene er derfor produsert for et annet formål enn mitt, og det er viktig å se dem i forhold til dette. Et dokument kan være nesten hva som helst og kjennetegnes av at det er informasjon i skriftlig format skrevet med et formål (Tjora 2012, s. 162). Fordi begrepet dokument i denne sammenhengen rommer så, mye vil ulike studier anse dokumentene som relevante av ulike grunner. For eksempel kan en studie fokusere på hvordan dokumentet ble til, eller hva dokumentet har betydd i en videre forstand. Uansett hva studiens utgangspunkt er, er det viktig å forstå dokumentet i lys av den kontekst det ble skapt, da dokumenter er skrevet for et formål som kan være et annet enn det formålet vi benytter dem til. Dette er hvorfor en dokumentstudie beskrives som en analyse av noen andres kvalitative informasjon (Tjora 2012, s. 163).

Jeg valgte denne måten å generere data på av hensyn til problemstillingen, som består av to spørsmål: hva består den digitale trusselsituasjonen i Norge av, og hva driver utformingen av den norske sikkerhetspolitikken på cyberfeltet? Disse spørsmålene tilsier etter mitt syn bruk

av kvalitative data. Deretter vurderte jeg hvorvidt det var mulighet for å gjennomføre intervjuer, men fordi jeg også ønsker å undersøke hvordan informasjonen presenteres for befolkningen anser jeg det som tilstrekkelig å gjøre en ren dokumentstudie. I dette tilfellet er store deler av informasjonen av sensitiv art som samtidig er så tett på situasjonen som mulig. Dette er grunnen til at jeg primært har valgt å primært benytte offentlige rapporter, fordi jeg anser disse som det nærmeste jeg kommer sikre kilder. All informasjon om trusselbildet og cybersikkerhet vil trolig ikke være offentlig tilgjengelig, og uten at det er mulig å vite hvilken informasjon man går glipp av er det naturlig å anta at den informasjonen som publiseres i rapportene gir et forenklet bilde av trusselsituasjonen. For dette formålet anser jeg ikke at oppgaven lider under dette, og de rapportene som er brukt til empirien anser jeg som svært informative.

Når det gjelder utvalgskriterier er det vanlig å vurdere dokumenter ut i fra autensitet, troverdighet, representativitet og hvorvidt man forstår informasjonen (Duedahl og Jacobsen 2009). Mine dokumenter er nesten utelukkende offentlige rapporter der troverdigheten i dokumentet ikke ligger i for eksempel mangelen på skrivefeil, men heller hvem avsenderen er. Autensitet er hensyn til hvorvidt dokumentet er det det utgir seg for å være, noe jeg ikke anser nødvendig å diskutere da jeg går ut fra at dette er tilfellet tross at dette ikke nødvendigvis innebærer at informasjonen er objektiv. Representativitet reiser spørsmål om hvorvidt informasjonen i dokumentet gir et godt bilde av situasjonen det gjelder for, altså at det ikke eksempelvis mangler vesentlig informasjon. Dette er et aspekt som vil gjelde for alle offentlige dokumenter knyttet til trusselsituasjonen fordi det er rimelig å anta at mye informasjon må holdes skjult. Likevel anser jeg at informasjonen i rapportene jeg har brukt gir et så godt bilde som mulig. Hensynet til betydning av dokumentene gjelder i større grad ved gamle papirer med kompliserte skrifttyper eller språk, og anses ikke relevant i denne sammenheng.

I en dokumentstudie er det viktig å ha kontekst in mente, og mine dokumenter er primært offisielle myndigheters rapporter om situasjonen på det tidspunktet de gis ut eller for den tidsrammen de er ment å gjelde for. For eksempel er Etterretningstjenestens (E-tjenesten) rapporter årlige og ment å gjelde for inneværende år, mens Stortingsmeldinger eller NOU'er har ofte oppgitt tidsramme i tittelen på dokumentet. For å skape et bredest mulig bilde av den

sikkerhetspolitiske situasjonen på cyberfeltet har jeg valgt å bruke flere årsutgaver av E-tjenestens Fokusrapporterfor å undersøke om situasjonen for eksempel har eskalert, eller hvorvidt informasjonen presenteres på merkbart ulike måter. Dette er gjort med henblikk på teorien jeg har redegjort for, som trekker frem aspekter som retorikk og bevisste formuleringer. Et videre sentralt aspekt knyttet til kontekst er formålet dokumentet har. I dette tilfellet er dokumentene rapporter som har til hensikt å informere om eksempelvis den digitale trusselsituasjonen. Selv om dette kan sies å være det jeg benytter dem til, er de ikke primært skapt for bruk i forskning. Hensikten bak åpenhet rundt slike temaer kan tenkes å være transparens som er knyttet til demokratiske rettigheter, samt å informere for å skaffe oppslutning rundt en sak.

Dokumentene er valgt med utgangspunkt i casespesifikke hensyn til temaet norsk cybersikkerhet. Utvalgskriteriene jeg har laget er at dokumentene skal gjelde cybersikkerhet, norske forhold, og må ha høy troverdighet. I tillegg må dokumentene gjelde den politiske retningen av cybersikkerhet, altså ikke for eksempel teknisk cybersikring, da dette ville være utenfor oppgavens tema. Jeg begynte på Forsvarets nettsider (forsvaret.no) og fant derfra E-tjenestens sider der det er publisert årlige Fokus-rapporter tilbake til 2011. Etter at jeg ble kjent med Fokusrapporten ble jeg oppmerksom på at disse gis ut som del av et "samarbeid" av rapporter om den norske trusselsituasjonen fordelt på organisasjonene E-tjenesten, Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Direktoratet for samfunnssikkerhet og beredskap (DSB). Jeg besøkte deretter de nevnte organisasjonenes nettsider og lastet ned siste utgave av rapportene. Denne formen for generering av data kalles snøballmetoden og innebærer at man får informasjon fra ett dokument som leder til neste dokument og så videre (Tjora 2012). Jeg anså umiddelbart alle rapportene som høyst troverdige grunnet deres posisjon som deler av det norske offentlige apparat. Etter nærmere undersøkelse anså jeg NSM og DSB sine rapporter som utenfor oppgavens nedslagsfelt, og de vil derfor ikke gjennomgås i empiridelen. PSTs samfunnsoppdrag gjelder primært etterforskning og forebygging av innlands kriminalitet, og er underlagt Justisdepartementet (pst.no). E-tjenesten er en forsvarsgren og er underlagt Forsvarsdepartementet, og E-tjenestens samfunnsoppdrag omfatter utenlandstrusler. Dette innebærer blant annet at PST er underlagt andre lover enn E-tjenesten. PSTs rapporter gjelder i mindre grad digitale trusler mot rikets sikkerhet, mens E-tjenestens Fokus-rapporter tar for seg dette som et av

hovedelementene. Fokus-rapportene utgjør derfor hoveddelen av empirigjennomgangen når det gjelder kartleggingen av den digitale trusselsituasjonen. Et annet aspekt ved bruken av E-tjenestens Fokus-rapporter er at den seneste Fokus-rapporten vil bli gitt ut etter at empiridelen skal være ferdigstilt (forventes utgitt i begynnelsen av mars 2018), men før oppgaven skal ferdigstilles. Dette gjør at jeg må gå tilbake og legge til ny informasjon og potensielt endre deler av empirien. Jeg har derfor valgt legge like stor vekt på Fokus 2017 og Fokus 2018.

I kvalitative undersøkelser er det ofte ikke like relevant å diskutere hensyn til reliabilitet, eller etterprøvbarhet, som er mer relevant for forskning på stabile faktorer, og en dokumentanalyse kan i større grad være subjektivt fortolket enn en objektiv observasjon. Derfor er det viktig å ta andre forskningsmessige hensyn på alvor, slik som validitet, transparens, kildekritikk og kvalitetssikring. Validitet er et sentralt moment i min oppgave og noe jeg har forsøkt å ha in mente mens jeg har søkt etter informasjon. Validitet er hensynet til hvor treffsikker målingen er, og det er vanlig å beskrive validitet som hvorvidt slutningene man trekker er basert på informasjonen man har (Ringdal 2011, s. 90). For min oppgaves del er dette sentralt når det gjelder tolkningen av informasjonen, både i presentasjonen av empirien og i diskusjonsdelen. Et tilknyttet tema til dette er å unngå forskningsmessig partiskhet, såkalt "bias" på engelsk. Dette er et fenomen som oppstår når forskeren overser informasjon som går imot ens eget argument. Jeg har forsøkt å være så årvåken som mulig når det gjelder dette, og informasjonen jeg har utelatt har vært fordi den har falt utenfor oppgavens tema. Å bruke offentlige myndigheters rapporter er også en måte å sikre at informasjonen er så objektiv som mulig, altså ikke beskrevet av for eksempel en avis med en bestemt politisk agenda. Slike rapporter vil trolig alltid ha en viss politisk agenda som naturlig vil variere ut fra hvem som sitter i regjering, men slik informasjon vil nødvendigvis måtte presenteres på en relativt objektiv måte, uten en tydelig politisk mening. Jeg må likevel ta høyde for at en del av problemstillingens formål er å tolke empirisk informasjon i ulike lys, hvilket naturligvis ikke vil være objektivt. Når det gjelder hensynet til transparens har jeg inkludert søkeord jeg har brukt, og i hvilke databaser jeg har søkt.

I den videre empiriinnsamlingen har jeg bevisst besøkt nettsider jeg på forhånd visste var kredible, fremfor å for eksempel google "trusselstiuasjon+Norge+cyber". Dette for å unngå

usikker informasjon av hensyn til kildekritikk. Med unntak av Forsvarets Fellesoperative Doktrine (FFOD) som jeg googlet og fant i BIBSYS Brage, har jeg ikke brukt google til empirisøk. Nettsidene jeg har brukt til å søke er Norsk Utenrikspolitisk Institutt (NUPI), Forsvarets Forskningsinstitutt (FFI), Regjeringen og Idunn. På disse sidene har jeg brukt søkeord som cyber, digital trussel, cyberangrep, og cybersikkerhet. Jeg har også besøkt flere universiteters databaser og brukt samme søkeord for å undersøke om det fantes masteroppgaver med tilknyttet tema, som var et forsøk på å finne flere relevante kilder som andre hadde brukt, hvilket jeg ikke gjorde. Dette skyldes trolig at temaet er relativt nytt.

I empiriinnsamlingen har kildekritikk vært hovedhensynet. Kildekritikk kan i en kvalitativ analyse beskrives som systematisert skepsis til troverdigeten i dokumentene (Duedahl og Jacobsen 2009: s. 53). Såkalte primærkilder er de data man har samlet inn selv, typisk ved intervjuer eller observasjon. I dokumentanalyse er sekundærdata kilder som allerede foreligger og som er åpne for alle i et begrenset tidsrom, mens primærkilder ofte er begrenset til de involverte (Ringdal 2011, s. 107; Brinkmann og Tanggaard 2012). Et dokument på tertiærnivå anses her som et helt åpent og offentlig dokument som er lett tilgjengelig for alle i ubegrenset tid, for eksempel en teoribok. Jeg anser rapportene fra Forsvaret, PST, Regjering og Storting for å være på sekundærnivå, fordi de er offentlig tilgjengelige men er gitt ut nært i tid og av beslutningstakere nært situasjonen. Et dokument på tertiærnivå vil for eksempel være de rapporter jeg har brukt fra NUPI eller FFI.

Svakhetene ved å bruke dokumentanalyse er knyttet til mengden tilgjengelig informasjon og utvalg. Som nevnt over er det sjanse for at forskerens perspektiv leder utvalget i retning av oppfatninger man har på forhånd, slik at dokumenter som ikke passer inn i den oppfatningen velges bort. I tillegg kan en dokumentanalyse ha nærmest ubegrenset omfang av kilder, eller relevant informasjon kan være svært vanskelig tilgjengelig. For å unngå slike problemer har jeg hatt strenge utvalgskriterier, og i tillegg fått hjelp fra teorien angående hva som er relevant for min problemstilling.

3.2 Policyanalyse

Som nevnt i begrepsavklaringsdelen i innledningskapittelet er en policy et slags politisk planverk knyttet til et bestemt politisk område. Mye av en policy avhenger av hvem som har medbestemmelsesrett og hva handlingsrommet tillater i det konkrete tilfellet (Hill 2003; Fermann 2013, s. 53). I denne oppgaven er det tatt utgangspunkt i en kombinasjon av policyanalysen beskrevet i Fermann (2013) som omhandler utenrikspolitisk analyse og krisehåndtering, og policyanalysen beskrevet i Hill (2003), som er en generell bok om foreign policy. I policyanalyser er det vanlig å operere med tre analysenivå: individnivå, statlig nivå og globalt nivå (Hill 2003). På individnivå er fokus på befolkningen og kultur innad, på dette nivået er personlige preferanser tema (Fermann 2013, s. 109). Strukturnivå har fokus på innenrikspolitiske forhold og på styringsverket, blant annet politisk styresettet og handlingsrommet til beslutningstakerne (Fermann 2013, s. 108 og s. 110). På dette nivået har jeg kombinert Fermanns (2013) to analysenivåer: "samfunnet" og "stats- og styringsverket", og har valgt å kalle dette stats- og styringsverket. Globalt nivå er eksterne fakorer som det internasjonale politiske klima, handelspartnere og allianser (Fermann 2013, s. 115). Den globale arena er som nevnt ansett som et anarki og vil derfor også trekke inn faktorer som normer.

De analytiske nivåene er videre delt inn i følgende faktorer: individer (befolkningen og beslutningstakerne), stats- og styringsverket, og globale omgivelser. Disse tre punktene utgjør inndelingen av analysekapittelet, der de tre teoretiske perspektivene skal brukes til å diskutere empirien. En policyanalyse illustrerer ulike egenskaper ved de tre analysenivåene, som varierer ut ifra teoretisk perspektiv. Felles for analysenivåene er at de legger føringer for hvordan man handler, enten det er bevisst (for eksempel politisk styresett og operativ kapasitet) eller ubevisst (som kultur og tidvis normer). Ofte brukes slike policyundersøkelser om en spesifikk situasjon og håndteringen av den, et typisk eksempel på dette er Cubakrisen. I situasjonen rundt Cubakrisen vil en policyundersøkelse analysere hva var forutsetningene som ledet til krisen og hvorfor den ble håndtert som den gjorde. Min problemstilling skal kartlegge den digitale trusselsituasjonen i Norge, og analysere hva som har preget utformingen av norsk cyberpolicy. De tre teoretiske perspektivene realisme, liberalisme og konstruktivisme vil legge føringer for hvordan den empiriske informasjonen tolkes.

4. Empiri

Kapittelet er tredelt mellom trusselbildet, nasjonalt rammeverk og internasjonale forpliktelser. De to sistnevnte kategoriene dreier seg om den norske sikkerhetspolitikken som berører cyber, og en redegjørelse for nasjonale og internasjonale faktorer som kan påvirke politikken. Empiridelen består av en redegjørelse av cyberfeltet med fokus på norske forhold, spesifikt trusselbildet, sikkerhetspolitiske hensyn, beslutningstagerne og interne forhold. Innledningsvis følger grunnleggende informasjon om cybersikkerhet.

Til enhver tid vil et samfunn i forandring stå overfor nye potensielle risiko og trusler, som for eksempel digitale trusler. Angrep og trusler i det digitale rom omtales her som cyberangrep og omfatter typisk hacking, spionasje, sabotasje og planting av informasjon i det digitale rom. Hacking og sabotasje kan ødelegge og sette ut av spill digital infrastruktur, noe som kan ha store konsekvenser for samfunnet. Spionasje omfatter informasjonsuthenting fra kritiske nasjonale kilder og er typisk et resultat av en form for hacking eller trojanere som plantes i programvaren uten at den hackede merker det (FFI-fakta 2013; Langø og Sandvik 2013, s. 223). Planting av informasjon er vanligst i sosiale medier og dreier seg ofte om å spre en bestemt type informasjon til visse grupper, og en annen type informasjon til andre grupper. Dette gjøres gjennom å utnytte sosiale mediers algoritmer som allerede sørger for at brukeren får mer av den informasjonen den allerede liker. Dette er hevdet gjort i det amerikanske valget der det ble utnyttet kunnskap om at visse grupper ble ansett som nødvendige hjemmesittere, mens andre ble oppfordret til å stemme (Lipton m. fl. 2016, Solon 2016, Ertesvåg 2017).

Cybersikkerhet anses som et viktig sikkerhetspolitisk fokusområde på grunn av Norges omfattende digitale infrastruktur som gjør oss sårbare. Risikoen for digitale angrep er altså stor på grunn av sårbarheten i vårt høyteknologiske samfunn (Lysne m.fl. 2016, s. 24). Dette bunner i et rasjonale om at "gevinsten" ved å angripe er størst der det gjør størst utslag. Et digitalt angrep på et fattig u-land vil trolig ikke gi samme effekt. Cyberangrep har også muligheten til å være mer kostnadseffektivt og kan trekke inn et bredere aktørbilde enn mange andre sikkerhetspolitiske emner (Langø 2013, s. 237), og "motivasjonen ligger i at angrep i

cyberdomenet har potensiale for å gi store fordeler i de fysiske domenene" (Johnsen 2013, s 241), gjennom for eksempel kaos og destabilisering. Videre vil det være kostnadseffektivt for avsenderen som slipper å forflytte seg fysisk, noe som "introduserer […] nye kontaktflater mellom Norge, norske virksomheter og omverdenen" (Kveberg og Johnsen 2013, s 21). Dette gir også stater mulighet til å gjennomføre skjulte angrep, altså angrep som ikke fremstår som statlige angrep, men i realiteten er gjort på bestilling av gjeldende stat.

Cyberdomenet har ingen landegrenser og det er dermed vanskelig for Forsvaret å drive suverenitetshevdelse, som er en av deres viktigste oppgaver. Overvåkning er den eneste muligheten til å oppdage og forhindre angrep, og derigjennom sikre mulighetene til suverenitetshevdelse. Digitalisering er en lang tids pågående trend som gjør at stadig flere systemer knyttes sammen, og Norge får stadig flere kontaktflater til andre stater. Slik sett er det enkelt å utnytte disse kontaktflatene til maktutøvelse (Kveberg og Tynes Johnsen 2013, s. 16). Dette har endret den sikkerhetspolitiske agenda og gjør at territorielle grenser ikke lenger er det viktigste aspektet (Beadle og Diesen 2015, s. 16-17).

Norge er et lite land og har behov for å kompensere for størrelsen på Forsvaret, og områder som teknologi og cybersikkerhet er naturlige alternativer i den sammenheng (Beadle og Diesen 2015, s. 35). Cyberdomenet er særlig relevant i krigføring når det gjelder påvirkning av vår forståelse av en situasjon. Som nevnt over er det gode muligheter for å bruke sosiale medier til spredning av falsk informasjon og dermed skape et forvridd bilde av motparten eller konflikten (Beadle og Diesen 2015, s. 44).

4.1 Trusselbildet

Denne redegjørelsen er basert på offisielle rapporter som søker å gi et innblikk i trusselbildet på cyberdomenet. PST (politiets sikkerhetstjeneste), DSB (Direktoratet for samfunnssikkerhet og beredskap), NSM (nasjonal sikkerhetsmyndighet) og Etterretningstjenestens (heretter E-tjenesten) årlige rapporter med deres beskrivelser av trusselbildet er den ferskeste, tilgjengelige ugraderte informasjonen, som samtidig har svært høy troverdighet. Som nevnt i foregående metodekapittel vil det jevnlig dukke opp avisartikler som redegjør for

cyberrelaterte hendelser, men slike artikler har ikke like høy troverdighet vil dermed ikke tillegges like mye vekt, selv om de brukes. Det er derfor primært tatt utgangspunkt i de offisielle rapportene fra sikkerhetsmyndighetene, og dernest er det supplert med forskningsrapporter fra andre instanser slik som FFI (Forsvarets Forskningsinstitutt) og NUPI (Norsk utenrikspolitisk institutt) i tillegg til mer generelle statlige rapporter, slik som NOU'er. Nyhetsartikler er inkludert for å utfylle det mer generelle bildet i rapportene med konkrete hendelser, men slike artikler og saker fra Norge finnes det kun et fåtall av.

4.1.1 Aktørene, motiv og metoder

I E-tjenestens årlige rapport "Fokus" (2018) trekkes såkalt hybrid krigføring frem som en særlig trussel, med cyberoperasjoner som en sentral del innenfor eksempelvis sabotasje, etterretning og påvirkning. Rapporten stadfester umiddelbart at det er en opptrapping i russisk påvirkningsaktivitet, som fungerer i følgende former: "kontakt med politiske partier og enkeltpersoner, mediekampanjer, samt nettverksoperasjoner med aktiv bruk av innhentet informasjon" (Fokus 2018, s. 30). Selv om noe av denne aktiviteten kan være vanlig lobbyisme stadfester E-tjenesten at deler av den fungerer i et tydelig lyssky område. Henvendelsene til politiske fløyer har enten vært i ytre høyre eller ytre venstre, og spredning av propaganda har gått mot sentrumskandidater, hvilket kan bære preg av et ønske om steilere fronter. E-tjenesten peker på at dette kan være for å skape generell mistro til det politiske systemet og å skape splid i befolkningen (Fokus 2018, s. 30). Aktiviteten generelt er først og fremst rettet mot politiske og militære mål, men har blitt mer utbredt og involverer nå et bredere spekter av aktører. Akademiske institusjoner og industribedrifter er også sentrale mål. Hensikten er ikke nødvendigvis like mye hvem man rammer, men omfanget. Noen cyberangrep har til hensikt å kartlegge digitale strukturer, mens andres mål er generell tilstedeværelse som kan brukes strategisk dersom det skjer politiske endringer aktøren ikke liker (Kristoffersen 2018). I 2016 angrep Russland et IT-system for jernbanetrafikk i Ukraina der datanettverkene var infiltrert et halvt år i forveien. E-tjenesten mener slike mindre angrep er gjort for å tilegne seg erfaring som på sikt vil gjøre Russland i stand til å utføre enda større digitale angrep (Fokus 2018, s. 31).

I rapporten “Helhetlig IKT-risikobilde for 2017” melder NSM om svært høy sårbarhet og risiko for angrep, der en særlig grunn er manglende sikring av de offentlige digitale systemene. NSM beskriver cyberangrep som jevnt økende i hyppighet og alvorlighetsgrad. Et videre problem knyttet til sikkerheten er mangel på kompetanse og innsikt hos ansatte, i tillegg til at menneskelig svikt er en sentral faktor når det gjelder sikring av systemer som er fordelt på et så stort antall ulike organisasjoner og individer (NSM 2017, s. 25).

I Fokus 2017 stadfestes det at "[d]ei mest alvorlege truslane mot digitale system i Noreg vil også i år komme frå russisk og kinesisk hald" (Fokus 2017, s 4). Rapporten innledes med noen ord fra Etterretningstjenestens sjef (heretter E-sjefen) generalløytnant Morten Haga Lunde som trekker frem tre fremtredende utviklingstrekk som er av særlig interesse for norsk sikkerhetspolitikk, der trusler i det digitale rommet nevnes først og omtales også som økende (Fokus 2017, s 6). E-sjefen hevder at

> [v]i kan forvente omfattande etterretningsoperasjonar mot Noreg i året som kjem. Russland gjennomførte omfattande digitale operasjonar for å påverke valkampen i USA, og ein kan ikkje sjå bort frå at framande makter også kan forsøkje å påverke valet på ulike måtar her i Noreg […]. (Fokus 2017, s 6).

Digitale angrep blir stadig mer avanserte og kan ifølge Lysne II-utvalget (2016) i dag "sidestilles med militært angrep og ulovlig maktbruk etter FN-paktens bestemmelser"(Lysne m.fl. 2016, s 11).

Aktørbildet fokuseres rundt statlige eller statlig sponsede trusselaktører (Fokus 2017, s 36), og E-tjenesten trekker ikke frem grupper eller enkeltindivider i det digitale trusselbildet i 2017, noe som heller ikke gjøres i PSTs rapport “Trusselvurdering 2018”. Dersom man går tilbake til Fokus-rapportene for årene 2014 og 2015 står det at aktørbildet

> spenner fra statlige etterretnings- og sikkerhetstjenester, via tradisjonelle militære motstandere, globale næringsbedrifter, terrorist- og ekstremistgrupper, til organiserte hacker-grupper […] Etterretningstjenesten har primært fokus på statlige aktører, dernest mer

> selvstendige, ikke-statlige aktører som opererer på vegne av, støttes eller utnyttes av statlige myndigheter. (Fokus 2014, s 59; Fokus 2015, s 83).

De nyere Fokus-rapportene (Fokus 2017; Fokus 2018) peker på at de ikke-statlige aktørene som står alene ikke besitter nok kunnskap eller evne til å utgjøre en reell trussel, hvilket er hvorfor E-tjenesten ikke fokuserer på disse. I Fokus-rapporten for 2016 heter det at et generelt trekk ved utenlandske digitale angrep er at stater gir ressurser til ikke-statlige grupper slik at angrepene skal være vanskeligere å oppdage. I Fokus 2014, 2015 og 2016 anerkjennes også enkeltgruppers angrep, men dette er ikke å finne i de to seneste rapportene (Fokus 2017; Fokus 2018). Hva som er grunnen til dette skiftet vites ikke og skal ikke være gjenstand for spekulasjon, men vil tas opp til diskusjon i drøftingskapittelet. Etterretningsinformasjon er i stadig forandring og det er naturlig og nødvendig å anse de nyeste rapportene som mest korrekte for situasjonen i dag. Det er derfor tatt utgangspunkt i at de relevante trusselaktørene på cyberfeltet i Norge per i dag er identifisert som statlige (Fokus 2017; Fokus 2018). Tross at cyberdomenet åpner for et bredt felt av aktører er disse ikke nevnt i offentlige sikkerhetsmyndigheters nyeste rapporter og vil dermed heller ikke tillegges vekt som relevante potensielle aktører i denne sammenhengen. Foruten endringen i aktørbildet tegner rapportene fra 2014-2018 det samme trusselbildet og vil dermed brukes på lik linje slik det er argumentert for i metodekapittelet.

E-tjenestens rapport (Fokus 2018, s. 28) trekker frem de tre mest fremtredende digitale truslene: etterretning, sabotasje og påvirkning, som alle anses som former for cyberangrep. Etterretning gjelder forsøk på skjult innsamling av norsk informasjon som er digitalt lagret. Slik informasjonsuthenting kan gjelde individuell informasjon som for eksempel er lagret i skynettverk, eller det kan gjelde myndigheters digitalt lagrede data. Informasjonen er lagret i lukkede nettverk, men nås ved inntrenging i systemene gjennom hacking eller ved hjelp av utro ansatte som gir andre tilgang til informasjonen. Slike operasjoner har potensiale for å forbli uoppdagede over lang tid og kan således føre til massive lekkasjer (se blant annet Fokus 2015). Påvirkning skjer typisk i sosiale medier og gjelder planting av desinformasjon som har til hensikt å påvirke virkelighetsoppfatningen til leseren og "å forme det strategiske handlingsrommet til eigen fordel" (Fokus 2017, s 36). Sabotasje er angrep som har til hensikt å påvirke eller stanse kritiske funksjoner, for eksempel kritisk infrastruktur. Ved å skaffe seg

kjennskap til kritisk infrastruktur i fredstid kan dette benyttes til andre staters fordel dersom krise eller krig oppstår, i tillegg kan sabotasje benyttes i den hensikt å skape kaos (Fokus 2015, s. 83).

Vedrørende det norske trusselbildet kan man skille mellom konkrete trusler som er basert på tidligere angrep eller avvergede angrep på Norge, og risikovurderinger som er basert på potensiale eller sårbarhet og samtidig faktiske hendelser i andre land. All informasjon som tas med i Fokus-rapportene er ment å vise trusselbildet mot Norge uten at det alltid er beskrevet eksplisitt hva trusselbildet eller risikovurderingen er basert på. Det vil derfor ikke legges avgjørende vekt på dette skillet i inneværende kapittel.

Det er to stater som nevnes når det gjelder cyberhendelser i Norge: Kina og Russland. Disse aktørene bruker forskjellige metoder i sine cyberangrep, da hensikten med angrepene er forskjellige. Kinesiske cybertrusler mot Norge dreier seg primært om industrispionasje. Generelt beskrives trusselen som mer rettet mot økonomiske fortrinn enn politiske formål (Fokus 2017), spesielt høyteknologisk industri som for eksempel kraftproduksjon og maritim sektor (Fokus 2014, s. 59; Fokus 2015, s. 84). Økonomiske interesser er relevante på flere måter når det gjelder cybersikkerhet, og på grunn av at Norge har en rekke samarbeidspartnere og drift i utlandet og det er potensielt avgjørende å sørge for at vi er en pålitelig aktør med hensyn til disse.

Russiske cyberangrep mot vesten gjelder primært påvirkning i sosiale medier i forsøk på å undergrave vestlig politikk og vestlige styresmakter. Angrep spesifikt på Norge har primært vært i form av inntrenging i norske digitale systemer for å hente ut etterretning og identifisere svakheter (Fokus 2017, s. 34). Russland beskrives i denne sammenheng som mer aggressivt og selvhevdende, og påstås å ha økt sitt fokus på utvikling av teknologi til cyberangrep i de siste årene i et forsøk på å jevne ut maktforskjellene mellom egen og vestens militære kapasitet (Fokus 2017, s. 34). Russland søker å forbedre sine metoder for cybersabotasje i den hensikt å utnytte vestlig sårbarhet for å skape størst mulig handlingsrom, hvilket i stor grad også kan ramme Norge som verdens mest digitaliserte land (Fokus 2017, s. 34; Vartdal Riise 2017). Fra 2015 har russiske cyberangrep mot norske myndigheter og virksomheter vært en vedvarende trend som hevdes å foregå med det formål skaffe informasjon om politiske

beslutninger, samt militære og finansielle forhold (Fokus 2016, s. 82; Fokus 2015, s. 82). Russland beskrives som å ha en "målrettet satsning på cybersikkerhet og militærberedskap i det digitale rom" (Fokus 2014, s. 60). En slik økning i finansieringen oppfattes av E-tjenesten som en indikasjon på at cyberoperasjoner prioriteres (Fokus 2014, s. 59-60). Russland beskriver sin militære doktrine som defensiv, samtidig som russisk forsvar har gått i retning av økt spesialisering og profesjonalisering med fokus på strategisk mobilisering (Beadle og Diesen 2015, s. 68-69). For å sikre legitimitet innad er Russland fokusert på å fremstå sterk internasjonalt (Beadle og Diesen 2015, s. 69). Oppfatningen av Russlands atferd internasjonalt de senere årene, i kombinasjon med det russiske fokuset på cyber, har gjort at samtlige land med grenser til Russland i nord har forbedret sitt cyberforsvar (Kveberg og Johnsen 2013. s. 16). Også i cyberdomenet er russisk militærmakt overlegen den norske, og denne implisitte trusselen tas på alvor.

Sentralt i cybersikkerhet er det såkalte attribusjonsproblemet: det er vanskelig å avdekke hvem som står bak et angrep, og dersom det avdekkes kan det heller ikke sies med sikkerhet hvem som i realiteten er avsenderen av angrepet (Kveberg og Tynes Johsen 2013, s. 18). At et angrep fremstår som fra en annen avsender enn det i realiteten er kalles et proxyangrep, og cyberdomenet er anerkjent som en særlig egnet arena for slike angrep. Attribusjonsproblemet blir ytterligere styrket av at slike angrep muliggjør samarbeid på ad hoc basis der partene ikke trenger å ha noen nevneverdig tilknytning til hverandre (Kveberg og Tynes Johsen 2013, s. 18 og s. 22).

4.1.2 Konkrete hendelser

NSM oppga i 2017 en økning i cyberangrepene på 10% fra året før, til totalt ca. 22000 angrep hvorav 5000 ble kategorisert som alvorlige (Hotvedt 2017). I januar 2018 ble det avdekket omfattende og alvorlige cyberangrep mot Helse Sør-Øst, som E-tjenesten mener viser hvor sårbare vi er for ødeleggelse av kritisk infrastruktur (Fokus 2018, s. 30). Det er ikke gitt ut konkret informasjon om hva som har skjedd, men det er antatt at angrepet har dreiet seg om informasjonsuthenting, altså spionasje (Byberg 2018). I januar 2017 ble PST,

Utenriksdepartementet (UD), Forsvaret og Arbeiderpartiet forsøkt hacket av en russisk aktør knyttet til den russiske sikkerhetstjenesten FSB (Braathen 2017; Skjeggestad m. fl. 2017). Sjef for Cyberforsvaret, generalmajor Inge Kampenes, beskriver Norges cybersikkerhet som "på et minimumsnivå" og peker på at muligheten for å oppdage slike angrep er svært begrenset (Eide 2017), hvilket samsvarer med NSMs rapport "Helhetlig IKT-risikobilde 2017". NSM beskriver det som et "jevnt trykk av målrettede digitale spionasjeoperasjoner fra statlige aktører" (NSM 2017, s. 7), der den vanligste metoden er å sende en e-post fra en tilsynelatende troverdig avsender med beskjed om å trykke på en link som i virkeligheten overfører en skadevare til dataen. PST (Trusselvurdering 2018, s. 8-9) viser til at den mest fremtredende trusselen er fremmede staters forsøk på å knytte kontakt med ansatte som kan fungere som såkalte "insidere" for å oppgi sensitiv informasjon om kritisk infrastruktur eller programvare, slik at de kan kartlegge mangler eller sårbarheter som kan utnyttes. I følge PST ble det i 2017 oppdaget skjult skadevare hos en bedrift som driver med sensitiv teknologi, og flere slike oppdagelser har blitt gjort der skadevaren har ligget skjult i flere år (Trusselvurdering 2018, s. 10). I følge Cyberforsvarets sjef Kampenes er fremmedstatlig spionasje eller forsøk på inntrenging vanlig og vanskelig å oppdage, og selv om det er vanskelig å spore kilden oppgir han Russland som mest fremtredende aktør også i sammenheng med forsøk på inntrenging i Forsvarets databaser (Eide 2017).

4.2 Nasjonalt rammeverk

4.2.1 Nasjonal sikkerhetspolitikk

Norge er et representativt demokrati, hvilket innebærer at vi velger politikere til å representere oss og våre meninger i politiske avgjørelser. I vårt demokratiske system er det viktig for beslutningstagerne å ha befolkningens støtte i sakene som vedtas, blant annet for å sikre sin egen videre posisjon. Norsk utenriks- og sikkerhetspolitikk dreier seg om å ivareta territoriell sikkerhet, nasjonens velferd, og landets selvbestemmelse og omdømme (Fermann 2013, s 13-14)

Norsk sikkerhetspolitikk kan hevdes å være et resultat av de erfaringer vi har gjort oss i store historiske hendelser. Norge betegnes som en relativt ung nasjon fordi vi har hatt flere århundrer med union med Danmark og med Sverige, og fordi vi ikke fikk en egen grunnlov før i 1814. Norges erfaringer fra den tyske okkupasjonen under andre verdenskrig, samt verden etter den kalde krigens slutt kan også sies å ha preget norsk sikkerhetspolitisk doktrine (Innset 2002; Knutsen 2013). Norge har videre en sentral geografisk plassering med grense til Russland, en lang kystlinje mot Atlanterhavet og Arktis. Et annet sentralt aspekt er Norges økonomiske posisjon. Norges oppdagelse av oljen på søttitallet har gjort oss til et av verdens rikeste land, hvilket gjør oss sentrale på den globale arena i forbindelse med handel i tillegg til at vår økonomiske posisjon har muliggjort teknologisk forskning og utvikling på svært høyt nivå. Vårt lave innbyggertall gjør at norsk forsvar er begrenset i form av personell i verdenssammenheng, men økonomiske ressurser kan i visse sammenhenger hjelpe til å jevne ut balansen.

For formålet i denne oppgaven vil det være nyttig å belyse både norsk militær doktrine som operativt rammeverk og Norges sikkerhetspolitiske policy. Det er tatt utgangspunkt i "Forsvarets fellesoperative doktrine" som ble gitt ut i 2014 og fungerer for syv år av gangen, og i Forsvarsdepartementets rapport "Kampkraft og bærekraft - Langtidsplan for forsvarssektoren" som ble vedtatt høsten 2016. Sistnevnte er en politisk rapport som er laget i samråd med blant annet Forsvarssjefen og NSM, og inneholder alle politiske beslutninger for Forsvarets drift. For formålet i denne oppgaven vil denne anses som Norges sikkerhetspolitiske policy, sammen med Utenriksdepartementets rapport "Internasjonal cyberstrategi for Norge 2017".

4.2.2 Doktrine

Målsettingen til en militær doktrine er å "formulere grunnlaget for Forsvarets virksomhet og gi normative retningslinjer for hvordan denne virksomheten bør utføres" (Innset 2002). Norsk militær doktrine har tradisjonelt ligget langs en defensiv linje, med fokus på diplomati og et minimumsforsvar i fredstid (Knutsen 2013). Forsvarets fellesoperative doktrine (FFOD) har

til hensikt å fungere som et rammeverk for sjefer og staber for å forstå hvordan de strategiske målene skal nås dersom en krise eller krig oppstår (Bruun Hansen 2014, s. 4). En doktrine fungerer som en "dialog mellom fortid og nåtid" i den forstand at det er fortidens erfaringer som former nåtidens tanker og planlegger for fremtidens utfordringer (Innset 2002). I følge FFOD er norsk militær doktrine defensiv, som også innebærer et stort fokus på forebyggende virksomhet - særlig innenfor digitale tjenester.

FFOD fungerer som et rammeverk som har til hensikt å sikre samsvar mellom norsk sikkerhets- og forsvarspolitikk og norske militære styrker (Forsvarsstaben 2014, s. 7), og kan derfor oppfattes som Forsvarets oversetting av de politiske retningslinjene. I følge FFOD er doktrinen et dokument som skal inneholde de retningslinjer Forsvaret skal forholde seg til og inneholder en kombinasjon av særnorske målsettinger og NATO-forpliktelser. Norsk militær doktrine fungerer dermed innenfor et rammeverk av NATO-forpliktelser, men forventes å ha et forsvar som kan håndtere en begrenset trussel før NATO engasjeres (Forsvarsstaben 2014). Det er derfor sentralt at vi har et troverdig og sterkt forsvar også på egenhånd. Cybersikringen av Norge kan antas å være avhengig av analyse av informasjon og en god situasjonsforståelse, og er først og fremst underlagt E-tjenesten.

Cyberangrep kategoriseres i doktrinen (Forsvarsstaben 2014, s. 66) på en skala fra hendelse, til episode og samfunnspolitisk krise, der sistnevnte er et nivå som anses som nasjonal krise der cyberangrepet likestilles med et væpnet angrep. En nasjonal krise er av et slikt omfang at samfunnets samlede ressurser må mobiliseres for å kunne løse den, under Forsvarets samlede kommando. Terrorhandlinger, herunder småskala digitale angrep, er ansett som kriminalitet og er dermed Politiets oppgave og ikke Forsvarets. Dersom et terrorangrep er av en slik natur at det anses som et angrep mot Norge er det imidlertid likevel Forsvarets oppgave, dette innebefatter cyberangrep på infrastruktur eller kritisk industri (for eksempel oljeinstallasjoner). Forsvaret, i samråd med Politiet, er ansvarlige for å kontinuerlig vurdere behovet for styrking av egen rolle innenfor kontraterror. FFOD understreker at en økt satsning på forebygging av cyberangrep forutsetter økt informasjonsovervåkning, hvilket trolig kun gjelder innenfor lovrammene hvor E-tjenesten arbeider (internasjonal overvåkning), siden annet ikke er nevnt.

FFODs målsettinger fokuseres rundt å sikre stats- og samfunnssikkerhet. Dersom disse er eksistensielt truet legitimerer det bruk av "alle tilgjengelige ressurser" (Forsvarsstaben 2014, s. 61). Hva som konkret menes med eksistensiell trussel blir ikke definert, men FFOD påpeker at selv et begrenset angrep, eller forsøk på et slikt, fra en stormakt vil oppfattes eksistensielt truende for småstaten Norge (Forsvarsstaben 2014, s. 18-19). Sentralt i vurderingen av hva som anses eksistensielt truet er statssikkerhet og samfunnssikkerhet. Statssikkerhet innebærer sikring av territoriet og sentrale myndigheters politiske suverenitet, mens samfunnssikkerhet innebærer sikring av sivilbefolkningen, og omfatter en rekke aspekter fra infrastruktur til trygghet og frihet fra angrep og skade (Forsvarsstaben 2014, s. 62).

FFOD trekker frem strategisk kommunikasjon, herunder informasjonsinnhenting, som et av de viktigste virkemidlene Norge og NATO har i konflikter der en part er vesentlig sterkere på ett område, såkalt asymmetrisk krigføring (Forsvarsstaben 2014, s. 61). Informasjonsmakt blir stadig viktigere både for å kontre motpartens forsøk på å spre falsk informasjon (påvirkningsforsøk) og for å sikre støtte hos egen befolkning til egne operasjoner. Strategisk kommunikasjon innebærer strategisk innhenting og bruk av relevant informasjon for å sikre retningen NATO-operasjonen søker. Slik sett kan det anses både som et operasjonelt virkemiddel og som legitimeringsstrategi (Forsvarsstaben 2014, s. 61). For eksempel er det viktig for NATO å selv publisere informasjon om egne operasjoner for å motvirke eventuelle motstanderes versjon. Dette omfatter at alle NATOs representanter (fra individuelle ansatte til stater) ikke publiserer informasjon om NATO-operasjoner som ikke samsvarer med den koordinerte informasjonen (NATO Strategic Communications Policy 2009). I følge FFOD er strategisk kommunikasjon viktig for å "redusere friksjonen mellom militærmakten og omverdenen og effektivt oppnå militære målsettinger" (Forsvarsstaben 2014, s. 61).

Norsk forsvar har etter andre verdenskrig operert etter det såkalte totalforsvarskonseptet, som innebærer at dersom nødvendig skal samfunnets samlede ressurser, militære og private, samles i ett forsvar av landet (Prop. 151 S (2015-2016) s. 45). Dette konseptet anses desto viktigere i dag når flere områder av det sivile liv krever militær sikring, eksempelvis cyber. Cyberoperasjoner anerkjennes som en egen form for krigføring av det norske forsvar og NATO (Forsvarsstaben 2014). Cyberdomenet berører de mest intime sfærer av individers liv ved at så mye sensitiv informasjon lagres i nettskyer og tilsvarende digitale lagringsmedier.

Cybersikkerhet er et typisk bilde på totalforsvaret som konsept i fredstid fordi det binder offentlig sikkerhetspolitikk sammen med private aktørers tjenester. I en fellesoperativ taktikk søker Forsvaret å møte motstanderens potensielle kvantitet med kvalitet, fordi vi tradisjonelt har færre styrker. Cyber omfattes som nevnt også av vår defensive strategi (Forsvarsstaben 2014, s. 64), men innenfor NATO-retningslinjer åpnes det for at offensive cyberoperasjoner er opp til hver enkelt medlemsstat (Forsvarsstaben 2014, s. 80). Digitale storskala-angrep av Norge vil omfattes av NATOs artikkel 5, som sier at et angrep på én er et angrep på alle, som sørger for støtte fra de allierte.

FFOD skiller mellom offensive og defensive cyberoperasjoner. Defensive cyberoperasjoner skal sikre handlefrihet i egne nettverk på tross av andres offensive cyberoperasjoner. Dette betyr at motangrep inngår som en del av krisehåndteringen også i en defensiv strategi. Cyberangrep kan ta mange former, og FFOD oppgir at de farligste angrepene ofte er de vi ikke detekterer (Forsvarsstaben 2014, s. 123), noe som gjør at norsk forsvar er avhengig av omfattende overvåkning for å forsøke å hindre infiltrasjon og angrep. Forsvaret har operative evner til også å drive offensive cyberoperasjoner med den hensikt å redusere motstanderens evne til å utnytte cyberdimensjonen mot oss (Forsvarsstaben 2014). Offensive cyberoperasjoner er E-sjefens ansvar, mens den defensive sikringen er underlagt Cyberforsvaret. Slike offensive operasjoner kan også bidra med informasjon som er verdifull for andre pågående operasjoner forsvaret driver, i tillegg til at de kan sabotere motstanderens nettverkssystemer.

4.2.3 Policy

Norges sikkerhetspolitiske utgangspunkt er definert i tittelen på Forsvarsdepartementets rapport "Kampkraft og bærekraft" (Prop. 151 S (2015-2016)), fordi den sikkerhetspolitiske situasjonen beskrives som mer krevende og kompleks enn på lenge. Policyen er skapt med utgangspunkt i at "Norges sikkerhet bygges sammen med andre" (Prop. 151 S (2015-2016) s. 3), altså våre alliansepartnere, NATO-medlemmene. Langtidsplanen for Forsvaret fokuser på modernisering og effektivisering av Forsvaret med en styrking av landmakten og den

operative evnen i form av fornyede systemer. Det er gitt en historisk økning i bevilgningene til forsvarsbudsjettet fordi de sikkerhetspolitiske utfordringene Norge står overfor beskrives som mer omfattende enn på mange år, og det anses dermed viktig å kunne sørge for en troverdig avskrekking. Den endrede globale trusselsituasjonen har gjort at det kreves mer av norsk forsvar alene og dermed at vi må ta større ansvar for vår egen sikkerhet, derav økningen i bevilgningene både til eget forsvar og til NATO. Rapporten peker spesifikt på utfordringer knyttet til Russlands økte militære evne og faktiske maktbruk.

Videre er teknologi et sikkerhetspolitisk relevant aspekt og det forventes at Forsvaret stiller med et fullgodt sikkerhetsapparat knyttet til digitale tjenester. Dette beskrives som et av de viktigste forebyggende tiltakene Forsvaret kan benytte for å motvirke trusler og "beskytte forsvarssektorens verdier" (Prop. 151 S (2015-2016) s. 8). Derfor er det viktig å ha oppdaterte digitale systemer som evner å fange opp spionasje og annen digital inntrenging. Rapporten anser også cyber som et felt som bør videreutvikles på grunn av mulighetene det gir både for innsamling og lagring av informasjon. Baksiden av medaljen er som kjent at også andre land har denne muligheten og har vist seg mer enn villige til å bruke den på mer "uredelig vis" via hacking og spionasje. Utenlandsk etterretning beskrives som den største sikkerhetspolitiske trusselen forsvarssektoren står overfor i dag. Norge har, som nevnt, en defensiv cyberpolicy der prioriteringen først og fremst er å forbedre systemene vi har, men det kan hevdes at cyberpolicyen viser offensive trekk i det at myndighetene anser det som et satsningsområde. Rammeverket ligger likevel langs den samme defensive linjen som resten av forsvarspolicyen. Andre land har vist en mer offensiv cybertaktikk hvilket blant annet innebærer sabotasjeoperasjoner som kan lamme kritisk infrastruktur. Det er derfor ansett som særlig viktig for vårt defensive forsvar å ha mulighet til å identifisere angrep eller forsøk på angrep raskt, da cyber er et felt som er særlig egnet til å destabilisere og skape kaos tidlig i en konflikt, for deretter å benytte andre angrepsmidler. Sabotasjeaksjoner rettet mot kritisk infrastruktur kan vanskeliggjøre nasjonale beslutningsprosesser der kommunikasjonsmidler rammes, hvilket understrekes av policyens fokus på forbedret overvåkning av de digitale systemene. I rapporten beskrives Norges sikkerhetspolitiske policy som fokusert rundt å ha "en avskrekkende effekt på mulige angripere og forsvare Norge og allierte mot eksterne trusler, anslag og angrep", der Forsvaret er vårt mest grunnleggende sikkerhetspolitiske

virkemiddel (Prop. 151 S (2015-2016) s. 5). Avskrekkingsstrategien anses for å redusere sannsynligheten for angrep.

Norge som NATO-land har implementert deres cyberstrategi som også understreker viktigheten av strategisk kommunikasjon. Dette er kommunikasjon som er rettet mot å forsøke å påvirke aktørers holdninger og handlinger. Strategisk er dette et virkemiddel som både har trekk av påvirkning og diplomati, og det er også et virkemiddel som forsøker å ta problemer ved roten (Prop. 151 S (2015-2016) s. 36). Også strategisk kommunikasjon anses som et defensivt virkemiddel for å redusere sannsynligheten for angrep eller kriser, i tillegg til at det fungerer som en motvekt til motstanderes forsøk på å påvirke ved å skape en forvridd situasjonsforståelse (Prop. 151 S (2015-2016) s. 36). Som virkemiddel krever dette mer av E-tjenesten i form av informasjonsinnhenting og situasjonsanalyser, dette understøttes av myndighetenes fokus på å knytte seg enda nærmere særlig relevante samarbeidspartnere for informasjonsutveksling.

Et videre forsøk på et forebyggende sikkerhetspolitisk tiltak er satsingen på forskning på høyteknologiske løsninger innenfor informasjons- og nettverksteknologi, som er et virkemiddel for å øke resiliens ved forsøk på angrep (Prop. 151 S (2015-2016) s. 103-104). Sannsynligheten for slike angrep anses som høy. Digitaliseringen og økningen i nettverksbaserte løsninger i Norge er ansett for å skape gode muligheter for Forsvarets utvikling innenfor dette fagfeltet, og policyen understreker dette som del av en defensiv strategi (Prop. 151 S (2015-2016) s. 103). På den annen side vil videre digitalisering ytterligere øke sårbarheten, hvilket skaper et internt kappløp for å sikre våre egne, stadig mer avanserte, systemer. Samspillet mellom sårbarhet og mulighet er en utfordring og et sentralt aspekt i Norges cyberpolicy.

4.2.4 Internasjonal cyberstrategi for Norge

For første gang ble det i 2017 lansert en cyberstrategi fra Utenriksdepartementet. Rapporten begynner med et forord fra Statsminister Erna Solberg som stadfester at

> "Norge arbeider for et digitalt rom som fremmer innovasjon og internasjonal handel, som bidrar til internasjonal stabilitet og sikkerhet og som ivaretar demokratiske verdier og universelle rettigheter" (Utenriksdepartementet 2017, s. 3)

I rapporten beskrives cyberdomenet som et av de viktigste arenaene for handel og informasjon og understreker viktigheten av å sørge for sikkerheten til kritisk infrastruktur. Cyberstrategien identifiserer både statlige og ikke-statlige aktører som trusler mot Norge, og peker på internasjonalt samarbeid om normutvikling som en av myndighetenes viktigste oppgaver i cyberdomenet. Strategien fokuseres særlig rundt demokratiske rettigheter og verdier og understreker viktigheten av en cyberstrategi som balanserer riktig mellom sikkerhet og individets rettigheter. De strategiske prioriteringene er først og fremst basert på økt samarbeid internasjonalt og på tvers av sektorer. Utenriksdepartementet beskriver cyber som et utviklingsområde som er særlig relevant for norske økonomiske interesser der det er viktig å legge til rette for internasjonale investeringer, dette gjøres best ved "internasjonal harmonisering av lovverk" (Utenriksdepartementet 2017, s. 8). Alle former for samarbeid bør i følge rapporten styrkes av hensyn til informasjonsutveksling og normutvikling, og det bør etableres mulighet til digital myndighetsutøvelse gjennom såkalt "internet governance" (Utenriksdepartementet 2017, s 10).

4.2.5 Lysne II-utredningen – en sterk signaleffekt

I 2014 oppnevnte daværende Forsvarsminister Ine Eriksen Søreide et utvalg for å utrede den norske trusselsituasjonen på cyberfeltet, samt norske kapasiteter på dette området. Utvalgets arbeid resulterte i en ugradert rapport som kom ut i 2016 og kartla samfunnets digitale sårbarhet og identifiserte tiltak for å redusere denne samt styrke beredskapen (NOU 2015: 13). Hovedkonklusjonen i rapporten var at Norge sterkt behøver et Digitalt Grenseforsvar (heretter DGF). Utvalgets rapport ble tatt til følge av Forsvarsministeren og Regjeringen, og på nåværende tidspunkt utredes det videre hvordan DGF kan implementeres som norsk policy.

Utvalget benytter betegnelsen DGF om målrettet innhenting og analyse av utenlandsk etterretningsinformasjon basert på tilgang til elektronisk informasjon som går inn og ut av Norge med den hensikt å kartlegge trusler mot rikets sikkerhet (Lysne m.fl. 2016, s 10). Hensikten med DGF er å gi E-tjenesten teknisk tilgang til informasjonskilden. Per i dag utfører E-tjenesten sin innsamling over satellittnett, mens størsteparten av relevant kommunikasjon gjøres over fiberoptiske kabler (Lysne m.fl. 2016, s. 6). Lysne II-utvalgets konklusjon er at DGF må innføres fordi det er nødvendig for nasjonens sikkerhet. Implementeringen bør gjøres med strenge begrensninger i filtrering av informasjon for å sikre juridiske personvernrettigheter. Hovedfokus i informasjonsinnhentingen vil være på handlinger og planlegging, ikke på meninger (Lysne m.fl. 2016, s. 66).

Hovedoppgaven til DGF vil være å avdekke og motvirke eksterne trusler og angrep slik at de kan stoppes før de materialiserer seg. Denne formen for overvåkning og kontroll er ikke mulig per i dag, og de mest avanserte truslene kan ikke avdekkes med tilgjengelige metoder (Lysne m.fl. 2016, s. 29). Lysne II-utvalget identifiserer to særlig relevante utviklingstrender: en kraftig eskalering av cybertrusler mot Norge, og at kommunikasjonsteknologi i økende grad endres til nettbasert, som igjen gjør at systemene i alle tilfeller behøver et skifte. Begge disse trendene peker ifølge utvalget mot opprettingen av DGF. I følge utvalget vil en slik styrking og videreutvikling av E-tjenesten bidra til å bedre responsevnen dersom noe skjer. Lysne II-utvalget understreker viktigheten av et troverdig forsvar som beskytter nasjonen utover det tradisjonelle trusselspektrum militæret har operert i (Lysne m.fl. 2016, s. 11). Informasjonskrigføring er en aktuell trussel i dag, og en teknologisk overlegen motstander kan destabilisere ved å påvirke befolkningens opplevelse av situasjonen (Beadle og Diesen 2015, s. 43). Slike angrep fungerer som en del av hybrid krigføring, altså en krig som benytter en kombinasjon av forskjellige typer angrep enten samtidig eller etter tur. Et digitalt angrep på kritisk infrastruktur kan komme tidlig for å skape kaos før en påvirkningsstrategi settes inn, da etter langvarig spionasje med innhenting av informasjon slik at påvirkningen er skreddersydd til å passe der skoen trykker (Lysne m.fl. 2016).

Slik Lysne-utvalget beskriver det vil de rettslige rammene for E-tjenesten og DGF behøve en utvidelse. I det såkalte Legalitetsprinsippet i Grunnloven §113 heter det at "Ethvert inngrep

overfor den enkelte må ha grunnlag i lov" (Lovdata 2018; Lysne m.fl. 2016 s. 37) som i følge rapporten ikke fullt ut eksisterer i dag (Lysne m.fl. 2016). Rapporten peker på flere problemer knyttet til lovhjemmel, blant annet tilgang til kommunikasjon over privateide kanaler, potensiell inngripen i Den Europeiske Menneskerettskonvensjonens (EMK) artikkel 8, og norske innbyggeres rettigheter gjennom det såkalte kommunikasjonsvernet (Lysne m.fl. 2016). Kombinasjonen av de juridiske problemstillingene som reises i rapporten kan føre til et svekket personvern for den enkelte, og det konkluderes med at "[u]tvalget legger til grunn at DGF vil utgjøre et inngrep i privatliv og korrespondanse" (Lysne m.fl. 2016, s 39). Av ovennevnte grunner refereres problemer knyttet til dette som potensiell inngripen i den enkeltes personvern.

Lysne-utvalget beskriver gjennomgående cyber-trusselsituasjonen som tiltagende og antatt økende også i årene som kommer. Det understrekes at fordi E-tjenestens analyser er av prediktiv karakter må sårbarhet ha en viktig plass i risikovurderingen. E-tjenestens analyser legger mye av grunnlaget for Forsvarets operative virksomhet og det er derfor viktig at systemene er oppdaterte slik at vi oppdager trusler og forsøk på angrep. Norges grense til Russland beskrives også som en grunn til å holde våre systemer på nivå med deres, der dette er mulig (Lysne m.fl. 2016, s. 28). DGF beskrives som nødvendig for at E-tjenesten skal kunne fullføre sitt samfunnsoppdrag (Lysne m.fl. 2016, s. 52).

4.3 Internasjonale forpliktelser og hensyn

4.3.1 Allierte

Norsk sikkerhetspolitisk strategi er formet på bakgrunn av at vi er en småstat med landegrense mot en stormakt, noe som igjen betyr at vi er avhengige av alliert hjelp ved konflikt og/eller krise (Beadle og Diesen 2015). Vår nærmeste allierte er NATO, som beskrives som "selve hjørnesteinen i norsk sikkerhetspolitikk" (Tynes Johnsen 2014, s. 4). Som beskrevet tidligere tar norsk sikkerhetspolitikk utgangspunkt i ivaretakelsen av en rekke hensyn, deriblant

territoriets sikkerhet, nasjonens velferd, samt statens selvråderett og autonomi (Fermann 2013, s. 13-14). Det er videre sentralt for Norge å sikre vårt demokratiske styresett og de verdiene som er knyttet til demokratiet, som også kan anses som et av de viktigste nasjonale hensynene. Som småstat er Norge avhengig av en rekke allierte og samarbeidspartnere der de mest sikkerhetspolitisk relevante er NATO, FN, OSSE og EU. For formålet av denne oppgaven er det primært fokusert på NATO, som er helt avgjørende for vår sikkerhetspolitikk. Dernest kommer rollen til EU som nær samarbeidspartner, tross at vi ikke inngår som medlem.

Sikkerhetspolitikk balanserer mellom forpliktelsen til å sikre nasjonale interesser og å ivareta befolkningens individuelle juridiske rettigheter, slik som personvern. Cyberdomenet er av de sikkerhetspolitiske felt med størst utfordring på dette området, da det meste av sikringen dreier seg om overvåkning. Overvåkningen vil nødvendigvis måtte innbefatte overvåkning også av nasjonale systemer på grunn av faren for at det er plantet spionasje-programvare i noen av våre digitale systemer (Lysne m.fl. 2016). Norsk sikkerhetspolitikk må også ta hensyn til våre allianseforpliktelser til NATO, som innebærer, på samme måte som de andre forpliktelsene, at vi forventes å ha så gode systemer som mulig til enhver tid. Dette bunner i NATOs artikkel 5 som stadfester at et angrep på én er et angrep på alle, og at dette med alle midler må forsøkes unngått (NATO 2017). Derfor er det nødvendig at vi som NATO-alliert ikke har mangelfulle systemer som gjør at vi for eksempel ikke oppdager informasjonsspionasje. Vi er nødt til å ha "et troverdig forsvar" (Lysne m.fl. 2016, s. 11).

NATO-alliansen er basert på overenstemmelse om en traktat bestående av de såkalte artiklene. Den mest kjente av disse er artikkel 5, videre hevder artikkel 4 at dersom en stat føler at sin sikkerhet er truet skal det vurderes hvorvidt dette skal omfattes av artikkel 5 (Tynes Johnsen 2014, s. 12). Krigen mot terror, som ble utløst av angrepet 9/11, er hittil det eneste tilfellet der artikkel 5 har blitt brukt. Det har vært en omfattende debatt om hvorvidt cyberangrep skal kunne omfattes av artikkel 5, der blant annet tidligere Utenriksminister Espen Barth Eide slo fast at et angrep må utløses fysisk dersom det skal omfattes av artikkel 5 (Kveberg og Tynes Johnsen 2013, s. 48). I alle tilfeller vil artikkel 4 gi mulighet for å diskutere hver enkel situasjon og åpner således for at cyberangrep kan omfattes av artikkel 5 (Tynes Johnsen 2014, s. 12). Per i dag anser norske offisielle meldinger at angrep i det

digitale rom omfattes av NATO artikkel 5 om kollektivt forsvar dersom det er av stor skala (Prop. 151 S (2015-2016) s. 35). I alle tilfeller fastslår Folkeretten at væpnet makt kan benyttes dersom FNs sikkerhetsråd anser det som nødvendig for å sikre internasjonal fred (Kveberg og Tynes Johnsen 2013, s 18).

NATOs retningslinjer er bindende for medlemslandene, og alliansen godkjenner og enes om disse på forhånd. Deriblant finnes det et sett av konsepter, doktriner og prosedyrer som landene må implementere så raskt som mulig (Forsvarsstaben 2014). Dette er viktig for å sikre høy grad av effektiv samhandling. Som nevnt over fungerer norsk militær doktrine innenfor et NATO-rammeverk, og i tillegg til dette har vi forpliktelser til FN og EU når det gjelder støtte til planlegging, gjennomføring og ledelse av internasjonale operasjoner (Forsvarsstaben 2014). FN-pakten sier at alle medlemsstater skal avstå fra trusler eller maktbruk mot andre staters territorielle integritet, og cyber er ansett underlagt denne bestemmelsen. Et EU-samarbeid om cybersikkerhet kan tenkes å ønske å fokusere mer på hensyn til de sivile aspektene ved cybersikkerhet kontra NATO som er en forsvarsallianse og dermed i større grad har fokus på statens sikkerhet (Kveberg og Tynes Johnsen 2013, s. 54).

Det hevdes at det har skjedd en global maktforskyvning fra vesten til nye fremvoksende stater (Beadle og Diesen 2015, s. 18), blant annet grunnet fremveksten av billigere militærteknologiske nyvinninger som cyber. For stater med begrensede ressurser kan slik teknologi gi muligheter for destabilisering av vestlige stater som tradisjonelt har hatt militærteknologisk hegemoni (Beadle og Diesen 2015, s. 40). Dette gjør at det er viktigere enn noen gang å beskytte informasjonen Norge besitter som NATO-alliert, og ikke kun industrispionasje mot vår egen teknologi. Cyberdomenet er et alliert satsningsområde, og et av få områder Norge har mulighet til å utpeke seg i NATO-sammenheng fordi vi er langt fremme med militærteknologisk forskning og har solide økonomiske ressurser (Tynes Johnsen 2014). Det er også et viktig signal å sende til NATO, på bakgrunn av USAs ønske om mer fordeling av byrdene i alliansen, i tillegg er et oppdatert cyberforsvar viktig for å sikre NATOs relevans i fremtiden (Tynes Johnsen 2014, s. 14).

NATO-medlemmene signerte i 2016 en ny avtale om cybersikkerhet, som følger avskrekkingsdoktrinen. Dette innebærer at landene skal forsøke å ha så god cybersikkerhet at

det forhindrer angrep fordi motparten anser at et angrep vil ha for stor risiko for sin egen del. NATOs cyberfokus skyldes ifølge NATOs generalsekretær Jens Stoltenberg at det er vanskelig å tenke seg en konflikt i dagens verden som ikke har en cyberdimensjon (Pijnenburg Muller og Stevens 2017, s. 1). Sammenlignet med andre NATO-virksomhetsområder har cyber vært ansett som et felt der trusselen er høy mens beredskapen er lav. Det er viktig at medlemslandene har et felles fokus på cybersikkerhet for å oppnå bedre situasjonsforståelse og informasjonsutveksling, og optimere samhandling (Kveberg og Tynes Johnsen 2013). NATO-strategien kan være svært kostbar grunnet attribusjonsproblemet da det potensielt må benyttes store ressurser til å identifisere motparten (Pijnenburg Muller og Stevens 2017, s. 2). Det anses videre usannsynlig at avskrekking hindrer størsteparten av cyberangrep samtidig som konflikter pågår kontinuerlig i cyberspace fordi terskelen er lav på grunn av lave kostnader og korte avstander (Pijnenburg Muller og Stevens 2017, s. 2).

4.3.2 Økonomiske interesser

Norge er et av verdens rikeste land og har en stor oljeformue (Statens Pensjonsfond Utland, heretter SPU) som både muliggjør en rekke investeringer og interne velferdsordninger. Av hensyn til nasjonalt inflasjonsnivå og valutakurs må store deler av SPU-investeringene legges til utlandet og vi er dermed avhengige av å samhandle med verden, på lik linje som verden er avhengige av å samhandle med oss (Kveberg og Tynes Johnsen 2013). Effektiv samhandling med verden rundt oss fordrer at vi har digitale løsninger med god sikkerhet. Cybersikkerhet kan dermed anses som et komparativt fortrinn som tiltrekker seg investeringer, og motsatt vil mangel på cybersikkerhet kunne skremme vekk investorer, og en måte å sikre seg et slikt komparativt fortrinn på er å ha lovbestemmelser for cybersikkerhet (Kveberg og Tynes Johnsen 2013, s. 34-35). Videre er det nødvendig å hindre industrispionasje gjennom god cybersikkerhet, aktualisert ved at det er oppdaget et marked for kjøp og salg av informasjon om digitale sårbarheter, altså smutthull som kan gjøre det mulig å trenge inn i programvaren (Kveberg og Tynes Johnsen 2013, s. 31). Sentralt for norske økonomiske interesser er petroleumssektoren, og NUPI har nylig utgitt en rapport som har utredet risikoen for et russisk

digitalt angrep på sentrale funksjoner i denne sektoren (Muller, Gjesvik, Friis 2018). I rapporten fremgår det at Russland i større grad kan anse Norge som en konkurrent innenfor olje- og gassproduksjon etter annekteringen av Krim, som ledet flere europeiske land til å begrense kjøpene av russisk olje og gass (Muller, Gjesvik, Friis: 2018, s. 11-12). Dette på tross av at Norge ikke er noen fanebærer i denne saken. Rapporten trekker i denne sammenheng frem viktigheten av et nært samarbeid om informasjonsutveksling mellom bedrifter og sikkerhetsmyndigheter (Muller, Gjesvik, Friis: 2018, s. 27). Risikoen for ulike digitale angrep på norsk petroleumssektor, enten det er industrispionasje eller sabotasje av kritisk infrastruktur, anses som betydelig og blir argumentert for ved å sammenligne russiske digitale angrep på liknende sektorer i andre land (Muller, Gjesvik, Friis: 2018).

5. Drøfting

Hensikten med dette kapittelet er å besvare problemstillingens to spørsmål: **hva består den digitale trusselsituasjonen i Norge av, og hva driver utformingen av den norske sikkerhetspolitikken på cyberfeltet**? Drøftingskapittelet vil diskutere de empiriske funnene sett i lys av de teoretiske perspektivene realisme, liberalisme og konstruktivisme. De tre perspektivene fungerer ikke som en fasit på hvordan politikken på cyberfeltet må forstås, men med sine ulike teoretiske utgangspunkt og grunnideer identifiserer de egne sett av spørsmål som kan belyse situasjonen. I empirigjennomgangen ble det tydelig at det finnes politisk vilje til å bedre sikkerheten på cyberfeltet i Norge. Dette gjør at problemstillingens andre spørsmål naturlig dreies mer mot hvilke faktorer som kan forklare denne politiske viljen.

Kapittelet er todelt og begynner med en diskusjon av problemstillingens første spørsmål i lys av de tre teoretiske perspektivene. Problemstillingens andre spørsmål diskuteres på tre analysenivåer: individnivå; statsnivå; og globalt nivå, i henhold til logikken i policyanalysen som ble beskrevet i metodekapittelet. Det vil være noe overlappende diskusjon av det digitale trusselbildet også i diskusjonen av cyberpolicyen, dette fordi temaene vanskelig lar seg diskutere helt isolerte, fordi drivkreftene bak cyber-sikkerhetspolitikken naturlig nok er preget av trusselbildet.

5.1 Trusselsituasjonen

5.1.1 Den direkte trusselen

I empirikapittelet ble det redegjort for flere ulike rapporter og dokumenter som alle pekte i retning av at den norske trusselsituasjonen på cyberfeltet krever bedre forsvar. Rapportene viste at for å sørge for et bedre digitalt forsvar må vi drastisk forbedre de digitale systemene våre. Samtidig er bredere overvåkning av kommunikasjon, der en av kontaktflatene er innenlands, trolig fører krav om endringer i personvernet (Fokus 2018; Lysne m.fl 2016, s.

39). Kombinasjonen av disse faktorene gjør cyberfeltet særlig vanskelig å gjøre endringer i tross at det finnes en rekke motivasjoner for dette, hvilket vil bli diskutert nedenfor.

På bakgrunn av de empiriske funnene er det grunn til å tro at Norge i dag opplever langt flere cyberangrep enn vi er klar over (se for eksempel Lysne m.fl. 2016). Formidlingen av trusselbildet fra E-tjenesten, både i medier og i Fokus-rapportene, gir dermed uttrykk for en alvorlig bekymring for at vi ikke engang evner å kartlegge trusselen fordi systemene våre ikke fanger opp alle angrepene. Klassisk realisme peker mot at det er en av statens viktigste oppgaver å sørge for fullgod sikkerhet for befolkningen (Glaser 2016, s. 16), og en forutsetning for dette må være at man vet hvor trusselen kommer fra og hvor stor trusselen er. Usikkerhet kan oppfattes som forsvarets verste fiende ifølge klassisk realisme. Fra dette perspektivet ser trusselsituasjonen dermed enda verre ut med bakgrunn i at usikkerhet danner en ytterligere dimensjon av trusselbildet. Som motsvar til dette kan securitiseringsteorien peke i retning av å ta et steg tilbake og se på de faktiske bevisene på cyberangrep. I følge securitiseringsteorien vil det være i beslutningstakernes interesse at trusselen på cyberfeltet overdrives, dermed vil det ifølge denne teorien kunne tilsi at momenter som usikkerhet tillegges uproporsjonalt mye vekt.

De empiriske dataene viste at særlig spionasje og planting av informasjon er vanlige former for cyberangrep mot Norge. Spionasje kan både gjøres for å kartlegge svake punkter i programvare og for å få informasjon om ny teknologi, særlig innenfor industri. Videre er personinformasjon en attraktiv salgsvare (Dunn Cavelty 2016, s. 401), og det kan dreie seg om så enkel informasjon som personlige preferanser ved netthandel, som igjen eksempelvis kan benyttes til strategisk markedsføring via annonser (Dunn Cavelty 2014, s. 705). NSM og E-tjenesten (NSM 2017; Fokus 2018) beskriver hvordan målrettede angrep til enkeltpersoners e-post er vanlig i Norge. Dette rammer ikke bare personer i utsatte stillinger, trolig forstår ikke de fleste som angripes hvorfor de er aktuelle for spionasje (Kristoffersen 2018). Konstruktivismen taler for et bredere syn på menneskelig sikkerhet, der tradisjonell sikkerhetspolitikk må oppdateres til å anerkjenne nye trusler (Hough 2008). Cybertrusselen viser klart at usikkerhet er et moment knyttet til menneskelig sikkerhet der enhver kan føle seg truet og relevant for angrep.

Trusselbildet slik det presenteres av myndighetene identifiserer aktørene bak cyberangrepene som stater, primært Russland og Kina (se for eksempel Fokus 2018). Likevel fremstår cyberfeltet i seg selv som åpent for nær sagt hvilken som helst aktør dersom vedkommende har kunnskap nok om dataprogramvare eller annen cyberrelatert kompetanse. I tillegg er teknologien i stor grad allment tilgjengelig og åpner dermed for et fleraktør-perspektiv i tråd med liberalismens syn. Fra et klassisk realistisk ståsted kan det hevdes at cyberfeltet kun er sikkerhetspolitisk relevant dersom avsenderen er en stat (Glaser 2016), hvilket også krever tradisjonelle sikkerhetspolitiske løsninger. I tråd med denne tankegangen kan det hevdes at det vil være vanskeligere å sørge for samhandling og informasjonsutvekslig om tiltak til cybersikring mellom offentlige instanser og private bedrifter, fordi problemet defineres som Forsvarets ansvarsområde. Attribusjonsproblemet viser hvor vanskelig det er å identifisere aktørene (Kveberg og Tynes Johnsen 2013, s. 18), og en eventuell identifisering av en stat som avsender av et cyberangrep er basert på den geografiske plasseringen til avsenderen i tillegg til en antagelse om at et storskala angrep behøver statlig støtte. Liberalismen åpner for et bredere syn på aktører og trekker inn både grupper og organisasjoner (Russett 2013, s. 106-107). Sett fra et liberalistisk perspektiv kan aktørbildet i cybersikkerhet trolig utvides fordi vi ikke alltid vet med sikkerhet hvem avsenderen er. En utvidelse av aktørbildet kan også åpne for flere løsninger som er tilrettelagt nettopp dette. Bedrifter og grupper kan oppfattes som relevante aktører, noe som åpner for forsøk på normstyring og lovendringer. Opprettelsen av tilsynsorganisasjoner for cybersikkerhet eller en organisasjon som kan samle og dele informasjon om hva trusselen består av, og hvor den kommer fra, kan være mulig. Konstruktivismen retter fokus på tradisjonelle skillelinjer i verden (Agius 2016), der et typisk er "vesten og resten" som betegnelse på vesten og de som er "venner" med dem, og alle andre. Sikkerhetspolitisk ble det benyttet slik retorikk i krigen mot terror, der G. W. Bush uttalte at enten er dere med oss, ellers er dere mot oss (Agius 2016, s. 73). På denne måten kan definisjonen av trusselbildet tolkes til at enhver aktør anses som en representant for en større motstander, eller snarere en representant for en stat. Samtidig kan dette oppfattes som et typisk eksempel på securitiseringsteoriens hovedargument: at et tema beskrives på en måte som gjør at det kan anses som et sikkerhetsanliggende.

Som vist i empirikapittelet beskrives den digitale trusselsituasjonen i Norge som et høyrisikofelt med høy sannsynlighet for angrep (Fokus 2017, s. 6). På den annen side er det stor usikkerhet knyttet til konsekvensene av et slikt angrep. Risikovurderingen skyldes en kombinasjon av årsaker, men mest sentralt er sårbarheten som ligger i et høyteknologisk samfunn der befolkningen har solid privatøkonomi (NSM 2017). En stor del av befolkningen har tilgang til internett og smarttelefon, hvilket gjør at befolkningen er midt i "skuddlinjen" der angrepene foregår. Fra et neo-realistisk synspunkt er det naturlig å anta at stater vil benytte seg av enhver tilgjengelig metode for å skaffe seg bedre posisjon, noe cyberfeltet er som skapt for. Med relativt enkle midler kan det videreutvikles teknologi for spredning av desinformasjon, tilrettelagt for gjennom allerede eksisterende programvare. En ytterligere kostnadsbesparende faktor for motparten er muligheten desinformasjon gir til å styre opinionen innad i Norge og derigjennom spre mistro til myndigheter og politiske prosesser. Dersom befolkningen ikke har tiltro til sin egen stat kan dette i verste konsekvens skape en situasjon der systemet angriper seg selv. Dette scenariet fremstår skremmende, og det er tydelig at med enkle retoriske grep er det kun fantasien som setter grenser for potensialet i et cyberangrep.

5.1.2 Beskrivelsen av trusselen

De empiriske dataene beskrev alle cybertrusselen mot Norge med ord som sårbarhet, risiko og usikkerhet, samt hvordan disse faktorene utgjør et stort potensiale for angrep mot Norge. Det virker å være en tendens til å anta at norske bedrifter, myndigheter og personer er i faresonen for cyberangrep fordi vi kan observere cyberangrep mot andre land (Fokus 2017, s. 6).

Et av securitiseringsteoriens mest sentrale argument er at usikkerhet rundt faktorer som risiko og sårbarhet gjør det enkelt å overbevise noen om at trusselen er stor, tross at det kanskje ikke finnes så mange konkrete eksempler (Emmers 2016). Med det sagt ligger statens overlevelsesgrunnlag i befolkningens tiltro til dens legitimitet, slik at det er kritisk nødvendig å sikre at befolkningen ikke gis desinformasjon som er skreddersydd for å skape mistro til systemet. Informasjonssikring kan i så måte anses som høyst rasjonelt fra et klassisk

realisme-perspektiv. På den annen side kan det fra et konstruktivistisk synspunkt stilles spørsmål om hvor grensen går mellom informasjonssikring og sensur, dersom informasjonssikringen går ut på å blokkere spredning av det som anses som falsk informasjon.

Et videre poeng knyttet til dette er at cyber er ganske nytt på den sikkerhetspolitiske agenda, hvilket gjør at vi må definere problemet og eventuelle prosedyrer i dag. Ut fra securitiseringsteorien er det særlig viktig å ikke skape et for bredt mandat i begynnelsen (Fierke 2016, 199-200), fordi vi ikke vet hvordan digital krigføring utvikles videre. Dersom potensialet for ødeleggelse fra cyberangrep anses som faretruende høy i dag og dette gir muligheten for et bredt politisk mandat for sikring og forsvar, kan det få uheldige konsekvenser dersom trusselen ikke aktualiseres. For å illustrere kan vi tenke oss en situasjon der den norske stat anser det som kritisk nødvendig å overvåke innlands digital kommunikasjon og får mandat til å gjøre dette, men det viser seg at mesteparten av kommunikasjonen foregår utenfor Norge. I et slikt tenkt tilfelle vil det potensielt være vanskelig å gå tilbake til de gamle retningslinjene for overvåkning av innlandskommunikasjon, og man har endret lovgivning tilknyttet personvern på potensielt sviktende grunnlag.

Et sentralt moment for det digitale trusselbildet er russisk atferd. Russland blir av E-tjenesten gjennomgående beskrevet som mer aggressivt, og bruker stadig mer ressurser på cyber (Fokus 2018, s. 30). Konstruktivismen vil her stille seg kritisk til hvorvidt dette bør tolkes som en reell trussel mot oss, med bakgrunn i at det er enkelt å tolke motpartens atferd som truende (Wendt 1995). Fokus-rapportene hevder at Russland er opptatt av å fremstå sterk internasjonalt for å få legitimitet internt (Beadle og Diesen 2015, s. 69). Dermed kan det, med konstruktivismens spørsmål in mente, hevdes at høyest på den russiske agenda er intern politisk overlevelse gjennom legitimitet fra egen befolkning. Altså kan det være interne faktorer som er styrende for russisk atferd, og ikke ekspansive internasjonale planer. Sett fra et neo-realistisk ståsted er det derimot liten tvil om at en stats økende aggressive atferd er et forsøk på å korrigere maktbalansen og hevde seg overfor andre stater (Mearsheimer 2013), ved å utnytte nye områder som krever færre folk og mindre penger.

Myndighetenes rapporter om cybertrusler peker alle i retning av at risikoen er høy og beskyttelsen for lav (Fokus 2018, NSM 2017, Lysne m.fl. 2016). Sett fra de teoretiske perspektivene kan det rettes flere ulike, kritiske spørsmål til hvorvidt denne vurderingen er overdrevet og om det er riktig å ta all informasjon for god fisk. Ut fra liberalismens fokus på individers innflytelse på definisjonsprosessen (Moravcsik 2008, s. 236-237) kan det tenkes at visse ønsker å overdrive problemet for å sikre sin egen stilling. Med utgangspunkt i et realistisk perspektiv kan det tenkes at trusselen oppfattes som skremmende fordi det er lett å tolke andre staters atferd feil (Glaser 2016). Securitiseringsteorien hevder at overdrivelse gjøres for at problemet skal anses som et sikkerhetsanliggende slik at det lettere kan oppnås ønskede tiltak (Buzan m.fl 1998, s. 24).

Med dette sagt er det viktig å ha in mente at etterretningsinformasjon i stor grad må holdes hemmelig og at det er E-tjenestens oppgave å innhente, tolke og videreformidle denne informasjonen. Dersom vi ikke stoler på at informasjonen myndighetene gir oss for det meste stemmer, har vi store problemer knyttet til statens legitimitet. Cyberdomenet er et nytt felt med stor usikkerhet knyttet til potensialet til digitale angrep, hvilket gjør det lettere å overvurdere farer og trusler. Samtidig er det dermed også lettere å overbevise andre om faren, og det er ikke urealistisk å anta at overdrivelse benyttes som politisk grep også innenfor cybersikkerhet.

5.2 Drivkrefter i cyber-sikkerhetspolitikken

I denne delen av kapittelet følger drøftingen av problemstillingens andre spørsmål: hva driver utformingen av den norske sikkerhetspolitikken på cyberfeltet? Spørsmålet diskuteres på tre analysenivåer gjennom faktorer på individnivå, statsnivå og globalt nivå. Som nevnt i innledningen vil det være noe overlappende diskusjon av problemstillingens to spørsmål, der trusselbildet også trekkes frem i diskusjonen av drivkreftene i cyber-sikkerhetspolitikken under.

5.2.1 Individ-nivå

På dette analysenivået er individuelle faktorer i fokus, herunder persepsjon og oppfatning av virkeligheten. Beslutningstakere er typisk politiske eliter og individer med tilgang til beslutningsprosessen, og deres meninger og personlige agenda er sentralt på individnivå (Fermann 2013, s. 109). Videre er oppfatninger i befolkningen viktig for elitene blant annet når det gjelder politisk oppslutning.

Den empiriske gjennomgangen viste særlig to sentrale personer knyttet til cybersikkerhet: den tidligere Forsvarsministeren og E-sjefen gjennom de siste to årene. E-sjefens analyser er av naturlige årsaker svært sentrale når det gjelder cybersikkerhet, og utgjør trolig også grunnlaget for den politiske elitens forståelse av trusselbildet. I denne sammenheng anses Regjeringen, og dels Stortinget, som politisk elite.

Sett fra et konstruktivistisk perspektiv er det nødvendig å stille noen kritiske spørsmål knyttet til hvem som har tilgang til prosessen med å definere et problem, og hvorvidt definisjonen er basert på reelle trusler. De offisielle rapportene som ble gjennomgått fokuserte i stor grad på faktorer som risiko og sårbarhet (Fokus 2011-2018; NSM 2017), og E-sjefen har ved flere tilfeller gjort intervjuer i media for å gi et statusbilde av cybertrusselen til befolkningen der trusselen beskrives som høy og problemet prekært (Veum 2017). Dette kan tolkes fra to ulike sider. På én måte er det trolig nødvendig for E-sjefen å gå bredt ut for å sikre seg oppslutning rundt cybersikkerhet. Det vil vanskelig bli politisk flertall for et vedtak befolkningen ikke bryr seg om og det er dermed nødvendig å informere befolkningen om farene. På den annen side kan det stilles kritiske spørsmål til hvorvidt trusselvurderingen er realistisk. For befolkningens egen del er det naturlig å ta slike spørsmål på alvor, fordi det potensielt kan gå utover den enkeltes personvernrettigheter. Med dette sagt bør det tas forbehold om at det er nødvendig at kritisk etterretning hemmeligholdes, og det kan grense til det konspiratoriske dersom vi skal mistro all informasjon vi blir gitt. På den annen side vil et konstruktivistisk perspektiv gi nødvendige innvendinger til å blindt akseptere informasjonen all den tid det kan ligge andre hensyn bak. I tråd med konstruktivismen kan det hevdes at det er en problematisk mangel på

faktiske eksempler på cyberangrep på norsk jord som gjengis i Fokus-rapportene, i alle fall når trusselen anses som høy og risikoen enda høyere. Likevel kan det tenkes at trusselen faktisk oppfattes som høy og at den informasjonen som legges frem dermed er basert på en reell oppfatning, slik konstruktivismen åpner for (Fierke 2013, s. 196-197).

Cyberspace er grenseløst og har korte digitale avstander på tross av lange geografiske avstander (Pijnenburg Muller og Stevens 2017, s. 2). For det høyteknologiske Norge er en stor del av befolkningen på internett via datamaskin og mobil, hvilket gjør at en helt vanlig person deler kontaktflate med aktører som potensielt planlegger å begå cyberangrep. Konstruktivismen retter oppmerksomhet mot at individuelle faktorer også må inkluderes i sikkerhetspolitikken og at vi må oppdatere den sikkerhetspolitiske forståelsen av menneskelig trygghet (Hough 2008). Det kan i denne sammenheng hevdes at internett er en svært intim arena der man googler spørsmål det kan være flaut å ta opp med andre, har personlige samtaler med sine nærmeste gjennom e-post og sosiale medier, og sender private bilder på for eksempel snapchat. Fra et konstruktivistisk ståsted kan det hevdes at den moderne vestlige verden kan oppfatte det som vel så ubehagelig å få sitt digitale liv truet, som andre mer fysiske former for terror. Dermed kan konstruktivismen tale for at cyberpolicyen drives av et forsøk på å modernisere av sikkerhetspolitikken, samtidig som man ønsker å sikre en arena som stadig øker i utbredelse.

Sentralt når det gjelder individuelle faktorer er retorikk, og gjennomgående i de empiriske funnene er bruken av ordene sårbarhet og risiko. Dette kan ses i sammenheng med securitiseringsteorien som hevder at visse sikkerhetspolitiske områder blir tillagt uproporsjonalt mye vekt fordi det er i noens interesse at feltet skal aksepteres som et eksistensielt truet sikkerhetsanliggende, og derfor krever umiddelbar krisehåndtering (Buzan m. fl. 1998, s. 23). De feltene som løftes opp til dette beredskapsnivået nyter færre muligheter for inngripen fra andre med beslutningsmyndighet og det er samtidig lettere å legitimere økonomiske bevilgninger. I dette ligger det et incentiv for overdrivelse av trusselen. Ifølge securitiseringsteorien kan cybersikkerhet anses som referentobjektet som krever gjennomføring av nye tiltak, og for å muliggjøre dette må befolkningen eller beslutningstakerne overbevises om at feltet er et sikkerhetsanliggende (Buzan m.fl. 1998, s.

1). Vellykket overbevisning, og dermed securitisering, kan gjøre det lettere for beslutningstakerne å bevilge de midlene de trenger.

Ifølge norske myndigheters rapporter er cyber ansett som et sikkerhetsanliggende, og beskrives sågar som et av de tre mest fremtredende truslene mot Norge (se for eksempel Fokus 2018). Samtidig oppgis det få konkrete eksempler i rapportene. Særlig problematisk blir det når det knyttes opp mot FFODs definisjon av hva som anses som et eksistensielt truende cyberangrep mot Norge: at ethvert angrep fra en stormakt vil kunne oppfattes eksistensielt truende for en småstat som Norge (Forsvarsstaben 2014, s. 18-19). Dette åpner i stor grad for subjektiv oppfatning og skjønnsutøvelse, noe som kan peke i retning av at Norges cyberpolicy er basert på en overvurdering av trusselen. Securitiseringsteoriens mest kritiske innvending i et slikt tilfelle er at dette er basert på en gruppe eliters ønske om å "løfte" problemet opp til høyeste sikkerhetsnivå; nasjonal interesse (Emmers 2016, s. 171). Det er ingen åpenbare eksempler på hva eventuelle eliter kan få ut av et slikt tilfelle, men med tanke på at personvernrettigheter står sentralt er det ikke uproblematisk.

Utenriksdepartementet og Statsministeren viser gjennom cyberstrategien at Norge ønsker å fokusere på normstyring og samarbeid på cyberfeltet (Utenriksdepartementet 2017). Dette er snarere en liberalistisk tilnærming til problemet og fremstår ikke som et politisk ønske om å løfte problemet til krisehåndtering. Sammenlignet med E-tjenestens Fokus-rapporter, som utpeker cyberfeltet som en av de fremste truslene mot Norge, kan det snarere se ut som et forsøk på å definere problemet slik at det holder egen stilling aktuell, i tråd med securitiseringsteorien. Konstruktivismens argument om at individer oppfatter situasjoner subjektivt og definerer problemer ut fra egen posisjon (Houghton 2007, s. 29-30) gjør det enklere å forstå hvorfor Forsvaret definerer cyber som et forsvarsområde, mens Utenriksdepartementet legger frem politiske løsninger. Liberalismens tilsvarende argument er at sosiale interesser driver sikkerhetspolitikken til å speile individuelle mål (Moravcsik 2008, s. 236-237) slik at drivkreftene bak norsk sikkerhetspolitikk på cyberfeltet både reflekterer Forsvarets og den politiske elitens individuelle preferanser.

Spesielt viktig for cybersikkerhet er informasjonssikring (Dunn Cavelty 2016, s. 401). Når det gjelder individuelle faktorer er det viktig å sørge for at befolkningen ikke gis falsk

informasjon som reduserer tiltroen til myndighetene (Fokus 2017, s. 36). Dette er som nevnt viktig for beslutningstakere for å beholde legitimitet. Neo-realismen viser som kjent til at strukturelle faktorer utgjør handlingsrommet statene handler i og at det er naturlig å utnytte strukturen til sin fordel (Glaser 2016, s. 16). For fiendtlig innstilte stater vil det dermed være naturlig å ønske å spre falsk informasjon til norske innbyggere, og dermed benytte seg av den anarkiske strukturen i cyberspace. Tilgang til informasjon er i større grad en individuell faktor i dag på grunn av internett, dette fordi det vil variere fra person til person hva slags informasjon som dukker opp først i Google, eller hva som dukker opp som annonser i sosiale medier. Tidligere kunne det hevdes at informasjonstilgang i større grad var en nasjonal faktor fordi informasjon ble gitt fra langt færre aktører enn i dag, for eksempel fra NRK Dagsrevyen eller VG. Strukturen i internett skaper et helt annet handlingsrom og kan gi en forklaring på hvorfor sårbarhet utgjør et desto viktigere moment i cybersikkerhet. Slik sett kan det fra et neo-realistisk perspektiv anses som viktig å gjennomføre preventive tiltak mot staters utnyttelse av potensialet i cyberspace. Dette kan også anses som et motsvar til securitiseringsteoriens kritikk av at sårbarhet er for høyt på agendaen for cybersikkerhet. Dermed kan en viktig drivkraft i prosessen, fra et neo-realistisk ståsted, være et rasjonelt ønske om å bedre cyber-sikkerhetspolitikken fordi den anarkiske strukturen i internett gjør det lett for stater å utnytte denne til blant annet spredning av desinformasjon.

5.2.2 Stats- og styringsverk

På dette analysenivået er rammebetingelser for myndighetsutøvelse sentralt. Fokus her er på faktorer som politisk styringsverk, nasjonal lovgivning, målsettinger, verdier, nasjonal identitet og kultur, moderniseringsnivå, handlingsrom og kapasitet (Fermann 2013, s. 108-110). Analysenivået gjelder dermed både samfunnsmessige, innenrikspolitiske omgivelser og det faktiske politiske rammeverket.

Det kan tas utgangspunkt i at Norges sikkerhetspolitikk på cyberfeltet er basert på statens kjerneoppgaver og målsettinger. Fra et klassisk realistisk perspektiv kan det hevdes at dette er, og må være, bakgrunnen for alle avgjørelser staten tar. Fra et realisme-perspektiv er sikkerhet best ivaretatt gjennom militærmakt fordi dette gir best mulighet for å forsvare seg (Glaser

2016), noe som gir en mulig forklaring på hvorfor Norge utreder muligheten for å forbedre det digitale grenseforsvaret. Staten er makt- og sikkerhetssøkende (Glaser 2016, s. 15), og slik sett kan Norges atferd i sikkerhetspolitikken forklares ut fra nasjonale interesser. Som kjent fra teoridelen har Regjeringen (2016) definert kjerneoppgavene i nasjonale interesser som ivaretakelsen av landets suverenitet, territorielle integritet og politiske handlefrihet. Cybersikkerhet er anerkjent som et sikkerhetspolitisk tema, men er likevel såpass nytt at det åpner for en rekke problemer i implementeringen av tilpassede lover.

Det liberalistiske perspektivet er mindre statssentrert enn realismen, og utvider aktørbildet til å inkludere grupper, myndighetspersoner, organisasjoner og institusjoner (Moravcsik 2008). Videre fokuserer liberalismen på det politiske rammeverket innad i staten som styrende for handling, i tillegg til at den reguleres av normer og regler (Morgan 2016, s. 31). Fra et liberalistisk synspunkt vil det være naturlig å implementere et lovverk som sørger for god datasikkerhet, da dette for eksempel senker risikoen for å investere i norske selskaper. På den annen side vil et slikt lovverk som nevnt potensielt gå utover den enkeltes personvern, hvilket fra et liberalistisk ståsted anses som svært problematisk på grunn av fokuset på individets frihet. Dette kan tale for forsøk på normstyring isteden. Rapporten "Internasjonal Cyberstrategi for Norge" (Utenriksdepartementet 2017) kan oppfattes som et klart eksempel på et liberalistisk politisk planverk. Rapporten identifiserer løsninger som forsøk på normstyring, og samarbeid i implementering og harmonisering av internasjonale lover for cybersikkerhet (Utenriksdepartementet 2017). Videre er cyberstrategien basert på et ønske om å legge til rette for internasjonal handel, som beskrives som en viktig verdi for Norge (Utenriksdepartementet 2017, s 8). Fra et metodisk ståsted er strategien både tilknyttet identitet og kultur, og rammebetingelser for myndighetsutøvelse. Inneværende regjering er betegnet som blå-blå, og slike partier har tradisjonelt fokus på næringsliv og handel. Cyberstrategien kan dermed oppfattes som en klar signaleffekt på at det er politisk vilje til å øke fokuset på cyberfeltet for å utnytte mulighetene i cyberspace for handel. I tillegg er det første gang i 2017 at det etableres en norsk cyberstrategi, noe som viser at cybersikkerhet anerkjennes som et satsningsområde også utenfor Forsvarets virkeområde. Drivkraften bak sikkerhetspolitikken på cyberfeltet kan dermed, fra et liberalistisk ståsted, være et ønske om å utvikle bedre cybersikkerhet for å sikre næringslivet.

Fra Forsvarets side er det ikke funnet empiriske eksempler på et ønske om å styre prosessen via normer, hvilket trolig kan være på grunn av Forsvarets behov for systemendring. Forsvaret har beskrevet et prekært behov for bedring av cybersikkerheten (Eide 2017), herunder endring fra satellittbaserte systemer for innsamling av etterretning til fibernettbaserte systemer (Lysne m.fl. 2016, s. 6). Dette poenget går tilbake til ivaretakelse av statens og Forsvarets kjerneoppgaver som er svekket på grunn av de utdaterte digitale systemene (Kveberg og Johnsen 2013). Dersom avgjørelsen om å godkjenne Lysne II-utvalgets anbefalinger skal tolkes fra et klassisk realistisk ståsted vil dette være helt i tråd med ivaretakelsen av statens viktigste oppgave: å sørge for best mulig nasjonal sikkerhet.

Når det gjelder rammebetingelser for myndighetsutøvelse bør det poengteres at Cyberstrategiens fokus på normstyring og implementering av lover trolig kan skyldes at dette er en politisk strategi utarbeidet av Utenriksdepartementet, og ikke et sikkerhetspolitisk planverk fra Forsvarsdepartementet eller Forsvaret. Dermed kan det hevdes at forskjellene i fokus skyldes naturlige ulikheter mellom offentlige instanser som har ulike virkeområder. Likevel kan det hevdes at Fokus-rapportene, Cyberstrategien og Lysne II-utvalgets rapport alle peker i samme retning og understreker behovet for økt fokus på cybersikkerhet.

Fra et neo-realistisk perspektiv er statens moderniseringsnivå relevant på grunn av teknologiske nyvinninger på cyberfeltet. Den anarkiske strukturen i verdenssamfunnet tilsier at enhver stat bør søke å utnytte ethvert område som kan bedre sin posisjon (Glaser 2016, s. 16). Empirien viser at det er et viktig poeng for Norges cyberpolicy at vi holder oss på nivå med Russland av sikkerhetsmessige grunner (Lysne m.fl. 2016). Samtidig er Norges moderniseringsnivå generelt svært høyt som et av de mest digitaliserte landene i verden, hvilket gjør det ytterligere problematisk at vi henger etter på sikkerheten. Vårt høye moderniseringsnivå gjør oss altså svært sårbare, noe som har vist seg å være en meget sentral faktor i de empiriske funnene (Lysne m.fl 2016; Fokus 2018). En mer liberalistisk løsning på sårbarheten er nevnt i NUPI-rapporten om petroleumssektoren (Muller, Gjesvik, Friis 2018, s. 27), der viktigheten av et nært samarbeid mellom norske myndigheter og private bedrifter for informasjonsutveksling ble understreket. Det mest oppsiktsvekkende ved dette forslaget er at det ikke allerede er iverksatt. Det er problematisk å føre en digital sikkerhetspolitikk som er alles ansvar fordi det åpner muligheten for at ingen tar nok ansvar. Et høyt

moderniseringsnivå i kombinasjon med høy grad av offentlig sektorinndeling peker i retning av behovet for strengere nasjonale retningslinjer. Dette kan gi en forklaring på valget om å følge Lysne II-utvalgets anbefalinger fremfor å forsøke å legge til rette for økt samhandling på tvers av sektorer.

I vårt representative demokrati handler de valgte politikerne på vegne av befolkningen. Spørsmål om potensielt svekket personvern blir dermed opp til den politiske eliten å vurdere nødvendigheten av. På den annen side er det ofte den samme politiske eliten som har tilgang til prosessen med å definere problemet. Fra et konstruktivistisk ståsted er dette en problematisk drivkraft bak cyberpolicyen, fordi det gir svært mye makt til den samlede eliten med tilgang til definisjonsprosessen. Konstruktivismen trekker gjentatte ganger frem 9/11 som eksempel på et problem der det kan stilles kritiske spørsmål til legitimeringen av et bredt mandat for krigen mot terror (Agius 2016; Fierke 2013). I dette tilfellet blir terrorangrepet på World Trade Center beskrevet som et angrep på amerikanske verdier (Agius 2016, s. 73), hvilket helt klart er en tolkning av hensikten bak angrepet, som sett fra et veldig rasjonelt ståsted var et flyangrep mot to bygninger. Med dette sagt er få som bestrider at 9/11 dreide seg om et angrep motivert av fiendtlighet mot vesten.

Også myndighetenes handlingsrom må diskuteres. Personvern er i høyeste grad et aktuelt og omdiskutert tema, og alt fra Facebook til iPhone blir beskyldt for å lagre, og potensielt dele, sensitiv informasjon om sine brukere. Det må antas at slike saker minsker det politiske handlingsrommet innenfor cybersikkerhet når det gjelder ny lovgivning som kan oppfattes som å svekke personvernet. Samtidig er et av få, kjente cyberangrep på Norges offentlige systemer på Helse Sør-Øst (Fokus 2018, s. 30), der hensikten er antatt å være informasjonsuthenting (Byberg 2018). Sett fra befolkningens side kan dette i verste fall tolkes som et pest eller kolera dilemma der man må velge hvem man ønsker skal ha tilgang til personsensitiv informasjon: egen stat eller ukjente stater. Tross at dette ikke er en reell problemstilling befolkningen skal ta stilling til, gjør det spørsmålet om ny lovgivning for overvåkning noe mer problematisk. Som nevnt opplyste Lysne II-utvalget at et forbedret digitalt grenseforsvar potensielt ville ha behov for endringer i lover knyttet til personvern, noe som vil kunne svekke den enkeltes rettigheter (Lysne m.fl. 2016, s 39). Dersom dette blir utfallet vil myndighetene potensielt ha vanskeligheter med å legitimere beslutningen. Dette

problemet kan fra et konstruktivistisk ståsted tale for politisk vilje til å male et tydeligere bilde av "oss" og "dem" ved å understreke faren for overvåkning fra motparten. Slik sett kan det gi en forklaring på hvorfor Fokus-rapportene har gått bort fra å beskrive en rekke aktører i cyber, potensielle og reelle (Fokus 2014, s. 59), til å identifisere to: Kina og Russland (Fokus 2017, s. 32).

Et videre aspekt ved politisk handlingsrom er reell kapasitet. Norge er et rikt land og kan ta en rekke friheter over statsbudsjettet, men dette kan ikke gjøres i en håndvending. For det første er forsvarsbudsjettene regulerte, og Norges innkjøp av 52 nye F-35 jagerfly har trolig tatt en stor del av potten, både nå og i fremtiden. Det er likevel ikke kjent hvor mye et nytt digitalt grenseforsvar vil koste, men i alle tilfeller vil det være mer enn status quo. Videre er Norges regjering, som del av et representativt demokrati, avhengige av støtte fra befolkningen for å gjennomføre vedtak. Utover det faktum at slik støtte ikke gis automatisk, er det en rekke hensyn sittende regjering må ta for å gå videre med er eventuelt tiltak, blant annet ønsker de fleste politikere gjenvalg og må derfor sørge for å ikke bli for upopulære.

5.2.3 Globale omgivelser

På dette analysenivået er eksterne faktorer eller ytre påvirkning tema, altså det som foregår internasjonalt og gjennom dette preger norsk politikk (Fermann 2013, s. 115). Globale omgivelser kan både gjelde det internasjonale politiske og økonomiske klima, samt hensyn til alliansepartnere. Globale forpliktelser kan både være militære allianseforpliktelser og økonomiske hensyn knyttet til Norges internasjonale handel (Fermann 2013). I begge tilfeller kan det både være tale om konkrete forpliktelser, men også samhandlingsnormer og incentiver for handling. Dette analysenivået er tredelt mellom eksterne faktorer knyttet til internasjonalt politisk klima, økonomiske interesser, og allianser.

Internasjonalt politisk klima

De senere årene har vært preget av konflikt og kaos i Midtøsten, særlig i Syria, hvilket har skapt store konsekvenser for Europa i form av flyktningestrømmer. Nord-Korea har vært synligere på den internasjonale arena og har i løpet av 2017 og tidlig 2018 blitt oppfattet som mer aggressiv i retorikk og handling (Aftenposten 21. April 2018). Våren 2018 har Nord-Korea vist tegn til et ønske om å tilnærme seg omverdenen (Aftenposten 21. April 2018), selv om det per i dag ikke er mulig å vite hvordan dette utspiller seg videre er dette et godt bilde på hvor raskt internasjonale politiske forhold kan endre seg. Storbritannia sjokkerte Europa ved å velge å gå ut av EU, det såkalte Brexit. Det er hevdet at valget i USA var gjenstand for ulike former for cyberangrep (blant annet spionasje og planting av desinformasjon) (Fokus 2017), og enkelte mener også at ulike former for digitale angrep ledet til valgseier for nåværende President Trump (Lipton m. fl. 2016, Solon 2016, Ertesvåg 2017). Den amerikanske presidenten gikk til valg på å sette Amerika først og har flere ganger uttrykt misnøye rundt lave økonomiske bidrag til NATO fra de øvrige medlemslandene (Langberg 2017). E-tjenestens rapporter beskriver i tillegg et mer aggressivt Russland som har vist økende villighet til å gå langt i digitale operasjoner (se for eksempel Fokus 2018). Dette er noen av faktorene som utgjør det internasjonale politiske klima, og de tegner et bilde preget av usikkerhet.

Det usikre internasjonale politiske klimaet kan ut fra et klassisk realisme-perspektiv alene anses som en tilstrekkelig grunn til å bedre den digitale sikkerheten. Klassisk realisme peker på at statens viktigste oppgave er å sørge for trygghet for befolkningen, samt sikre politisk og territoriell suverenitet (Glaser 2016). Samtlige rapporter i empirikapittelet viste at Norges digitale forsvarssystemer ikke engang klarer å oppfatte alle de digitale truslene grunnet at systemene er så utdaterte. Dette gir tyngde til Forsvarets argumentasjon for en bedring av cybersikkerheten.

Cyberangrep krever i seg selv ikke egnet geografisk beliggenhet og territorielle grenser (Pijnenburg Muller og Stevens 2017, s. 2), hvilket kan sies å skape ytterligere usikkerhet samtidig som en trussel på avstand trolig føles mindre akutt. Cyberangrep anses som en viktig

del av hybrid krigføring, og et cyberangrep er trolig et av de første stegene i et angrep for å skape kaos og forvirring (Meld. St. 37 (2014-2015) s. 11), deretter vil det for eksempel være enklere å sende inn regulære styrker. I et slikt scenario vil geografisk beliggenhet imidlertid være avgjørende. Fokus-rapportene beskriver et mer aggressivt og aktivt Russland når det gjelder cyberangrep (se f.eks Fokus 2017), og Russland er den eneste av kun to land som utpekes som en digital trussel mot Norge (Fokus 2018, s. 31). I tillegg er det observert en opptrapping og styrking av russisk tilstedeværelse i Nordområdene (Fokus 2018, s. 30). Dersom Russland planlegger å bruke cyberangrep som første steg i hybrid krigføring, vil våre grenser til Russland utgjøre et skremmende potensial. Dette er et typisk neo-realistisk scenario der strukturen på den anarkiske internasjonale arena skaper uante muligheter for konflikt. Ut fra dette perspektivet vil det som tidligere nevnt være rasjonelt å anerkjenne også mindre typiske former for trusler med bakgrunn i at den anarkiske strukturen tilsier bruk av ethvert verktøy der muligheten byr seg. Slik sett bør cyber være en naturlig del av sikkerhetspolitikken, i like stor grad som den er en naturlig del av potensielle angrepsmetoder. Med det sagt er det å planlegge for det hypotetisk potensielle, slik et storskala digitalt angrep er antatt å være (Dunn Cavelty 2016, s. 414), problematisk i tråd med securitiseringsteorien fordi dette potensielt gir for stort mandat når det gjelder tiltak for cybersikring. Securitiseringsteorien peker på hvordan sikkerhetspolitiske områder nyter færre motsigelser fordi problemet er på et så kritisk nivå at det krever alle mulige midler (Taureck 2006, s. 56).

Norges militære doktrine slår fast at norsk forsvar, herunder cyberforsvar, skal være troverdig avskrekkende (Prop. 151 S (2015-2016) s. 18). For at dette skal kunne gjennomføres må det ligge politiske vedtak bak, og Forsvarsministerens godkjenning av Lysne II-anbefalingen kan fra et realisme-perspektiv ses på som rasjonell politisk vilje til å styre landets forsvar i retning av bedre sikkerhet. E-tjenestens analyser om økt antall digitale angrep fra Russland vil fra dette perspektivet fremstå som naturlig og helt i tråd med staters maktsøken. Det eneste riktige motsvaret fra Norge fra et klassisk realisme-ståsted er å øke egen sikkerhet ved å bedre de digitale systemene. Avskrekkingsdoktrinen hviler på en realistisk tankegang om at gjensidig avskrekking er den beste måten å sørge for sikkerhet på fordi begge parter er gjensidig redde for utfallet av et angrep (Glaser 2016, Mearsheimer 2013, Lebow 2013). Et typisk eksempel på gjensidig avskrekking i praksis er frykten for atomangrep under den kalde krigen. Problemet når det gjelder cyberangrep er at det ikke finnes noen ekvivalent til

atomfrykten, altså ingen form for "cyber-nuke" (Petallides 2012, s. 1; Langø 2013, s. 236). På den annen side kan det hevdes at myndighetene ønsker å avskrekke i form av så god sikkerhet at et forsøk på angrep vil være fånyttes.

E-tjenestens rapporter argumenterer for Norges svekkede sikkerhet basert på at Russland de siste årene har økt ressursbruken i sin satsning på cyber (Fokus 2014, s. 60). Ut fra et neo-realistisk ståsted kan dette anses som et godt eksempel på sikkerhetsdilemmaet i praksis dersom Norge i sin tur øker sin sikkerhet basert på dette. Det kan hevdes at å øke sikkerheten på et nytt felt er naturlig, og dermed at Norge bør forsøke å forhindre et opprustingskappløp. Slik sett kan man hevde at en neo-realistisk tanke om å unngå et slikt kappløp bremser prosessen med å endre sikkerhetspolitikken på cyberfeltet i Norge. Likevel rapporteres det samtidig om at Russland i stor grad viser større vilje til å utføre digitale angrep i form av spredning av desinformasjon, spionasje og sabotasje (Fokus 2018, s. 30), noe som vanskelig kan tolkes som sikkerhetstiltak.

Sikkerhetsdilemmaet er basert på en påstand om at stater ofte tolker andre staters atferd feil (Wohlforth 2008, s. 133). Konstruktivismen hevder på sin side at den sosiale virkeligheten er subjektiv og alltid må tolkes, og at det alltid må åpnes for alternative tolkninger av dette (Wendt 1995, s. 71-72). Derfor kan det hevdes at den virkelighetsforklaringen som finnes i eksempelvis Fokus-rapportene er en tolkning av Russlands atferd som lesere av rapporten serveres som en objektiv beskrivelse av virkeligheten. Fra et konstruktivistisk ståsted vil dette åpne for kritiske spørsmål til tolkningen av hendelsene, og hvorvidt det stemmer overens med faktiske hendelser. Konvensjonell konstruktivisme retter fokus på at globale forhold formes relasjonelt og er basert på subjektive fortolkninger (Wendt 1995, s. 71-72). Dette betyr ikke nødvendigvis at norske myndigheter forsøker å villede eller overdrive, men heller at de globale relasjoner Norge er del av gjør det lettere for sikkerhetsmyndighetene å tolke Russlands atferd som truende. Et konstruktivistisk poeng i den sammenheng er viktigheten av å tolke situasjonen én gang til, slik at en ikke uten videre tyr til samme fortolkning. I tillegg bør det nevnes at tolkningene vi i Norge, eller norske myndigheter, gjør om globale omgivelser kun er "sanne" fra et norsk ståsted, og derfor kan tolkes helt ulikt fra et russisk ståsted.

Økonomiske hensyn

Som nevnt i empirikapittelet er Norge i en særstilling globalt når det gjelder økonomi. Det er liten tvil om at vår store nasjonalformue veier opp for rollen som småstat med grense til en stormakt. Samtidig er vi svært avhengige av utlandet for eksport av varer, nesten 80% av norsk produksjon eksporteres til utlandet (Meld. St. 1 (2016-2017)). Ut fra et liberalistisk perspektiv er dette interessant på flere måter. Liberalismen taler for en rasjonell politisk prosess som er drevet av økonomiske incentiver, og en global arena som binder stater sammen gjennom gjensidig avhengighet (Morgan 2016, s. 31). Dette bunner i en liberal idé om at handelssamarbeid mellom stater lønner seg økonomisk, dermed er stater samarbeidssøkende på tross av at de handler ut fra egeninteresse. Gjensidig avhengighet gjennom handel er også fredsskapende fordi det er i statens egeninteresse å bevare samarbeidet mellom statene, og dermed unngå konflikt (Morgan 2016, s. 31). Utenriksdepartementets (2017) rapport "Internasjonal Cyberstrategi for Norge" er et godt eksempel på en liberalistisk strategi for å skape gjensidig avhengighet mellom Norge og omverdenen. Strategien understreker viktigheten av samarbeid på cyberfeltet når det gjelder utvikling av lovverk for å "redusere barrierene for investering" (Utenriksdepartementet 2017, s 8). Dette kan tolkes som å redusere risikoen knyttet til dårlig sikkerhet.

Cyber er som nevnt et av få forsvarsområder hvor Norge har mulighet til å hevde seg internasjonalt, noe som kan skape et komparativt fortrinn dersom vi utvikler ny teknologi for cybersikkerhet som kan kjøpes av andre land (Kveberg og Tynes Johnsen 2013, s. 8). Dersom Norge på den annen side ikke tar digital sikkerhet på alvor vil det i verste konsekvens gjøre at risikoen for å investere i våre selskaper blir for høy grunnet at sikkerheten er for lav. Et videre trekk ved globaliseringen er at teknologien utvikles raskt, og gevinsten ved å være førstemann til mølla er stor da programvare og teknologi i stor grad er overførbar og dermed ikke krever egne nasjonale ekvivalenter. Eksempelvis vil det trolig være liten interesse og behov for en norsk utgave av Facebook. Ut fra et liberalistisk syn vil det være helt rasjonelt å forme politikken i retning av økte inntekter, slik Internasjonal Cyberstrategi for Norge 2017 (Utenriksdepartementet 2017) også taler for. Derfor kan det hevdes at den politiske dreiningen vi ser i dag, der den tidligere Forsvarsministeren godkjente Lysne II-utvalgets anbefalinger

samt opprettelsen av cyberstrategien, er basert på en rasjonell liberalistisk tankegang om økonomisk vinning. De politiske incentivene for å øke cybersikkerheten fra et liberalistisk perspektiv gjelder både for å sikre informasjon om norsk industri og teknologi, sørge for teknologiske fortrinn, og for å opprettholde nivået i de økonomiske ressursene vi allerede har.

Etter annekteringen av Krim anser Russland i større grad Norge som konkurrent i petroleumssektoren, fordi en rekke europeiske land har innført straffesanksjoner mot Russland og kjøpt mindre russisk olje (Muller, Gjesvik, Friis: 2018, s. 11-12). Dette kan tolkes som et forsøk på normstyring fra europeisk side der hensikten er å få Russland til å endre atferd. Gjensidig avhengighet gjennom handel kan skapes for å oppnå sikkerhetspolitiske mål også i dette tilfellet, dersom det blir inngått en avtale mellom Europa og Russland som opphever sanksjonene i bytte mot en cyberfredsavtale, for eksempel.

Allianser

I empirikapittelet ble det tatt forbehold om at selv om Norge er med i flere samarbeid og fellesskap av stater, er NATO den mest toneangivende for norsk politikk. Med bakgrunn i dette vil det også her utelukkende fokuseres på NATOs innvirkning på utformingen av den norske cyberpolicyen.

NATO-alliansen er frivillig for Norge å være med i, og retningslinjene er utformet i fellesskap. Som nevnt gjør vår geografiske posisjon, og det faktum at vi er en rik småstat, at det er ansett som viktig å delta i forsvarsallianser (Beadle og Diesen 2015, s. 35), altså NATO. Det er bred politisk enighet om Norges NATO-medlemskap, men det bør likevel nevnes at partier på ytre venstre fløy ikke støtter dette (Folk og Forsvar 2017). Det vil ut i fra et liberalistisk perspektiv være rasjonelt å ønske å skape meningsfellesskap og samarbeidspartnere som kan gi oss økonomiske fordeler og øke sikkerheten. NATO er en allianse av suverene stater, og slik sett har ikke Norge gitt opp noen form for politisk suverenitet ved å være en del av forsvarsalliansen. Samtidig er det utformet retningslinjer for opprettholdelsen av et troverdig forsvar i alle NATO-land (Prop. 151 S (2015-2016) s. 5), og dermed kan det argumenteres for at vi egentlig ikke står i posisjon til å kunne velge vekk å implementere nye cyberretningslinjer. Basert på dette er Norge pliktige til å forme

sikkerhetspolitikken på cyberfeltet slik at det oppfyller NATO-kravene og ikke utgjør en sikkerhetsrisiko for NATO. Dermed vil dreiningen mot økt cybersikkerhet og et nytt digitalt grenseforsvar være rasjonelt ut fra et liberalistisk ståsted fordi samarbeid er ansett som svært verdifullt. Videre er det fra et liberalistisk synspunkt viktig å sørge for en videreføring av den gjensidige avhengigheten som er opparbeidet mellom Norge (og Europa generelt) og USA gjennom NATO. Norge er en viktig aktør når det gjelder innhenting av etterretningsinformasjon knyttet til Russland, og vårt bidrag er også verdifullt for USA (Bye Skille 2018). Dette kan hjelpe til å veie opp i det tilsynelatende asymmetriske størrelsesforholdet mellom det amerikanske og norske forsvaret.

Liberalismen poengterer også at en av de sterkeste mulighetene for å kontrollere handling ligger i å skape styrende normer, og er også en sterk pådriver for verdien av organisasjoner for å implementere og opprettholde slike effektive normer (Morgan 2016, s. 31). Effektive normer er normer som styrer handling uten at det kreves tilsyn, altså noe man gjør fordi man vet at det er riktig (Wendt 1995). Fra et slikt liberalistisk perspektiv vil stater på et vis indoktrineres i et felles tankesett der samarbeidet og fellesskapet i organisasjonen står høyt på prioriteringslisten. Verdien av samarbeid, og anerkjennelsen av organisasjoner og fellesskap som relevante aktører for Norges sikkerhetspolitikk, kan ut fra et liberalistisk tankesett fremstå som den største og mest naturlige drivkraft for utformingen av cyberpolicyen.

Realismen er generelt pessimistiske til verdien av samarbeid og mener at staten til syvende og sist ikke kan regne med andre enn seg selv (Lebow 2013, 62). Slik sett utgjør ikke NATO-samarbeidet en god nok forklaring på å øke cybersikkerheten i Norge. På tross av dette kan det hevdes at også fra et klassisk realisme-perspektiv er tilknytningen til NATO rasjonell fordi ønsket om å holde oss på NATOs "godside" er nødvendig av hensyn til gruppetilhørighet. Hensynet til gruppetilhørighet er for realistene et slags motsvar på identitetsfellesskap og samarbeid mot et felles mål, slik NATO kan tolkes som av liberalister. Et realistisk perspektiv kan tale for et fortsatt samarbeid med NATO på grunn av Norges forsvarsevne, som i møte med eksempelvis Russland, bør styrkes ved hjelp av alliansepartnere. Dermed kan det hevdes at også en realistisk rasjonell tankegang vil drive cyberpolicyen i retning av implementering av NATO-standarder for cybersikkerhet. På den annen side peker neo-realismen på faren ved å drastisk øke sikkerheten på et område, særlig

for sikkerhetssøkende status quo-stater som Norge. Dette kan tolkes feil av andre stater og lede til et opprustingskappløp, slik sikkerhetsdilemmaet hevder.

Med dette sagt er det nødvendig å poengtere at NATO-kravene i seg selv kan sies å legge sterke føringer for norsk sikkerhetspolitikk på cyberfeltet, hvilket må kunne antas å påvirke det reelle politiske handlingsrommet i stor grad. Norge har per i dag mulighet til å "kjøpe seg" velvilje fra NATO som følge av de store økonomiske ressursene vi har, noe som i sin tur peker mot det liberalistiske argumentet om å sikre økonomien ved å bedre cybersikkerheten. Hvorvidt en innføring av felles NATO-regler på cyberfeltet kan påvirke norsk suverenitet vil ikke bli diskutert nærmere her.

Den empiriske dataen viste også at noe av det viktigste for NATO-alliansen er strategisk kommunikasjon i form av samsvar i informasjonen som spres (Forsvarsstaben 2014). Slik strategisk kommunikasjon kan fra et konstruktivistisk perspektiv anses som nødvendig for å skape et felles verdensbilde, som også vil gjøre det lettere å skille mellom "oss" og "dem". I flere rapporter kritiseres Russland for å spre såkalt desinformasjon der de gir et forvridd bilde av virkeligheten som en del av sine cyberangrep (Fokus 2017, s. 36). Dersom Norges cyberpolicy primært er formet av NATO-krav, åpner konstruktivismen for å stille spørsmål om hvorvidt verdensbildet som portretteres i realiteten er så fiendtlig. Fra et kritisk konstruktivistisk perspektiv kan det med dette hevdes at det som former og driver sikkerhetspolitikken på cyberfeltet er prosessen med å repetere et verdensbilde med steile fronter, som igjen gjør det lett å oppfatte motparten som truende og derav overvurdere risikoen.

NATO-samarbeidet hviler særlig på to sentrale artikler som regulerer atferd dersom krise eller konflikt oppstår. For at en stat skal kunne påberope seg artikkel fem, som stadfester at et angrep på én i alliansen er et angrep på alle, kan artikkel fire avgjøre hvorvidt angrepet skal omfattes av artikkel fem (Tynes Johnsen 2014, s. 12). Artikkel fire innebærer en subjektiv vurdering av statens følelse av trusselen den står overfor. I norsk militærdoktrine slås det fast at fordi Norge er en småstat med begrenset kapasitet, vil trolig ethvert forsøk på angrep fra en stormakt kunne føles eksistensielt truende og dermed kunne utløse artikkel fem (Forsvarsstaben 2014, s. 18-19). Samtlige rapporter som identifiserer sentrale aktører utnevner

stormakten Russland som den største trusselen mot norsk digital sikkerhet, med hyppige forsøk på ulike former for cyberangrep mot Norge. På grunn av Norges strategiske, geografiske beliggenhet har vi et nært forhold til USA og NATO, og har lenge bidratt med verdifull etterretning (Bye Skille 2018). Det er trolig i særlig grad i NATOs interesse at etterretningsinnsamlingens digitale systemer ivaretas og at sikkerheten forbedres, både slik at informasjonsinnhentingen kan fortsette og slik at informasjonen etterretningstjenesten lagrer er trygg. Med dette som utgangspunkt er det ikke utenkelig at cybertrusselen kan anses som så høy at det krever umiddelbare tiltak for sikring av systemene. Artikkel fire og fem omhandler angrep som krever motangrep (Tynes Johnsen 2014, s. 12), og ikke hvilket trusselnivå som kreves for å gjennomføre forsvarstiltak. Derimot kan dette være et argument for å overbevise om hvor alvorlig cyberangrep er og slik sett legitimere innføringen av nye systemer som potensielt lovfester retten til overvåkning eller lagring av innenriks kommunikasjon. Det kan hevdes at dette er nettopp den typen uproporsjonal eskalering av et problem som securitiseringsteorien advarer mot.

6. Avslutning

6.1 Sentrale funn

På verdensbasis er cyberangrep et sentralt tema i sikkerhetspolitikken, og stadig flere stater ønsker å forbedre sin digitale sikkerhet for å unngå hacking, spionasje og planting av desinformasjon. Norge har vist politisk vilje til å forbedre cybersikkerheten, og utreder i tillegg muligheten for opprettelsen av et digitalt grenseforsvar. Etterretningstjenesten (E-tjenesten) oppgir at cybertruslene mot Norge er mange, men at den største trusselen mot norsk cybersikkerhet er at vi ikke vet hvor stor trusselen er. Dette fordi flere av cyberangrepene er mer avanserte enn våre digitale systemer evner å fange opp.

Denne studien har hatt til hensikt å analysere cyber-trusselsituasjonen i Norge og å undersøke hvilke faktorer som former cyber-sikkerhetspolitikken. Utgangspunktet for studien har vært problemstillingen: hva består den digitale trusselsituasjonen i Norge av; og hva driver utformingen av den norske sikkerhetspolitikken på cyberfeltet? For å analysere temaene i problemstillingen fra flere ulike innfallsvinkler ble det benyttet tre teoretiske perspektiver: realisme, liberalisme og konstruktivisme.

I oppgavens teorikapittel ble det redegjort for sikkerhetspolitikk, samt de tre teoretiske perspektivene. Det ble videre forklart at realisme og liberalisme som teoretiske tanketradisjoner er basert på at aktøren handler rasjonelt. Klassisk realisme anser stater som de eneste relevante aktørene, og at disse handler rasjonelt ut fra et ønske om å maksimere sikkerhet og makt. Neo-realismen mener at det er den anarkiske strukturen på den internasjonale arena som skaper konflikt. Fordi det ikke finnes noe overnasjonalt styrende organ vil rasjonelle stater søke enhver mulighet til å øke sin evne til å hevde seg globalt. Den liberalistiske tradisjonen mener også at aktører handler rasjonelt, men at rasjonalitet leder stater til samarbeid med hverandre. Dette fordi samarbeid skaper vinn-vinn løsninger der stater tjener på for eksempel handelssamarbeid. Dermed er det ikke rasjonelt å gå til krig mot

hverandre fordi gevinsten ved samarbeid er betydelig. Den liberalistiske tanketradisjonen mener at gjensidig avhengighet er løsningen globalt, snarere enn realistenes gjensidige avskrekking. De reflekterende perspektivene mener ikke at aktørers atferd skyldes rasjonalitet. Klassisk konstruktivistisk tradisjon mener at oppfatninger om verden skapes relasjonelt og skyldes faktorer som kultur og identitet. Det finnes dermed ikke én objektivt beste løsning i valget mellom to, men aktørens identitet former tolkningen av valget den skal ta. Securitiseringsteorien hevder at det kan finnes politisk vilje til å overdrive trusselen av et fenomen slik at fenomenet løftes opp til sikkerhetspolitisk nivå, og dermed får et bredere mandat med færre muligheter for inngripen.

I oppgavens diskusjonsdel ble de empiriske funnene diskutert i lys av de teoretiske perspektivene for å besvare problemstillingen. De teoretiske perspektivene utgjorde utgangspunktet for at problemstillingens første spørsmål ble todelt mellom en drøfting av de faktiske eksemplene på cyberangrep og en beskrivelse av trusselbildet. Problemstillingens andre spørsmål ble diskutert på tre analysenivå: individ, statlig og globalt, i henhold til policyanalyse-modellen.

Rapporter fra E-tjenesten viste at Norge er mål for en rekke cyberangrep fra Russland. Disse angrepene er typisk forsøk på spredning av informasjon og hacking av systemer for å kartlegge svakheter i programvare, som potensielt kan brukes ved en senere anledning. Den andre, nevnte aktøren Norge mottar cyberangrep fra er Kina, som særlig driver med spionasje mot industri og teknologi. Potensialet i cyberangrep mot Norge anses som høy på grunn av hvor digitalisert Norge er, samt hensynet til blant annet petroleumsindustrien. I tillegg trekker E-tjenesten frem potensialet for hybrid krigføring, der cyber kan benyttes som et første steg for å skape kaos og forvirring. Norge er i denne sammenheng i en utsatt posisjon blant annet på grunn av grensen til Russland. Cyber-trusselbildet presenteres som et høyrisiko-felt grunnet sårbarheten i det digitaliserte Norge, i tillegg er de digitale systemene utdaterte i så stor grad at vi ikke vet hvor stor trusselen er. Cyber-trusselbildet er dermed først og fremst preget av usikkerhet, i tillegg til en predikert antakelse om at Norge er utsatt. Sett fra et klassisk realistisk perspektiv tilsier usikkerhet rundt statens og befolkningens sikkerhet at det er rasjonelt å iverksette tiltak for å bedre sikkerheten fordi usikkerhet er farlig. På den annen side viste diskusjonsdelen også hvordan usikkerhet som sikkerhetspolitisk fenomen kan

forstås på en annen måte. Konstruktivistisk tradisjon kan forklare hvordan Norges oppfatninger av trusselbildet er formet av våre relasjoner i verden. Norge er en vestlig småstat med tette bånd til Vest-Europa og USA, og denne tilhørigheten kan potensielt forme vårt verdensbilde til å tolke russisk atferd som mer truende enn den i realiteten er. Securitiseringsteorien forklarer dette som at det er i beslutningstakernes interesse at cyber skal anses som et sikkerhetspolitisk problem slik at problemet får et vidt mandat og enkelt får de midlene som ønskes.

Denne studien har vist hvordan Norges sikkerhetspolitiske policy på cyberfeltet er formet av en rekke faktorer som påvirker utformingen av politikken, samt oppfatningen av trusselen. Et overordnet tema knyttet til andre del av problemstillingen er hva som påvirker utformingen av norsk sikkerhetspolitikk.

På individnivå er et særlig viktig aspekt ved norsk cybersikkerhet å sørge for at befolkningen ikke gis desinformasjon. Dette er målrettet informasjon som er laget for å villede mottakeren og skape splid og mistro til de politiske systemene innad i Norge. Informasjonen er basert på analyser som gjøres av for eksempel individuelle nettpreferanser. Trusselbildet ifølge E-tjenesten viste at denne formen for cyberangrep er av de mest vanlige i Norge, og tendensen til slik informasjonsspredning har vært økende de senere år. Fra et neo-realistisk ståsted ble det argumentert for at cyberdomenet kan anses som den perfekte arena for stater som vil endre maktbalansen i sin favør med så enkle midler som mulig. I tråd med dette ble det argumentert for at norsk cyber-sikkerhetspolitikk drives av ønsket om å hindre andre stater fra å utnytte cyberdomenet til spredning av desinformasjon i Norge, samt for å øke egen makt.

På det andre analysenivået, stats- og styringsverk, ble det særlig trukket frem hensyn til moderniseringsnivå som drivende faktor for utformingen av norsk cyberpolicy. De empiriske dataene viste at Forsvaret, særlig E-tjenesten, har behov for systemendring for å kunne gi en fullgod trusselvurdering på cyberfeltet. Ut fra klassisk realisme kan dette tolkes som en rasjonell vurdering i tråd med ivaretakelse av statens kjerneoppgaver, som blant annet innebærer å sørge for statens suverenitet og nasjonens sikkerhet. Arbeidet i Lysne II-utredningen, og Forsvarsministerens godkjenning av deres anbefalinger, anses som en sterk

signaleffekt og kan tolkes som et argument for en realistisk forklaring bak Norges cyberpolicy.

På tredje analysenivå, globale omgivelser, kan særlig hensynet til økonomiske interesser trekkes frem. Norge som handelspartner er tjent med å kunne tilby lav politisk risiko ved invest i våre selskaper, hvilket kan underbygges av god digital sikkerhet. Et liberalistisk utgangspunkt kan dermed argumentere for at norsk cyberpolicy er formet særlig med hensyn til økonomiske interesser. Videre er NATO-samarbeidet også svært viktig for Norge, og fra et liberalistisk synspunkt er det helt rasjonelt at det er i Norges interesse å fortsette dette samarbeidet. NATO har utarbeidet retningslinjer for cybersikkerhet, og det kan tolkes som at norsk sikkerhetspolitikk dreier i retning av implementering av disse retningslinjene.

6.2 Avsluttende bemerkninger

Denne studien er gjort som en policyanalyse med utgangspunkt i tre teoretiske tanketradisjoner. I arbeidet med analysen av sikkerhetspolitikken på cyberfeltet ble det tydelig at også andre teorier kunne bidratt med forklaringsfaktorer. Oppgaven er dermed ikke ment som en konklusjon på hva som former norsk cyberpolicy, ei heller å gi et fullstendig bilde av trusselsituasjonen. Snarere er det en analyse av hvilke forklaringsfaktorer som kan identifiseres i utformingen av politikken på cyberfeltet. De tre teoretiske tanketradisjonene bidrar imidlertid med en rekke verdifulle innsikter til hva som kan forklare sikkerhetspolitikken på cyberfeltet. Videre kan det tenkes at drivkreftene bak utformingen av cyberpolicyen fremstår tydeligere dersom Lysne II-utvalgets anbefalinger implementeres og det dannes et nytt digitalt grenseforsvar. Situasjonen på cyberfeltet i Norge er per i dag preget av usikkerhet på en rekke områder, blant annet når det gjelder den potensielle utviklingen i policyen og lovverket, hvilket gjør analysen av situasjonen noe mer utfordrende. Videre ligger det en klar begrensning i tilgangen på informasjon på feltet. Detaljert informasjon om cybertrusler er trolig i stor grad hemmeligholdt av hensyn til E-tjenesten, og myndighetene for øvrig, sitt videre arbeid. Det kan anses problematisk å analysere eksempler på reelle bevis opp

mot beskrivelser av trusselbildet når det må antas at mye av denne informasjonen holdes hemmelig.

Når det gjelder videre forskning er det en rekke spennende innfallsvinkler til cybersikkerhet, utover bruk av andre teoretiske perspektiver. Først og fremst vil det være interessant å analysere den konkrete beslutningsprosessen dersom de vedtatte anbefalingene fra Lysne II-utvalget blir implementert. Gjennom studien har det dukket opp flere interessante aspekter knyttet til cyberfeltet, men som likevel har vært utenfor oppgavens rekkevidde. Eksempelvis etiske retningslinjer og personvern i cyberdomenet, eller nasjonalstatens rolle i en stadig mer globalisert, markedsbasert og digital verden.

Referanseliste

Aftenposten (2018) Nord-Korea varslet at de vil stanse atomprøvesprengninger. *Aftenposten* [Internett] 21. April 2018. Tilgjengelig fra: https://www.aftenposten.no/verden/i/XwBLro/Nord-Korea-varsler-at-de-vil-stanse-atomprovesprengninger Hentet 1. Mai 2018 klokken 11:38

Agius, Christine (2016) Social Constructivism. I: Collins, Alan (2016) *Contemporary Security Studies*. 4. utg. Oxford: Oxford University Press. S. 70-87

Balzacq, Thierry (2010) Constructivism and Securitization Studies. I: Dunn Cavelty, Myriam og Mauer, Victor (2010) *The Routledge Handbook of Security Studies*. London/New York: Routledge. S. 56-73

Beadle, Alexander William og Diesen, Sverre (2015) *Globale trender mot 2040 - implikasjoner for Forsvarets rolle og relevans*. FFI-rapport 2015/01452. Kjeller: Forsvarets Forskningsinstitutt

Braathen, Frøydis (2017) - Moderne kriger handler ikke bare om bomber og maskingevær. *Aftenposten* [Internett] 6. Oktober 2017. Tilgjengelig fra: https://www.aftenposten.no/norge/i/9Rwgw/-Moderne-kriger-handler-ikke-bare-om-bomber-og-maskingevar Hentet 17. Februar 2018, klokken 14:30

Brinkmann, Svend og Tandggaard, Lene (red.) (2012) *Kvalitative metoder*. Oslo: Gyldendal Akademisk

Bruun Hanse, Haakon (2014) Forsvarssjefens forord. *Forsvarets Fellesoperative Doktrine*. Oslo: Forsvarsstaben

Buzan, Barry; Wæver, Ole; de Wilde, Jaap (1998) *Security: a new Framework for Analysis*. Boulder: Lynne Rienner Publishers

Byberg, Øystein (2018) Spioner stod bak cyberangrepet mot Helse Sør-Øst? Hegnar [Internett] 16. Januar 2018. Tilgjengelig fra: http://www.hegnar.no/Nyheter/Politikk/2018/01/Spioner-stod-bak-cyberangrepet-mot-Helse-Soer-OEst Hentet 09. Mars 2018

Bye Skille, Øyvind (2018) Antennene som samler inn data om norske borgere. *NRK* [Internett] 1. Mars 2018. Tilgjengelig fra:

https://www.nrk.no/dokumentar/xl/antennene-som-samler-inn-data-om-norske-borgere-1.13881286 Hentet 1. Mars 2018.

Collins, Alan (2016) *Contemporary Security Studies*. 4. utg. Oxford: Oxford University Press

Datatilsynet (2017) Skytjenester - en veiledning. *Datatilsynet* [Internett] 26. August 2014. Tilgjengelig fra: https://www.datatilsynet.no/regelverk-og-skjema/veiledere/skytjenester---cloud-computing/?id=2156 Hentet 15. desember 2017 ca klokken 08:00

Duedahl, Poul og Jacobsen, Michael Hviid (2009) *Introduktion til dokumentanalyse*. Odense: Syddansk Universitetsforlag

Dunn Cavelty, Myriam (2010) Cyber-threats. I: Dunn Cavelty, Myriam og Mauer, Victor (2010) *The Routledge Handbook of Security Studies*. London/New York: Routledge. S. 180-190

Dunn Cavelty, Myriam (2014) Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*. (September 2014) Vol 20 (3), s. 701-715

Dunn Cavelty, Myriam (2016) Cyber-Security. I: Collins, Alan (2016) *Contemporary Security Studies*. 4. utg. Oxford: Oxford University Press. S. 400-417

Dunne, Tim og Brian C. Schmidt (2011). Realism. I Steve Smith, John Baylis og Patricia Owens (red.) *The Globalization of World Politics: An Introduction to International Relations*. (5. utgave.) Oxford: Oxford University Press.

Eide, Ole Kåre (2017) - Vi holder ikke lenge. *Forsvarets Forum* [Internett] Tilgjengelig fra: https://forsvaretsforum.no/vår-evne-til-å-stå-i-mot-et-cyberangrep-er-marginal Hentet 20. Januar 2018

Emmers, Ralf (2016) Securitization. I: Collins, Alan (2016) *Contemporary Security Studies*. 4. utg. Oxford: Oxford University Press. S. 168-183

Ertesvåg, Oda (2017) Rapport: - Putin beordret hacking for å hjelpe Trump. *Dagbladet* [Internett] 6. Januar 2017. Tilgjengelig fra: https://www.dagbladet.no/nyheter/rapport---putin-beordret-hacking-for-a-hjelpe-trump/66599457
Hentet 8 desember 2017, klokken 12:18

Etterretningstjenesten (2011) *Fokus 2011*. Oslo: Etterretningstjenesten

Etterretningstjenesten (2014) *Fokus 2014*. Oslo: Etterretningstjenesten

Etterretningstjenesten (2015) *Fokus 2015*. Oslo: Etterretningstjenesten

Etterretningstjenesten (2016) *Fokus 2016*. Oslo: Etterretningstjenesten

Etterretningstjenesten (2017) *Fokus 2017*. Oslo: Etterretningstjenesten

Etterretningstjenesten (2018) *Fokus 2018*. Oslo: Etterretningstjenesten
Alle Fokus-rapporter tilgjengelig fra:
https://forsvaret.no/fakta/undersokelser-og-rapporter/fokus

Fermann, Gunnar. (2013) *Utenrikspolitikk og norsk krisehåndtering.* Oslo: Cappelen Damm Akademisk.

FFI Fakta (2013) *Cybermakt: nye utfordringer i et nytt domene*. Tilgjengelig fra: https://www.ffi.no/no/Publikasjoner/Documents/2013_FFIFakta_Cybermakt.pdf Hentet 20. November 2017

Fierke, K. M. (2013) Constructivism. I: Dunne, Tim; Kurki, Milja og Smith, Steve (2013) *International Relations Theories: Dicipline and Diversity*. 3. utg. Oxford: Oxford University Press

Folk og forsvar (2017) Stortingsvalg 2017: Hva mener partiene om forsvarspolitikken? *Folk og forsvar* [Internett] tilgjengelig fra: http://www.folkogforsvar.no/aktuelt/andre-aktuelle-saker/stortingsvalg-2017-hva-mener-partiene-om-forsvarspolitikken Hentet 4. Mai 2018, klokken 13:14

Forsvarsstaben (2014) *Forsvarets fellesoperative doktrine*. Oslo: Forsvarsstaben

Glaser, Charles L. (2016) Realism. I: Collins, Alan (2016) *Contemporary Security Studies*. 4. utg. Oxford: Oxford University Press. S. 13-30

Haugan, Bjørn (2017) Slik skal Karl Johan sikres mot terror. VG [Internett]. 6. November 2017. Tilgjengelig fra: https://www.vg.no/nyheter/innenriks/krigen-mot-terror/slik-skal-karl-johan-sikres-mot-terror/a/24179966/ Hentet 8 desember 2017, klokken 11:35

Hill, Christopher (2003) *The Changing Politics of Foreign Policy*. Basingstoke: Palgrave Macmillan

Holst, Johan Jørgen (1967) *Norsk sikkerhetspolitikk i strategisk perspektiv*. Oslo: Norsk Utenrikspolitisk Institutt

Hook, Steven W. og Spanier, John W. (2010) *American Foreign Policy Since World War II*. 18. Utg. California: Sage Publications

Hotvedt, Signe Karin (2017) Cyberangrep mot Norge øker sterkt. *NRK* [Internett] 17. Januar 2017. Tilgjengelig fra: https://www.nrk.no/norge/cyberangrep-mot-norge-oker-sterkt-1.13326267 Hentet 19. April 2018, klokken 13:34

Hough, Peter (2008) Understanding Global Security. 2. Utg. London/New York: Routledge

Houghton, David Patrick (2007) Reinvigorating the Study of Foreign Policy Decision Making: Toward a Constructivist Approach. *Foreign Policy Analysis* (3) 2007, s. 24-45

Huntington, Samuel P. (1960) Strategic Planning and the Political Process. *Foreign Affairs* (38) 1960, s 285-299

Innset, Bjørn (2002) Foredrag: Forsvarets doktriner. *Oslo Militære Samfund* [Internett] 25. Februar 2002. Tilgjengelig fra: https://www.oslomilsamfund.no/forsvaret-forsvarets-doktriner/ Hentet 3. Februar 2018

Internet Live Stats (2017) Cybersecurity. *Internet Live Stats* [Internett] Tilgjengelig fra: http://www.internetlivestats.com/cybersecurity/ Hentet 21. November 2017, klokken 11:35

Johnsen, Roger (2013) Cyberkrigføring og Forsvarets operative evne. *Internasjonal politikk*. (71) Nr 2. 2013. S. 241-251

Knutsen, Torbjørn Lindstrøm (2013) Diskusjonene om norsk utenriks- og sikkerhetspolitikk. I: Fermann, Gunnar. (2013) *Utenrikspolitikk og norsk krisehåndtering.* Oslo: Cappelen Damm Akademisk. S. 141-175

Lovdata, Grunnloven, *Kongeriket Norges Grunnlov Lov 17. mai. 1814*, §113 20. Juni 2014, nr. 778. Hentet fra https://lovdata.no/dokument/NL/lov/1814-05-17/KAPITTEL_5#§113

Kurki, Milja og Wight, Collin (2013) International Relations and Social Science. I: Dunne, Tim; Kurki, Milja og Smith, Steve (2013) *International Relations Theories: Dicipline and Diversity*. 3. utg. Oxford: Oxford University Press

Kristoffersen, Martin Jacob (2018) Cyberangrep: - Du er naiv hvis du tror du ikke har noe å skjule. ABC-Nyheter [Internett] 20. Januar 2018. Tilgjengelig fra: https://www.abcnyheter.no/nyheter/norge/2018/01/20/195363921/cyberangrep-du-er-naiv-hvis-du-tror-du-ikke-har-noe-skjule Hentet 24. April 2018, klokken 08:13

Kveberg, Torbjørn og Tynes Johnsen, Siw (2013) *Cyberdomenet, cybermakt og norske interesser*. FFi-rapport 2013/02712. Kjeller: Forsvarets Forskningsinstitutt

Langberg, Øystein Kløvstad (2017) Alle landene har signert NATOs pengemål. I realiteten mener mange det er helt urealistisk. *Aftenposten* [Internett] 26. Mai 2017. Tilgjengelig fra: https://www.aftenposten.no/verden/i/3A0Bv/Alle-landene-har-signert-pa-NATOs-pengemal-I-realiteten-mener-mange-det-er-helt-urealistisk Hentet 4. Mai 2018 klokken 11:44

Langø, Hans-Inge (2011) Nye sikkerhetstrusler: cyberangrep. *Hvor hender det?* (11) 2011

Langø, Hans-Inge (2013) Den akademiske debatten om cybersikkerhet. *Internasjonal Politikk*. (71) nr 2. 2013

Langø, Hans-Inge og Sandvik Kristin (2013) Cyberspace og sikkerhet. *Internasjonal Politikk*. (71) nr 2. 2013

Lebow, Richard Ned (2013) Classical Realism. I: Dunne, Tim; Kurki, Milja og Smith, Steve (2013) *International Relations Theories: Dicipline and Diversity*. 3. utg. Oxford: Oxford University Press

Lewis, James A. (2002) *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington DC: Center for Strategic & International Studies

Lipton, Eric; Sanger, David E.; Shane, Scott (2016) The Perfect Weapon: How Russian Cyberpower Invaded the U.S. *The New York Times* [Internett], 13. Desember 2016. Tigjengelig fra: https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking Hentet 8 desember 2017, klokken 12:22

Lunde, Leiv og Thune, Henrik m.fl. (2008): *Norske interesser; utenrikspolitikk for en globalisert verden*. Oslo: Cappelen Damm.

Lysne, Olav (leder) (2016) *Digitalt Grenseforsvar DGF*. Forsvarsdepartementet. Oslo: 2016

Mabee, Bryan (2013) *Understanding American Power: The Changing World of US Foreign Policy*. Basingstoke: Palgrave Macmillan

March, David og Stoker, Gerry (2010) *Theory and Methods in Political Science.* 3. utg. Basingstoke: Palgrave Macmillan

Meld. St. 1 (2016-2017) *Nasjonalbudsjettet 2017*.

Meld. St. 37 (2014-2015) *Globale sikkerhetsutfordringer i utenrikspolitikken*.

Mearsheimer, John J. (2013) Structural Realism. I: Dunne, Tim; Kurki, Milja og Smith, Steve (2013) *International Relations Theories: Dicipline and Diversity*. 3. utg. Oxford: Oxford University Press

Moravcsik, Andrew (2008) The New Liberalism. I: Reus-Smit, Christian og Snidal, Duncan (2008) *Oxford Handbook of International Relations*. Oxford: Oxford University Press. S. 234-254

Morgan, Patrick (2016) Liberalism. I: Collins, Alan (2016) *Contemporary Security Studies*. 4. utg. Oxford: Oxford University Press. S. 30-44

Moses, Jonathon og Knutsen Torbjørn (2012) *Ways of knowing*. 2. Utg. Basingstoke: Palgrave Macmillan

NATO (2017) Topic: Collective defence - Article 5. *NATO* [Internett] Tilgjengelig fra: https://www.nato.int/cps/ua/natohq/topics_110496.htm Hentet 17. Februar 2018

NOU 2015: 13. *Digital sårbarhet - sikkert samfunn*.

Nasjonal Sikkerhetsmyndighet (2017) *Helhetlig IKT-risikobilde 2017*. Oslo: NSM

Oxford Dictionaries (2017) Where is the origin of 'cyber'? *OxfordWords Blog* [Internett] Tilgjengelig fra: https://blog.oxforddictionaries.com/2015/03/05/cyborgs-cyberspace-csi-cyber/ Hentet 15. Desember 2017 ca klokken 14:00

Petallides, Constantine J. (2012) Cyber Terrorism and IR Theory: Realism, Liberalism and Constructivism in the New Security Threat. *Inquiries Journal*. 2012 No. 4, vol. 3, s. 1

Pijnenburg Muller, Lilly; Gjesvik, Lars og Friis, Karsten (2018) *Cyber-weapons in International Politics: Possible sabotage against the norwegian petroleum sector*. Oslo: NUPI (Norsk Utenrikspolitisk Institutt)

Pijnenburg Muller, Lilly og Stevens, Tim (2017) *Upholding the NATO cyber pledge*. Oslo: NUPI

Politiets Sikkerhetstjeneste (2018) *Trusselvurdering 2018*. Oslo: PST

Regjeringen (2017) Sikkerhetspolitikk. *Regjeringen.no* [Internett] Tilgjengelig fra: https://www.regjeringen.no/no/tema/utenrikssaker/sikkerhetspolitikk/id1111/# Hentet 15. Desember 2017 klokken 09:04

Ringdal, Kristen (2011) *Enhet og mangfold: samfunnsvitenskapelig forskning og kvantitativ metode*. Bergen: Fagbokforlaget

Russett, Bruce (2013) Liberalism. I: Dunne, Tim; Kurki, Milja og Smith, Steve (2013) *International Relations Theories: Dicipline and Diversity*. 3. utg. Oxford: Oxford University Press. S. 94-114

Savigny, Heather og Marsden, Lee (2011) *Doing Political Science and International Relations*. Basingstoke: Palgrave Macmillan

Skjeggestad, Sunniva Rebekka m. fl (2017) Norge utsatt for et omfattende hackerangrep. *NRK* [Internett] 3. Februar 2017. Tilgjengelig fra: https://www.nrk.no/norge/norge-utsatt-for-et-omfattende-hackerangrep-1.13358988 Hentet 09. Mars 2018, kl 09:35

Solon, Olivia (2016) Facebook's failure: did fake news and polarized politics get Trump elected? *The Guardian* [Internett], 10. November 2016. Tilgjengelig fra: https://www.theguardian.com/technology/2016/nov/10/facebook-fake-news-election-conspiracy-theories Hentet 8 desember 2017, klokken 12:20

Sterling-Folker, Jennifer (2013) Neo-liberalism. I: Dunne, Tim; Kurki, Milja og Smith, Steve (2013) *International Relations Theories: Dicipline and Diversity*. 3. utg. Oxford: Oxford University Press. S. 114-132

Stranden, Roy og Rosvold, Knut A. (2015) Sikkerhet. *Store Norske Leksikon* [Internett] 30. Juni 2015. Tilgjengelig fra: https://snl.no/sikkerhet Hentet 17. Desember 2017, klokken 09:20

Taureck, Rita (2006) Securitization theory and securitization studies. *Journal of International Relations and Development*. (9) 2006. S. 53-61

Tjora, Aksel (2012) *Kvalitative forskningsmetoder i praksis*. 2. Utg. Oslo: Gyldendal Akademisk

Tynes Johnsen, Siw (2014) Norway, *NATO and cyber defense*. FFI-rapport 2014/01328. Kjeller: Forsvarets Forskningsinstitutt

Utenriksdepartementet (2017) *Internasjonal cyberstrategi for Norge*. Oslo: Utenriksdepartementet

Vartdal Riise (2017) Norge er verdens mest digitaliserte land. *Dagens Næringsliv* [Internett] 15. Juni 2017. Tilgjengelig fra https://www.dn.no/nyheter/2017/06/15/1329/Teknologi/norge-er-verdens-mest-digitale-land Hentet 08. Februar 2018

Veum, Eirik (2017) Etterretningssjefen: Landet ligger åpent for cyberangrep. *NRK* [Internett] 4. Februar 2017. Tilgjengelig fra https://www.nrk.no/norge/etterretningssjefen_-landet-ligger-apent-for-cyberangrep-1.13360031 Hentet 3. Mars 2018.

Wendt, Alexander (1995) Constructing International Politics. *International Security*, Volume 20 (1), sommer 1995, s. 71-81

Winterfeld, Steve og Andress, Jason (2013) *The Basics of Cyber Warfare*. 1. Utg. Waltham: Syngress

Wolforth, William C. (2008) Realism. I: Reus-Smit, Christian og Snidal, Duncan (2008) *Oxford Handbook of International Relations*. Oxford: Oxford University Press. S. 131-150

Wæver, Ole og Buzan, Barry (2016) After the Return to Theory: The Past, Present, and Future of Security Stidies. I: Collins, Alan (2016) *Contemporary Security Studies*. 4. utg. Oxford: Oxford University Press. S. 417-436

Østerud, Øyvind (2014) *Statsvitenskap: Innføring i Politisk Analyse*. 5.utg. Oslo: Universitetsforlaget