FORSVARET

Forsvarets høgskole

Skjevt ut fra hoppkanten?

Myndighetenes organisering av sikkerhet i cyberdomenet

Ole Jørgen Arvesen

Masteroppgave

Forsvarets høgskole

høst 2020

Forord

Å skrive master ved siden av full jobb har vært krevende. Denne oppgaven har tatt all min fritid i over 1 år. Jeg vil ikke med det første involvere meg i et lignende prosjekt, men på en annen side er erfaringen noe jeg ikke ville vært foruten. Prosessen har vært lærerik og utfordrende.

Prosessen er muligens det jeg har lært mest av. Her har min meget kunnskapsrike veileder, Anders Romarheim spilt en sentral rolle. Han har løpende utfordret meg og bidratt til refleksjon.

Tusen takk til Rune Utne Reitan for sparring og hjelp.

Min yrkeserfaring fra både Forsvaret og politiet er først og fremst årsaken til interessen av grensesnittet mellom militær- og sivil sektor. Jeg har vært heldig å få oppleve begge etatene fra innsiden i over 30 år. Forbindelsen til Forsvaret har jeg beholdt gjennom deployeringer og øvelser. Erfaringene har utviklet meg som person og gitt mange opplevelser og utfordringer. "Grundighet gir trygghet" er parolen på Rena, noe jeg kan bekrefte er tilfelle.

Digitalisering og globalisering endrer begge institusjonene. Viktigheten av kunnskap og forståelse for hverandres oppdrag er sentralt i en tid hvor det sikkerhetspolitiske landskap er i utvikling. Jeg vil takke sjef Kripos og Forsvarets høgskole for at jeg fikk anledning til å gå stabsstudiet i 2018 – 2019. Det var et svært lærerikt år.

Å skrive en master har bidratt til erkjennelsen av hvor lite jeg faktisk kan, men motiverer meg til fortsatt å søke ny lærdom.

Oslo, 14. oktober 2020

Ole Jørgen Arvesen

Sammendrag

Digitalisering og globalisering har bidratt til et enklere og mer effektivt samfunn, men også økt sårbarheten. Utviklingen påvirker trusselbildet og har introdusert nye sikkerhetsutfordringer. Det tradisjonelle skillet mellom indre og ytre sikkerhet, fred og krig er mindre tydelig enn før. Grensesnittet mellom stat- og samfunnssikkerhet er krevende. Her ligger kjernen i statens utfordring. Hvordan fordele ansvar når norsk sikkerhetsarkitektur organiseres etter sektorprinsippet? Digitaliseringen skaper store utfordringer med å avdekke hvem som står bak en hendelse i cyber.

Studiets problemstilling omhandler tilpasninger til det endrede trusselbilde og ser på hvilke faktorer som påvirker myndighetenes veivalg i form av lovutvikling og organisering av sikkerhetsarkitekturen i cyber. Datainnsamlingen er i all hovedsak fra offentlige dokumenter som trusselvurderinger, offentlige utredninger, forarbeider og høringssvar. Først sees det på utviklingen i cyberdomenet, både fra akademia og myndighetene. Så gjennomgås tilpasninger til det nye scenario ved analyse av forarbeidene til to lovforslag, Etterretningstjenesteloven og Fullmaktsloven. Sist sees det på oppståtte gråsonescenario som følge av det utvidede trusselbilde og myndighetens plassering av ansvar.

Myndighetenes situasjonsforståelse bygger på at statlige aktører representerer den største trusselen. Det fremmes likevel at majoriteten av cyberangrep er kriminalitet. Politiet, som er primæraktøren innen samfunnssikkerhet utgir ingen offentlige trusselvurderinger. Narrativet kan således sies "å eies" av EOS tjenestene. Dette kan påvirke lovutviklingen. Fellesnevneren for begge lovforslagene er at de utfordrer grunnleggende prinsipper som rettssikkerhet og maktfordeling vårt liberale demokrati er tuftet på. Oppgaven redegjør for at det i høringsrundene ble reist en rekke grunnleggende spørsmål om ansvarsfordeling, gråsoneproblematikk og hjemmelsgrunnlag. Fordi trusselaktør er vanskelig å identifisere i cyber, oppstår et behov for tverrsektorielle løsninger. Spesielt Nasjonal sikkerhetsmyndighet har fått en utvidet rolle i å ivareta cybersikkerheten. Utvidelse av mandatet kan øke gråsonen hva gjelder hvem som er ansvarlig for hva og til hvilken tid.

Dagens sikkerhetsarkitektur kan fremstå som overlappende og til dels uoversiktlig. Trusselbildet bør sees i dimensjoner og ikke sekvensielt. Fordi statlige aktører utpekes som den største trusselen oppfattes sikkerhetssituasjonen som eksistensiell. Frykt kan derfor medføre en aksept for statlig overvåkning i bytte mot frihet. Cyber kan i så måte være i ferd med å bli sikkerhetisert. Samfunnssikkerhetsrelaterte trusler er ikke definert og derav ikke vurdert i sin fulle bredde og betydning. Norsk sikkerhetsarkitektur tar tilsynelatende utgangspunkt i statlige aktører, og sektor- og ansvarsprinsippet tvinger ansvarsfordelingen inn i tradisjonelle strukturer. Følgen er at koordineringsutfordringene øker og statens totale ressurser søkes samordnet ved at tverrsektorielle institusjoner og sentre vokser, og motstandskraften mot trusselen i cyber kan fremstå som fragmentert.

Summary

Digitisation and globalisation have made life easier and more efficient, but they have also increased our vulnerability. The nature of the threat picture is evolving while new threats emerge. The traditional division between internal and external security, war and peace is blurred. The interface between state and public security is demanding and is at the core of the state's challenge. How should responsibilities be divided when Norwegian security architecture is organised along sector lines?
This thesis discusses how government authorities adapt to changed threat levels and what elements influence their decisions with respect to legislative changes and organisation of the country's cybersecurity. Data has been collected mainly from threat assessments, government white papers, preparatory works and consultation responses. First, I discuss developments in cyberspace from the perspectives of both academia and government authorities. Then I discuss how the new scenario is reflected in two proposed new laws by analysing the preparatory works. Finally, I discuss the grey areas created by the extended threat picture and the adopted division of responsibilities.

The current understanding is that other state actors represent the biggest threat. However, the vast majority of cyberattacks are criminal. The police, who are the primary actors in public security, do not publish threat assessments. Thus, it may be said that the narrative is "owned" by the intelligence, surveillance and security services, and this may shape legislation. The common denominator in both the new acts is that they challenge the fundamental principles, e.g. due process and power sharing, on which our liberal democracy is built.

The thesis describes how, during the consultation phase, a number of fundamental issues were raised about division of responsibilities, grey areas and authorisation. Because threat actors in cyberspace are hard to identify, they require a multi-sectorial approach. The National Security Authority in particular, has been given an expanded role in protecting national cybersecurity. The expansion of their mandate may enlarge the grey area with respect to who is responsible for what and when. The current security architecture can appear overlapping and complex. Current threat should be analysed in dimensions, not sequentially, and because state actors are identified as representing the biggest threat, the threats facing us are considered existential. Fear can then lead to greater acceptance of state surveillance in exchange of freedom. In this way, cyberspace can be said to become "securitised".

Threats against public security are therefore not identified or discussed in necessary detail. Private actors who on a global scale own and manage the vast majority of data, are not discussed in national threat assessments. This may lead to a "blind zone" in situational understanding. The security architecture in Norway is apparently built to counter state actors, and the sector principle of organising divides responsibilities along traditional sectorial lines. As a result, the challenges in coordinating efforts increase and the state seeks to coordinates its overall resources by enlarging multi-sectorial institutions and centres, and the forces combatting threats in cyberspace can appear fragmented.

Innholdsfortegnelse

1 Innledning

Den raske teknologiske utviklingen har bidratt til et tryggere, enklere og mer sikkert samfunn. Stadig flere enheter og tjenester kobles til internett som har utviklet seg til å bli verdens viktigste infrastruktur. Internett utgjør i dag ryggraden i den globale flyten av informasjon, varer og tjenester (NOU2018:14, s.20). Avhengigheten av internett gjør samfunnet også mer sårbart. Samfunnets risikobilde endres som følge av denne utviklingen og få nasjoner kan i dag kontrollere sin digitale sårbarhet fullt ut (Justisdepartementet, 2017, s.11).

Statens overordnede oppdrag er å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser (Sikkerhetsloven, 2019, §1-5). Globaliseringen gjør at de nasjonale grensene til dels viskes ut, og tett integrering med andre stater påvirker vår sikkerhet i langt videre forstand enn tidligere. Dette utvidede trusselbilde har introdusert nye sikkerhetsutfordringer (Beadle & Diesen, 2015, s.14). Utfordringene vokser dermed som følge av at utviklingen skaper avhengigheter og sårbarheter som går på tvers av sektorer og landegrenser. Endringene skaper et behov for ny sikkerhetstenkning. Staters forståelse av begrepet «sikkerhet» utvides og påvirker den sikkerhetspolitiske adferd. Sikkerhetsbegrepet knyttes nå også til forsvar av vitale verdier som samfunnssystem og velstand, faktorer som tidligere ikke tradisjonelt er omhandlet i sikkerhetspolitikken. Vi snakker derfor om sikkerhet på flere nivåer enn tidligere (Kjølberg & Jeppesen, 2001, s.20).

Trusselen i cyberdomenet beskrives primært i dag av våre etterretning- og sikkerhetstjenester. Deres fokus er å ivareta statssikkerheten og vurderingene er orientert rundt dette tema. At truslene defineres til å høre inn under statssikkerheten kan bidra til at domenet sikkerhetiseres. Tiltak, rolle og ansvar for å forebygge og håndtere situasjonen, utfordrer på denne måten ellers forbudte og begrensede rammer som gjelder for hendelseshåndtering i fredstid. Narrativet som etableres er at ekstraordinære hendelser krever ekstraordinære virkemidler. En slik tilnærming har en rekke spørsmål ved seg, spørsmål som bør belyses og diskuteres i et større perspektiv.

Denne oppgaven ser på hvilket situasjonsbilde som legges til grunn for myndighetenes lovutvikling og organisering av sikkerhetsarkitekturen i cyberdomenet, og videre hvordan det igjen legger føringer for respons. Der hvor det tidligere var enkelt å definere en tjeneste sitt myndighetsområde, har digitaliseringen medført et tilnærmet grenseløst scenario. Fordi de ulike myndigheters ansvarsområder delvis overlapper hverandre på viktige områder, oppstår uklarheter i hvem som har ansvar for hva og hvordan arbeidet skal organiseres og koordineres.

Ansvarsfordelingsspørsmålet er både viktig og vanskelig. Det reiser sentrale maktfordelings- og rettssikkerhetsspørsmål (Auglend, 2015a, pkt.1). Den tradisjonelle fordelingen av oppgaver bygger på

skillet mellom ytre og indre sikkerhet, men dette utfordres i dagens hybride trusselbilde. Utviklingen har gjort det mer krevende å skille statssikkerhet og samfunnssikkerhet (Friis & Hansen, 2020, s.186). Vanskeligheter med å klassifisere en krise som sivil eller sikkerhetspolitisk legger til rette for et økende behov for tverrsektorielle løsninger. Romarheim (2019, s.136) påpeker at «Norges sentralforvaltning preges av stramme vertikale styringslinjer». En slik sektorvis tilnærming kan legge hindre i veien for et tverrsektorielt samarbeid som er helt nødvendig for å håndtere truslene i cyber. Et uklart og mangespektret trusselbilde kan gi opphav til en rekke gråsonescenarioer. Gjensidig forståelse av roller og ansvar er dermed en forutsetning (Forsvarsdepartementet & Justisdepartementet, 2018, s. 8).

1.2 Oppgavens problemstilling

Studiet tar utgangspunkt i den digitale revolusjon og konsekvensene av at verden knyttes sammen gjennom forskjellige nettverksløsninger. Dette representerer en endring av trusselbildet og i norsk sammenheng bygger situasjonsforståelsen i all hovedsak på de nasjonale trusselvurderingene. Hvilken innretning og fokusområde disse har, vil derfor ha stor påvirkning på hvordan myndighetene organiserer seg. På bakgrunn av dynamikken i trusselbildet er problemstillingen for oppgaven formulert som følger:

Hvordan tilpasser norske myndigheter seg til et endret trusselbilde og hvilke faktorer kan påvirke utviklingen av sikkerhetsarkitekturen for cyberdomenet?

1.3 Avgrensninger

Oppgaven tar ikke mål av seg til å dekke alle elementer av sikkerhetspolitisk art i cyber, men tar utgangspunkt i problemstillinger som har utspring i det digitale domenet og hvordan dette påvirker vår sikkerhetstenking. Studien avgrenses til relasjonene mellom sivil- og militær sektor innenfor norsk jurisdiksjon. Totalforsvaret som institusjon er ikke berørt ut over som eksempel på en tilpasning til samfunnsendringen i stort.

Oppgaven omhandler faktorer som påvirker ansvar og myndighetsplassering i møte med et mer komplekst trusselscenario, herunder hvilke prinsipper som legges til grunn og hvilke utslag dette får i forhold til fordeling av ansvar og myndighet. Problemstillingen fokuserer på situasjoner hvor digitaliseringen representerer et skifte i tradisjonell tenkning mellom stat- og samfunnssikkerhet. Forhold som konvensjonell militær styrke og maktbalansen mellom stormaktene omhandles ikke ut over tangeringspunkter mot cyber. Oppgaven søker å identifisere om ansvarsforhold forskyves samt de overordnede årsakene og konsekvenser av dette. Hensikten er å se de store linjene og om hvordan komplekse trusselscenario blir imøtegått av myndighetene. I dagens situasjon kan ikke oppgaveløsningen lenger sees på som sekvensiell og lineær (fred, krise, krig), men snarere i hvilken dimensjon (stat- og samfunnssikkerhet) trusselen skal forstås. Definisjonen av trusselbildet og hva

som trues har derfor en sentral rolle i myndighetenes beslutningsprosesser. Oppgaven tar for seg etterretning og sikkerhetstjenestene (EOS) sine trusselvurderinger. Trusselvurderingene fra Direktoratet for samfunnssikkerhet (DSB) er gjennomlest, men ikke inntatt i analysen da disse i hovedsak omhandler hendelser som naturkatastrofer og store ulykker (DSB, 2019a, s.5).

Denne tilnærmingen utfordrer oppgavens avgrensning, men er samtidig selve poenget, nemlig å se sammenhengen mellom endringene i trusselbildet og hvordan myndighetene forholder seg til dette.

1.4 Struktur

For å kunne besvare problemstillingen må det gjøres rede for det endrede trusselbildet i cyberdomenet, hvilke faktorer som kan påvirke sikkerhetsarkitekturen og hvordan myndighetene tilpasser seg dette.

Oppgaven søker å løse dette ved først å beskrive sentrale begreper og prinsipper knyttet til problemstillingen, før den metodiske fremgangsmåten beskrives i kapittel 2. I kapittel 3 beskrives teoretiske perspektiver på cyberdomenet ved å ta utgangspunkt i relevant forskning på dette feltet. I kapittel 4 omhandles cybersikkerhet i åpne trusselvurderinger gjennom en analyse av trusselvurderinger fra EOS tjenestene.

I kapittel 5 sees det på lov og strukturendringer i møte med cybertrusselen. Hvilke faktorer myndighetene vektlegger når de tilpasser seg det endrede bildet i cyberdomenet, herunder hvordan sikkerhetspolitikken er i endring og hvordan lovverket tilpasses i tråd med dette. Kapittel 6 ser på hvordan gråsonen mellom ulike etater vokser og hvordan dette håndteres av myndighetene. Til slutt sammenfattes funnene fra oppgaven og konklusjon i kapittel 7.

1.5 Begreper og prinsipper

Digitaliseringen utfordrer balansegangen mellom en stats sikkerhet og individets rettigheter samt juridiske skiller mellom egne og andre staters borgere (Kvernberg & Johnsen, 2013, s.7). Begrepene statssikkerhet og samfunnssikkerhet må derfor forstås i lys av samfunnsutviklingen de senere år, som i stor grad har medført at det tradisjonelle skillet mellom statssikkerhet, samfunnssikkerhet og individuell sikkerhet og trygghet har blitt visket noe ut (NOU2016:19, s.100). Det samme kan sies om kategoriseringen "rikets sikkerhet" som med samme begrunnelse er noe utdatert sett i lys av den senere tids utvikling. Begrepene bør ha en dynamisk karakter og tilpasses den generelle samfunnsutviklingen og endringer i det internasjonale trusselbildet (NOU2016:19, s.101).

Statssikkerhet

Statssikkerhet vil si å ivareta statens eksistens, suverenitet, suverene rettigheter og territorielle integritet. Statssikkerheten kan utfordres gjennom væpnet angrep, politisk og militært press mot politiske myndigheter, og alvorlige anslag mot norske interesser fra statlige eller ikke-statlige aktører.

Trusler mot Norges økonomiske handlefrihet kan også utfordre statssikkerheten (Forsvarsdepartementet, 2018, s.97). Statens grunnleggende nasjonale funksjoner er sikkerhetspolitisk ansvar for Norges suverenitet, territorielle integritet og demokratiske styreform (NOU2016:19, s.18). Med grunnleggende nasjonale funksjoner menes tjenester, produksjon og andre former for virksomhet som er av slik betydning at ved helt eller delvis bortfall vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser (Forsvarsdepartementet & Justisdepartementet, 2018, s.63). Dette er oppgaver som tradisjonelt sett tilfaller forsvarsstrukturen i en stat (Kvernberg & Johnsen, 2013 s.14) da trusler mot statssikkerheten kan legitimere innsats av alle militære virkemidler.

Statssikkerheten handler altså om å ivareta nasjonale sikkerhetsinteresser som landets suverenitet, territorielle integritet og demokratiske styreform og sikkerhetspolitiske interesser i sin videste forstand (Forsvarsdepartementet & Justisdepartementet, 2018, s.12).

Samfunnssikkerhet

Samfunnssikkerhet omhandler samfunnets evne til å verne seg mot og håndtere uønskede hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være utslag av tekniske eller menneskelige feil eller bevisste handlinger (NOU2019:13, s.33). Samfunnssikkerhet er det som ikke truer statens eksistens direkte, men truer befolkningens trygghetsfølelse samt viktige samfunnsinstitusjoner og infrastruktur. Begrepet har vokst frem spesielt i lys av ikke-statlige trusler i tiden etter den kalde krigen, men er like fullt noe som tilfaller politimyndighetene innad i en stat. Forsvaret kan imidlertid stille kompetanse til disposisjon i henhold til bistandsinstruksen dersom politimyndighetene skulle finne det nødvendig i sin håndhevelse av samfunnssikkerhet (Kvernberg & Johnsen, 2013 s.14).

Sektor og beredskapsprinsippene

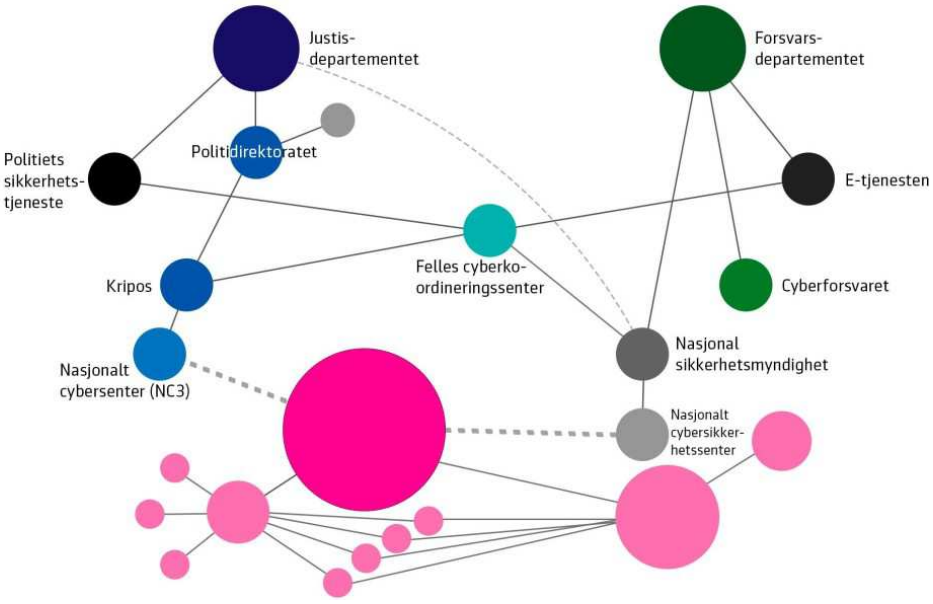
I Norge er makten og ansvaret fordelt mellom den utøvende, lovgivende og dømmende makt (Simonsen, 2019, s.43) og sektorprinsippet er muligens det mest sentrale trekk ved den norske styringsmodellen. Tydelige ansvarslinjer og tett kontakt til bakkenivået er andre sentrale trekk ved Norges sikkerhetsarkitektur. Dette kan sees som en form for villet desentralisering (NOU2016:19, s.29). Det er Regjeringen som har det øverste utøvende ansvaret for både den militære og sivile beredskap og krisehåndtering i fredstid, kriser og væpnet konflikt. Det enkelte departement er imidlertid ansvarlig gjennom sektorprinsippet å forebygge og ivareta nødvendig beredskap og kompetanse til krisehåndtering (Forsvarsdepartementet & Justisdepartementet, 2018, s.16). Samfunnssikkerheten tar utgangspunkt i fire grunnleggende prinsipper:

Ansvarsprinsippet innebærer at den myndighet, virksomhet eller etat, som har daglig ansvar for et område, også har ansvaret for forebygging, beredskapsforberedelser og for iverksetting av nødvendige tiltak ved kriser og katastrofer. Ansvarsprinsippet regnes som hovedprinsippet.

Likhetsprinsippet betyr at den organisasjon man opererer med under kriser skal være mest mulig lik den organisasjon man har til daglig.
Nærhetsprinsippet innebærer at kriser organisatorisk skal håndteres på lavest mulig nivå.
Samvirkeprinsippet stiller krav til at myndighet, virksomhet eller etat har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering (Forsvarsdepartementet & Justisdepartementet, 2018, s.16).

En følge av digitalisering er økt gjensidig avhengighet på tvers av tradisjonelle skillelinjer mellom sivile samfunnssektorer og landets militære forsvar. Samtidig har fremveksten av et nettverksbasert samfunn ført til at de samme skillelinjene er blitt mindre markante (NOU2016:19, s.18). For departementer med samordningsansvar, som Justis- og beredskapsdepartementet, kan det være utfordrende å utøve rollen som samordningsdepartement innenfor rammen av det konstitusjonelle system med ministerstyre som en grunnleggende forutsetning. Et departement kan ikke uten videre pålegge andre departementer oppgaver, tiltak eller roller. De er likestilte enheter i en flat styringskultur. Det fører til en horisontal styringsutfordring mellom departementene (NOU2018:14, s. 43; Smith, 2015). En konsekvens kan være at relevante departementer ikke engasjeres i oppdragsløsningen. Dette kan svekke Norges totale evne til å håndtere hendelser som potensielt kan utfordre våre grunnleggende nasjonale funksjoner og interesser. En kan hevde at sektorprinsippet fungerer godt hva gjelder ansvarsfordeling, men potensielt være til hinder for optimal oppdragsløsning. Sektor- og samvirkeprinsippet vil derfor i noen tilfeller fremstå som motstridene (NOU2016:19, s.31).

En av utfordringene i cyberdomenet og sikkerhetsarkitektur, er mangfoldet av ulike myndigheter. Disse kan illustreres slik:



Figur 1. En oppskrift på cyberlapskaus (Trædal, 2018)

Feltene som ikke er navngitt illustrerer at det eksisterer en rekke andre koblinger til resten av samfunnet, som privat sektor, øvrig offentligsektor, KraftCERT, FinansCERT, HelseCert, EkomCERT, NorSIS, Telenor mv. Disse er som nevnt ikke omhandlet, da oppgaven er avgrenset til å se på forholdet mellom sivil- og militær sektor.

2 Metode

I det følgende redegjøres det for valget av kvalitativ metode, samt begrunnelser for valget om å benytte dokumentanalyse. Videre beskrivelses utvalgsprosessen av kilder og hvilke kvalitetskriterier som er lagt til grunn. Metodedelen avsluttes med en redegjørelse for oppgavens validitet og reliabilitet.

2.1 Generelle metodiske spørsmål

En hypotese viser til noe som er antatt og foreløpig, som etter alt og dømme er en rimelig forklaring på et fenomen. Gjennom hypoteser danner vi oss et bilde på forhånd av hva vi forventer å finne gjennom undersøkelsen (Johannessen, Christoffersen & Tufte, 2016, s. 46) .

Basert på egne erfaringer og roller i både politiet og Forsvaret, hadde jeg på forhånd en formening om hvordan sikkerhetsarkitekturen i cyberdomenet er organisert. Før undersøkelsen hadde jeg en hypotese om at ansvar og rollefordelingen i cyber er fragmentert mellom ulike aktører. Videre satt jeg med et inntrykk av at tverrsektorielle myndigheter som NSM og DSB, stadig får utvidet sitt mandat.

Formålet med undersøkelsen

For å svare på oppgavens problemstilling, har jeg undersøkt hvordan trusselen i cyberdomenet beskrives ved å gjennomgå de nasjonale trusselvurderingene fra EOS tjenestene. Vurderingene danner fundamentet og derav beslutningsgrunnlaget for myndighetene. Formålet har vært å klarlegge tjenestenes innretning og konklusjoner, og se disse mot forskningens syn på utviklingen.

For å beskrive hvilke tilpasninger som gjøres, er to lovforslag analysert. Her er det inntatt et utvalg høringssvar fra berørte instanser og interessenter. Hensikten er å belyse mulige komplikasjoner som oppstår i forlengelsen av myndighetenes lovutforming og grensesnittutfordringer som følger av dette.

Cyberdomenets kompleksitet tilsier en helhetlig tilnærming for å etablere en robust motstand mot angrep og hendelser. Jeg har derfor sett på hvilke faktorer som kan påvirke organisering og gråsoneproblematikk som kan oppstå. Formålet er å avdekke om dagens sikkerhetsarkitektur er hensiktsmessig. Jeg har tatt utgangspunkt i hvordan sektor- og ansvarsprinsippet påvirker myndighetens beslutninger, samt konsekvensene ved å kategorisere en trussel som enten statssikkerhet eller samfunnssikkerhet.

Valg av metode

Dokumentundersøkelser er spesielt godt egnet når det er umulig å samle inn primærdata direkte fra kildene. Enten at kildene ikke eksisterer lenger eller at de ikke er tilgjengelige for forskeren til å gi intervju eller observeres (Jacobsen, 2015, s.170). I denne oppgaven baseres analysene primært på dokumenter produsert av offentlige utvalg, organisasjoner og forskningsrapporter hvor det gis anbefaling eller innspill til konkrete problemstillinger innenfor cyberfeltet. Dokumentene taler således i noe grad for seg selv.

Vurderingskriteriene som er lagt til grunn er at innsamlet data må kunne danne grunnlag for å beskrive og analysere utviklingen i cyberdomenet. Videre kunne redegjøre for faktagrunnlaget myndighetene tar utgangspunkt i ved lovutvikling og organisatoriske beslutninger.

2.2 Dokumentinnsamling

I kvalitative dokumentstudium er kildekritikk viktig. Vurderingene av kildenes relevans, reliabilitet og validitet vil være avgjørende (Grønmo, 2016, s.177). Da studiets problemstilling omhandler hvordan myndighetene tilpasser seg trusselen i cyber, er majoriteten av kildene i oppgaven offentlige dokumenter. Tekst utgitt av offentlige etater som Stortingsmeldinger, lovforslag, offentlige utredninger og rapporter. For å kunne avdekke om det er sammenheng mellom teori og empiri starter oppgaven med et teoretisk utgangspunkt. Hva sier faglitteraturen om cybersikkerhet, digitalisering, sikkerhetisering, attribusjon og gråsoneproblematikk? Hvilke tema opptar forskerne og hvilke problemstillinger løftes frem?

Undersøkelser av teoretiske perspektiver på cyberdomenet

Til teorikapittelet startet jeg med å søke i Oria og Google Schoolar. Det avdekket hvilke institusjoner og tidsskrifter som publiserer mest om tema problemstillingen omhandler, sikkerhetsspørsmål relatert til cyberdomenet. Da oppgaven er konsentrert til hvordan norske myndigheter tilpasser seg et endret trusselbilde og faktorer som kan påvirke sikkerhetsarkitekturen, ble utvalget primært gjort til norske forskningsinstitutter og Skandinaviske tidsskrifter. Tidsskriftet *Internasjonal Politikk*, utmerket seg i denne sammenheng. For å belyse tema cybersikkerhet og faktorer som påvirker organisering og myndighetsplassering, er også noen internasjonale publikasjoner inntatt. Utvalgsprosessen har i noe grad benyttet «snøballmetoden, som i korthet innebærer at kildehenvisningen i valgte publikasjoner er benyttet for å avdekke ny litteratur (Tjora, 2017, s. 135; Johannessen, Tufte & Christoffersen, 2016, s. 119). Temaet cyber er stort og berører en rekke forhold. Avgrensningen er derfor søkt konsentrert rundt tema som kan operasjonalisere problemstillingen.

Undersøkelse av Cybersikkerhet i åpne trusselvurderinger

Innsamling av offentlige dokumenter er lett tilgjengelig ved å søke i nettsidene til Regjeringen og Stortinget. Formålet var å undersøke hvilke tiltak som er iverksatt og organisatoriske beslutninger hva

gjelder trusselen i cyber. Det ble relativt tidlig klart at utfordringene er omfattende og at det ikke er åpenbart hvilken institusjon i samfunnet som «eier» problemet. For å operasjonalisere problemstillingens utgangspunkt, et endret trusselbilde, er det sentralt å etablere en forståelse av hvilket situasjonsbilde som blir presentert for beslutningstagerne. De offentlige kildene refererer kategorisk til Etterretning og sikkerhetstjenestene (EOS) sine nasjonale trusselvurderinger. For å belyse utviklingen digitaliseringen representerer er disse tjenestene sine vurderinger de siste 10 år gjennomgått. Kapittel 4 har et komparativt element ved at undersøkelsen har konsentrert seg om hvordan de tre ulike tjenestene beskriver trusselutviklingen i cyber, aktører og hvordan modusbildet beskrives. Trusselvurderingene er hentet fra den enkelte tjeneste sine nettsider. Trusselen i cyber treffer hele samfunnet. Da EOS tjenestene omtaler trusler mot statssikkerheten er det relevant å undersøke hvordan trusselen beskrives i et samfunnssikkerhetsperspektiv. Det er derfor også gjennomført søk på politiets nettsider for å se hvordan kriminaliteten i cyber beskrives.

Kapittel 5 tar for seg lovutviklingen. Valg av første case var relativt enkelt. Den nye Etterretningstjenesteloven. Etterretningstjenestelovens utvidede hjemmelsgrunnlag representerer et vesentlig skifte hva gjelder tilpasning til et endret trusselbilde. Loven reiser også en rekke prinsipielle problemstillinger som er relevant å se rekkevidden av. I denne sammenheng er spesielt tjenesten sin anledning til å overvåke datastrømmen ut og inn av Norge (tilrettelagt innhentning), og forvaltningen av innsamlet informasjon sentralt. Neste case stod mellom Sikkerhetsloven og den foreslåtte Fullmaktsloven. Den nye Sikkerhetslovens utvidelsen av virkeområde, til også å gjelde beskyttelse av grunnleggende samfunnsfunksjoner er relevant for problemstillingen. I høringsrunden var det i stor grad enighet om tilførslene (NOU2016:19). Valget falt derfor på forslaget om ny Fullmaktslov. Dette begrunnes med at denne skiller seg ut ved at den er foreslått til å virke over departementsnivå, noe ikke Sikkerhetsloven gjør. Forslaget om, og beskrivelsen av, et behov for sektorovergripende beslutningsmyndighet, reiser nye spørsmål som kan påvirke sikkerhetsarkitekturen. Lovforslaget representerer således en vesentlig endring av maktstrukturen i en gitt krisesituasjon. Dokumentinnsamlingen baserer seg på dokumenter lastet ned fra regjeringen.no eller stortinget.no.

Offentlige dokumenter vurderes som en god kilde ettersom de inneholder det offentliges syn på utvalgte tema, forløpet, praksis og lover og regler. En utredning er imidlertid et utvalgs syn. Utvalgets sammensetning eller hvilket departement som utreder kan derfor være relevant å vurdere. I denne oppgaven er det vist til en rekke høringsinnspill nettopp for å avdekke avvik fra utvalgets tolkninger eller prinsipielle spørsmål som utledes av forslagene. Valg av høringsinstanser som nyanserer dette behovet er basert på to forhold. Først der hvor det oppstår overlappende og uklare grensesnitt, som mellom justismyndighetene og Forsvaret, og dernest institusjoner som utfordrer de prinsipielle konsekvensene av endringer som var på høring. Hensikten er å belyse motsetninger og løfte frem

argumentasjon som myndighetene må ta stilling til i beslutningsprosessen om hvem som skal gjøre hva, med hvilken myndighet og hjemmelsgrunnlag.

For å aktualisere problemstillingen er det henvist til enkelte presseoppslag. Innsamlingen er begrenset til tidsperioden 2019 frem til september 2020. Valg av mediehus er avgrenset til NTB, NRK og Aftenposten. Dokumentinnsamlingen har dermed hatt en trinnvis utvikling. Fra faglitteraturen til offentlige dokumenter og høringssvar, til relevante presseoppslag som relaterer seg til problemstillingen. Formålet har vært å tilkjennegi utviklingen hva gjelder sikkerhet i cyberdomenet og hvilket beslutningsgrunnlag myndighetene legger til grunn, og til sist hvilke utfordringer som oppstår i kjølvannet av disse.

2.3 Validitet og reliabilitet

Kildenes relevans, reliabilitet og validitet må vurderes (Grønmo, 2016, s. 177). Som beskrevet er utvalg gjort i datainnsamlingen naturlig nok innrettet mot problemstillingen, men temaet er stort og vinklingen kan medføre at relevante poenger i analysen ikke er tatt med. Som eksempel kan nevnes at EOS tjenestene sine trusselvurderinger er de offentlige versjonene. En må kunne anta at trusselbildet, og derav konklusjonene, også baseres på informasjon som ikke kan offentliggjøres. Dette faktum endrer ikke på vurderingenes konklusjoner, men det kan finnes variabler eller nyanser som ikke fremkommer i de offentlige publikasjonene. En må forutsette at myndighetene blir gjort kjent med slik kunnskap og at beslutningsgrunnlaget således omfatter et bredere og dypere situasjonsbilde enn det som fremkommer i det offentlige rom. Likefullt er det innen norsk forvaltning et offentlighetsprinsipp hjemlet i Offentleg lova, som innebærer at det skal gis mulighet til å sette seg inn i saker som berører grunnleggende rettigheter og forhold som angår demokratiet. Med andre ord, trusselbildet som EOS tjenestene beskriver i sine trusselvurderinger, skal være tilstrekkelig belyst til å fremme lovforslag og fatte vedtak om ansvarsfordeling og organisering av sikkerheten i cyber.

Ved å velge kvalitativ dokumentanalyse som forskningsdesign er det noen svakheter. Creswell (2014, s. 207) påpeker at fordi datainnsamlingen gjøres av forskeren selv, kan personlige verdier, antakelser og forutinntatthet svekke studiets objektive innretning. Det er spesielt lagt vekt på at søkeord og vurderingskriterier er relevant for oppgaven og skillet mellom stats- og samfunnssikkerhet i cyber. Da min primære erfaring er fra politiet, og derav oppgaver innen samfunnssikkerhetsdomenet, er det lagt vekt på begge disse perspektivene i datainnsamlingen. Som følge av mitt linjeansvar for politiets (Kripos) inntreden i Felles cyber koordineringssenter (FCKS), er det overlappende ansvar mellom politiet og EOS tjenestene et forhold jeg har innsikt i. Dette er både en styrke og svakhet. En styrke for forståelse og innsikt i gråsoneproblematikken, og en svakhet sett hen imot kunnskap om problemstillinger som omhandler statssikkerheten. Dette kan medføre at jeg ubevisst har lett etter argumentasjon i datainnsamlingen som belyser gråsonen, med et polisiært utgangspunkt. Jeg har hatt bevissthet rundt problemet og forsøkt å korrigere for bias underveis.

Cyberdomenet er komplekst og digitaliseringen gjør seg gjeldene på alle nivå, fra ytterpunktene sikkerhetspolitikk til den enkeltes personvernrettigheter. Dette faktum gjør det utfordrende å balansere datainnsamlingen sett opp imot problemstillingen. I både utvalg, gjennomgang og tolkning av data er validitet og reliabilitet søkt ivaretatt. Kildene er i analysen primært basert på offentlige dokumenter som gir høy intern gyldighet i form av at dokumentene gir en virkelighetsnær beskrivelse basert på fakta. Den eksterne gyldigheten ligger i studiens overordnede funn. Et endret trusselbilde har større rekkevidde enn det digitale domenet, og sikkerhetisering av truslene visker ut det tradisjonelle skillet mellom politiet og Forsvaret. Strukturingen av oppgaven søker å understøtte gyldighet ved først å ta utgangspunkt i teori og så analysere trusselbildet. Videre ved å analysere to konkrete lovforslag og til sist belyse konsekvensene hva gjelder myndighetenes organisering og derav myndighetsområde. Studiet kan i en slik kontekst generaliseres til å ha en viss relevans ut over cyberdomenet.

3 Teoretiske perspektiver på cyberdomenet

Hva sier faglitteraturen om cyberdomenet og hva opptar forskerne? Jeg vil i det følgende beskrive hvordan sentrale temaer og utviklingstrekk er beskrevet i en akademisk kontekst. Et av oppgavens formål er å se om det er samsvar mellom teori og empiri. Hvilke premisser legges til grunn når myndighetene organiserer samfunnets ressurser - gjennom delegering av myndighet, lov utvikling og opprettelsen av funksjoner som skal håndtere den endrede sikkerhetssituasjonen? Teorigjennomgangen belyser noen av faktorene som påvirker sikkerhetssituasjonen som følge av den teknologiske utvikling.

I et velfungerende samfunn som det norske er internett og funksjonalitetene digitaliseringen gir en forutsetning for utvikling og vekst. Det er tre faktorer som særlig former vårt digitale fundament: (1) digitalisering, (2) trusselbildet og (3) militarisering. Debatten om hvilke følger denne utviklingen har sentreres i stor grad rundt temaet sikkerhet (Svenungsen, 2019b, s.1), men også individets rettigheter. Grensesnittet mellom nasjonens sikkerhet og rettssikkerhet for den enkelte skaper nye utfordringer. På den ene siden har den sosiale dimensjon som skapes ved digitale nettverk åpnet opp for meningsytringer og politisk engasjement som har innvirkning på den politiske sfære. På den andre siden gis det nye muligheter for myndigheter til å overvåke individer og samfunnet i stort. Det oppstår dermed en potensiell spenning mellom det som oppfattes som samfunnets sikkerhetsbehov gjennom overvåkning på den ene siden, og beskyttelsen av individenes sivile rettigheter på den andre. Definisjon av hva som er samfunnets sikkerhetsbehov og hvilke tiltak som er legitime er derfor kontinuerlig gjenstand for diskusjon (Steen-Johnsen, Enjolras & Wollebæk, 2013, s.265). Dette kommer blant annet til uttrykk i lovutvikling og organisering av samfunnets ressurser.

Teknologien vever sammen en rekke sektorer og funksjonaliteter. En fare er at det kan oppstå et etterslep hvor man bruker gamle forklaringsmodeller og metoder for å forstå nye tider. Svenungsen (2019a, s.238) omtaler i sin artikkel om cyber og geopolitikk: «Vi bruker tradisjonelle mekanismer i internasjonal politikk for å forstå en ny virkelighet og vi forsøker å løse konflikter i fora som ikke nødvendigvis er egnet».

I det følgende beskrives et utvalg av faktorer som omhandles i faglitteraturen hva gjelder cybersikkerhet. Som det fremkommer er tema stort og mangespektret. Oppgaven utspiller seg i forholdet mellom Forsvaret og det sivile maktapparat, sektorprinsippet og såkalt sikkerhetisering av cyberdomenet, og det er dermed disse aspektene som vektlegges i gjennomgangen. Først redegjøres det for cybersikkerhet og omfanget av dette tema. Videre om hvordan digitalisering og globaliseringen påvirker sikkerhetsutfordringene ved mangfold av aktører og det faktum at store deler av infrastrukturen kontrolleres av private selskaper. Deretter omtales kort faktorer som har betydning for sikkerhetisering av domenet, før det avslutningsvis sees gjennom andre elementer som har innvirkning på cybersikkerhet i tilknytning til organisering og sektorprinsippet. Hovedkapittelet avrundes med en del-konklusjon.

3.1 Cybersikkerhet

I norsk sammenheng deles sikkerhetsbegrepet opp i to hovedinnretninger: *Statssikkerhet* og *samfunnssikkerhet*. Innholdsmessig retter internasjonal sikkerhet seg mot statssikkerheten og har tradisjonelt oppheng i maktpolitikken. Samfunnssikkerheten omhandler sosial sikkerhet og vinkles derav mot justis og rettsvesen. Det som skiller disse to kategoriene er at statssikkerheten, som handler om statens overlevelse, rettferdiggjør bruk av ekstreme maktmidler for å håndtere en sikkerhetsutfordring (Buzan, Wæver & De Wilde, 1998, s.21). Utviklingen i det digitale rom har gjort det mer krevende å skille klart mellom disse kategoriseringene (Friis & Hansen, 2020, s.186).

Sikkerhet i cyber er mangespektret. Selve begrepet cyber er i seg selv upresist og et prefiks. Terminologien som benyttes er; det digitale rom, cyberspace eller cyberdomenet mv. I oppgaven benyttes begrepene i all hovedsak slik kildene gjør, nemlig at uansett hva man kaller det, så er dette et menneskeskapt miljø bestående av informasjon, data og IKT-infrastruktur. Strukturen er global og knytter mennesker sammen ved å tilrettelegge for kommunikasjon, informasjonssøk, styre og kontrollere ulike prosesser og foreta forretningstransaksjoner. Det fremstår å være en omforent oppfatning at cyber er et informasjonsmiljø hvor en rekke handlinger gjøres gjennom et nettverk som bruker informasjons og kommunikasjonsteknologi (Langø & Sandvik, 2013, s.221).

Cybersikkerhet kan betraktes som reaksjonen på en risiko eller trussel mot den globale informasjonsteknologiske infrastruktur, oftest kjent som internett (Muller, 2016, s.3). Som faglig nisje er cybersikkerhet i konstant utvikling. Det finnes en rekke tilnærminger som står i motsetning til

hverandre. Sikkerhetsutfordringene krever dermed en grundig og bred forståelse av de forskjellige problemstillingene (Langø, 2013, s.229). Cybersikkerhet angår en rekke sektorer og ulike utfordringer (Langø & Sandvik, 2013, s.222), og handler med andre ord om sikkerheten vi har både i og gjennom cyberdomenet. Cybersikkerhet uttrykker hvordan vi kan opprettholde samfunnssikkerheten gjennom organisering, sikring av informasjon og integriteten til systemene (Muller, 2016, s.3). Reguleringen av dette er komplekst og består av en rekke nasjonale og internasjonale instrumenter. Dette innbefatter datalovgivning, menneskerettigheter, strafferett, sikkerhetslovgivning, krigens folkerett og stadig mer cyber-spesifikke standarder og normer (Sandvik, 2013, s.254).

3.2 Digitalisering og globalisering

Digitale nettverk er ryggraden i moderne samfunn. Det er et komplekst økosystem som er avhengig av en rekke aktører og tekniske løsninger. Alt digitaliseres og internett er antageligvis verdens viktigste infrastruktur (Svenungsen, 2019b, s.2). Den gjensidige avhengigheten betyr at grensene mellom de ulike sektorene viskes ut (Langø & Sandvik, 2013, s.222). Alle digitale nettverk er sårbare for ondsinnede handlinger og sårbare for infiltrasjon (Svenungsen, 2019b, s.3). Aktørenes motivasjon er ikke bare kommersiell vinning eller kriminalitet, men representerer også trussel mot statssikkerheten. At både statlige og ikke-statlige aktører operer om hverandre i både konflikt og fredstid, har gjort sikringen av cyberdomenet mer komplekst (Muller, 2019, s.289). Trusselen mot statssikkerheten *kan* rammes indirekte av ikke-statlige aktører som retter anslag mot samme type mål, med samme type virkemidler, som statlige aktører (Larssen, 2020, s.351). Det er likevel viktig å understreke at de fleste angrep som oppdages i Norge er kriminalitet (Røislien, 2020, s.214).

Digitaliseringen gir nye sårbarheter. Lange verdikjeder og avhengigheter i cyberdomenet gjør aktør- og trusselbildet i nåtidens konflikter svært sammensatt og dynamisk (Johnsen, 2013, s.242). Det produseres stadig nye metoder og programvare med formål å kompromittere styringssystemer og IKT infrastruktur. Disse sårbarhetene er årsaken til at vi stadig må oppdatere operativsystemer og applikasjoner for å hindre stjeling og manipulering av informasjon eller at styringssystemer settes ut av spill. Aktørene kan være stater, kriminelle eller andre med ulike motiv (Svenungsen, 2019b, s.4). De fleste angrepene representerer ikke trusler mot nasjonal sikkerhet på høyt nivå, men kan snarere karakteriseres som kriminell aktivitet. Å sikre seg mot slike hendelser krever tverretatlig og offentlig-privat samarbeid (Muller, 2019, s.293).

Internetts arkitektur er i liten grad konstruert for å ta hensyn til geografiske grenser. Dette utfordrer staters behov for kontroll og derav suverenitetshevdelse. «Cybersuverenitet» er et tilsvar på denne utfordringen og er i ferd med å endre internett slik vi kjenner det i dag (Svenungsen, 2019a, s.225). Med cybersuverenitet menes at stater etablerer egne nettverk med statlig kontroll (Svenungsen, 2019a, s.231). Staters søken etter kontroll uten å endre på internetts arkitektur er sammensatt da nettverket er

en sentral premissleverandør for økonomisk vekst og utvikling. Man kan spørre seg om «point of no return» er passert hva gjelder staters mulighet for kontroll.

3.3 Private selskaper

Sikkerhet i cyberdomenet er ikke et område som stater alene kan kontrollere da det er private selskaper som eier og kontrollerer infrastrukturen og teknologien (Singer & Friedman, 2014, s.197). Private selskaper, stiftelser og individer legger i stor grad premissene for hvordan internett fungerer og utvikles. Rundt 80% av internettets infrastruktur er i privat eie (Svenungsen, 2019a, s.238). Da kontrollen i stor utstrekning er i privat regi, samt at innovasjon og spisskompetansen ligger hos de multinasjonale tech-selskapene, oppstår en maktforskyvning. I tillegg må stater forsvare et bredere spekter og forholde seg til et større antall aktører, enten det er privat næringsliv eller fiendtlige aksjoner fra både statlige og ikke-statlige elementer (Langø, 2013, s.237). Da private selskaper i stor utstrekning kontrollerer utviklingen, samtidig som stater søker å legge til rette for økonomisk vekst, oppstår en avhengighet hvor stater gir vekk makt til privat sektor. Dette medfører at stater initierer samarbeidsinitiativer for å sikre effektivisering (Muller, 2016, s.11). Suverenitetshevdelse knyttes tradisjonelt mot selvbestemmelse innen et definert geografisk område, men på internett er kontrollen overlatt til ikke-statlige aktører og i tillegg grenseløst (Svenungsen, 2019a, s.225). Der hvor stater søker å sikre staten, samfunnet og individet, har privat sektor helt andre styringsparametere, profittmaksimering og selskapets markedsposisjon. Cybersikkerhet blir således en «business-case» hvor kontinuitet er målsetningen og ikke det statlige sikkerhetsperspektivet (Muller, 2016, s.12). Multinasjonale tjenesteleverandører har videre mulighet til å regulere og sensurere det som publiseres på deres plattform gjennom bruksregler og policy. En kan hevde at ytringsfriheten reduseres ved at det offentlige rom privatiseres (Steen-Johnsen, Enjolras & Wollebæk, 2013, s.267). Faren er at sosiale medieplattformer ikke styres etter demokratiske grunnprinsipper da maktkonsentrasjonen ligger hos private aktører og interesser (Steen-Johnsen et al., 2013, s.268).

Telenor kan tjene som eksempel på interessekonflikt mellom statens behov for sikkerhet og private selskapers "bunnlinje orientering". Selskapet, som har en sentral rolle innen norsk beredskap, avstår fra å knytte seg til Nasjonal Sikkerhetsmyndighets (NSM) overvåkningsarkitektur av kritisk infrastruktur. Selskapet hevder at dette vil være i konflikt med kundenes personvern (Muller, 2016, s.14). Selskapets interesser vurderes dermed opp imot stat- og samfunnssikkerheten og kundens personvern. Kundens rettsvern vektes tyngst (Telenor, 2015, s.13).

3.4 Sikkerhetisering av cyberdomenet

Den økende frekvensen av alvorlige cyberangrep gjør stor skade. At angripernes identitet er vanskelig å fastslå vanskeliggjør håndteringen. Kompleksiteten hindrer effektiv rettshåndheving da jurisdiksjonsspørsmål enten er uavklart eller begrensende for mottiltak (Sandvik, 2013, s.254). I dette vakuumet ser en eksempler på at myndigheter implementerer overvåkningssystemer på internett som

rettferdiggjøres ut ifra behov for å bekjempe terror og av sikkerhetshensyn (Steen-Johnsen et al., 2013, s.267). Skillelinjene viskes ut og militære operasjoner blir dermed vevet inn i sivilsamfunnets virksomhet. Trusselbildet endres som følge av cyberdomenets verdensomspennende utbredelse og endringen vil øke i omfang (Johnsen, 2013, s.249).

Utviklingen av effektive strategier for å sikre cybersikkerhet reiser kompliserte spørsmål om forholdet mellom militær og sivil makt, offentlig regulering og privat initiativ og nasjonale og overnasjonale institusjoner. Fagmiljøer og akademia har ulikt syn på hva trusler i cyber vil bety for sikkerhet nasjonalt og internasjonalt (Langø & Sandvik, 2013, s.221). I dette udefinerte trusselbilde operasjonaliseres trusselen ved at for eksempel NATO definerer cyber som et operasjonelt domene. Cyber blir i denne sammenheng militarisert og «våpenifisering» av domenet kan høyne risikoen for internasjonale konflikter (Svenungsen, 2019b, s.6). Forskningsinstituttet RAND påpekte allerede i 1996 at sårbarheten i IKT infrastrukturen var så stor, at et angrep kunne oppnå strategiske effekter. Cyberkrigføring ble i dette tidsrommet hevet opp på samme nivå som andre former for strategisk krigføring (Langø, 2013, s.232).

Buzan, Wæver & De Wilde (1998) argumenterer for et nytt rammeverk for analyse av sikkerhetsbegrepet. De mener at den tradisjonelle tilnærmingen hvor militærmakt og staten er de viktigste elementene i analyse av sikkerhet, nå også må omfatte aspekter som økonomi, miljøvern og sosiale forhold. Utgangspunktet og premissene for debatten om hvordan cybersikkerhet skal forstås, har i stor utstrekning sin opprinnelse i militærakademiske kretser i USA og konseptet Revolution of Military Affairs (RMA). Sentrale forskere tilknyttet de amerikanske forskningsinstitusjonene har i stor utstrekning satt narrativet om vår forståelse av cybersikkerhet (Langø, 2013, s.231). Forskerne kan på ingen måte sies å ta feil, men det er mangelfullt å kun ta utgangspunkt i cyberdomenet relatert utelukkende til militære forhold og bruk av makt. Med en slik tilnærming blir sikkerhetsbegrepet og den innholdsmessige betydning ensidig knyttet til statssikkerheten. Cyberdomenets natur er imidlertid ikke så enkelt å seksjonere opp og klassifisere. Når det i et militært perspektiv benyttes retorikk om fare for statens overlevelse, om forhold som i andre sammenhenger betraktes som «normaltilstand», oppstår sikkerhetisering av domenet (Buzan et al., 1998, s.24).

Utgangspunktet for cybersikkerhet blir i denne sammenheng da et spørsmål om statssikkerhet og trusselpersepsjonen av eksistensiell art. Tiltak, rolle og ansvar for å forebygge og håndtere situasjonen utfordrer på denne måten ellers forbudte og begrensede rammer som gjelder for hendelseshåndtering i fredstid. Narrativet som etableres er at ekstraordinære hendelser krever ekstraordinære virkemidler. Det er imidlertid ikke nok at trusselen beskrives, det er først når beskrivelsen aksepteres av beslutningstakere at det har skjedd en endring (Buzan et al., 1998, s.25).

Politikere, forskere og analytikere trekker frem cybersikkerhet som den nye store sikkerhetsutfordringen. Retorikken er sterk og det advares mot scenarioer som «cyber Pearl Harbor» eller «cyber 9/11». Flere forskere mener imidlertid at oppstyret rundt cybersikkerhet er dårlig belagt empirisk, og at cybertrusler er preget av uklar analyse og forståelse av truslene (Langø, 2013, s.233). Et tilbakevendende problem i diskursen er manglende empiri, at det rett og slett er for lite data til å trekke kvalitative konklusjoner. Informasjonsrevolusjonen går fort og bruk av tradisjonelle analytiske rammeverk som ikke tar hensyn til «nye» elementer ved cyber (Langø, 2013, s.235), kan snevre inn forståelsen og derav fremstille trusselen i et mangelfullt perspektiv. Forsvaret og etterretningstjenestene anerkjente dette domenet tidlig. De er således langt fremme kunnskapsmessig. Kunnskapen deles med andre myndigheter der hvor dette er mulig, men en utfordring er behovet for hemmelighold av operasjonelle grunner. Spesielt sikkerhetstjenestene operer i det skjulte med mindre kontroll og transparens enn andre myndigheter. Dette er utfordrende i cybersikkerhetssammenheng hvor informasjonsdeling er avgjørende (Singer & Friedman, 2014, s. 199-200).

Diskusjonen om cybermaktens virkning og bruk av forklaringsmodeller som har sitt utspring i konvensjonelle maktmidler, kan gjøre cybermakt mer forståelig. Men risikoen med et slikt utgangspunkt er at det kan gi ufullstendige analyser, fordi man tar utgangspunkt i andre maktformers premisser. Kompleksiteten og relevansen faller bort når ikke cyberdomenet blir definert som noe eget (Langø, 2013, s.236). Om cybersikkerhet blir tolket inn i «konvensjonelle» analyserammer utelates på veien spesifikke elementer som skiller dette domenet fra de øvrige.

Med basis i maktteori og retorikk som henleder mot eksistensielle scenario som krig, trekkes oppmerksomheten bort fra samfunnssikkerhetsdomenet. Trusselen beskrives som så overhengende at det må ekstraordinære virkemidler til for å løse krisen. Trussel mot statssikkerheten kan i en slik kontekst forstås som siste utvei og bør derfor ikke idealiseres. På samme måte kan også innenriksrelaterte trusler sikkerhetiseres. «Krigen mot narkotika og krigen mot terror» er eksempler på dette og gir på samme måte en beskrivelse om nødvendigheten av virkemidler som krever større handlingsrom og utvidede hjemler enn det eksisterende (Buzan et al., 1998, s.29).

At cyberdomenet omtales som grenseløst og derav ikke forholder seg til landegrenser eller sektorer, er et stående uttrykk som gjentas av den enkle grunn at det er sant. Skal man forstå dette domenets implikasjoner må det gjøres på fenomenets egne premisser, og ikke gjennom gamle fargede linser (Langø, 2013, s.238). Neste kapittel søker å forklare hvordan retorikken har betydning for klassifisering av truslene i cyberdomenet.

3.5 Retorikken påvirker klassifisering av trussel

Cyberkrig er en term som av mange oppfattes som et upresist begrep. Domenet omfatter et bredt spekter av trusler mot både stater og individer og treffer således i et videre omfang enn i det militære

domene. Det er svært sjelden at slike hendelser isolert kan kvalifisere som krigshandlinger i folkerettslig forstand (Svenungsen 2019b, s.6).

Definisjonen av cyberkrig varierer. Lewis (2011, s. 23-29) beskriver cyberkrig som bruk av teknologi og teknikker i den hensikt å skade, ødelegge eller forårsake tap av menneskeliv for å oppnå en politisk målsetning utført av stater. Lewis' definisjon følger dermed den Clausewitziske linje. Andre forskere er imidlertid ikke enig i dette utgangspunktet, da handlinger som ikke har et voldspotensiale ikke er en krigshandling. Handlingen må kunne settes i kontekst og aggressoren må gi seg tilkjenne, da poenget er å tvinge en part til å etterkomme motstanderens vilje (Rid, 2013, s.2). Cyberangrep betraktes dermed å ha et sekundært voldspotensial. Skal en handling klassifiseres som en krigshandling, må denne være voldelig, instrumentell og politisk (Rid, 2013, s.4).

I cyberdomenet er det vanskelig å skille mellom militære og sivile mål da samme nettverk benyttes av både militære og sivile. Noen systemer i nettverket er militære, mens majoriteten er sivile. Sivile systemer kan imidlertid være relevante og legale mål i en sikkerhetspolitisk konflikt. Denne dualiteten gjør at cyberdomenet undergraver antakelsen i internasjonal rett, at det er mulig å skille mål fra hverandre (distinksjonsprinsippet) (Drmola et al., 2015, s.25).

Å militarisere angrep i cyber medfører ikke bare utfordringer med identifisering, men også hvordan proporsjonalitetsprinsippet i Folkeretten skal forvaltes, og ikke minst hva som utgjør terskelen for respons (Kristiansen & Hoem, 2019, s.258). Usikkerhet, uklarhet og manglende presisjon på en hendelse i cyber gjør dermed begrepet cyberkrig vanskelig å omsette til politiske beslutninger. Kredibiliteten til den som beskriver trusselen blir dermed avgjørende, trusselbeskrivelsen må aksepteres av beslutningstakere (Buzan et al., 1998, s.33). En ytterligere utfordring er at sammenvevingen av nettverk og systemer medfører en risiko for dominoeffekt. Et angrep mot et militært mål kan også ramme flere sivile nettverk som ikke er omfattet av hensikt og intensjon. Dette kompliserer grunnleggende regler om målutvelgelse i cyberdomenet, da prinsippene om distinksjon, proporsjonalitet og beskyttelse av sivile er vanskelig å beregne. Dette kan også medføre uintenderte følgeskader av rettslig art som kan medføre nye konflikter som følge av en militær operasjon i dette domenet (Drmola et al., 2015, s.25).

En tradisjonell tilnærming til cyberangrep er dennes begrensninger til å være et effektivt tvangsmiddel, og dermed nytte som verktøy til å oppnå politiske mål. Fokuset på nødvendigheten av vold og kontroll er basert på tradisjonelle konflikter hvor erobring og underkastelse er de fremste strategiske målene for en militærkampanje. Men cyberkrigføring mangler landmaktens evne til å okkupere territorium og svekke fiendens moral. På grunn av sin operasjonelt distinkte karakter vil konseptet dermed være nødt til å være underlagt landstyrker for å oppnå kontroll (Langø, 2013, s.234-235). Cyber vil trolig være et

viktig element i en militær kampanje, men kan vanskelig isoleres fra øvrige maktmidler i militær sammenheng. Å militarisere domenet isolert fra disse eller ta utgangspunkt i maktteorien alene synes mangelfullt. Det teoretiske utgangspunkt kan dermed ha stor innvirkning på hvordan truslene i cyber klassifiseres og påvirkning av sikkerhetstenkningen på politisk nivå.

Attribusjon er en av de mest sentrale utfordringene i cyberdomenet. Neste kapittel beskriver mulige konsekvenser av at identifisering av bakenforliggende aktør er vanskelig.

3.6 Konsekvenser av manglende attribusjon

Attribusjonsproblematikken er i litteraturen et tema som diskuteres i sikkerhetspolitisk sammenheng. Med attribusjon menes å kunne fremstille ugjendrivelige bevis på at en spesifikk aktør står bak en handling (Kvernberg & Johnsen, 2013, s.18). Hvilke problemstillinger oppstår ved angrep som truer statssikkerheten hvor identifisering av aktør er vanskelig eller usikker? Det digitale rom er et domene som er vanskelig å kontrollere da det i sin natur er grenseløst og mulighetene til å skjule sin identitet gjør myndighetskontroll vanskelig.

Trusselbildet endres kontinuerlig. Etter den kalde krigen har utvidelse av markedsøkonomien ved global finans, investering og produksjon av varer og tjenester medført et utvidet sikkerhetsdomene (Buzan et al., 1998, s.211). Denne utvidelsen skaper et sikkerhetspolitisk paradoks. Om en stat blir utsatt for angrep oppstår en forpliktelse til å respondere for å ivareta egen kredibilitet. Imidlertid vil respons mot feil aktør eller hva som ansees som normativt proporsjonalt, ha motsatt effekt (Kristiansen & Hoem, 2019, s.258). Identifisering, eller attribusjon er dermed helt avgjørende.

Å avskrekke en fiendtlig aktør fra å gå til angrep er en av primærstrategiene innen sikkerhetspolitikken. En stats evne til å gjengjelde og påføre fienden så store tap at kostnadsratioen blir så høy at motstanderen avstår fra å angripe. Cyberdomenet skiller seg her vesentlig fra konvensjonell krise ved at motstanderen er meget vanskelig å identifisere. Kjernen er altså at man ikke vet hvem som står bak et angrep og derav hvilken intensjon, da er det vanskelig å avskrekke fra gjennomføringen av det (Muller, 2019, s.290). Avskrekking som strategi i cyberdomenet og utfordringene ved attribusjon, representerer et av de mest fremtredende problemene som blir identifisert og diskutert av både praktikere og akademikere i debatter om cyberavskrekkning (Muller, 2019, s. 290). Mangelen på en returadresse er til hinder for en troverdig avskrekkingsposisjon i cyber (Lynn III, 2010, s. 99). Rid referer til kjente cyberangrep som mot Estland i 2007 og Georgia 2008, og anfører at da angrepene ikke lar seg attribuere kan de heller ikke kategoriseres som en krigshandling (Rid, 2013, s. 6-8). Rid definerer dermed angrep i cyber ut ifra den tradisjonelle analyserammen om militærmakt og voldselementet.

Gjengjeldelse oppstiller krav til identifisering. Det påhviler den angrepne part en viss bevisbyrde dersom det skal utøse en proporsjonal reaksjon (Kristiansen & Hoem, 2019, s.258). Beviskravet legger strenge vilkår for hva og hvilke virkemiddel responsen kan bestå av. Mottiltak i cyberdomenet er i tillegg utfordrende i forhold til hva slags konsekvenser et motangrep kan ha, spesielt om risikoen ved å ramme sivil infrastruktur (Kvernberg & Johnsen, 2013 s.23). Fravær av beviser hindrer dermed muligheten til legitime og presise mottiltak, da en mistenkt aktør kan påberope seg plausibel fornektbarhet. Denne usikkerheten bidrar til å skape tvil om både de folkerettslige, politiske og etiske sidene ved å anklage en part for å stå bak. Dette handlingsrommet utnyttes, og manglende bevis kan hindre eller forsinke iverksetting av beredskapstiltak (Diesen, 2018, s.15).

Ved bruk av konvensjonelle våpen er identifisering av den som øver makt selve formålet for å påtvinge sin vilje, mens i cyber er det motsatt (Rid, 2013, s. 141-142), det vil si å påvirke uten å gi seg til kjenne. Dette er et "nytt" scenario og har innvirkning på utøvelse av sikkerhetspolitikken. Sikkerhetspolitikken har sitt fundament i trusselvurderinger. Der hvor det er tvil, i gråsonen mellom krig og fred, vil det i praksis være situasjonsforståelsen myndighetene har og hvorledes de klassifiserer krisen som er avgjørende (Simonsen, 2019, s.237). Attribusjonsutfordringene gjør det vanskelig å avgjøre om en krise er sivil eller sikkerhetspolitisk. Vår sikkerhetsarkitektur legger opp til at det er mulig å definere et slikt skille (Larssen, 2020, s.352). Manglende mulighet til presisjon og derav usikker identifisering tilsier anvendelse av «det minste ondes prinsipp», som går ut på at midlere alternativer må være forsøkt før selvforsvarsoperasjonen igangsettes (Simonsen, 2019, s.175).

For å kunne slå fast når cyberangrep er «krig», er det behov for å avklare hva slags maktbruk cyberangrep utgjør og hvilke hendelser som utløser retten til selvforsvar. Internasjonal lov om maktbruk og krigens folkerett er hjørnesteinene. Samspillet mellom rettslige normer, geopolitiske begivenheter og cyberkrigdiskursen, domineres av sikkerhetseksperter og det voksende militær- og sikkerhetsindustrielle miljø. Debatten preges av forsøk fra militære, politiske og kommersielle aktører på å flytte cybersikkerhetsproblematikken over i krigføringsdomenet (Sandvik, 2013, s.253). Her oppstår det et spenningsforhold. Denne utviklingen kan bidra til å skape større statlig og militær kontroll som utfordrer hensynet til privatlivets fred og andre sentrale politiske og sosiale menneskerettigheter (Sandvik, 2013, s.260). Å ikke handle på en trusselsituasjon med henvisning til at identifisering ikke lar seg gjøre, er problematisk. I slike gråsonetilfeller kan det være hensiktsmessig og sågar påkrevet, at både Forsvaret og politiet agerer ut ifra sine primæroppgaver med hjemmel i sine respektive rettsgrunnlag. Dette stiller krav til at etatene evner å samarbeide og samvirke til landets og borgernes beste (Simonsen, 2019, s.385).

Neste kapittel omhandler koordineringsutfordringer som kan oppstå når det ikke klart fremkommer hvem som har ansvaret og hvordan denne utfordringen søkes løst.

3.7 Koordinerings- og rolleutfordringer i cyberdomenet

Etter den kalde krigen har sikkerhetsbegrepet utvidet seg. Fra et ensidig fokus på militære aspekter til samfunn og individ. Det omhandler nå sikkerhet innen flere sektorer på flere nivåer. Blant forskere og politikere i den vestlige verden har sikkerhet i sin tradisjonelle betydning, forstått som statens militære sikkerhet, mistet sitt primatur (Kjølberg & Jeppesen, 2001, s.20). Økonomiske verdier har videre fått en mer dominerende plass i verdihierarkiet. Dette medfører at trusler mot utvikling og velstand innlemmes i sikkerhetspolitikken (Kjølberg & Jeppesen, 2001, s.21).

Ved å sikkerhetisere områder som tradisjonelt ivaretas av sivile myndigheter, står man i fare for å overlate samfunnets debatt om hva som utgjør en trussel mot staten, til sikkerhetsmyndighetene. En konsekvens kan være at den demokratiske debatt uteblir (Rottem, 2007, s.52). Når myndigheter velger å definere noe som et sikkerhetsproblem, innebærer det implisitt at løsningen finnes i sikkerhetspolitikkens repertoar (Kaufmann, 2018, s. 21-31). Utvidelsen av sikkerhetsbegrepet innebærer imidlertid nå også forsvar av vitale verdier generelt og ikke bare mot militære trusler spesielt. Det omfatter ikke bare forsvar av territorium, men også samfunnssystem og velstand (Kjølberg & Jeppesen, 2001, s.18).

På nasjonalt nivå er ansvaret for cybersikkerhet i Norge i stor grad desentralisert og organisert etter sektorprinsippet (Langø, & Sandvik, 2013, s.225)**.** Digitaliseringen gir utviklingstrekk som henger tett sammen og som er vanskelig å skille fra hverandre. Samarbeid på tvers av alle sektorer i samfunnet er derfor nødvendig. Offentlig-privat samarbeid og sivilt-militært samarbeid i tillegg til internasjonal samhandling. Koordineringsutfordringene er store (Svenungsen, 2019b, s.7).

Forskning viser at manglende overnasjonal rollefordeling mellom myndigheter internt og mellom offentlig og privat sektor svekker sikkerheten i cyberdomenet. Myndighetene samarbeider i stor grad på ad hoc basis og sikkerhetstenkningen i private selskaper er dimensjonert etter lønnsomhetshensyn (Jensen, 2019, s.270). I diskusjoner om hvilke styringsform som sikrer cybersikkerhet er den såkalte «multistakeholder-modellen» det store mantraet. En åpen form for samarbeid basert på likeverdige partnere. Grunntanken er at samarbeid mellom private og offentlige aktører gir den beste formen for styring og sikring i cyber. Mye tyder på at denne modellen fungerer suboptimalt (Muller, 2016, s.2). Sektor- og ansvarsprinsippet har både en styrke og svakhet da den enkelte gis et selvstendig ansvar for egen virksomhet, mens desentralisering samtidig hindrer koordinering og beslutningsmyndighet på tvers av sektornivåene. Det som er best for en sektor er nødvendigvis ikke best for landet (Svenungsen 2019b, s.8).

Mangfoldet av aktører i cyber gjør at myndigheters forsøk på å etablere sikkerhet blir fragmentert. Nye etater og prosjekter etableres, ofte med et uklart mandat og myndighetsområde (Singer & Friedman,

2014, s.199). Fremveksten av en rekke koordinerende institusjoner som ikke er tildelt myndighet over sektornivået kan være en svakhet i den norske sikkerhetsarkitekturen (Svenungsen 2019b, s.8). Tverrsektorielle myndigheter er bra for å etablere et nasjonalt situasjonsbilde, men uten tvangshjemler vil slike organisasjoner ha liten effekt i hendelseshåndtering (Singer & Friedman, 2014, s. 200).
Felles cyberkoordineringssenter (FCKS), Nasjonalt cybersikkerhetssenter (NCSC) og Felles kontraterrorsenter (FKTS) er eksempler hvor det reises spørsmål om hva disse sentrene faktisk kan oppnå, og om opprettelsene er et symptom på et problem, mer enn en løsning (Friis & Hansen, 2020, s.188).

Erfaringer fra alle de nordiske land viser store utfordringer med sektoransvar innen cyberområdet. Det er behov for klarere oppgave- og ansvarsplassering for å styrke motstandsdyktigheten (Jensen, 2019, s.267). Vår bruk av teknologi og dennes stadige utvikling gjør det vanskelig å forutse fremtidens sårbarheter og trusler. Dette skaper implikasjoner for hvordan stater organiserer sikkerhet i cyberdomenet. Det er nødvendig med en dynamisk politikk og fokus på både teknologi og organisatorisk innovasjon (Langø, 2013, s.238). Her ligger kjernen i statens utfordring. Hvordan fordele oppgaver og plassere ansvar når sektoransvaret skal administreres i praksis (Jensen, 2019, s.274). Flere aktører påpeker svakheter med en sektorprinsipiell tilnærming. Anførslene har sin begrunnelse i at angrep ofte går på tvers av sektorer, noe som igjen krever ustrakt samarbeid og informasjonsdeling. Nettopp informasjonsdeling fremheves som særlig vanskelig (Langø & Sandvik, 2013, s.226).

Den sektorovergripende utviklingen innebærer at en rekke samfunnsaktører har behov for informasjon om trusselen (Jansen & Haugestad, 2020, s.163). En effektiv krisehåndtering i cyberdomenet forutsetter deling av informasjon og kollektiv innsats (Røislien, 2020, s.215). At dagens organisering i hovedsak legges til etterretning- og sikkerhetstjenestene (EOS) reiser dermed en rekke problemstillinger, både hva gjelder disse tjenestenes behov for hemmelighold og statens forpliktelser til transparens og legale rammer i form av informasjonsinnsamling og overvåkning av egne borgere (Singer & Friedman, 2014, s.199). Mangelfull forståelse mellom de ulike aktørene medfører maktkamper og interessekonflikter. Sektorinndelingen bidrar dermed til å øke heller enn å svekke maktkampene mellom aktørene, både statlige og private. Denne formen for styringsrasjonalitet gjør statens rolle mindre sentralisert og mer nettverksbasert (Muller, 2016, s.2-4). Endringer i lovverket er et steg mot tydeliggjøring av ansvar i cyberdomenet, men også dette møter kompliserte hensyn og skaper uklare roller (Muller, 2016, s.17).

Sikkerhet i cyber angår hele samfunnet og sikkerhetsarkitekturen må derfor ta opp i seg bredden og ikke utvalgte sektorer. En sektor kan ikke bære ansvaret alene. Cybersikkerhet må kobles til andre domener av nasjonal makt i et nøye overveid rammeverk, ikke kun de militære aspekter (Muller, 2019, s.294). Cybersikkerhet og retorikken rundt truslene i dette domenet blir i stor grad kontekstuelt

definert som en trussel mot statssikkerheten og dermed sikkerhetisert. På denne måten avskjæres øvrige sektorer, noe som vanskeliggjør overordnet organisering sett hen til ulike hjemmelsgrunnlag og begrensninger i myndighetsområde. Når vi snakker om nasjonal sikkerhet er det militærmakten som vektlegges (Svenungsen, 2019a, s.235). Et betimelig spørsmål er om våre etterretningstjenester i for stor grad setter agendaen i sikkerhetsspørsmål gjennom sine overordnede analyser av trusselbildet (Maaø, 2020, s.125).

Det er ovenfor redegjort for hvordan utfordringene i cyberdomenet beskrives i faglitteraturen. Neste kapittel ser på hvordan myndighetene selv beskriver utfordringene. I hvor stor grad er det sammenheng mellom teoretiske innsikter og anvendt forståelse av truslene, og hvordan dette eventuelt har betydning for myndighetenes situasjonsforståelse og beslutninger.

4 Cybersikkerhet i åpne trusselvurderinger

Trusler i cyberdomenet er ikke et helt nytt fenomen. Bruk av skadevare for å sette en virksomhet, stat eller organisasjon ut av spill har siden begynnelsen av 2000 tallet økt i omfang og skadepotensiale. Av nyere hendelser som har rammet Norge er Helse Sør-Øst saken i 2017 hvor datasystemet ble utsatt for en omfattende nettverksoperasjon, da Hydro i 2019 ble infisert av et løsepengevirus, samt kompromitteringen av flere epostkontoer i Stortinget i 2020. Dette er kun et utvalg av hendelser som beskriver hvor potent og mangespektret nettverksangrep kan være.

Terrorangrepet mot USA 11. september 2001 har videre medført et radikalt skifte i den globale sikkerhetspolitikk hvor grensesnittet mellom terror og krig snart er visket ut. Uforutsigbarhet, ustabilitet og fremveksten av grenseoverskridende terrortrusler preger sikkerhetssituasjonen i stadig større grad. En konsekvens er at etterretningsbehovene øker. Beslutningsgrunnlaget som forelegges myndighetene er avgjørende for valg av tiltak og er et viktig premiss for å unngå at militære operasjoner gjennomføres i strid med krigens folkerett og politiske og militære målsettinger (Forsvarsdepartementet, 2018, s.24).

PST sitt grensesnitt mot politiet er vesentlig å påpeke. Tjenesten er direkte underlagt Justisdepartementet (Justisdepartementet, 2005, §2) og ikke Politidirektoratet. Enheten er primært en sikkerhetstjeneste. PST kan bistå politiet, men deres viktigste samarbeidspartnere er Etterretningstjenesten og NSM, i tillegg til andre lands etterretnings- og sikkerhetsmyndigheter (Justisdepartementet, 2005, §§ 10,11). Da det er vanskelig å skille terror fra organisert og annen alvorlig kriminalitet, er Kripos og PST underlagt samme statsadvokatembete (Påtalemyndigheten, 2020). Det innebærer at PST har et viktig, men avgrenset ansvarsområde for trusler mot rikets sikkerhet. Forebygging, etterforskning og iretteføring av øvrig kriminalitet hører dermed inn under

politiets oppdragsportefølje. Dette er en viktig distinksjon når ansvar og organisering av samfunnets samlede ressurser diskuteres.

Analysen omfatter EOS tjenestens trusselvurderinger fra 2011 til 2020 med fokus på trusler i cyberdomenet. Hvilken plassering og rolle kan en se av rapportenes oppbygning og omfang av sin beskrivelse av trusler i cyberdomenet? Det finnes en rekke trusselvurderinger og utredninger, men det er Politiets sikkerhetstjeneste, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet som danner stammen i beskrivelsen av det norske trusselbilde. Sikkerhetspolitikken har sitt fundament i trusselvurderinger. I praksis er det den situasjonsforståelsen myndighetene har og hvordan de klassifiserer krisen som det avgjørende (Simonsen, 2019, s.237). Analysen søker å operasjonalisere problemstillingens første del, et trusselbilde i endring.

4.1 Etterretningstjenesten

Etterretningstjenesten er Norges utenlandsetterretningstjeneste. Tjenestens hovedoppgave er å varsle om ytre trusler mot Norge og prioriterte norske interesser og understøtte politiske beslutningsprosesser innen norsk utenriks-, sikkerhets- og forsvarspolitikk (Etterretningstjenesten, 2020, s.2). Utenlandsetterretning står sentralt i en globalisert verden. Maktstrømninger og endringer i den sikkerhetspolitiske sfære får konsekvenser for hvordan staten organiserer og tilpasser seg. Trusselvurderingene fra Etterretningstjenesten har derfor en sentral plass i vår forståelse av trusselbildet. Som omtalt i kapittel 3.5, har forsvarsmakten høy kunnskap om hvilke endringer cyberdomenet representerer.

Tjenestens beskrivelse av trusler i det digitale rom har gradvis økt i omfang. I perioden 2011 – 2017 ble imidlertid denne trusselkategorien omtalt i korte trekk og helt sist i rapportene. Beskrivelsen av cybertrusselen har de senere år vokst til å få en sentral plassering i vurderingene. Gjennomgangen viser at trusler i det digitale rom og variablene av angrepsmetoder tiltar og at cyberdomenet ikke er adskilt fra andre virkemidler, men settes i sammenheng. Trusselvurderingen av 2020 går lenger enn noen gang med å nyansere dette bildet. Her konkluderes det med at teknologien medfører et skifte i form at ikke-militære virkemidler i økende grad kan brukes som et alternativ til militær makt i forfølgelse av målene. Nettverksoperasjoner, økonomisk maktbruk og desinformasjonskampanjer er alle eksempler på disse endringene (Etterretningstjenesten, 2020, s.9).

Trusselvurderingenes beskrivelse av aktører favner vidt, fra andre lands etterretningstjenester, organiserte kriminelle, hackere og konkurrerende forretningsvirksomheter. Allerede i 2011 poengterer tjenesten at de mest sofistikerte og derav alvorligste truslene kommer fra andre stater som utnytter datamaskiner og datanettverk til etterretningsvirksomhet (Etterretningstjenesten, 2011, s. 31). Aktørenes motiver omfatter idealisme, terrorisme, økonomi, kriminalitet og sikkerhetspolitiske hensyn (Etterretningstjenesten, 2014, s.59).

I hele den analyserte perioden omtales statlige aktører som primærtrusselen. Vurderingen er at det er statlige aktører som har størst kapasitet til å utvikle avanserte digitale kapasiteter (Etterretningstjenesten, 2014, s.59), men at også kriminelle og terrorister i økende grad tar i bruk teknologi for å oppnå sine mål (Etterretningstjenesten, 2014, s.60). Tjenesten beskriver at i dag opererer stater, amatører og svært kompetente kriminelle om hverandre i cyberdomenet. Noe som medfører at det er komplisert å identifisere aktør. Dette skaper et uoversiktlig trussellandskap (Etterretningstjenesten, 2020, s.73). Fra 2012 til dags dato fremheves Russland og Kina som de største trusselaktørene. Spesielt Russland omtales som en aktør som tidlig anerkjente cyber som et viktig domene i militær sammenheng. Dette kommer klart til uttrykk ved å stadfeste at et angrep i cyber, kan betraktes som en krigserklæring (Etterretningstjenesten, 2013, s.44).

Tjenesten omtaler tidlig at digitaliseringen gir et komplekst modusbilde. Utfordringen er attribusjon. Det benyttes ofte stedfortredere og krypteringsmulighetene er mange. Mulighetene for å stille aktørene til ansvar eller å gå til motreaksjon reduseres dermed (Etterretningstjenesten, 2012, s.27), og risikoen for sanksjoner er liten (Etterretningstjenesten, 2017, s.34). Endringen bruk av teknologi representerer, gjør at geografisk avstand ikke lenger er en avgjørende faktor, internett løser på langt vei denne problemstillingen. Geografisk nærhet er dermed av mindre betydning. Trusselen fra andre mer fjerntliggende stater er nå en realitet. Kina har som en av verdens største økonomier globale interesser og benytter ofte stedfortredere til å innhente informasjon (Etterretningstjenesten, 2013, s.44; Etterretningstjenesten, 2015, s.84).

Begrepet hybride trusler omtales ikke spesifikt i trusselvurderingene, men bruk av digitale virkemiddel i kombinasjon med andre mer tradisjonelle tiltak som militære og politiske, antas å gi betydelig effekt (Etterretningstjenesten, 2014, s.60). Ukraina-konflikten trekkes frem som eksempel på denne kombinasjonen av handlemåter da Russland benyttet nettverksoperasjoner som et destabiliserende tiltak (Etterretningstjenesten, 2015, s.85). Påvirkning og provokasjoner i sosiale medier gir videre mulighet til å skape spenning i det politiske og militære domene. Usikkerhet rundt hvem som er aktør og med hvilken intensjon er dermed med på å utvide gråsonen mellom fred, krise og krig (Etterretningstjenesten 2017, s. 34; Etterretningstjenesten, 2018, s. 28). Anslag mot grunnleggende nasjonale funksjoner som kritisk infrastruktur innen Telecom, kraftforsyning, betalingstjenester og politiske beslutningsorganer vil kunne forårsake betydelig skade (Etterretningstjenesten, 2015, s.85).

Attribusjonsproblematikken adresseres allerede i 2012 og tjenesten peker på behov for samarbeid på flere nivå innen sivil og militær sektor – sikkerhetsmyndigheter, politi og etterretningstjenesten (Etterretningstjenesten, 2012, s.27). Trusselbildet utvikles i takt med digitaliseringen i verden og Etterretningstjenesten peker på at et generelt trekk er at stater i større grad enn tidligere støtter

kommersielle interesser som driver etterretningsvirksomhet. Dette gir et uklart og komplekst fiendebilde. Sabotasjehandlinger rammer både sivilt og militært i det digitale rom (Etterretningstjenesten, 2016, s.82). I årets trusselvurdering fremmer tjenesten at truslene blir stadig mer sektorovergripende og at angrep også rammer sivil infrastruktur. Handlingsrommet til både statlige og ikke-statlige aktører har vokst som følge av den teknologiske utviklingen (Etterretningstjenesten, 2020, s.6).

Oppsummert har beskrivelsen av digitale trusler i perioden 2011 frem til i dag økt i omfang og detaljeringsnivå i trusselvurderingene. Fra å bli noe stemoderlig nevnt sist i vurderingene, til etter 2017 å bli omtalt tidlig. Dette er en indikasjon på hvordan tjenesten i økende grad ser cyber som et område av betydning hva gjelder norsk sikkerhet i stort. I innledningen til FOKUS 2020 beskrives trusselbildet som mer sammensatt og kompleks enn noen gang (Etterretningstjenesten, 2020, s.6). Dette antyder at Etterretningstjenesten anser trusler i cyber som sentralt i sitt oppdrag å ivareta Norges suverenitet, handlefrihet og integritet. Etterretningstjenestens vurderinger i den analyserte tidsperioden referer gjennomgående til de andre tjenestenes vurderinger. Endringer i trusselbildet omfatter glidende overganger mellom indre og ytre sikkerhet som følge av økt angrepsflate og globalisering. Det innebærer at det i liten grad er formålstjenlig å skille mellom statlige og private interesser når det gjelder vurderinger som har betydning for Norges nasjonale sikkerhet (Etterretningstjenesten, 2020, s.9). Tjenesten nyanserer i 2020 at trusselpotensialet også eksisterer utenfor det man tradisjonelt har orientert seg rundt, nemlig statlige virksomheter.

4.2 Politiets sikkerhetstjeneste

PST har ansvar for å forebygge og etterforske straffbare handlinger mot rikets sikkerhet og har derav påtalekompetanse. Trusselvurderingene omhandler forhold som kan skade nasjonale interesser og påvirke norsk sikkerhet. Vurderingene omhandler både statlige og ikke-statlige aktører (PST, 2020b, s.1). Politiets sikkerhetstjeneste har innelandsetterretning som sitt primære ansvarsområde. Tjenesten har i den analyserte perioden hatt økende oppmerksomhet på utviklingen i det digitale domene. En mulig årsak er at Norge er et av de mest digitaliserte land i verden.

PST predikerer i 2011 at datanettverksoperasjoner vil bli en stadig viktigere metode fra andre lands etterretningstjenester, men at cyberetterretning ikke erstatter tradisjonell etterretningsvirksomhet – den er et tillegg til annen tradisjonell informasjonsinnhenting (PST, 2011). Økt kapasitet innen cyberetterretning fra statlige aktører gir nye muligheter for informasjonsinnhenting og sabotasje mot vårt digitaliserte samfunn (PST, 2011). I trusselvurderingen av 2014 fremheves avsløringene av datanettverksbaserte etterretningsoperasjoner som en beskrivelse på hvor omfattende og kompleks etterretningsvirksomheten mellom stater er. I tillegg til det tekniske potensiale metoden gir for å tilsløre identitet og aktivitet (PST, 2014, s.8).

I 2019 omhandles nettverksoperasjoner for første gang i eget kapittel. Statlig styrte nettverksoperasjoner fremheves som en vedvarende trussel mot norske verdier (PST, 2019c, s.8). PST løfter dermed frem trusselen i cyber som et mer selvstendig tema og ikke kun en alternativ metode innen statlig etterretningsvirksomhet. Opinionspåvirkning og kartleggingsoperasjoner rettes nå mot konkrete virksomheter og personer (PST, 2019c, s.10). Denne utviklingen representer dermed en ny og mer selvstendig trussel som det er vanskelig å føre bevis for hvem som faktisk står bak.

Årets trusselvurdering (2020) har ny struktur sett i forhold til de siste 5-6 år. Trusselen i det digitale rom er ikke lenger et eget kapittel, men er inkorporert som en faktor som gjør seg gjeldene i hele trusselbildet. Konsekvensene av at digitaliseringen av samfunnet gir nye og mer komplekse sårbarheter og muliggjør påvirkning av opinion og politiske strømninger, sabotasje og skade på kritiske samfunnsfunksjoner. Risikobildet PST beskriver kan derfor hevdes å ha endret karakter de siste år. Nå omtales trusselen i det digitale rom først og i innledningen som en faktor som påvirker alle PSTs ansvarsområder (PST, 2020b, s.2).

Tjenesten sitt aktørfokus er mangfoldig, men trusselen fra ekstreme islamistiske aktører ansees som den primære (PST, 2017, s.13). Fiendebildet som trekkes opp samsvarer med Forsvarets etterretningstjeneste og det henvises gjennomgående til disse vurderingene. Russland og Kina fremheves som sentrale aktører ved siden av ekstreme islamister. Russland identifiseres som den med størst skadepotensiale (PST, 2018, s.7). Den russiske okkupasjonen av Krim-halvøya og Russlands innblanding i politiske prosesser i Ukraina, trekkes frem som bevis på vilje til å benytte et mangfold av virkemidler for å oppnå sin intensjon (PST, 2015, s.11). Tjenesten viser til at russiske og kinesiske aktører har forsøkt å kompromittere datasystemer som forvalter grunnleggende nasjonale verdier i Norge (PST, 2017, s. 9). PST viser til at andre lands etterretningstjenester benytter kriminelle aktører for å skjule sine operasjoner og derav intensjon (PST, 2020b, s.10).

PST beskriver endringene i det komplekse modusbilde og skiftet digitaliseringen representerer. Datanettverksoperasjoner og trusselen mot kritisk infrastruktur fremheves som en etterretningsmetode i sterk utvikling med stort skadepotensiale i hele spekteret av norske interesser (PST, 2015, s.12). Spionasje i det digitale rom er nå en integrert kapasitet i andre staters etterretningstjenester. Det vises til at metoden er kostnadseffektiv og har potensielt et høyt etterretningsutbytte og er derav potent til å skade grunnleggende nasjonale interesser. Digitale angrep er vanskelig å forutse og kan slå ut kritisk infrastruktur – og forårsake betydelig skade (PST, 2016, s.8). En tiltakende metode er andre staters forsøk på å påvirke mediebildet ved å plante falske dokumenter, falske nyhetsoppslag og støtte nettrollaktivitet (PST, 2017, s.9-10). PST konkluderer med at datanettverksoperasjoner i dag utgjør en vedvarende trussel mot Norge. Landegrenser er ingen begrensing og en aktør kan med stor grad av anonymitet og mulighet for benektelse, stjele, manipulere sensitiv informasjon og skade kritisk

infrastruktur. Konsekvensen er at datanettverksoperasjoner i dag kan påføre stat og samfunn skade og ødeleggelse som tidligere kun var mulig ved bruk av militærmakt (PST, 2020b, s.9). Digitaliseringen gir dermed et omfattende og mangespektret trusselbilde. Sammenvevingen av kapasiteter og tjenester gjør hele samfunnet til et mål for statlige etterretningsorganisasjoner. Dette som følge av at en rekke virksomheter og næringer er helt avgjørende for at samfunnet skal fungere og kan derfor karakteriseres som sikkerhetsrelaterte mål (PST, 2020b, s.9).

Oppsummert har PST beskrevet trusselen fra andre staters etterretningstjenester mot norske interesser og ekstrem islamistisk terror som den største trusselen i den analyserte perioden. Årets trusselvurdering tilkjennegir imidlertid digitalisering og globalisering som en gjennomgående faktor for hele trusselbildet. Kryptering og bruk av stedfortredere gjør videre attribusjon utfordrende. Den mer tradisjonelle oppstilling av fiendebildet nyanseres som følge av denne utviklingen. Informasjon, økonomisk vekst og teknologi, fremheves som faktorer som påvirker balansen innen sikkerhetspolitikken.

4.3 Nasjonal sikkerhetsmyndighet

NSM er Norges fagmyndighet for forebyggende nasjonal sikkerhet. NSM har nasjonalt ansvar for å detektere, varsle og koordinere håndtering av alvorlige IKT-angrep, samt gi råd og føre tilsyn med sikring av informasjon, objekter og kritisk infrastruktur (NSM, 2020, s.2). NSM avgir årlig en gradert rapport om sikkerhetstilstanden til Forsvarsdepartementet og Justisdepartementet. Selv om tjenesten rapporterer til etater som har forskjellig sektoransvar er fellesnevneren at fokuset er innen etterretnings- og sikkerhetsdomenet. Rapportenes formål er å redegjøre for etterlevelsen av sikkerhetsloven med forskrifter, samt gi en vurdering av sårbarheter og verdier i samfunnet som må beskyttes mot spionasje, sabotasje og terror. Vurderingene skal danne grunnlag for beslutningstakere for å iverksette tiltak for å redusere risiko i både privat og offentlig sektor (NSM, 2015, s.2). NSM sitt oppdrag omfatter både stat- og samfunnssikkerheten. Trusselbildet sees dermed i en videre kontekst enn Etterretningstjenesten og PST da utfordringene i det digitale rom går på tvers av stater, sektorer og virksomheter. Tjenesten poengterer at strategiske valg og tiltak fra myndighetene for å redusere denne risikoen er avgjørende (NSM, 2017, s.4).

Myndighetens beskrivelse av utviklingen i cyber kommer tydelig frem i trusselvurderingene. NSM har god informasjonstilgang som følge av sitt oppdrag gjennom overvåkning av kritisk infrastruktur. NSM viser tidlig til at Norge er et av verdens mest digitaliserte land og at den gjensidige avhengigheten mellom samfunnskritiske funksjoner går på tvers av sivil-militære og offentlig-private virksomheter (NSM, 2011, s.6; NSM, 2012, s. 6). Skillet mellom stats- og samfunnssikkerhet er mer glidende enn for bare få år siden (NSM, 2019b, s.9). NSM påpeker at en effekt ved at digitaliseringen øker, er at dataakkumulasjon stiger hver dag og nye avhengigheter skapes. Trusler mot våre viktigste funksjoner, systemer og infrastruktur i form av spionasje og potensielt sabotasje dominerer. Den nye

sikkerhetsloven tar opp i seg mangfoldet og har derfor et større virkeområde enn tidligere. Loven griper inn i samfunnssikkerhetsdomenet og omfatter nå også samfunnets grunnleggende nasjonale funksjoner og befolkningens grunnleggende sikkerhet. Rekkevidden til loven er dermed ikke avgrenset mot skjermingsverdige statlige virksomheter (NSM, 2019b, s.23).

NSM følger Etterretningstjenesten og PST sine analyser og legger tidlig til grunn at det er andre staters etterretningstjenester som representerer den største trusselen. Begrunnelsen som gis er at virkemidlene som benyttes er kostbare og ressurskrevende (NSM, 2011, s.8). Også NSM peker ut Russland og Kina som hovedaktørene i cyberdomenet mot norske interesser, men poengterer manglende kunnskap om angrep mot sivile virksomheter (NSM, 2014, s.5). NSM vurderer at den høyeste IKT risikoen mot offentlig forvaltning er fra nettverksoperasjoner hvor fremmede stater står bak (NSM, 2017, s. 8). Samtidig er vurderingen at det store volumet av IKT-hendelser i Norge er kriminalitet med økonomisk vinning som formål (NSM, 2017, s.18). At informasjonsmengden øker kraftig, både i volum og verdi, reiser nye problemstillinger. Aktører som Google og Facebook sitter på store mengder data om nordmenn og norske forhold (NSM, 2019b, s.9). At multinasjonale selskaper eier og forvalter slik informasjon reiser nye spørsmål relatert til motstand mot påvirkning og manipulasjon - som i ytterste konsekvens kan ha innvirkning på statens politiske klima og beslutningsprosesser (NSM, 2020, s.31).

Myndigheten vurderer at det komplekse modusbildet gir manglende risikoerkjennelse og ledelsesinvolvering. Følgen er at grunnleggende IKT sikkerhetstiltak ikke gjennomføres og sårbarheten i det norske samfunn øker (NSM, 2014, s.8). NSM påpeker i 2016 at fravær av verdivurderinger, risikovurderinger og risikoforståelse gjør at risiko ikke blir akseptert med den følge at det ikke iverksettes tilstrekkelige tiltak for å redusere sårbarheter mot spionasje (NSM, 2016, s.24). Kompleksiteten i cyber kan være en av årsakene til at store deler av samfunnet er i utakt med sikkerhetstenkningen med den konsekvens at sårbarheten øker. NSM benytter begrepet hybride trusler og at denne metoden visker ut det tradisjonelle skillet mellom fred og krig med den følge at tradisjonell ansvarsplassering mellom sivil og militær sektor utfordres (NSM, 2017, s.4). Deteksjon og motstand mot hybride trusler krever at den enkelte virksomhet kjenner sin verdi og funksjon i samfunnet. Næringslivet er en sentral medspiller i sikkerhetsarbeidet som forvalter av viktige samfunnsfunksjoner og leverandør av varer og tjenester til offentlige etater (NSM, 2019b, s.6).

Oppsummert konkluderer NSM med at statlige aktører representerer den største trusselen mot Norges sikkerhet, og Russland og Kina identifiseres som de viktigste aktørene. Da NSM sitt ansvarsområde omfatter både forsvars- og justissektoren, favner risikobildet hele spekteret innen stat- og samfunnssikkerhet. Vurderingene omhandler derfor også andre sivile aktører og virksomheter som påvirker risikobildet. NSM går lenger enn Etterretningstjenesten og PST i sin beskrivelse av IKT-sikkerhet i stort. Myndighetens ansvar for at alle sektorer oppfyller sine plikter etter sikkerhetslovens

bestemmelser (Sikkerhetsloven, 2019, § 2-2), gir et presist grunnlag for å vurdere trusselbildet i cyberdomenet. Truslene mot norske verdier beskrives som dynamiske som følge av at den teknologiske utviklingen skjer raskt. NSM peker også på at virksomheter og funksjoner på tvers av samfunnet er avhengig av hverandre i større grad nå enn før, og at dette skaper en rekke gråsonescenarioer.

I de neste to kapitelene sees det på likhetstrekk, utvikling og konklusjoner, før det avsluttes med en delkonklusjon som oppsummerer hovedkapittel 4.

4.4 Statlige aktører utgjør den største trusselen

Alle tre tjenestene sine vurderinger har likelydende konklusjoner hva gjelder aktørbeskrivelse. Det er bred enighet om at trusselen er størst fra andre staters etterretningstjenester. Teknologi og kapasitet til å utvikle sofistikerte angrep vurderes å kreve både tilgang på kunnskap og materiell som kun stater antas å besitte. Alle vurderingene belyser angrepene i perioden 2007 til 2015 som statlig virksomhet og ikke kriminalitet. I tidsrommet 2016 – 2020 vurderes angrepene imidlertid ikke kategorisk hva gjelder aktør. I norsk sammenheng vises det til Helse Sør-Øst og Hydrosaken i henholdsvis 2018 og 2019. Begge disse sakene etterforskes som kriminalitet av politiet. Analysene er i de senere år ikke like definitive i sin aktørbeskrivelse da flere nettverksangrep treffer globalt og påvirker en rekke virksomheter og nasjoner. Eksempler på dette er WannaCry som rammet både Storbritannia, Russland, Ukraina, India og Taiwan og virus og tjenestenektangrep mot selskaper som Twitter, Amazon og Spotify i 2016, samt MAERSK i 2017 (Etterretningstjenesten, 2020, s.78-79).

Teknologiutviklingen skjer raskt og tilgjengeligheten til skadevare og kunnskap gjør at nettverksoperasjoner benyttes som metode av både statlige og ikke-statlige aktører. En ser en likeartet tendens i alle tjenestenes vurderinger. Flere aktører, større angrepsflate og sammenvevingen av digital infrastruktur gjør trusselbildet komplekst. At alle tjenestene i stor utstrekning konkluderer likt kan være et kvalitetstegn, men også indikere en svakhet. Norske myndigheters persepsjon av trusselbildet baseres så og si utelukkende på EOS tjenestene sine vurderinger. Spørsmålet er om dette er tilstrekkelig til å gi et fullstendig bilde.

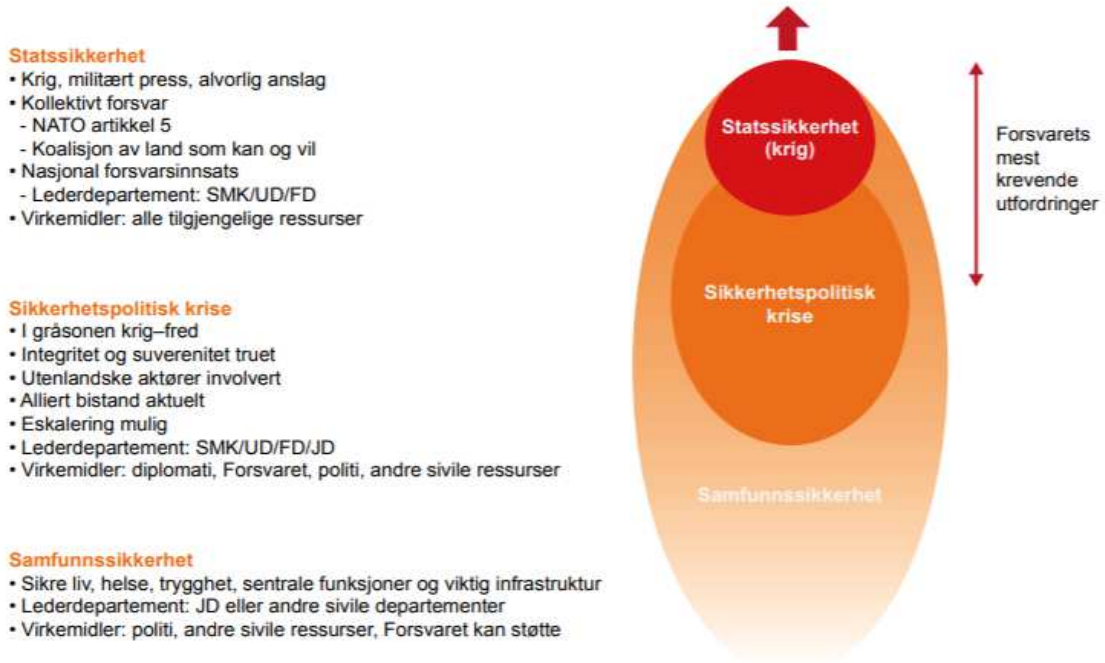
EOS tjenestene sitt hovedanliggende er statssikkerheten og fokuset rettes dermed mot de som truer vår nasjonale sikkerhet, noe som i tradisjonell forstand er andre stater og terrororganisasjoner. Alle beskriver utfordringer med attribusjon og at dette er et tiltakende problem. Mulighetene til å skjule sine spor er mange, enten ved bruk av kryptering, stedfortredere eller indirekte angrepsmål. Kompleksiteten øker og identifisering omtales som svært utfordrende. Det vises til at teknologiutviklingen og tilgjengeligheten til kunnskap og skadevare åpner opp for andre aktører uten at det beskrives nærmere om hvilken konsekvens og rekkevidde dette representerer.

Status i dag er at dages trusselbilde gir potensielt en rekke gråsonescenarioer som utfordrer fordelingen av ansvar og myndighet mellom forsvar, politi og andre myndighetsorganer. En svakhet med analysen er at den baserer seg på de ugraderte rapportene. Den gjennomgående enighet om at Russland og Kina representerer den største trusselen må antas å baseres på kunnskap tjenestene ikke kan gå ut med. En mer presis og spesifikk henvisning vil potensielt kunne avdekke metoder, ramme samarbeidende tjenester og kapasitet. Ivaretakelsen av statssikkerhet er som nevnt EOS tjenestene sitt primære oppdrag. Som omhandlet i kapittel 3.5, kan fokuset på statssikkerhet alene bidra til at cyberdomenet sikkerhetiseres.

4.5 Et asymmetrisk situasjonsbilde?

Trusselen beskrives som kompleks og konsekvensene rammer i en sfære som også omfatter samfunnssikkerheten. Dette bekreftes av de analyserte vurderingene. Et ensidig fokus på statlige aktører kan gi et asymmetrisk situasjonsbilde. Spørsmålet er om det er relevant å se *hele* trusselbildet under ett, og om beskrivelse av kriminalitetens virkning vil ha betydning for beslutningsgrunnlaget. At statssikkerheten alene omtales, medfører at fokuset trekkes mot farligste mål. Digitaliseringen gir imidlertid nye angrepsvarianter og hybride trusler kompliserer dette bildet. Angrep i sivil sektor kan potensielt ha relevans for statssikkerheten. Cyberdomenet oppstiller dermed behov for å se de ulike stadier i sammenheng.

Ekspertgruppen for Forsvaret av Norge illustrerer de ulike stadiene og at det eksisterer overlappende ansvar. Det innebærer at statssikkerhet, sikkerhetspolitisk krise og samfunnssikkerhet kan være utfordret på samme tid.



Figur 2. Kriseskalaen og Forsvarets mest krevende utfordringer (Ekspertgruppen, 2015)

Tar en utgangspunkt i figurens dimensjonering av stadiene, omfattetes EOS tjeneste sine trusselvurderinger kun en del av risikobildet. Videre at det kan være utfordrende å avgjøre lederdepartement som følge av overlappende ansvar. Attribusjonsutfordringer skaper ytterligere usikkerhet. Ekspertgruppen eksemplifiserer ved at "[S]amfunnssikkerheten også kan være utfordret i en situasjon hvor statssikkerheten er truet" (Ekspertgruppen, 2015, s.9).

Samfunnssikkerheten er det flere etater og institusjoner som har ansvar for i Norge. Det er likevel politiet som tillegges en stor del av dette oppdraget gjennom det såkalte politimonopolet. Det produseres imidlertid ingen offentlig trusselvurdering. Kriminalitet i cyber beskrives dermed ikke på strategisk nivå.

Næringslivets sikkerhetsråds (NSR) årlige mørketallsundersøkelser har en synlig plass i offentligheten. Undersøkelsene omhandler kriminalitet og sikkerhet for næringsliv og myndigheter og er gjennomført siden 2006 (NSR, 2019, s.2). Det er med andre ord en interesseorganisasjon som søker å fylle dette tomrommet. I mørketallsundersøkelsen av 2018 vises det til at kun 9% av rapporterte hendelser blant respondentene anmeldes til politiet (NSR, 2018, s.28). Fravær av anmeldelser har den uheldige konsekvens at politiet ikke får oversikt over modus og omfang av IKT-kriminaliteten..

4.6 Delkonklusjon – Konsekvenser av et komplekst trusselbilde

Aktørene som står bak trusler i det digitale rom spenner fra statlige etterretnings- og sikkerhetstjenester, via tradisjonelle militære motstandere, globale næringsbedrifter, terrorist- og ekstremistgrupper til organiserte hackergrupper (Forsvarsdepartementet, 2018, s.100). Grensesnittet mellom trusler mot staten, individet, ytre og indre trusler er som følge av digitaliseringen i stor grad i ferd med å viskes ut. Konsekvensen er at trusselbildet er i kraftig endring og utvikling. Skillet mellom terror, krig og kriminalitet utfordres da virkemidlene i mange sammenhenger er de samme og tidsmessig varierer. Dette utfordrer den norske modellen hvor sektorprinsippet er førende for hvem, hvordan og på hvilket rettsgrunnlag et angrep skal håndteres.

Narrativet kan sies å «eies» av etterretning og sikkerhetstjenestene. Trusselvurderingene er på langt vei fundamentet for offentlige utvalg og kommisjoner hva gjelder beskrivelse av trusler mot Norge som stat og samfunnet forøvrig. EOS tjenestene har tradisjonelt konkludert med at statlige aktører representerer den største trusselen, men at cyberangrep de siste årene også benyttes som metode av en rekke ulike aktører. Teknologien og kompetansen er ikke lenger eksklusiv for stater, den er gripbar for "alle" i prinsippet. Det innebærer at flere aktører opererer mot samme mål, men med forskjellig formål og intensjon.

Situasjonsforståelsen og beslutningsgrunnlaget myndighetene støtter seg på, baseres langt på vei av tjenestenes vurderinger. Endringene medfører imidlertid at samfunnssikkerheten kan være utfordret i en situasjon hvor statssikkerheten kan være truet og motsatt. Trusler i cyberdomenet oppstiller dermed behov for å se de ulike stadier i sammenheng. At det ikke lages vurderinger som beskriver trusselens virkning i et samfunnssikkerhetsperspektiv, kan gi et asymmetrisk situasjonsbilde.

Faglitteraturen omhandler utviklingen i cyber i en annen dimensjon og kontekst enn trusselbildet alene. Utfordringene digitaliseringen fører med seg hva gjelder sikkerhet, omhandler i stor grad samme problemstillinger som reises i trusselvurderingene. Forskningen løfter imidlertid blikket og ser på hvilke konsekvenser dette kan ha på samfunnet i stort. Både hva gjelder utfordringer med organisering, men også rekkevidden av at trusselen tilsynelatende er sikkerhetisert. At utviklingen i cyberdomenet av forskjellige årsaker defineres som eksistensiell, kan rettferdiggjøre utvidede hjemler til statlige virksomheter i bytte mot sikkerhet. Faglitteraturen beskriver at utfordringene er store og at fremveksten av en rekke koordinerende institusjoner kan være en svakhet i den norske sikkerhetsarkitekturen. Friis & Hansen (2020, s.188) viser til at "flere uttrykker derfor at det er begrenset hva disse sentrene kan oppnå, og [at] de heller er et symptom på et problem, enn en løsning". Hvordan og på hvilke vilkår staten fordeler oppgaver og ansvar, når sektorprinsippet er det førende prinsipp, løftes som kjernen i statens utfordring.

Neste hovedkapittel ser på tilpasninger til endringene i cyberdomenet. Hvordan håndterer myndighetene et endret trusselbilde og hvilke grep gjøres og med hvilke konsekvenser?

5 Lov og strukturendringer i møte med cybertrusselen

Dette kapittelet analyserer hvordan myndighetene søker å tilpasse seg det nye trusselbilde i cyber. Analysen tar utgangspunkt i to lovforslag. Først den nylig vedtatte Lov om Etterretningstjenesten (Etterretningstjenesteloven, 2020), som under høringsrunden avdekket en rekke prinsipielle spørsmål. Dette inkluderer både grensesnittet mellom PST og Etterretningstjenesten, samt tjenestens overvåkning av norske borgere. Deretter behandles forslaget om ny Fullmaktslov (NOU2019:13) hvor det foreslås at regjeringen gis utvidede fullmakter i en krise. Felles for dem begge er at de utfordrer flere av verdiene rettsstaten er tuftet på og den norske modellen for beredskap med sektoransvar.

Formålet er å undersøke om det er vesentlige avvik mellom forslagenes argumenter for endringsbehov, og høringsinstansenes respons på disse, samt i hvilken grad myndighetens forståelse og beskrivelse av trusselen har innvirkning på valg av løsning. Valg av høringsinstanser i analysen er i hovedsak basert på hvilke instanser som har vært mest kritiske og som berører oppgavens overordnede tema, nemlig forholdet mellom Forsvaret og sivile maktmyndigheter. Seleksjonen er dermed avgrenset til etater som

omfattes av endringene eller har innsigelser til forslagene av prinsipiell karakter, som Datatilsynet, Riksadvokaten og Norges institusjon for menneskerettigheter (NIM).

Analysen innledes med en kort beskrivelse av sikkerhetspolitikken i endring og rettslige skranker. Hensikten er å gi et bakteppe på endringsfaktorer og rekkevidden av lovendringer. Videre omhandles grensesnittet mellom PST og Etterretningstjenesten og det tradisjonelle skillet mellom indre og ytre sikkerhet. Oppgaven ser så på hvordan truslene i cyberdomenet reiser nye problemstillinger sett hen til sektor- og ansvarsprinsippet, maktfordeling, menneskerettigheter og grunnleggende prinsipper det norske demokratiet bygger på.

Analysen viser at høringsinstansene i stor utstrekning tar utgangspunkt i gjeldene hjemmelsgrunnlag, mens lovforslagene redegjør for behov for tilpasninger som følge av et endret trusselbilde. Diskusjonen oppstår når behov for utvidet myndighet for å trygge sikkerheten i cyber settes opp imot rettssikkerhetsgarantier og personvern. Analysen ser på hvordan og med hvilken begrunnelse, myndighetene søker å demme opp for utfordringen som oppstår når en trussel treffer flere sektorer, eller der det er vanskelig å konkludere hvem som står bak og med hvilken intensjon. Avslutningsvis drøftes hvorvidt disse tiltakene bidrar til klarere ansvarsforhold og som igjen kan gi bedret sikkerhet i cyberdomenet.

5.1 Sikkerhetspolitikken i utvikling

Sikkerhetspolitikkens sentrale formål er å ivareta statssikkerheten. Med dette så menes å ivareta sikkerhetsbehov knyttet til interesser som statens eksistens, suverenitet og integritet (Forsvarsdepartementet & Justisdepartementet, 2018, s.12). Tradisjonelt har Forsvaret vært et av de viktigste virkemidlene i så måte. Glidninger i trusselbildet påvirker imidlertid rollen og relevansen av militærmaktens evne til å håndtere det nye trusselscenario (Beadle & Diesen, 2015, s.17). Forsvar av landet og folket er statens primære oppgave. Evnen til å håndtere krise og væpnet konflikt på norsk territorium må gis høyeste prioritet. Men endringer i våre sikkerhetspolitiske omgivelser kan komme svært raskt og være vanskelig å identifisere intensjonen bak (DSB, 2019a, s.194). Angrep i cyber gjør at trusselen mot statssikkerheten nå opptrer i nye former, former som ikke alene kan stanses i det fysiske domenet.

Disse nye sikkerhetsutfordringene har ført til at selve samfunnsstrukturen er utsatt for nye farer og anslag relatert til økt avhengighet av og sårbarhet i kritisk infrastruktur. En følge av dette er økt fokus på samfunnssikkerhet (Forsvarsdepartementet & Justisdepartementet, 2018, s.13). Den teknologiske utviklingen går raskere enn utvikling av internasjonal cyberpolitikk, med den konsekvens at det ikke finnes en overordnet aktør som styrer infrastrukturen globalt. Det er få mellomstatlige arenaer for å utvikle kjøreregler for statlig oppførsel i det digitale rom og få internasjonale konvensjoner som spesifikt regulerer dette (NOU2018:14, s.20).

Norge som småstat kan dermed ikke i like stor utstrekning støtte seg på internasjonale organisasjoner som vi har tradisjon for. Også NATO setter sivil-militært samarbeid på dagsordenen. Organisasjonen anerkjenner at sivil beredskap, krisehåndtering og beredskapssamarbeid er en forutsetning for de enkelte lands, og derav alliansens, samlede beredskap og forsvar (Justisdepartementet, 2017, s.21). Militærmaktens rolle i å håndtere sikkerhetsutfordringene vi står overfor har dermed endret seg. Det er ikke militærmaktens nytteverdi i seg selv, men utviklingen i våre omgivelser som legger andre premisser for dens anvendelighet (Beadle & Diesen, 2015, s.16).

Løsningene ligger i hensiktsmessig ansvarsfordeling og organisering slik at samfunnets totale ressurser utnyttes best. Å identifisere grensesnitt mellom ulike myndigheter og etablere funksjoner som har sektorovergripende myndighet er imidlertid en krevende øvelse. En utfordring er å håndtere trusselen i både det fysiske- og digitale rom samtidig - og se disse i sammenheng. Det ene diskvalifiserer ikke det andre. Her oppstår en rekke dilemmaer da vår sikkerhetsarkitektur bygger på sektor- og ansvarsprinsippet. En hendelse i cyber kan både være kriminalitet og samtidig et angrep som truer statssikkerheten. Det avhenger av hvilken kontekst og tidsperspektiv en tar utgangspunkt i. Videre er attribusjon utfordrende og beslutningsgrunnlaget i en tidlig fase ofte mangelfull. Konklusjonen eller valget om hva man faktisk står ovenfor legger føringer for hvilken myndighet, hvordan og med hvilket hjemmelsgrunnlag angrepet skal håndteres. Satt på spissen om angrepet skal håndteres med militærmakt eller straffeforfølgning.

Liberale demokratier som Norge er styrt av en rekke grunnleggende verdier og prinsipper. Et lands lovgrunnlag og rettssystem tar opp i seg disse. Norge er en rettsstat som setter menneskerettigheter og rettssikkerhet høyt. Dette er verdier som hindrer totalitært styre og ivaretar maktfordelingsprinsippene. Disse verdiene legger en rekke føringer på hvilke tiltak og maktmidler som kan benyttes i Norge mot norske rettssubjekter.

5.2 Tilpasning av lovverket – rettslige skranker

Forsvaret og politiet er statens maktinstrumenter. Tradisjonelt har det vært et skarpt skille mellom disse. Dette skillet er ikke lenger like åpenbart. Tilpasninger til det nye trusselbildet skjer på flere fronter og et viktig tidsskille er lovendringene som i 2015 ble gjort i Politiloven. Forsvarets bistand til politiet er nå forankret i lov gjennom bestemmelsen i politiloven § 27a (Forsvarsdepartementet & Justisdepartementet, 2018, s.58-59). Endringen løser en mangeårig legalitetsutfordring og letter bruk av Forsvarets kapasiteter i fredstid på gitte vilkår. Lovendringen kom som følge av debatten etter terroranslaget på Utøya i 2011 og Gjørv-kommisjonens anbefalinger. Det var problematisk, om nærmest umulig, å kunne forsvare at myndighetene ikke tillater at alle tilgjengelige ressurser staten rår over kan benyttes til å redde uskyldige liv. Kontinuerlig tilpasning av lovgrunnlaget til det faktiske trusselbildet er derfor nødvendig. Det viser også at det er en forventning at samfunnets totale

maktkapasiteter i gitte situasjoner, forventes å samarbeide om utfordringene innen en av sektorene med denne sektorens rammer og spilleregler.

Det er relativt få eksempler på tverrsektorielle lover som inneholder krav om IKT-sikkerhet. I denne sammenheng er det primært sikkerhetsloven, personopplysningsloven, lov om elektroniske tillitstjenester og forvaltningsloven som gir skranker for behandling av opplysninger og lagring. I tillegg til nasjonale lover og forskrifter er det også en rekke internasjonale avtaler, lover og standarder som regulerer IKT-sikkerhet. Disse har gyldighet for norske virksomheter og legger føringer for regelverk i Norge (NOU2018:14, s.32).

I en demokratisk rettsstat gjelder noen grunnleggende prinsipper som regulerer statens maktanvendelse ovenfor sine borgere. Legalitetsprinsippet er en slik hjørnesten. Myndighetenes inngrep overfor den enkelte skal være basert på en demokratisk prosess og være forankret i folkeflertallets vilje (NOU2016:19, s.91). I korthet betyr det at ingen kan straffes uten etter lov og at staten kan ikke gjøre inngrep i borgernes rettsstilling uten at dette fremkommer i lovverket. Dette kravet er ment å beskytte individene mot statsmakten.

Begrunnelsen for hjemmelskravet er todelt. For det første skal det ivareta maktfordelings- og kontrollhensyn i forholdet mellom statsmaktene. For det andre skal det sikre forutberegnelighet for borgerne (Auglend, 2015a, punkt 6). En viktig forutsetning for å kunne forutberegne sin rettsstilling er at inngrepshjemlene er tilgjengelige for allmennheten, slik at borgerne har mulighet til å sette seg inn i det aktuelle regelverket. En annen grunnleggende rettssikkerhetsgaranti er forholdsmessighetsprinsippet. Dette prinsippet innebærer at det må gjøres en konkret vurdering av hvorvidt det aktuelle tiltaket vil utgjøre et uforholdsmessig inngrep, sett opp mot de sikkerhetsmessige gevinstene et slikt tiltak vil antas å få. Staten må derfor foreta en konkret vurdering om virkemiddelet står i forhold til det rettsvern det skal beskytte (NOU2016:19, s.91).

I et uoversiktlig trusselbilde og nødvendigheten av bruk av samfunnets samlede ressurser for å ivareta vår sikkerhet, oppstår et spenningsfelt mellom ivaretakelse av nasjonal sikkerhet og individets rettigheter. Her ligger det til dels motstridende interesser og verdier som må veies opp mot hverandre (NOU2016:19, s.85). Kompleksiteten i cyber gjør det vanskelig å avgjøre hva trusselen består av og derav hvilke verdier som skal beskyttes.

Første case er Etterretningstjenesteloven hvor det redegjøres for selve lovforslaget og utfordringer med det territorielle skille i cyber. Så behandles Etterretningstjenestens mulighet til å overvåke datastrømmen ut og inn av Norge og utvalgte høringsinstanser sine anførsler til dette. Avslutningsvis drøftes mulige konsekvenser og utfordringer som følge av uklarheter rundt rettsvern, statens plikt til å beskytte og ansvarsfordeling.

5.3 Etterretningstjenesteloven

19. juni 2020 ble lovforslaget sanksjonert i Stortinget med ikrafttredelse 1. januar 2021. Formålet med loven er å bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser. Loven søker å ta utviklingen av trusselbildet, styrkningen av menneskerettighetenes stilling og digitaliseringen av samfunnet på alvor. Under lovforarbeidet møtte forslaget imidlertid motstand, da lovens utvidede fullmakter til Etterretningstjenesten var i konflikt med tidligere fastlagte prinsipper.

Behovet for lovendring er begrunnet i et endret trusselbilde. Forsvarsdepartementet viser til trusselbeskrivelsene til PST og Etterretningstjenesten og at gråsoneaktiviteter svekker tradisjonelle skillelinjer mellom fred, krise og væpnet konflikt. Det sammensatte trusselbildet kan skape usikkerhet og dermed redusere Norges motstandsdyktighet og evne til krisehåndtering (Forsvarsdepartementet, 2020b, s.15-16). Skillet mellom indre og ytre sikkerhet definerer i første rekke ansvarsområde mellom Etterretningstjenesten og PST. Dette skillet omtales som den *territorielle begrensning* og deler etterretningsansvaret mellom Justisdepartementet med ansvar for innenlandsetterretningen og Forsvarsdepartementet med ansvar for utenlandsetteretningen. Fordelingen følger den tradisjonelle inndeling av ansvar innen norsk sikkerhetsforvaltning. Dette skillet er imidlertid ikke like tydelig i cyber, som i sin natur er grenseløst (Forsvarsdepartementet, 2018, s.114).

Forsvarsdepartementet argumenterte med at tjenesten må kunne rette innhentning av informasjon mot utenlandske eller norske personer eller virksomheter i Norge, for å være i stand til å løse sitt oppdrag. En forutsetning er at det foreligger konkrete holdepunkter for etterretningsvirksomhet mot beskyttelsesverdige objekter (Forsvarsdepartementet, 2018, s.129). Flere sentrale aktører har vært kritiske til at det åpnes opp for tjenestens adgang til å innhente informasjon på norsk jord, og gitt uttrykk for at forslaget er uklart eller legger opp til en vanskelig avgrensning (Forsvarsdepartementet, 2020b, s.48). Myndighetene har imidlertid hensyntatt forslagets pragmatiske anbefaling, om at tjenesten er avhengig av denne muligheten for å kunne varsle om ytre trusler mot staten. Slik aktivitet, også i Norge, er av åpenbar interesse for tjenesten (Forsvarsdepartementet, 2018, s.116).

Forutsetningene har dermed endret seg som følge av digitalisering og globalisering. Forsvarsdepartementet påpeker at den territorielle begrensning legger hindringer for at Etterretningstjenesten skal kunne løse sitt oppdrag, sett i lys av dagens dynamiske og uoversiktlige trusselbilde. Overordnet har Forsvaret som nevnt primæransvaret for truslene mot statssikkerheten – uavhengig av om de kommer innenfra eller utenfra, og politiet har på sin side primæransvaret for trusler mot samfunnssikkerheten. Også her uavhengig om truslene er av ytre eller indre art (Simonsen, 2019, s.299).

I cyberdomenet er dette skillet nærmest ikke-eksisterende, noe som utfordrer Etterretningstjenestens evne. Kravene til tjenesten har økt i takt med et tilspisset sikkerhetspolitisk landskap (Forsvarsdepartementet, 2018, s.77). De siste 10-15 årene har trusselen mot samfunnskritiske IKT-systemer økt i betydelig omfang. Fremmed etterretningsvirksomhet, subversjon og sabotasje har tatt skrittet inn i det digitale rom med økt omfang og hastighet (Forsvarsdepartementet, 2018, s.99). Grensen mellom politisk påvirkning og konvensjonell og ukonvensjonell krigføring er ikke så skarp og entydig som tidligere. Angrep i det digitale domenet kan ramme nasjonale beslutningsprosesser og utfordre både samfunns- og statssikkerheten. I ytterste konsekvens kan slike angrep true statssikkerheten og omfattes derfor av NATO-traktatens artikkel 5 (Forsvarsdepartementet, 2018, s.101). NATO tar dermed stilling til alvorligheten og indirekte påvirker hvordan truslene skal kategoriseres. Et massivt angrep i cyber kan i ytterste konsekvens true en stats eksistens. I et slikt scenario må beskyttelsesmekanismene og hjemmelsgrunnlaget samsvare med trusselen.

Tilrettelagt innhentning

Loven gir Etterretningstjenesten anledning til å innhente elektronisk kommunikasjon som transporteres over den norske grensen når grunnvilkårene er oppfylt. Dette innebærer innhentning av metadata i bulk (Stortinget, 2020, s.5-6). Et grunnleggende premiss er at innhentingen skal være i overensstemmelse med menneskerettighetene. Det er oppstilt rettssikkerhetsmekanismer som skal verne mot misbruk og vilkårlighet. Dette er søkt ivaretatt ved domstolkontroll.

Flertallet av høringsinstansene anerkjenner Etterretningstjenestens behov for lovregulering av innhentningshjemler og metodebruk, samt at tjenesten på nærmere vilkår gis tilgang til grenseoverskridende elektronisk kommunikasjon. Imidlertid er flertallet også enige om at lovforslaget representerer en for vid og uklar regulering. Både lovteknisk og prinsipielt sett hen imot den territoriale begrensning, rettssikkerhet og retten til privatliv.

Overordnet var det tre forhold som gjorde at lovforslaget møtte motstand. For det første er Etterretningstjenestens utvidede rett til å drive etterretningsvirksomhet på norsk territorium og det uklare grensesnittet mot andre myndigheter. Det andre at selve innsamlingen og overvåkningen av all elektronisk kommunikasjon vil krenke rettsvernet om retten til privatliv og grunnleggende rettssikkerhetsgarantier. Sist og ikke minst kan ikke en offentlig myndighet unnlate å varsle om trusler mot norske borgere sitt liv. Dette bryter med en rekke prinsipper og forpliktelser den norske stat har ovenfor den enkelte borger. Jeg vil nå gå nærmere inn i de ulike motforestillingene.

Overvåkning, rettsvern og plikten til å beskytte

Utgangspunktet er at elektronisk informasjon innsamlet av tjenesten ikke skal deles med andre myndigheter (Forsvarsdepartementet, 2018, s.264). Datatilsynet uttaler i sitt høringssvar at slik innsamling ikke bør innføres. De henviser til at krenkelsen av personvernet og retten til privatliv er for

stort. Det vises til at dette vernet er en "grunnleggende forutsetning for et demokratisk samfunn" (Datatilsynet, 2019b, s.1). og at "rettigheten er nedfelt i Grunnloven § 102, EMK art. 8 og FNs internasjonale konvensjon om sivile og politiske rettigheter (SP) art. 17" (Datatilsynet, 2019b, s.24). Også Norges nasjonale institusjon for menneskerettigheter (NIM) setter spørsmål ved forslaget. Deres hovedinnvending er at "retten til privatliv setter grenser for statens overvåkning" og viser til at begrunnelsen for disse grensene i den Europeiske Menneskerettsdomstol (EMD), er «at slik overvåkning kan underminere, og i ytterste konsekvens ødelegge demokratiet under dekke av å forsvare det» (NIM, 2019 s.15). Overvåkning i det godes hensikt kan dermed rokke ved fundamentet demokratiet er bygget på, særlig tilliten og samfunnskontrakten mellom borger og stat.

Overvåkingssystemer må i denne sammenheng nødvendigvis ta utgangspunkt i etterretningsfaglig skjønn, men lovgivningen må sette rammer for skjønnsutøvelsen. Det må videre være presisjon for hvordan skjønnet skal utøves for å sikre at overvåkingen er "forholdsmessig sett i lys av det legitime formålet den skal ivareta" (NIM, 2019, s.19). Formålet med innsamlingen regulerer dermed bruk av opplysningene. I den etterfølgende debatt av lovforslaget fremkommer forskjellige prinsipielle utgangspunkt og tolkning av formålet og konsekvensene av såkalt formålsutglidning. Med formåslutglidning menes at opplysninger innhentet med et bestemt formål ikke kan benyttes til et annet. Prinsippet om at formålet med innsamlingen skal være klart og avgrensende er "begrunnet i kravet til forutberegnelighet, åpenhet og tillit" (Datatilsynet, 2019b, s.22). Lysne II-utvalget (2016, s. 60) vurderte at overskuddsinformasjon, som er data som ikke tjener formålet med "etterretningstjenestens oppgaveløsning skal slettes". Utvalget tok her et prinsipielt standpunkt, at hensynet til rikets sikkerhet er viktigere enn å tillate bruk av overskuddsinformasjon til andre formål, som kriminalitetsbekjempelse eller vern av liv og legeme.

Både PST, Riksadvokaten og Kripos viser til at dette bryter med prinsippet at staten skal beskytte norske borgere etter den lovfestede avvergeplikten i loven (Straffeloven, 2005, §196). Helt overordnet er man i en situasjon hvor to prinsipper står mot hverandre. Vurderingen blir da hvilket prinsipp som veier tyngst. Kripos finner det "så vel rettslig som etisk uholdbart at offentlige myndigheter skal kunne komme til kunnskap om grov vold og misbruk" som ikke følges opp (Kripos, 2019, s.10). Kunnskap forplikter og PST anfører at tilbakehold av slike opplysninger i praksis er et bevisforbud som ikke kan gjelde bevis knyttet til terrorhandlinger (PST, 2019b, s.9). Også Riksadvokaten (2019a, s.5) finner det "meget problematisk om Etterretningstjenestens personell og operative kilder fritas fra den alminnelige avvergeplikten". I FD sitt lovforslag tas høringsinstansenes motbør delvis tilfølge og foreslår at slike opplysninger *kan* utleveres for å forhindre alvorlig fare for noens liv, helse eller at noen blir uriktig tiltalt eller domfelt (Forsvarsdepartementet, 2020b, s.136). Departementet valgte en åpning, men heller ikke mer. Det er stor avstand mellom *kan* og *skal*. I den vedtatte loven tas FD's sin anbefaling tilfølge (Etterretningsloven, 2020, §7-13, 2. ledd).

Hva er grunnen til at forskjellige myndigheter har så vidt forskjellig utgangspunkt på helt sentrale og grunnleggende spørsmål? En forklaring kan være de ulike sektorers oppdrag og ansvarsfordeling. Etterretningstjenesten skal sikre statssikkerheten, mens politi og påtalemyndighet skal sikre samfunnssikkerheten. I utgangspunktet to ulike ansvarsområder. PST har i denne sammenheng oppgaver innen begge domener. Som anført med utgangspunkt i sektorprinsippet er dette to forskjellige øvelser.

En slik kategorisk inndeling av ansvar passer imidlertid ikke i dagens trusselbilde. Dette viser at ansvarsområdene er overlappende og ikke sidestilt. Det er en krevende øvelse å trekke opp en grense hvor den ene myndighets ansvar begynner og den andres slutter. Denne problemstillingen blir tydelig i et grenseløst cyber hvor mangfoldet av aktører med ulike motiver opererer om hverandre, på samme plattform og til samme tid. Isolert er det naturlig å forstå at Etterretningstjenesten har behov for slike verktøy for å løse sitt oppdrag. Tjenestens funksjon er å gi beslutningsstøtte i sikkerhetspolitiske spørsmål som angår statens suverenitet og handlefrihet. I en vekting mellom stat- og samfunnssikkerhet mener nå Stortinget gjennom vedtakelsen av den nye loven at statssikkerheten kommer først, noe som kan forsvares etisk med en utilitaristisk begrunnelse. Et nærliggende spørsmål er om det i det heletatt er mulig å skille mellom ytre og indre trusler i cyber. Videre om kategoriseringen stat- og samfunnssikkerhet kun er et teoretisk skille som vil bidra til ytterligere gråsoneproblematikk hva gjelder ansvar og hjemmelsgrunnlag mellom Etterretningstjenesten og sivile myndighetsorganer.

Utvidet handlingsrom tåkelegger ansvarsprinsippet

Loven følger oppdragsfokuset mot statssikkerheten og utfordrer det etablerte skille mellom *indre* og *ytre* sikkerhet. PST (2019b, s.11) er bekymret for at "rekkevidden av Etterretningstjenestens mandat på norsk jord blir uklart". Også Riksadvokaten etterlyser "hvor tjenestens handlingsrom faktisk slutter" da dette ikke begrunnes nærmere i lovforslaget. Manglende presisjon er dermed egnet til å skape "uklarheter om hvor grensene for Etterretningstjenestens faktiske ansvar- og myndighetsområde går" og tjenestens "grenseflatene mot andre myndigheter som også har funksjoner innen stat- og samfunnssikkerheten" (Riksadvokaten, 2019a, s.4). PST (2019b, s.1) understreker at lovforslaget " kan skape uklarheter og tolkningstvil […] i anledning tjenestens innhentning og ansvar på norsk territorium, samt grensedragningen mot PST". Kripos på sin side peker på at en slik gråsone mellom de to tjenestene skaper utfordringer i et personvern- og menneskerettsperspektiv. Grunnloven og EMK setter skranker for lovgivers handlingsrom (Kripos, 2019, s.7).

Et viktig element er forutberegnelighet overfor hva staten har anledning til å gjøre mot norske rettssubjekter på norsk jord. Hvilke regler som gjelder må borgerne kunne tilpasse seg etter og være kjent med. Videre må tiltakene være proporsjonale sett i forhold til hva som oppnås og de rettigheter

som krenkes. Dette er grunnleggende rettsstatsprinsipper. Krenker staten et rettssubjekts rettigheter skal det være hjemlet i lov og som hovedregel transparent i forhold til innsyn. Utfordringen oppstår når den som krenker rettighetene er en statlig myndighet som opererer i det skjulte og hvor aktiviteten er hemmeligstemplet. Manglende mulighet til innsyn, hvor privatlivets fred krenkes, kan utfordre tilliten mellom borger og myndighetene. En tillit som er selve fundamentet i vårt liberale demokrati.

EOS utvalget (2019, s.2) påpeker i sitt høringssvar at med «de hjemler som foreslås gitt til Etterretningstjenesten, reiser utvalget spørsmål om kontrollmodellen er vurdert i slik bredde som synes forventet av Stortinget». Tolkninger, skjønnsutøvelse og uklar legalitetskontroll kan få store konsekvenser som i Danmark, hvor sjefen for danske Forsvarets etterretningstjeneste måtte fratre på grunn av beskyldninger om feilinformering til kontrollorganet og ulovlig overvåkning på dansk territorium (NTB, 2020).

Uønsket aktivitet på norsk territorium i det digitale domenet er komplekst å definere. Et økende behov for tettere samhandling mellom utenlands-, innenlandsetterretning og politi, er en klar trend i de fleste vestlige demokratier. Behov for samhandling er blant annet en direkte konsekvens av grenseoverskridende trusler og kommunikasjonsteknologi. En forutsetning for å operere i et skiftende og dynamisk trusselbilde er utveksling av informasjon og samarbeid. Samarbeid er derfor avgjørende for å lykkes med å avdekke og motvirke trusler mot Norge (Forsvarsdepartementet, 2018, s.144). Tettere samhandling krever at grensesnitt og myndighetsområde er tydelig og definert, noe som er utfordrende når trusselen er vanskelig å kategorisere. Den tradisjonelle distinksjonen mellom tjenestene utfordres da de i økende grad har sammenfallende oppgaver og arbeider svært ofte mot de samme truslene, men med ulike formål (Forsvarsdepartementet, 2018, s.118). Dette kompliserer bildet og reiser en rekke prinsipielle spørsmål. Riksadvokaten (2019a, s.2) er tydelig i sitt høringssvar at man "ikke rokker ved den etablerte rollefordelingen mellom politiet og Forsvaret". En utfordring er som nevnt graden av transparens. Etterretningstjenestens praktisering av loven vil i stor grad være hemmelig med den konsekvens at kravet om klarhet og forutberegnelighet vanskelig kan oppfylles.

Oppsummert kan loven fremstå som om at myndighetene søker å tilpasse en «firkant ned i et rundt hull». Utvalget beskriver i forarbeidene hvilken betydning og effekt digitalisering og globalisering har for statssikkerheten. Skal tjenesten kunne løse sitt oppdrag må hjemmelsgrunnlaget og virkemidler tilpasses det nye trusselbildet. Majoriteten av høringsinstansene anerkjenner tjenestens oppdrag og viktighet. Utfordringen oppstår når de ulike etater, institusjoner og myndigheter skal kommentere forslagene fra sitt ståsted. Den enkelte tar utgangspunkt i nåsituasjonen hva gjelder organisering og hvilke prinsipper den norske sikkerhetsarkitekturen er bygget på. Sektor og ansvarsprinsippet, legale rammer og forpliktelser, samt grunnleggende demokratiske verdier norsk forvaltning støtter seg på. Når disse momentene møtes oppstår friksjon. Mye tyder på at kompleksiteten i dagens trusselbilde

ikke passer inn i den norske beredskapsmodellen, og overlappende ansvarsområder øker i både bredde og dybde.

Personvern og individets rettigheter står sterkt i Norge. Datasikkerhet og eierskap til brukerinformasjon og forvaltningen av disse er et vanskelig område å regulere. Mangfoldet av aktører og avhengigheter mellom sivile og militære funksjoner gjør det videre krevende å sortere ut oppgaver og hvilke virkemidler som skal tillates. Disse sammenknytningene medfører at endringer hos en myndighet, som her Etterretningstjenesten, får innvirkning for en rekke andre. En konsekvens er at gråsonen hva gjelder ansvar utvides som følge av overlappene oppgaver. Det klare skillet Riksadvokaten påpeker og hegner om, er meget krevende i praksis. PST, politiet og Riksadvokaten er de som stiller flest spørsmål i høringsrunden. Spesielt prinsippet om statens grunnleggende plikt ovenfor sine borgere, å beskytte samfunnet og enkeltindividet mot fare og vold. En statlig myndighet kan ikke med viten og vilje la være å hindre planlagte drap eller grov kriminalitet som terror. Dette strider mot helt grunnleggende prinsipper. Tenkningen rundt at noen må lide for flertallets nytte er i dagens rettighetsbevisste samfunn en krevende øvelse.

Lovens skille mellom stat- og samfunnssikkerhet er ikke like åpenbart som for få år siden. Politi og påtalemyndigheten tar utgangspunkt i samfunnssikkerheten og FD i statssikkerheten. Spørsmålet som oppstår er om ikke begge etatene sin tilnærming er gyldig i dagens trusselbilde. En kompliserende faktor i cyber er utfordringer med attribusjon. Realiteten er at beslutningsgrunnlaget som initialt legges til grunn vedrørende ansvarsfordelingen er høyst usikker. Dette viser at politiet og Forsvaret i realiteten neppe kan anses som to sideordnede etater som har ansvaret for hver sin klart avgrensede banehalvdel (Simonsen, 2019, s.252). Vanskeligheter med å definere hvem og hva, bereder grunnen for nye løsninger som er tilpasset trusselbildet. Noen må bestemme og ta tidsriktige beslutninger.

Neste case omhandler forslaget om ny Fullmaktslov som gir Regjeringen utvidede fullmakter i krise er eksempel på en slik tilpasning.

5.4 Forslag om ny Fullmaktslov

Først redegjøres det for formålet med lovforslaget og behovet for raske beslutninger i kriser som treffer tverrsektorielt, slik hendelser i cyber nesten alltid gjør. Deretter drøftes lovforslaget ved å innta utvalgte høringsinstanser sine sonderinger rundt grensesnittet mellom fred, krise og krig. Hvordan en krise skal defineres, om det er stat- eller samfunnssikkerheten som utfordres står sentralt. Lovforslaget er interessant da flere de siste årene har etterlyst et mer overordnet ledelsesapparat som kan virke over sektornivå. Romarheim (2019, s.141) påpeker at «silotenkning som hinder for effektiv samordning i sentraladministrasjonen er for lengst ferdigdiagnostisert [...]. Rekken av offentlige dokumenter og utredninger som påpeker at problemet er formidabelt, er lang». Også Difi-rapporten om samordning i

norsk forvaltning fra 2014, løfter frem utfordringer med at om ministeransvaret tolkes for strengt kan dette hindre oppgaveløsning på tvers av sektorer (Difi, 2014, s. 3).

Beredskapsutvalget overleverte sin rapport 14. juni 2019 (NOU2019:13). Utvalgets mandat hadde sitt utspring i asylsituasjonen i 2015. Utvalget argumenterer for et behov for en sektorovergripende fullmakts- og suspensjonshjemmel. Dagens praksis med konstitusjonell nødrett er upresis i forhold til hvilke vilkår som gjelder for anvendelse av nødrettsbeslutninger i krisesituasjoner (NOU2019:13, s.21). Lovforslaget gir myndighetene mulighet til raskt å iverksette tiltak for å redusere et stort skadeomfang. Tiltak som er vanskelig å hjemle i lovgivningen fullt ut da krisen krever en annen samordning enn hva som følger av dagens hjemler og ansvarsfordeling.

Koronaloven, som ble hastevedtatt med relativt kort varighet ble opphevet 27. mai 2020 (Koronaloven, 2020) er et eksempel på et slikt scenario. Lovforslaget tar opp i seg det uventede og kan dermed hevdes å anerkjenne utfordringene i dagens dynamiske trusselbilde. Beredskapshjemmelsutvalget så behov for en legal forankring av de tilfeller hvor alvorlige hendelser som krever ekstraordinære tiltak når landet ikke befinner seg i en krig eller krigslignende tilstand. Et eksempel er når flere alvorlige hendelser inntreffer på samme tid, eller situasjonen tilsier at man ikke er i stand til å se konsekvensene eller ringvirkningene av disse (NOU2019:13, s.18). Et klassisk scenario er hybrid krigføring. I forarbeidene er imidlertid endringer i trusselbildet og såkalt intenderte handlinger som danner grunnlag for lovforslaget.

Digitaliseringen, nye samhandlingsmønstre og avhengigheter kompliserer analysen av hvilket trusselbilde nasjonen står ovenfor. Attribusjon er som nevnt vanskelig i cyber. Usikkerhet om man står ovenfor et angrep på staten eller ren kriminalitet kan hemme responsevnen. En kan tenke at en *fait accompli* situasjon oppstår uten at dette er oppdaget eller erkjent av myndighetene. Med dette menes ekstraordinære kriser eller sammentreff av flere hendelser som kan true kritiske samfunnsfunksjoner eller andre tungtveiende samfunnsinteresser. Slike scenario vil generere store koordineringsutfordringer. Det fremheves at Norge er sårbart både fordi vårt samfunn er åpent og et av verdens mest digitaliserte. Slike ekstraordinære hendelser vil sette den alminnelige beredskapen under et press som innebærer at situasjonen ikke kan håndteres etter sektorprinsippet. Det kan videre oppstå utfordringer med rettslige rammer eller at ansvarlig myndighet mangler nødvendige fullmakter til å iverksette rasjonelle tiltak (NOU2019:13, s. 19).

Utvalget vurderer like fullt at gjeldende beredskapshjemler fortsatt bør dekkes opp innenfor den enkelte sektor gjennom særlovgivingen slik som i dag. Men peker samtidig på at operasjoner som involverer flere sektorer krever bruk av en rekke forskjellige sektorhjemler, noe som vil kunne lede til manglende gjennomsiktighet, pulverisering av ansvar, mindre demokratisk kontroll og løsninger som

er mindre samordnet. Den nye loven søker å løse disse utfordringene og hindre faren for at manglende hjemler gjør at myndighetene nøler med å iverksette nødvendige tiltak. Slike situasjoner kan utløse handlingslammelse og fravær av klare retningslinjer kan i ytterste konsekvens koste liv eller ramme andre viktige verdier. Utvalget foreslo derfor at nødretten konkretiseres gjennom en sektorovergripende fullmakts- og suspensjonshjemmel (NOU2019:13, s.20).

Formålet med en slik sektorovergripende hjemmel er å tydeliggjøre hvilke prosesser og vilkår som gjelder for anvendelse av nødrettsbeslutninger i krisesituasjoner. Stortinget som lovgiver har her oppstilt krav og på denne måten presisert når, hvem og på hvilket grunnlag loven kan anvendes. Utvalget konkluderer med at det er flere fordeler enn ulemper med en slik sektorovergripende hjemmel (NOU2019:13, s. 21-22).

Sektorovergripende kriser i fredstid og kriser med sikkerhetspolitisk dimensjon omfattes av nasjonalt beredskapssystem (NBS), som igjen består av sivilt beredskapssystem (SBS), Politiets beredskapssystem (PBS) og beredskapssystem for Forsvaret (BFF) (Forsvarsdepartementet & Justisdepartementet, 2018, s.26). Beredskapsplanene må sees i sammenheng med Totalforsvaret. Totalforsvaret omfatter gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn i forbindelse med beredskapsplanlegging, krisehåndtering i hele krisespekteret fra uønskede hendelser i fred til sikkerhetspolitisk krise og væpnet konflikt. Totalforsvarskonseptet har fulgt samfunnsutviklingen, fra primært å omhandle statssikkerheten til i nyere tid å basere seg på dagens bredere samfunnsperspektiv (NOU2019:13, s. 35). Jeg vil nå gå nærmere inn i de ulike motforestillingene.

Et lovforslag tilpasset en ny tid

Forslaget om en ny fullmakt- og suspensjonshjemmel bryter med vår eksisterende grunntenkning rundt ansvar- og sektorprinsippet. Utvalget argumenterer med at lovforslaget har flere fordeler enn ulemper. Trusselbildet er med andre ord så komplekst at det er vanskelig å finne en logisk og enhetlig organisering av statens totale ressurser. Dette søkes ivaretatt med å gi regjeringen myndighet til å fatte beslutninger som ikke følger etablert praksis hva gjelder ansvar og rollefordeling mellom ulike sektorer. Hybride hendelser trekkes frem som eksempel på den nye sikkerhetssituasjonen staten må forholde seg til. Et slikt scenario vil i dag måtte håndteres på tvers av forskjellige sektorer med fare for mangelfull håndtering eller uklare ansvarsforhold. Fordeling av ansvar vil tilkjennegi hvordan regjeringen oppfatter trusselen i spørsmålet om det er stat- eller samfunnssikkerheten som trues. Premissene, eller kunnskapen om hvilke trusler som truer og kontekst disse settes i, vil i så måte legge føringer. Myndigheter som utgir nasjonale trusselvurderinger vil som nevnt ha stor påvirkning på beslutningsgrunnlaget som legges til grunn.

Høringsinstansene er delt i spørsmålet om behovet og begrunnelsen for en fullmakts- og suspensjonshjemmel. DSB støtter forslaget og begrunner dette med det moderne samfunns kompleksitet og utfordringsbilde. Regjeringen som utøvende makt må ha verktøyene som trengs for å handle raskt og effektivt i kriser og ekstraordinære hendelser. Fremtiden er uforutsigbar og det er "vanskelig å forutse hvilke sektorer som kan bli rammet i fremtidige kriser". DSB anfører at Regjeringen har behov for et handlingsrom en slik lov vil gi (DSB, 2019b, s.1). Det vises til at det i en akutt krisesituasjon kan skape beslutningsvegring hvis ikke det gis nødvendig ryggdekning til de ansvarlige myndigheter som har kompetanse og kapasitet til raskt å agere og normalisere situasjonen (DSB, 2019b, s.2).

Også NSM slutter seg til forslaget. De anfører at det vil være av "avgjørende betydning for den nasjonale responsevnen å kunne handle raskt. Spesielt ved større cyberangrep kan omfanget og konsekvensene være svært uoversiktlig". Slike hendelser krever koordinering og eventuell omdisponering av samfunnets samlede ressurser. Det er en rekke faktorer som det kan være "vanskelig å vurdere hvor man befinner seg i krisespennet mellom krig og fred". I cyber vil det ta tid å kartlegge trusselbildet og vanskelig å sammenfatte årsaken, da det i de fleste tilfeller er krevende å avdekke hvem som står bak (NSM, 2019a, s. 1). PST er også positivt innstilt til forslaget og bemerker at "det konvensjonelle skille mellom væpnet konflikt og fred stadig blir mer utydelig". Hybride scenario trekkes frem som et eksempel på den nye trusselsituasjonen (PST, 2020a, s. 1-2). Riksadvokatembetet fokuserer naturlig nok på det prinsipielle at forutberegnelighet og lovregulering er viktig i rettssikkerhets sammenheng. De støtter forslaget på et overordnet nivå (Riksadvokaten, 2019b, s.1-2).

Der hvor forslaget møter noe motstand er i høringssvarene til Forsvarsdepartementet og Politidirektoratet. Forsvarsdepartementet erkjenner hensiktsmessigheten av en fullmaktslov, men er tydelig på at denne "skal virke under terskelen for dagens beredskapslovgiving". Departementet trekker opp en grense ved å presisere at lovens virkeområde kun skal gjelde ved "kriser som ikke truer statssikkerheten". Etter deres syn bør rettslige reguleringer som det er behov for ved kriser, og som ikke truer statssikkerheten, kunne løses ved " at de enkelte sektorlovene som utformes tar høyde for løsninger ved uforutsette kriser" og at "en helt generell fullmaktslov vil kunne virke som en sovepute" (Forsvarsdepartementet, 2020a, s.1). Til tross for at departementet viser til et uklart skille mellom myndighetsområde i det utvidede trusselbilde, fremheves nødvendigheten av å opprettholde et klart skille mellom stat- og samfunnssikkerhet.

Politidirektoratet anfører at det ikke er klart at fordelene overstiger ulempene. Politidirektoratet er derfor ikke enig i forslaget (Politidirektoratet, 2020, s.2). Direktoratet bemerker, som Forsvarsdepartementet, at det ikke fremkommer et klart skille mellom krig og fred og at dette vil representere uklarheter mellom lovforslaget og beredskapslovgivningen. Hybride hendelser trekkes

frem også her som særlig vanskelig å avgjøre hvor grensene skal gå. Det reises tvil om dette enkelt vil la seg praktisere (Politidirektoratet, 2020, s. 3). Både Forsvarsdepartementet og Politidirektoratet etterlyser klarhet mot beredskapslovgivingen.

En forklaring kan være at de begge disponerer samfunnets maktmidler. Hvem som gjør hva og når, berører dermed disse to i større utstrekning enn mange av de andre aktørene. Lovforslaget hever seg imidlertid over spørsmålet om ansvarsplassering og derav grensedragning mot beredskapslovgivningen. Det tar utgangspunkt i et endret og komplekst trusselbilde hvor selve hensikten er å stå fritt til å avvike fra tradisjonell organisering. Selve formålet er et behov for en lovmessig forankring av myndighet, underlagt gitte kriterier, til den utøvende makt – regjeringen. Til tross for at utvalget anfører at eksisterende beredskapshjemler fortsatt skal gjelde, åpnes det for løsninger som suspenderer dagens fordeling av ansvar.

En fellesnevner for de som er positive til forslaget er at de har et tverrsektorielt ansvar. DSB og NSM er slike institusjoner. PST har også flere ben å stå på. PST har i så måte grensesnitt på begge flanker, mot politiet i samfunnssikkerhet sammenheng og mot Etterretningstjenesten og NSM i statssikkerhetsspørsmål. På samme måte som det er vanskelig å skille mellom hva som er indre eller ytre trusler, er det også utfordrende å definere hva som er terror eller organisert kriminalitet. En kan hevde at Forsvaret og politiet i denne sammenheng er de sektorer med klarest selvstendige oppdrag. Grenseflatene mot andre myndigheter viskes imidlertid ut ettersom digitalisering og globaliseringen tiltar. Nye løsninger som revitaliseringen av Totalforsvaret og veksten av tverrsektorielle organers ansvarsområde og myndighet er tydelig.

Utfordringen oppstår når et komplekst trusselbilde møter en gjennomregulert og seksjonert sikkerhetsarkitektur, hvor ansvarsfordeling gjennom sektor- og ansvarsprinsippet er førende. Fullmaktsloven er et tiltak for å møte denne usikkerheten, men også andre tiltak besluttes, tiltak som skyver forsvarsmakten og politiets ansvarsområder lengere ut på «flankene» med den følge at gråsonen utvides. Utvidelsen av NSM sitt mandat er fremtredende i så måte.

5.5 Delkonklusjon - samordning eller samrøre?

Angrep i cyber gjør at trusselen opptrer i nye former som må løses tverrsektorielt. Utviklingen i våre omgivelser legger nye premisser for hvordan sikkerhetsarkitekturen bør organiseres. Kompleksiteten i cyber gjør det vanskelig å avgjøre hva trusselen består av og derav hvilke verdier som skal beskyttes. Beslutningen er førende for hvilket rammeverk som gjelder og hvilke virkemidler som kan benyttes. Et sammenvevet og integrert samfunn skaper et uoversiktlig scenario. Å skille stat- fra samfunnssikkerhet er krevende.

Organisering og ansvarsfordeling er dermed utfordrende da det oppstår et avvik fra gjeldende hjemmelsgrunnlag og det faktiske situasjonsbildet. Sektorprinsippet fungerer godt i de tilfeller det raskt er mulig å plassere et ansvar og mindre godt der hvor det er overlappende oppgaver. Det oppstår et behov for å balansere ansvars- mot samvirkeprinsippet.

Spenningsfeltet mellom statens behov og individets rettigheter er en krevende øvelse, og i noen tilfeller direkte motstridene. Kollektiv digital overvåkning kan underminere demokratiet i sitt forsøk på å forsvare det, og i tillegg utfordre tilliten og samfunnskontrakten mellom borger og stat. Frykt for en overhengende fare kan sette demokratiske reflekser under press (Øverenget, 2020). Inngripende tiltak kan imidlertid være nødvendig for å kunne ivareta statssikkerheten, men da på bekostning av individets rettigheter. I ytterste konsekvens kan den ultimate rettighet – retten til liv bli en vurderingssak. Statens plikt til å beskytte sine borgere kan tolkes forskjellig. Individorientert eller til fellesskapets beste er en prinsipiell og etisk diskusjon. Stortinget er den lovgivende forsamling som definerer grensedragningen og gir myndighet. Balanseøvelsen definerer vår demokratiske styreform.

For Etterretningstjenesten gir det endrede trusselbilde utfordringer hva gjelder den territorielle begrensning. Et tydelig skille mellom indre og ytre trusler er ikke åpenbart i en verdensorden hvor statsgrenser i mange sammenhenger ikke er meningsfylte. Det samme dilemma oppstår også mellom PST og politiet, skillet mellom terror og organisert kriminalitet er høyst uklart i mange tilfeller.

Begge lovforslag representerer behov for tilpasning til et nytt trusselbilde. Endring i lovgrunnlaget til Etterretningstjenesten, og et behov for beslutningsmyndighet over sektornivå i gitte tilfeller. Tilpasningene er imidlertid kompliserte da endringene reiser nye spørsmål om grensesnitt mot andre aktører, rettsikkerhet og maktbalanse mellom Storting og Regjering. Utfordringene gjør seg gjeldene i hele den norske beredskapen og stiller den nasjonale sikkerhetsarkitektur på prøve.

Jeg vil nå gå over til å se nærmere på gråsoneproblematikk som kan oppstå i kjølvannet av myndighetenes forsøk på å tilpasse seg et dynamisk og komplekst trusselbilde.

6 Gråsonen vokser og kompliserer respons

Forrige kapittel omhandlet hvordan et komplekst trusselbilde påvirker myndighetens utfordringer med organisering og ansvar. I dette kapittelet sees det nærmere på mulige konsekvenser knyttet til usikkerhet om det er stat- eller samfunnssikkerheten som trues og gråsoneproblematikken som følger av dette.

Formålet er å se på faktorer og konsekvenser av organisatorisk art når grensesnittet mellom *normaltilstand* på den ene siden og *krigstilstand* på den andre er uklar. Først omhandles mulige årsakssammenhenger til at gråsonen mellom ulike myndigheters ansvarsområder øker, deretter om

hvordan det hybride scenario påvirker kategoriseringen av cybertrusselen. Er domenet i stor grad sikkerhetisert? Hensikten er å avdekke mulige grunner til at myndighetene satser på tverrsektorielle løsninger. Løsninger som kan bidra til å fragmentere hvem som skal gjøre hva, i hvilken rekkefølge, basert på hvilken situasjonsforståelse og hjemmelsgrunnlag. Analysen tar så for seg myndighetenes innretning og forståelse av truslene. Hvordan påvirkes sikkerhetsarkitekturen når ansvarsprinsippet ikke samsvarer med trusselens kompleksitet, og tas beslutninger med utgangspunkt i verstefallsteorien, til tross for at identifisering i mange sammenhenger er meget vanskelig?

6.1 Gråsonen vokser i takt med utviklingen av trusselbildet

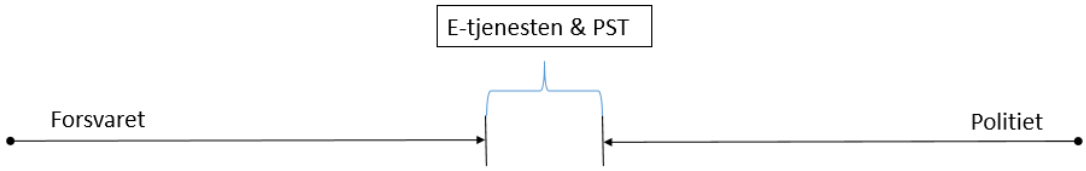
Store multinasjonale tech-selskaper akkumulerer og lagrer store mengder data. Vår avhengighet av teknologi øker i takt med utviklingen. Vi er snart koblet på internett i alle sammenhenger, både privat og profesjonelt ved bruk av smarttelefoner, GPS teknologi i kjøretøy, smart-løsninger. Med avhengighet øker sårbarhet. Tradisjonell tenkning innen sikkerhetspolitikken orienters i stor grad rundt relasjonene mellom stater og internasjonale organisasjoner som FN og NATO. I dag gjør imidlertid en rekke andre faktorer seg gjeldende. Kontroll på informasjonsstrømmen og datamengde gir nye muligheter og makt. Tech-industrien vokser med eksepsjonell fart og selskapene er nå så store at man ikke kan ignorere deres maktposisjon globalt. Vi er nå i et veiskille hvor maktforskyvningen fra stater til selskaper er en realitet. De fem største selskapene representerer nå verdens 3. største økonomi. Kongressen i USA er bekymret over utviklingen og det vurderer å stykke opp selskapene, slik det gjort med olje- og tobakkselskapene på 1900 tallet (Pletten, 2020).

Ansvarsfordelingsspørsmålet er både viktig og vanskelig. Det reiser sentrale maktfordelings- og rettssikkerhetsspørsmål. Beredskapsfeltet er utfordrende å regulere rettslig og det kreves helhetlig tilnærming til de respektive etatenes beredskapsmessige roller. Trusselbildet er ikke lenger like statisk som for få år siden. Dette faktum har klare politiske overtoner og en eventuell ansvarsoverføring i en konkret beredskapssituasjon vil måtte utløses av en politisk beslutning (Auglend, 2015a, punkt.1).

Privatisering og samfunnets raske teknologiske utvikling gjør at skillelinjene mellom Forsvaret, politiet og det sivile samfunn blir stadig mindre. Sammenvevingen tilsier at den gjensidige avhengigheten øker. Komplekse systemer og eierskapsforhold gir nye sårbarheter (NOU2016:19, 2016, s.35). Næringslivet blir stadig en viktigere medspiller i sikkerhetsarbeidet, både i kraft av å forvalte viktige samfunnsfunksjoner og som leverandør til offentlige etater (NSM, 2019b, s.6). Sett i lys av de senere års hendelser og bruk av teknologiske virkemidler for å destabilisere stater, kompliseres bildet ytterligere. Trusselen om hybrid krigføring er høyst reell og må tas på alvor. Terrorisme er videre et grenseoverskridende fenomen som umuliggjør et klart skille mellom ytre og indre trusler. Terrortrusselen kommer fra enkeltpersoner og ikke-statlige organisasjoner som forflytter seg over landegrensene. Teknologi muliggjør forberedelser og styring av terroranslag på tvers av ulike jurisdiksjoner (Forsvarsdepartementet, 2018, s.117).

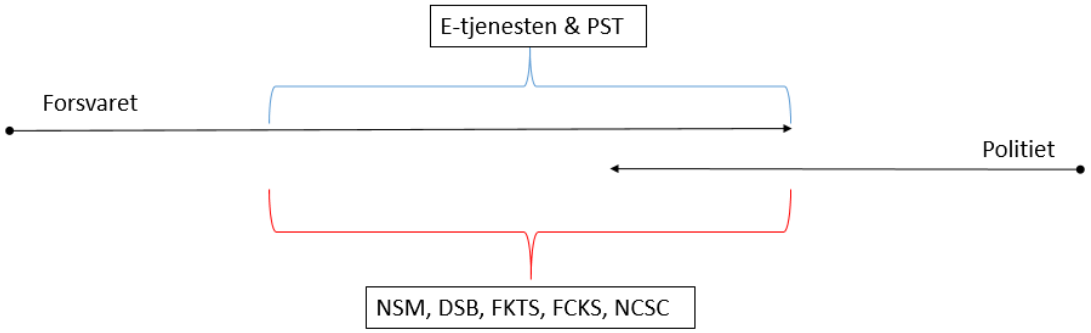
Grensesnittet mellom PST og Etterretningstjenesten er i dag mindre klart (NOU2016:19, s.38). Dette fremkommer tydelig i høringsrunden til ny lov om Etterretningstjenesten. Følgen er at gråsonen vokser, da det er komplisert å definere hvordan trusselen skal oppfattes og attribueres. Jurisdiksjon og overlappende oppgaver kompliserer bildet. Det handler om hvilket perspektiv som legges til grunn. Ansvarsplassering blir dermed vanskelig å definere og mye tyder på at konklusjonen ofte ender midt i mellom. Forskerne Friis og Hansen (2020, s.192-193), foreslår at PST må styrke sin etterretningsfaglige kompetanse og skille ut politi (etterforskning) og påtalemyndighet. De fremmer forslag om at PST bør konsentrere seg om etterretnings- og sikkerhetsfaglige spørsmål og at Etterretningstjenesten i større grad burde bli en nasjonal og sivil tjeneste. En slik løsning vil bidra til å rydde opp i en rekke gråsonekonflikter mellom tjenestene selv og mellom PST og politiet.

Særlig trusler i cyberdomenet er av sektorovergripende karakter. Behovet for informasjonsdeling om slike trusler på tvers av samfunnssektorene og sikkerhetstiltak for å forebygge disse truslene, underbygger viktigheten av et helhetlig og sektorovergripende ansvar (NOU2016:19, s.137). Dette behovet genererer mange grensesnitt mellom forskjellige etater og myndigheter som igjen har ulike roller. Gråsonen kommer som nevnt til uttrykk i både utredninger, rapporter og høringssvar. Endringene kan *meget grovt* illustreres slik i to egenutviklede figurer:



Figur 3. "kald krig" trusselbilde

Figuren søker å illustrere «kald krig» scenarioet, hvor det var klare grensedragninger mellom indre og ytre trusler og tydelig ansvarsfordeling mellom forsvars- og justissektoren.



Figur 4. "utvidede" trusselbilde

Figuren forsøker å visualisere dagens organisering og de ulike etater og enheters overlappende oppgaver. Forsvarets oppdrag er utvidet og er nå tettere knyttet til sivile myndigheter i fredstid enn tidligere. Etterretningstjenestens handlingsrom er betydelig utvidet som følge av ny lov og PST sitt virkeområde er mer internasjonalt etter 9/11 og terrortrusselen. I et dynamisk trusselbilde har ulike tverrsektorielle etater og koordinerende enheter blitt etablert eller fått utvidet mandat. Hybride trusler og digitaliseringen medfører et nytt scenario hvor flere aktører har oppgaver *i samme hendelse*. Dette kan utfordre håndtering når det er flere «interessenter» med ulike oppgaver og hjemmelsgrunnlag. Figuren er ment å illustrere at gråsonen om hvem som skal gjøre hva vokser og det oppståtte behov for en rekke koordinerende institusjoner er tiltagende. Politiets ansvarsområde er relativt konstant i begge tilfeller.

6.2 Tverrsektorielle myndigheters ansvarsområde øker

Utfordringene ved IKT-sikkerhet gjør det vanskelig med et for statisk regelverk eller en for fastlåst organisering av etater (NOU2018:14, s.67). Både organisering og regulering må være fleksibel og kunne tilpasses nye trusler, sårbarheter, teknologier og forretningsmodeller.

Det siste 10 år har en rekke IKT sikkerhetsrelaterte funksjoner blitt etablert. Behovet for overvåkning av kritisk infrastruktur står sentralt innen finans, helse, kraft og kommunikasjonstjenester. NSM er tildelt den nasjonale oppgaven å overvåke samfunnskritisk infrastruktur gjennom et sensornettverk som overvåker kritisk infrastruktur (VDI). NSM har en koordineringsrolle og responsfunksjon hva gjelder digitale trusler. Den primære oppgaven er hendelseshåndtering og gjenoppretting av normalsituasjonen i kritisk infrastruktur (Forsvarsdepartementet & Justisdepartementet, 2018, s.56).

Myndigheten har ikke påtalekompetanse og kan derfor ikke benytte tvangsmidler eller gi pålegg i sine undersøkelser. Enhetens sentrale posisjon innen cybersikkerhet genererer dyp innsikt og kunnskap, men nedsiden er at den er «passiv». Ingen stilles til ansvar og hverken allmenn- eller individualpreventiv effekt oppnås. Attribusjonsproblematikken og staters behov for bevis på hvem som står bak, burde i størst mulig grad tilsi krav til metoder som tilfredsstiller rettslige standarder, og ikke en sannsynlighetsvurdering. Anvendbarheten av kunnskapen i sikkerhetspolitisk kontekst krever presisjon og etterprøvbare bevis. Politiets grensesnitt mot NSM er et eksempel hvor gråsoneproblematikken og valget av kategorisering har stor innvirkning på hvordan en hendelse håndteres. At cyberdomenet i stor grad er sikkerhetisert ved at statlige aktører utpekes som den største trusselaktør, kan avskjære disse hendelsene fra å bli etterforsket som kriminalitet. Angrep i cyberdomenet blir således i stor utstrekning håndtert av etterretning og sikkerhetstjenestene, noe som kan være problematisk i en rettsstat.

Norsk sikkerhetsarkitektur utvikles raskt. Jeg vil nedenfor beskrive hvilke faktorer som påvirker myndighetens organisering. Cyberdomenets kompleksitet og derav vanskeligheter med å identifisere

aktør og intensjon, avstedkommer en rekke tiltak for å fremme samhandling. De siste tre år har først og fremst opprettelsen av Felles cyberkoordineringssenter (FCKS) og Nasjonalt cybersikkerhetssenter (NCSC) i NSM markert myndighetenes satsning. I tillegg er politiets nasjonale cybercrime senter (NC3) blitt opprettet og i 2019 fikk Norge sin første digitaliseringsminister.

6.3 Opprettelsen av det Nasjonale cybersikkerhetssenter (NCSC)

I september 2017 ble IKT-sikkerhetsutvalget oppnevnt i statsråd. Utvalget fikk i mandat å se på dagens regulering av IKT sikkerhet og om dette er hensiktsmessig organisert ovenfor de samfunnsutfordringer Norge har (NOU2018:14, s, 9). En av anbefalingene var opprettelsen av nevnte NCSC underlagt NSM. Utvalget bemerket imidlertid at før senteret kan opprettes er det behov for en nærmere behovs- og kostnadsanalyse som avklarer senterets *myndighetsforankring* og *grensedragning mot øvrige myndigheter*. Høringsfristen på utredningen ble satt til 22. mars 2019.

Uklar grensedragning mellom etater er også berørt av flere høringsinstanser. PST (2019a, s.3) stiller spørsmål om nok et senter vil bidra til det motsatte. Det reises tvil om svaret på koordineringsutfordringer er å øke antall aktører med utydelig mandat. Videre er grensesnittet mot FCKS sin koordinerende rolle og PSTs ansvar for terrorbekjempelse momenter som ikke er definert. Datatilsynet (2019a, s. 2) er også inne på om et nytt senter er hensiktsmessig og foreslår at et bedre alternativ vil være å gi eksisterende departementer klarere føringer om samarbeid. Forsvarsdepartementet (2019, s. 4) foreslår at senteret bør bygges på eksisterende responsmiljøer i NSM og påpeker at eksisterende "oppgaver relatert til statssikkerheten ikke blir svekket" som følge av et utvidet mandat. Politidirektoratet (2019, s. 2-3) er enig med utvalgets anbefaling at det er flere forhold som må utredes før et slikt senter etableres, og bemerker at "utredningen synes kun å vektlegge politiets rolle ved etterforskning og påtale av straffbare forhold og […] ikke i tilstrekkelig grad tar innover seg politiets forebyggende og beredskapsmessige rolle".

13. august 2018 bekjentgjorde NSM på sine hjemmesider at de skal opprette et nasjonalt cybersikkerhetssenter. Senterets oppdrag er å sikre god utnyttelse av samfunnets samlende ressurser. Hovedleveransen vil være rettet mot Forsvarets behov (NSM, 2018). Opprettelsen av senteret undergraver høringsinstituttet da opprettelsen ble besluttet flere måneder før høringsfristens utløpt. I tillegg til at etableringen var imot utvalgets anbefaling om at senteret må ha en tydelig forankring i sivile myndigheter, da behovet først og fremst er knyttet mot sivile samfunnsfunksjoner (NOU2018:14, s.10). Gråsoneproblematikken er her tydelig. Utvalget anbefaler at senteret bør ha knytning mot sivile samfunnsinstitusjoner og NSM selv proklamerer at hovedleveransen skal være rettet mot Forsvarets behov. En forklaring kan være at statlige aktører vurderes til å utgjøre størst trussel i de nasjonale trusselvurderingene. Årsaken kan være sikkerhetstjenestenes omforente konklusjon, at det er stater som er den største fienden.

Neste kapittel omhandler mulige utfordringer med kategoriseringen om en trussel hører hjemme i stat- eller samfunnssikkerhetsdomenet.

6.4 Gråsoneproblematikken i praksis

Tradisjonelt har det vært et mer eller mindre skarpt skille mellom begrepene statssikkerhet og samfunnssikkerhet (NOU2016:19, s.28). Begrepenes innhold og betydning legger føringer for hvordan staten organiserer seg. Da trusselbildet endres tvinges frem behov for justering av meningsinnholdet. Den generelle samfunnsutviklingen kan tilsi behov for en dreining av fokus fra et rent statssikkerhetsperspektiv, til også å omfatte det som tradisjonelt har blitt ansett som en del av den generelle samfunnssikkerheten (NOU2016:19, s.113). Denne dreiningen innebærer imidlertid ikke en avgrensning for Forsvarets ansvarsområde, snarere tvert imot. Trusler som i utgangspunktet berører samfunnssikkerheten kan også ha gyldighet for statssikkerheten. Denne dualismen utfordrer organisering og ansvarsplassering i det norske beredskapssystemet.

Terrortrusselen er også en faktor som påvirker sikkerhetsarkitekturen og som kan sees i forskjellige perspektiv - kriminalitet eller et anslag som truer staten. Ordskiftet om Forsvarets rolle under terroranslaget 22. juli 2011, er senere omtalt og debattert i en rekke sammenhenger. Simonsen (2019, s.62-66) redegjør for gråsoneproblematikken i sin bok «Til forsvar av landet», og diskuterer her om beslutningen til Regjeringen i det heletatt var mulig i en så tidlig fase som tilfelle var. Han reiser spørsmålet om situasjonsbildet var tilstrekkelig til å utelukke at angrepet ikke var en statlig aktør. Uavhengig av beslutningen, anfører han at Forsvarets ansvar for rikets sikkerhet ikke blir suspendert bare fordi handlingen også er en forbrytelse som skal håndteres av politiet. Det ene (kriminalitetsbekjempelse) utelukker ikke det andre (forsvar av landet).

Et komplekst trusselbilde krever at etatene må kunne håndtere de ulike aspekter av situasjonen parallelt om situasjonen skulle tilsi det. Simonsen (2019, s.253 - 254) mener at Forsvaret i slike tilfeller må agere på selvstendig initiativ, uten å måtte vente på anmodning fra politiet. De begge er profesjonelle aktører og vil kunne håndtere et skifte av kommando om situasjonen skulle kreve det. Han får støtte av forskerne Dyndal og Larssen (2020, s.440), som i tillegg påpeker at en slik løsning vil ta bort uklarheter hva gjelder forsvarspersonell og handlingsplikten. Simonsens analyser i boken treffer godt på gråsoneproblematikken. Terror kan godt tenkes å være en hendelse som i sammenheng med andre hendelser, kan indikere at en statlig aktør står bak, med helt andre intensjoner enn hva som kan klassifiseres som kriminalitet. En av utfordringene i dagens trusselbilde er tidsaspektet. I cyberdomenet er responshurtighet av avgjørende betydning. Riktige tiltak til rett tid står sentralt for å begrense skadeomfanget. Spørsmålet er dermed relevant, om ikke flere aktører bør respondere samtidig, men at kommandoforhold og eventuelt beslutningspunktet for overføring av ansvar defineres grundig.

Tidsaspektet og hvilket situasjonsbilde som foreligger når beslutninger tas er viktig når styresmaktene står i et veiskille. Er det statssikkerheten eller samfunnssikkerheten som trues – eller begge? Det samme beslutningspunkt gjør seg gjeldene for avgjørelser som tas på lavere nivå. I cyber er det som nevnt NSM som i stor utstrekning har ansvaret for den initiale hendelseshåndteringen av saker som varsles eller oppdages i VDI nettverket. Mangelfulle opplysninger tidlig i en hendelse kan i mange tilfeller medføre at beslutningen begrunnes i etablert kunnskap og risikoforståelse. Verstefallsteorien er da en sunn tilnærming, men faren for bias er høyst tilstede.

Et eksempel er konklusjonene fra teknologiselskapet Visma som ble utsatt for hacking i 2019. Selskapet gikk ut i pressen og redegjorde for hendelsen og at Kina stod bak. Dette ble imidlertid tilbakevist som en ubegrunnet påstand og Visma måtte gå tilbake på sin initiale konklusjon. Selskapet viste til at identifiseringen var basert på kunnskap *før* angrepet og ikke som følge av analyse av den *konkrete* hendelsen. Sikkerhetsselskapet Mnemonic uttaler i denne sammenheng at det er vanskelig å finne ut hvem som står bak og at det er fort gjort å skylde på Kina og Russland (Skille, 2019).

Eksemplet viser at attribusjonsproblematikken leder til konklusjoner basert på eksisterende kunnskap om modus. Da narrative i stor utstrekning defineres av de hemmelige tjenestene kan situasjonsforståelsen bli preget av et fokus mot statlige aktører. Manglende innsikt om andre aktører kan videre medføre en ensidig klassifisering av trusselsituasjonen i cyber. I Næringslivets sikkerhetsorganisasjons Mørketallsundersøkelse av 2018, fremkommer det at kun 9% av respondentene rapporterer sikkerhetshendelser til politiet, 3 % til NSM NordCert og 2% varsler egen CERT funksjon (NSR, 2018, s.28). Legges disse funn til grunn er det mye som tyder på at det er store mangler hva gjelder kunnskap om totalbildet av trusler i cyber. Manglende trusselvurderinger som tar utgangspunkt i samfunnssikkerheten kan gi en «blindsone». At virksomheter ikke varsler om angrep innebærer at majoriteten av tilfellene ikke blir analysert og satt inn i et nasjonalt trusselperspektiv. I ytterste konsekvens kan dette medføre at myndighetene fatter beslutninger på et manglende empirisk grunnlag. Som omhandlet i kapittel 3.5, mener flere forskere at cybersikkerhet og cybertrusler er dårlig belagt empirisk og preget av uklar analyse og forståelse (Langø, 2013, s.233).

Neste kapittel kan påstås å være en betydelig faktor som påvirker statens utfordring med å tilpasse seg et nytt scenario. Hybride trusler utfordrer sikkerhetsarkitekturen på alle nivå og kompliserer responsevnen, da utfordringen kan sees i flere dimensjoner.

6.5 Hybride trusler – gråsoneproblematikkens mor

I dette komplekse scenario må det tas stilling til hva som er viktigst. Det åpenbare svaret er statens overlevelse. Spørsmålet er hvilke virkemidler og tiltak som er hensiktsmessig i et uoversiktlig og mindre forutsigbart sikkerhetspolitisk bilde. Til tross for at begrepet hybrid krigføring ikke omtales i utstrakt grad i de nasjonale trusselvurderingene, beskrives hendelser hvor dette samsvarer med meningsinnholdet og definisjon. Statssikkerheten trues dermed av angrep hvor det er vanskelig å

identifisere en begynnelse og slutt på fiendtlige handlinger**.** Denne utviskingen utfordrer faseinndelingen som vårt beredskapssystem er bygget på (fred, krise, krig). Resultatet er at man står i en konstant «krigstilstand» (Cullen & Reichborn-Kjennerud, 2016, s.3). Grensesnitt mot normaltilstanden blir dermed uklar og åpner opp for tolkning.

Statens virkemidler til å øve diplomatisk press og i siste instans bruk av militære midler i selvforsvar, vanskeliggjøres da mistenkte stater kan hevde plausibel fornektbarhet som følge av manglende attribusjon. Bruk av mer tradisjonelle handlemåter som militærmakt endres i et slikt scenario. Denne nye virkeligheten kan påvirke maktbalansen mellom stater.

Økonomisk styrke er et virkemiddel som benyttes i økende grad. Den senere tids økonomiske sanksjonsutveksling mellom USA og Kina er et eksempel på dette. Det eksisterer dermed ikke noe klart skille mellom det militære, politiske og sivile innen hybrid krigføring. Elementene kan enkelt studeres separat (militær, politisk og sivilt), men det er essensielt å forstå de i sammenheng for å kunne fastslå at en blir utsatt for angrep på flere nivåer samtidig (Cullen & Reichborn-Kjennerud, 2016, s.4).

Å destabilisere en stat gjennom psykologiske operasjoner eller påvirkning av valg ved bruk av kommunikasjonsteknologi, har i dag et mye større potensiale enn for få år siden. Alle hendelser kan imidlertid ikke settes inn i et slikt scenario. For det første er det attribusjonsutfordringer og for det andre strider en slik tilnærming med sektorprinsippet. I et ensidig statssikkerhetsperspektiv vil dermed «alt» kunne gjøre seg gjeldene.

I det hybride scenario kan en hevde at gråsonen dekker hele spekteret. Gråsone både i forhold til hva, hvem og hvordan – og derav med hvilken intensjon. Kompleksiteten og konsekvensene er så gjennomgående at det er vanskelig å etablere en hensiktsmessig ansvarsfordeling som er balansert mot vårt styresett. Trusselen er som nevnt reell og må derfor løses gjennom kunnskap og utveksling av informasjon. Videre kreves unntaksbestemmelser som kan trekke på alle kapasiteter i samfunnet når situasjonen krever det. Ny fullmaktslov er et slikt tiltak.

Dynamikken i dagens trusselbilde hvor intensjoner, kapasiteter, mål og metoder er i stadig utvikling tilsier at bildet må nyanseres. Vi står ovenfor en felles risiko mer enn en felles fiende som følge av digitalisering og globalisering. Dagens sikkerhetsarkitektur utfordres da ansvarsprinsippet tilsynelatende ikke samsvarer med trusselens mangfold og kompleksitet. I disse overgangene mellom sektorer oppstår gråsoner og glidende overganger (Auglend, 2015a, punkt 2).

Gråsoner forsterkes og utvides ved opprettelse av tverrsektorielle løsninger. Flere skal koordinere, informere og håndtere. Arbeidsdelingen spres ut over på en rekke myndigheter, etater og instanser. Kompleksitet søkes løst med å lage et mer komplekst system som utfordrer kommando og kontroll. På en annen side opprettholdes maktbalansen og demokratisk styring med en slik tilnærming. Skillet mellom stat- og samfunnssikkerhet og hvilken myndighet som er ansvarlig, kan muligens forklares med et verdimessig utgangspunkt. Hvilke prinsipper vårt samfunn skal bygges på for å ivareta våre grunnleggende verdier som menneskeverd, rettssikkerhet og demokrati. En pragmatisk og oppdragsfokusert tilnærming kan komme i konflikt med disse verdiene. Fenomenet hybride trusler er således meget vanskelig å omsette i konkrete organisatoriske beslutninger da selve poenget er å komplisere respons.

6.6 Digitalisering åpner for flere aktører

Skifte i hvordan stater samhandler og integrasjon i verdensøkonomien øker i takt med teknologiutviklingen. Digitale løsninger fremmer informasjonsflyt og knytter produsent og konsument nærmere sammen. Globaliseringen påvirker dermed midlene og kanalene som brukes til å utøve makt. Mykere maktmidler som økonomi og opinionspåvirkning blir som følge av dette vanligere å benytte som virkemiddel for å oppnå nasjonale målsetninger. Dette har innvirkning på militærmaktens rolle (Beadle & Diesen, 2015, s.21). Uavhengig av dette skiftet vil alltid militære maktmidler og alliansetilknytninger måtte ligge som fundament i en stats arsenal av virkemidler.

Globalisering og internasjonalisering øker kontakten, sårbarheten og avhengigheten på tvers av landegrenser. En konsekvens er mulighetsrommet som oppstår for ikke-statlige aktører, som organiserte kriminelle nettverk og terroristgrupperinger. Denne endringen kan medføre en omfordeling eller glidning av makt. Aktørene får dermed mulighet gjennom bruk av teknologi å påvirke den sikkerhetspolitiske situasjonen på bekostning av stater. Flere aktører enn tidligere har nå større mulighet å influere den internasjonale dagsorden (NOU2016:19, s.56). Nye former for makt oppstår dermed ut over størrelse på en stats konvensjonelle kapasiteter. Dette skifte gjør at man må forholde seg til flere elementer enn militærmakt alene. Vendingen representerer en grunnleggende endring fra tidligere (Beadle & Diesen, 2015, s.22-23).

Ikke-statlige aktører disponerer ikke konvensjonell militærmakt. Bruk av irregulære virkemidler er derfor det fortrukne middel. Jo mer sømløs integrering av verdensøkonomien og digitale kommunikasjonsplattformer blir, jo mer sårbar blir stater for innslag av irregulær maktbruk som terror, påvirkning og angrep i cyber (Diesen, 2018, s.34). I erkjennelsen av at all krigføring til sist handler om å påvirke motstanderens adferd ved å påvirke viljen, er informasjonsoperasjoner ved bruk av kommunikasjonsteknologi et sentralt element. Påvirkning av narrative og det faktiske hendelsesforløp er i dagens sikkerhetspolitiske bilde en velkjent strategi (Beadle & Diesen, 2015, s.160).

Utviklingen av kunstig intelligens og maskinlæring bringer overvåkning, utvikling av propaganda og falske nyheter til et helt nytt nivå. Automatiserte prosesser øker kraft og omfang bak både angrep mot kritisk infrastruktur og opinionspåvirkning. Desinformasjon og falske nyheter fremstår nå som mer troverdig og persontilpasset (NOU2018:14, 2018, s.22). Presisjonsnivået øker i takt med den eksplosive økning av datamengde og teknologiutviklingen. Trusselbildet kompliseres jo mer sofistikert angrepene blir og de blir vanskeligere å forsvare seg mot (NOU2018:14, s.23).

Valutaen i denne sammenheng er data. Eierskap til data vurderes til å være verdens mest verdifulle ressurs (Dyndal, 2020, s.50). Data er ingrediensen som brukes til forskjellige formål og den som har mest, har flest muligheter. Informasjonssamfunnet er tett knyttet til internett. Den som kontrollerer kanalene og plattformene vil ha stor mulighet til å øve innflytelse. Denne omfordelingen av makt gjør at ikke-statlige aktører som multinasjonale selskaper får relativt større innflytelse enn tidligere. Staten har ikke lenger like stor kontroll over informasjonsflyten (Beadle & Diesen 2015, s.20). Som eksempel kan nevnes NRK sin avsløring av tilgjengelige «anonymiserte posisjonsdata» kjøpt av et engelsk selskap, en såkalt dataforhandler. Dataene er isolert sett anonyme, men sammenholdt med annen offentlig tilgjengelig informasjon er de identifiserende. NRK kartla en rekke forsvarspersonell som i kraft av sin rolle har strategisk viktige posisjoner (Gundersen, Skille & Lied, 2020). Kunnskap og forvaltning av informasjon kan sies i stor utstrekning å ha skiftet hender fra stater til andre aktører. Sett i lys av Cambridge Analytica skandalen (Grassegger & Krogerus, 2017) og påvirkning av valget i USA, er denne trusselen høyst aktuell. En kan hevde at vi er på vei fra et informasjonssamfunn, til et desinformasjonssamfunn. Helt sentrale beslutninger fattes av kommersielle aktører utenfor den tradisjonelle mellomstatlige arena. (Justisdepartementet, 2017, s.20). I et sikkerhetspolitisk perspektiv kan det være nødvendig at stater tar tilbake initiativet i dette domenet. At de nasjonale trusselvurderingene ikke omhandler dette tema, kan representere en «blindsone» i beslutningsgrunnlaget til myndighetene.

6.7 Delkonklusjon – faktorer i ulike dimensjoner

Utgangspunktet i sikkerhetspolitikken er relasjonen mellom stater og internasjonale organisasjoner som FN og NATO, men dagens trusselbilde omhandler en rekke andre faktorer i tillegg. Privatisering og den raske teknologiske utvikling gjør skillelinjene mellom Forsvaret, politiet og det sivile samfunn mindre. Den gjensidige avhengigheten tiltar og digitaliseringen åpner for flere trusselaktører. Kompleksiteten søkes løst ved å opprette koordinerende sentre og tverrsektorielle myndigheter. Utvidelsen kan bidra til at sikkerhetsarkitekuren i cyber kan fremstå som uklar. Dagens trusselbilde utfordres da ansvarsprinsippet tilsynelatende ikke samsvarer med trusselens kompleksitet.

Attribusjonsproblematikken gjør at kategorisering av aktør baseres på eksisterende kunnskap om modus. Da narrativet tilsynelatende defineres av de hemmelige tjenestene blir hendelser i stor utstrekning håndtert av disse, noe som kan være problematisk for en rettsstat. Faglitteraturen peker på

at cybersikkerhet og cybertrusler er dårlig belagt empirisk og preget av uklar analyse og derav forståelse (Langø, 2013, s.233). Å forstå trusselens virkning i en sammenheng er essensielt for en hensiktsmessig respons. Fenomenet hybride trusler vanskeliggjør responsorganisering av den grunn at modusen nettopp er designet for å skjule intensjon.

Jo mer sømløs integrering av verdensøkonomien og digitale kommunikasjonsplattformer blir, jo mer sårbare blir stater for påvirkning og angrep i cyberdomenet (Diesen, 2018, s. 34). At datafangsten i form av lagring og forvaltning av brukerdata domineres av private aktører reiser nye problemstillinger. Data selges og benyttes til opinionspåvirkning og sosial manipulasjon. Å skape splittelse og polarisere en debatt kan svekke tilliten til både myndighetene og internasjonale organisasjoner som NATO og FN. Faller tilliten mellom borger og stat bort, vil troen på en demokratisk styreform gradvis forvitre. I det frie marked er det lønnsomhet og markedsandeler som er førende. I dette markedet kan stater og andre med onde hensikter kjøpe «ammunisjon» som indirekte har samme effekt som våpen med sprengstoff og krutt. Noe tabloid sagt, er tech-selskapene vår tids våpenforhandlere, kun styrt av finansielle regler for handel og ikke av staters sikkerhetspolitikk eller internasjonale avtaler.

7 Sammenfatning og konklusjon

Oppgavens utgangspunkt er et endret trusselbilde og nødvendigheten av ny sikkerhetstenkning som følge av digitalisering og globalisering. Hendelser i cyberdomenet er vanskelig å attribuere og angrep kan true både stats- og samfunnssikkerheten på samme tid. Dette utfordrer ansvarsfordelingen da trusselen nesten alltid kan sies å være sektorovergripende. Disse endringene utledet til oppgavens problemstilling.

Hvordan tilpasser norske myndigheter seg til et endret trusselbilde og hvilke faktorer kan påvirke utviklingen av sikkerhetsarkitekturen for cyberdomenet?

For å finne ut av hvordan myndighetene tilpasser seg, er det sentralt å avdekke hvilket trusselbilde som blir presentert. Beslutningsgrunnlaget utarbeides av våre etterretnings- og sikkerhetstjenester som konkluderer med at det er statlige aktører som representerer den største trusselen. Gjennomgangen av vurderingene viser imidlertid at teknologiutviklingen går raskt og at en rekke andre aktører opererer mot samme mål, men med forskjellig formål og intensjon. Denne dimensjonen blir ikke tillagt vekt da det ikke utarbeides nasjonale vurderinger som beskriver trusselens virkning i et samfunnssikkerhetsperspektiv. Dette kan gi et asymmetrisk situasjonsbilde. Tilpasninger myndighetene gjør innen lovutvikling og strukturendringer for å imøtekomme truslene, kan derfor hevdes å ha sitt utspring i statssikkerheten.

Sikkerhetsarkitekturen får dermed sitt omdreiningspunkt rundt våre hemmelige tjenester. Forskerne ser utfordringene i et større perspektiv og diskuterer hvilke konsekvenser dette kan ha på samfunnet i stort. At trusselen av forskjellige årsaker defineres som eksistensiell, kan rettferdiggjøre utvidede hjemler til statlige virksomheter i bytte mot sikkerhet. Flere forhold peker mot at cyberdomenet er sikkerhetisert.

Spenningsfeltet mellom statens behov og individets rettigheter er en krevende øvelse, og i noen tilfeller direkte motstridene. Kollektiv digital overvåkning, som den nye Etterretningstjenesteloven gir anledning til, kan underminere demokratiet i sitt forsøk på å forsvare det, og i tillegg utfordre tilliten og samfunnskontrakten mellom borger og stat. Et fokus på statssikkerheten alene kan derfor ha uheldige sider ved seg.

Oppgaven viser at der hvor det tidligere var enkelt å definere en tjeneste sitt myndighetsområde, har digitaliseringen medført et tilnærmet grenseløst scenario. Ulike myndigheter overlapper hverandre på viktige områder, og det oppstår uklarheter om hvem som har ansvar for hva og hvordan arbeidet skal organiseres og koordineres. Utviklingen har gjort det krevende å skille statssikkerhet og samfunnssikkerhet da skillelinjene mellom fred, krise og krig er mindre tydelige. Slik det kan fremstå så er myndighetens tilpasninger i hovedsak en øvelse i å bygge sikkerhetsarkitekturen på eksisterende rammeverk hvor sektoransvar er det førende prinsipp, og opprettelse av ulike koordineringssentre for å sikre samhandling. Virkningen er, som flere påpeker, at gråsonen mellom forsvar, politi og andre myndighetsorganer øker. Spørsmålet er om denne tilnærmingen bedrer eller svekker motstandsdyktigheten.

Å avdekke alle faktorer som kan påvirke sikkerhetsarkitekturen, evner ikke denne oppgaven å svare på. Faktorer som imidlertid kan ha innvirkning er som nevnt først og fremst hvordan trusselnivået beskrives og oppfattes av myndighetene. Situasjonsforståelsen er utgangspunktet for beslutninger. For det andre er den norske modellen med sektoransvar relevant. Et dynamisk og komplekst trusselbilde er vanskelig å organisere seg i forhold til. En modell som bygger videre på en arkitektur etablert i en annen tid, kan medføre uklare ansvarslinjer. Den tredje faktoren er myndighetens søken etter å klassifisere trusselens virkning. Er det stats- eller samfunnssikkerheten som trues? I cyberdomenet tyder mye på at det er begge. Den fjerde faktoren er attribusjonsutfordringer som tvinger frem et veivalg om hvordan og av hvem trusselen skal håndteres. Dette kan avskjære andre myndigheter fra å respondere. Siste faktor jeg velger å løfte frem er gråsoneproblematikk som følge av trusselens kompleksitet og myndighetenes organisatoriske beslutninger.

En konklusjon de fleste kan slutte seg til er at den raske teknologiske utviklingen og sammenvevingen av kapasiteter og tjenester gjør hele samfunnet mer sårbart. Det utvidede trusselbilde har introdusert

nye sikkerhetsutfordringer. Sikkerhetsbegrepet knyttes nå også til forsvar av vitale verdier som samfunnssystem og velstand. Det materialet oppgaven baserer seg på, indikerer at myndighetenes tilnærming til truslene i cyberdomenet i all hovedsak er et sikkerhetsproblem, og implisitt at løsningen ligger i sikkerhetspolitikkens repertoar. Hvis en legger til grunn at trusselen i cyberdomenet omfatter mer enn statssikkerheten, kan en hevde at myndighetene allerede på hoppkanten kommer skjevt ut.

Litteraturliste

Auglend, R. L. (2015a). Fordelingen av ansvar og myndighet mellom politi og forsvar ved indre beredskap. *Tidsskrift for strafferett, 15*(03), 316-347.

Auglend, R. L. (2015b). Polisiær handleplikt, kommandomyndighet og lydighetsplikt i operativ og innsatsrettet virksomhet. I: Doktorgradsavhandling. Universitetet i Bergen, Juridisk fakultet, Bergen.

Beadle, A. W. & Diesen, S. (2015). *Globale trender mot 2040 - implikasjoner for Forsvarets rolle og relevans* (2015/01452). Hentet fra https://publications.ffi.no/nb/item/asset/dspace:2517/15-01452.pdf

Buzan, B., Wæver, O. & De Wilde, J. (1998). *Security: A new framework for analysis* Lynne Rienner Publishers.

Creswell, J. W. (2014). *Research design : qualitative, quantitative, and mixed methods approaches* (4th ed.; International student ed. utg.). Los Angeles, Calif: SAGE.

Cullen, P. & Reichborn-Kjennerud, E. (2016). What is Hybrid Warfare. *Norwegian Institute of International Affairs Policy Brief, 1*, 2016.

Datatilsynet. (2019a). *Høringssvar NOU2018:14, IKT-sikkerhet i alle ledd*. Hentet fra https://www.regjeringen.no/contentassets/53124f4f93514d0eae3969076c3ca7bc/datatilsynet.pdf?uid=Datatilsynet

Datatilsynet. (2019b). *Høringsuttalelse om forslag til ny lov om Etterretningstjenesten*. Hentet fra https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=e0b87829-2c74-4f2c-8066-c75801bcd0d5

Diesen, S. (2018). Lavintensivt hybridangrep på Norge i en fremtidig konflikt. *FFI 18/00080*. Hentet fra https://publications.ffi.no/nb/item/lavintensivt-hybridangrep-pa-norge-i-en-fremtidig-konflikt

Difi. (2014). *Mot alle odds? Veier til samordning i norsk forvaltning* (2014:07). Hentet fra https://www.difi.no/sites/difino/files/mot-alle-odds.-veier-til-samordning-i-norsk-forvaltning-difi-rapport-2014-7_0.pdf

Drmola, J., Pavlíková, M., Maďar, T., Budirská, L., Suchý, P., Harašta, J., … Schmidt, N. (2015). *Perspectives on Cybersecurity* MASARYKOVA UNIVERZITA.

DSB. (2019a). *Analyser av krisescenarioer 2019*. Hentet fra https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf

DSB. (2019b). *Høringssvar til NOU2019:13 Når krisen inntreffer*. Hentet fra https://www.regjeringen.no/contentassets/d19f56d9f240423f9a935543dc4f5270/direktoratet-for-samfunnssikkerhet-og-beredskap.pdf?uid=Direktoratet_for_samfunnssikkerhet_og_beredskap

Dyndal, G. & Larssen, A. K. (2020). Om handlingsprinsippet, "gråsonekriser" og korona. I A. K. Larssen & G. Dyndal (Red.), *Startegisk ledelse i krise og krig - det norske systemet* (s. 437-447). Oslo: Universitetsforlaget.

Dyndal, G. L. (2020). Fremsyn om sikkerhets-dynamikken og truslene. I A. K. Larssen & G. Dyndal (Red.), *Strategisk ledelse i krise og krig* (s. 35-57). Oslo: Universitetsforlaget.

Ekspertgruppen. (2015). *Et felles løft*. Forsvarsdepartementet. Hentet fra https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/et-felles-loft-webversjon.pdf

EOS-utvalget. (2019). *Høringssvar om forslag til ny lov om Etterretningstjenesten*. Hentet fra https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=7fb7c142-e17d-4ca4-bf49-3f7afb1ee1fc

Etterretningstjenesteloven. (2020). *Lov om Etterretningstjenesten* (LOV-2020-06-19-77). Hentet fra https://lovdata.no/dokument/NL/lov/2020-06-19-77?q=etterretningstjenesteloven

Etterretningstjenesten. (2011). *FOKUS 2011*. Hentet fra https://forsvaret.no/fakta_/ForsvaretDocuments/FOKUS-2011.pdf
Etterretningstjenesten. (2012). *FOKUS 2012*. Hentet fra https://forsvaret.no/fakta_/ForsvaretDocuments/FOKUS-2012.pdf
Etterretningstjenesten. (2013). *FOKUS 2013*. Hentet fra https://forsvaret.no/fakta_/ForsvaretDocuments/FOKUS-2013.pdf
Etterretningstjenesten. (2014). *FOKUS 2014*. Hentet fra https://forsvaret.no/fakta_/ForsvaretDocuments/FOKUS-2014.pdf
Etterretningstjenesten. (2015). *FOKUS 2015*. Hentet fra https://forsvaret.no/ForsvaretDocuments/FOKUS2015-endelig.pdf
Etterretningstjenesten. (2016). *FOKUS 2016*. Hentet fra https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus%202016.pdf
Etterretningstjenesten. (2017). *FOKUS 2017*. Hentet fra https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus2017.pdf
Etterretningstjenesten. (2018). *FOKUS 2018*. Hentet fra https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus2018_bokmaal_oppslag_godkjent.pdf
Etterretningstjenesten. (2020). FOKUS 2020. Hentet fra https://forsvaret.no/presse_/ForsvaretDocuments/Fokus2020-web.pdf
Forsvarsdepartementet. (2018). *Forslag til ny lov om Etterretningstjenesten*. Oslo. Hentet fra https://www.regjeringen.no/contentassets/556459ec77bd448f828af034dd573e11/horingsnotat---forslag-til-ny-lov-om-etterretningstjenesten.pdf
Forsvarsdepartementet. (2019). *Høringssvar NOU2018:14, IKT-sikkerhet i alle ledd*. Hentet fra https://www.regjeringen.no/contentassets/53124f4f93514d0eae3969076c3ca7bc/forsvarsdepartementet.pdf?uid=Forsvarsdepartementet
Forsvarsdepartementet. (2020a). *Høringssvar til NOU2019:13, Når krisen inntreffer*. Hentet fra https://www.regjeringen.no/contentassets/d19f56d9f240423f9a935543dc4f5270/fd.pdf?uid=Forsvarsdepartementet
Forsvarsdepartementet. (2020b). *Lov om Etterretningstjenesten (etterretningstjenesteloven)* (Prop. 80 L (2019-2020)). Hentet fra https://www.regjeringen.no/contentassets/b7bada5f31bc482092318df675a2019d/no/pdfs/prp201920200080000dddpdfs.pdf
Forsvarsdepartementet & Justisdepartementet. (2018). *Støtte og samarbeid - en beskrivelse av totalforsvaret i dag*. Hentet fra https://www.regjeringen.no/contentassets/5a9bd774183b4d548e33da101e7f7d43/stotte-og-samarbeid-en-beskrivelse-av-totalforsvaret-i-da.pdf
Friis, K. & Hansen, V. V. (2020). Etterretningstjeneste og det nye trusselbildet: Er de beredt? I A. K. Larssen & G. Dyndal (Red.), *Strategisk ledelse i krise og krig - det norske systemet* (s. 183-195). Oslo: Universitetsforlaget.
Grassegger, H. & Krogerus, M. (2017). Dataene som snudde verden på hodet. *NRK*. Hentet fra https://nrkbeta.no/2017/02/04/dataene-som-snudde-verden-pa-hodet/
Grønmo, S. (2016). Samfunnsvitenskapelige metoder (2. utg.) Oslo: Fagbokforlaget.
Gundersen, M., Skille, Ø. B. & Lied, H. (2020). Når mobilen blir fienden. *NRK*. Hentet fra https://www.nrk.no/norge/xl/norske-offiserer-og-soldater-avslort-av-mobilen-1.14890424
Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser? : innføring i samfunnsvitenskapelig metode* (3. utg. utg.). Oslo: Cappelen Damm akademisk.

Jansen, P. T. & Haugestad, E. T. (2020). Etterretningstjeneste: Bidra til politisk og militær ledelse. I A. K. Larssen & G. Dyndal (Red.), *Strategisk ledelse i krise og krig - det norske systemet* (s. 154-165). Oslo: Universitetsforlaget.
Jensen, M. S. (2019). Cyber resilience, sectoral principle and responsibility placement-Nordic experience. *Internasjonal Politikk, 77*(3), 266-277.
Johannessen, A., Christoffersen, L. & Tufte, P. A. (2016). *Introduksjon til samfunnsvitenskapelig metode* (5. utg. utg.). Oslo: Abstrakt forlag.
Johnsen, R. (2013). Cyberkrigføring og Forsvarets operative evne. *Internasjonal Politikk, 71*(2), 241-251. Hentet fra http://www.idunn.no/ip/2013/02/cyberkrigfoering_og_forsvaretsoperative_evne
Justisdepartementet. (2005). *Instruks for Politiets sikkerhetstjeneste* (FOR-2005-08-19-920). Lovdata. Hentet fra https://lovdata.no/dokument/INS/forskrift/2005-08-19-920
Justisdepartementet. (2017). *IKT-sikkerhet et felles ansvar* (Meld. St. 38). Oslo. Hentet fra https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf
Kaufmann, M. (2018). Kriminalitetskontroll eller sikkerhetspolitikk? *Nytt Norsk Tidsskrift, 35*(01), 21-31.
Kjølberg, A. & Jeppesen, M. (2001). *En modell for sikkerhetstenkning etter den kalde krigen* (2001/04595). Hentet fra https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/1017/01-04595.pdf?sequence=1&isAllowed=y
Koronaloven. (2020). *Midlertidig lov om forskriftshjemmel for å avhjelpe konsekvenser av utbrudd av Covid-19* (LOV-2020-03-27-17). Hentet fra https://lovdata.no/pro/#document/NLO/lov/2020-03-27-17
KRIPOS. (2019). *Høringssvar om forslag til ny lov om Etterretningstjenesten*. Hentet fra https://www.regjeringen.no/contentassets/287d2d52ddb847849cddb49796456129/horingssvar-med-merknader---kripos.pdf?uid=Kripos
Kristiansen, M. & Hoem, N. (2019). Avskrekking som element i cybersikkerhetsstrategi fra et småstatsperspektiv. *Internasjonal Politikk, 77*(3), 252-265.
Kvernberg, T. & Johnsen, S. T. (2013). *Cyberdomenet, cybermakt og norske interesser* (2013/02712). Hentet fra http://rapporter.ffi.no/rapporter/2013/02712.pdf
Langø, H.-I. (2013). Den akademiske debatten om cybersikkerhet. *Internasjonal Politikk, 71*(02), 229-240.
Langø, H.-I. & Sandvik, K. B. (2013). Cyberspace og sikkerhet. *Internasjonal Politikk, 71*(2), 221-228. Hentet fra http://www.idunn.no/ip/2013/02/cyberspace_og_sikkerhet
Larssen, A. K. (2020). Strategisk ledelse av sikkerhetspolitiske kriser. I A. K. Larssen & G. Dyndal (Red.), *Strategisk ledelse i krise og krig - det norske systemet* (s. 352-367). Oslo: Universitetsforlaget.
Lewis, J. (2011). Cyberwar thresholds and effects. *IEEE Security & Privacy, 9*(5), 23-29.
Lynn III, W. F. (2010). Defending a new domain-the Pentagon's cyberstrategy. *Foreign Aff., 89*, 97.
Lysne II-utvalget. (2016). *Digitalt grenseforsvar (DGF)*. Hentet fra https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/lysne-ii-utvalgets-rapport-2016.pdf
Maaø, O. J. (2020). En introduksjon til fagfeltet sivil-militære relasjoner. I A. K. Larssen & G. Dyndal (Red.), *Strategisk ledelse i krise og krig - det norske systemet* (s. 122-135). Oslo: Universitetsforlaget.
Muller, L. P. (2016). Makt og avmakt i cyberspace: hvordan styre det digitale rom? *Internasjonal Politikk, 74(4)*.
Muller, L. P. (2019). Inn i gråsonen: avskrekking som forsvar av cyberspace? *Internasjonal Politikk, 77*(3), 288-295.

NIM. (2019). *Høringssvar om forslag til ny lov om Etterretningstjenesten*. Hentet fra https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=1b03fe18-1d1e-4be5-a7ce-5f1dc785695a
NOU2016:19. (2016). *Samhandling for sikkerhet - beskyttelse av grunnleggende samfunnsfunksjoner*. Hentet fra https://www.regjeringen.no/contentassets/03960058f3f94fbe9d290593bee22c1a/no/pdfs/nou201620160019000dddpdfs.pdf
NOU2018:14. (2018). *IKT-sikkerhet i alle ledd* (NOU 2018:14). Hentet fra https://www.regjeringen.no/contentassets/0d408600df2f4738a9bbb85040b02b59/no/pdfs/nou201820180014000dddpdfs.pdf
NOU2019:13. (2019). *Når krisen inntreffer*. Hentet fra https://www.regjeringen.no/contentassets/65139848c9b2437cb0596e53705314fb/no/pdfs/nou201920190013000dddpdfs.pdf
NSM. (2011). *Rapport om sikkerhetstilstanden 2011*. Hentet fra https://nsm.no/getfile.php/133753-1592918149/Demo/Dokumenter/Rapporter/rst_2011.pdf
NSM. (2012). *Rapport om sikkerhetstilstanden 2012*. Hentet fra https://nsm.no/getfile.php/133741-1592917181/Demo/Dokumenter/Rapporter/rst_2012.pdf
NSM. (2014). *Sikkerhetstilstanden 2014*. Hentet fra https://nsm.no/getfile.php/133738-1592917122/Demo/Dokumenter/Rapporter/rst_2014.pdf
NSM. (2015). *RISIKO 2015*. Hentet fra https://nsm.no/getfile.php/133732-1592916559/Demo/Dokumenter/Rapporter/nsm_risiko_2015-web.pdf
NSM. (2016). *RISIKO 2016 - Kan sikkerhet styres?* Hentet fra https://nsm.no/regelverk-og-hjelp/rapporter/risikorapporter-fra-2019-og-tidligere/
NSM. (2017). *RISIKO 2017 - Risiko og sårbarheter i en ny tid*. Hentet fra https://nsm.no/getfile.php/133726-1592915950/Demo/Dokumenter/Rapporter/nsm_risiko_2017_lr_0404_enkelts_v3.pdf
NSM. (2018). NSM etablerer Nasjonalt cybersikkerhetssenter. Hentet 30. august 2020 fra https://nsm.no/aktuelt/nsm-etablerer-nasjonalt-cybersikkerhetssenter
NSM. (2019a). *Høringssvar til NOU2019:13, Når krisen inntreffer*. Hentet fra https://www.regjeringen.no/contentassets/d19f56d9f240423f9a935543dc4f5270/nasjonal-sikkerhetsmyndighet.pdf?uid=Nasjonal_sikkerhetsmyndighet
NSM. (2019b). *RISIKO 2019 - Krafttak for et sikrere Norge*. Hentet fra https://nsm.no/getfile.php/133696-1592910347/Demo/Dokumenter/Rapporter/nsm_risiko_2019_final_enkeltside.pdf
NSM. (2020). *RISIKO 2020*. Hentet fra https://nsm.no/getfile.php/131421-1587034764/Hermans%20undermappe%20med%20bilder/NSM_Risiko_2020_web_0104.pdf
NTB. (2020). Etterretningsskandale i Danmark - sjef permitert. *Aftenposten*. Hentet fra https://www.aftenposten.no/verden/i/Wb987K/etterretningsskandale-i-danmark-sjef-permittert
Næringslivets-sikkerhetsråd. (2018). *Mørketallsundersøkelsen 2018*. Oslo: NSR. Hentet fra https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen
Næringslivets-sikkerhetsråd. (2019). *Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO)*. Oslo: NSR. Hentet fra https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/krisino
Pletten, C. (2020). Monopolmakten til Big Tech. *Aftenposten*. Hentet fra https://www.aftenposten.no/meninger/kommentar/i/0nMn3A/monopolmakten-til-big-tech-christina-pletten

Politidirektoratet. (2019). *Høringssvar NOU2018:14, IKT-sikkerhet i alle ledd*. Hentet fra https://www.regjeringen.no/contentassets/53124f4f93514d0eae3969076c3ca7bc/politidirektoratet-med-uttalelse-fra-kripos.pdf?uid=Politidirektoratet_(med_uttalelse_fra_Kripos)
Politidirektoratet. (2020). *Høringssvar til NOU2019:13, Når krisen inntreffer*. Hentet fra https://www.regjeringen.no/contentassets/d19f56d9f240423f9a935543dc4f5270/politidirektoratet.pdf?uid=Politidirektoratet,_Oslo_politidistrikt,_Politih%C3%B8gskolen,_Innlandet_politidistrikt_og_Politiets_utlendingsenhet
PST. (2011). *Trusselvurdering 2011*. Hentet fra https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2011/
PST. (2014). *Trusselvurdering 2014*. Hentet fra https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2014/
PST. (2015). *Åpen trusselvurdering 2015*. Hentet fra https://www.pst.no/globalassets/artikler/trusselvurderinger/trusselvurdering-2015.pdf
PST. (2016). *Trusselvurdering 2016*. Hentet fra https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2016/
PST. (2017). *Trusselvurdering 2017*. Hentet fra https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2017.pdf
PST. (2018). *Trusselvurdering 2018*. Hentet fra https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2018.pdf
PST. (2019a). *Høringssvar NOU2018:14, IKT-sikkerhet i alle ledd*. Hentet fra https://www.regjeringen.no/contentassets/53124f4f93514d0eae3969076c3ca7bc/politiets-sikkerhetstjeneste.pdf?uid=Politiets_sikkerhetstjeneste
PST. (2019b). *Høringssvar om forslag til ny lov om Etterretningstjenesten*. Hentet fra https://www.regjeringen.no/contentassets/287d2d52ddb847849cddb49796456129/horingssvar-med-merknader---pst.pdf?uid=PST
PST. (2019c). *Trusselvurdering 2019*. Hentet fra https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf
PST. (2020a). *Høringssvar til NOU2019:13, Når krisen inntreffer*. Hentet fra https://www.regjeringen.no/contentassets/d19f56d9f240423f9a935543dc4f5270/politiets-sikkerhetstjeneste.pdf?uid=Politiets_sikkerhetstjeneste
PST. (2020b). *Nasjonal trusselvurdering 2020*. Hentet fra https://pst.no/globalassets/artikler/utgivelser/2020/nasjonal-trusselvurdering-2020-print.pdf
Påtalemyndigheten. (2020). Det nasjonale statsadvokatembetet (NAST). Hentet fra https://www.riksadvokaten.no/oversikt-over-statsadvokater-og-embeter/
Rid, T. (2013). *Cyber war will not take place* Oxford University Press, USA.
Riksadvokaten. (2019a). *Høringssvar om forslag til ny lov om Etterretningstjenesten*. Hentet fra https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=26e56eae-1e99-4300-8ff1-368ff7802abc
Riksadvokaten. (2019b). *Høringssvar til NOU2019:13, Når krisen inntreffer*. Hentet fra https://www.regjeringen.no/contentassets/d19f56d9f240423f9a935543dc4f5270/riksadvokaten.pdf?uid=Riksadvokaten
Romarheim, A. (2019). Totalforsvaret - en uunværlig umulighet? I P. M. Norheim-Martinsen (Red.), *Det nye Totalforsvaret* (bd. 1). Oslo: Gyldendal Norsk Forlag AS.
Rottem, S. V. (2007). Forsvarets mal og strategi: sikkerhet for hvem? *Internasjonal Politikk, 65*(1), 39.

Røislien, H. E. (2020). Cyberdomenet: Frihet med slagside. I A. K. Larssen & G. Dyndal (Red.), *Strategisk ledelse i krise og krig - det norske systemet* (s. 196-215). Oslo: Universitetsforlaget.
Sandvik, K. B. (2013). Cyberkrig og internasjonal rett. *Internasjonal Politikk, 71*(2), 252-262. Hentet fra http://www.idunn.no/ip/2013/02/cyberkrig_og_internasjonal_rett
Sikkerhetsloven. (2019). *Lov om nasjonal sikkerhet*. Hentet fra https://lovdata.no/dokument/NL/lov/2018-06-01-24
Simonsen, S. (2019). *Til forsvar av landet - rettslige rammer og gråsoner i fred, krise og krig*. Bergen: Fagbokforlaget.
Singer, P. W. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What everyone needs to know*. N.Y USA: Oxford University press.
Skille, Ø. B. (2019). Tvil om hvem som står bak dataangrepet mot Visma. *NRK*. Hentet fra https://www.nrk.no/norge/tvil-om-hvem-som-star-bak-visma-hackingen-1.14420262
Smith, E. (2015). «Ministerstyre»-et hinder for samordning? *Nytt Norsk Tidsskrift, 32*(03), 258-266.
Steen-Johnsen, K., Enjolras, B. & Wollebæk, D. (2013). Sosiale medier, samfunnspolitisk deltagelse og kontroll. *Internasjonal Politikk, 71*(2), 263-273. Hentet fra http://www.idunn.no/ip/2013/02/sosiale_medier_samfunnspolitisk_deltagelse_og_kontroll
Stortinget. (2020). *Lovvedtak 134 (2019-2020)*. Hentet fra https://www.stortinget.no/globalassets/pdf/lovvedtak/2019-2020/vedtak-201920-134.pdf
Straffeloven. (2005). *Lov om straff* (LOV-2005-05-20-28). Hentet fra https://lovdata.no/dokument/NL/lov/2005-05-20-28/KAPITTEL_2-5#KAPITTEL_2-5
Svenungsen, B. (2019a). Internett som geopolitisk arena? *Internasjonal Politikk, 77*(3), 225-240.
Svenungsen, B. (2019b). Vårt digitale fundament. *IFS Insight 5/2019*. Hentet fra https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2614405/IFS%20Insight%205_2019.pdf?sequence=1&isAllowed=y
Telenor. (2015). Høringsuttalelse om forslag til endringer i sikkerhetsloven. Hentet fra https://www.regjeringen.no/no/dokumenter/horing---forskrifter-til-ny-sikkerhetslov/id2606681/?uid=f61c6605-cc43-4f2d-ba9e-cd06ebef4222
Tjora, A. (2017). *Kvalitative forskningsmetoder i praksis*. Oslo: Gyldendal Akademisk.
Trædal, T. (2018). En oppskrift på cyberlapskaus? *Politiforum*. Hentet fra https://www.politiforum.no/cyberkriminalitet-fcks-nasjonalt-cybersikkerhetssenter/en-oppskrift-pa-cyber-lapskaus/147152
Øverenget, E. (2020). Vi bør frykte frykten. *NRK*. Hentet fra https://www.nrk.no/ytring/vi-bor-frykte-frykten-1.15150428