Cybersikkerhet

Digitale sårbarheter i totalforsvaret

Christian Lien

Masteroppgave i statsvitenskap, institutt for statsvitenskap

UNIVERSITETET I OSLO

Vår 2018

Antall ord: 31 071

Cybersikkerhet - Digitale sårbarheter i totalforsvaret

År 2018

Cybersikkerhet - Digitale Sårbarheter i Totalforsvaret

Christian Lien

http://www.duo.uio.no/

Trykk: Reprosentralen, Universitetet i Oslo

Sammendrag

Formålet med denne oppgaven er å undersøke totalforsvarets relevans, i lys av et stadig mer komplekst og omskiftelig trusselbilde. Norge står overfor en betydelig risiko for å bli rammet av sikkerhetstruende hendelser, da den nasjonale sårbarhetsflaten øker ved at digitale sårbarheter, i tråd med feil, forplantes raskt mellom leddene i verdikjedene. Digitaliseringen av samfunnet har resultert i betydelige endringer i samfunnets strukturer hvor trusselbildet omhandler en stadige økende tematisering av sivile utfordringer, fremfor militære utfordringer. Det teknologiske paradigme skifte innen sikkerhets- og forsvarspolitikk har forenklet fremmede staters etterretningsvirksomhet i det digitale rom, hvor digitale sikkerhetsutfordringer utfordrer totalforsvarets rolle i henhold til forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering.

Gjennom innholdsanalyse av trussel- og risikovurderinger fra Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Etterretningstjenesten (E-tjenesten) kartlegges sikkerhetstilstanden og digitale sikkerhetsutfordringer som totalforsvaret står overfor i fredstid. Analyseformens underliggende ambisjon om å trekke slutninger til forhold utenfor teksten, viser dermed til at vedvarende russisk etterretningsvirksomhet ikke fremstår som en handling med utelukkende etterretningsinnhentingsformål, men som i kombinasjon med å teste sårbarheter i sentrale norske systemer. Ved å benytte *cybersikkerhetsdilemmaet* som hovedteori analyseres prosessen før en eventuell konflikt finner sted, med utgangspunkt i at etterretningsaktivitet som i hovedsak kun skal innhente informasjon som en defensiv aktivitet, kan misforståes og oppfattes som om et angrep er nært forekommende. Deteksjonsmekanismene i det sivile samfunn utfordres, dermed aktualiseres Forsvaret, ettersom det ikke er de angrepene vi kjenner som utgjør det største samfunnsrelaterte problemet, men de angrepene vi ikke kjenner. Oppgaven konkluderer med svikt i totalforsvaret da den sivile støtten angripes ved forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering av digitale sikkerhetsutfordringer som følge av digitale sårbarheter. Samfunnets totale sårbarhetsflate økes da digitale sårbarheter og feil forplantes mellom virksomheter og resulterer i strukturelle samfunnsmessige sårbarheter.

Forord

Teori er når man forstår alt, men ingenting virker. Praksis er når alt virker, men ingen forstår hvorfor.

Jeg vil gjerne benytte anledningen til først og fremst å takke mine to veiledere, Janne Haaland Matlary og Siri Strand, for tilbakemeldingene som har vært grunnlaget for et godt samarbeid. Deres ekspertise og faglige dybde har tilført oppgaven utelukkende positive bidrag. Videre vil jeg takke medstudenter som ble til venner for innholdsrike debatter og trivelige lunsjpauser i 9 etg. på Eilert Sunds hus, dere gjorde livet på Blinder lettere.

Eventuelle faktafeil og mangelfull informasjon er mitt ansvar alene.

Oslo, mai 2018

Christian Lien

Innholdsfortegnelse

1 Introduksjon 1
1.1 Bakgrunn for oppgaven 1
1.1.1 Resiliens 4
1.2 Valg av problemstilling 5
1.3 Tidligere og pågående forskning 7
1.4 Avgrensing og Aktualitet 9
1.4.1 Cybersikkerhet 9
1.4.2 Cyberoperasjoner/datanettverksoperasjoner 10
1.4.3 Aktualitet 12
1.5 Disposisjon av oppgaven 13
2 Teoretisk tilnærming og utvalg av forskningslitteratur 14
2.1 Sikkerhets- og forsvarspolitiske mål 14
2.1.1 Forsvarets oppgaver 15
2.2 Den realistiske fagtradisjonen 16
2.3 Sikkerhetsdilemmaet 17
2.3.1 Den kalde krigen 17
2.3.2 Operasjon misforståelse 20
2.4 Cybersikkerhetsdilemmaet 21
3 Metode 26
3.1 Valg av forskningsdesign 26
3.2 Datainnsamling 28
3.3 Validitet og reabilitet 29
3.3.1 Validitet 29
3.3.2 Reliabilitet 31
4 Empiri 33
4.1 Den nye trusseldimensjonen 33
4.1.1 Politisk motivert cyberoperasjon mot Estland 34
4.1.2 Russlands posisjon: Georgia og Ukraina 35
4.1.3 Stuxnet 37
4.1.4 NotPetya 38
4.2 Statlig etterretning 39

4.2.1 Alle piler peker mot Russland 39
4.2.2 Russiske simulerte angrep mot norske mål 41
4.2.3 Cyberoperasjon mot Norge 42
4.2.4 Internasjonale trender 45
5 Analyse 47
5.1 Ny Normaltilstand 47
5.1.1 Sikkerhetstilstanden 48
5.1.2 Etablering av bakdører – fremmede staters etterretningsvirksomhet fremlagt av PST, NSM og E-tjenesten 52
5.1.3 Første delkonklusjon 55
5.2 Etterretningsmål 57
5.2.1 Metode og målvalg 59
5.2.2 Digital sabotasje 60
5.2.3 Kritisk infrastruktur og kritiske samfunnsfunksjoner 62
5.2.4 Andre delkonklusjon 67
5.3 Realpolitikk i det digitale rom? 69
5.3.1 Kanarifugl i kullgruve 71
5.3.2 Sårbarhetsreduserende tiltak 73
5.3.3 En mulig trussel 74
5.3.4 En potensiell sikkerhetspolitisk krise? 76
5.3.5 Sivilt- militært samarbeid 77
5.3.6 Tredje delkonklusjon 81
6 Konklusjon 84
6.1 Oppgavens funn 85
6.2 Kritikk og forslag til videre forskning 89
Litteraturliste 92
Vedlegg 101
Vedlegg 1 101
Vedlegg 2 108
Vedlegg 3 109

Illustrasjoner:

Figur 1.0 Krisespekteret (Daae, 2017:7). 4
Figur 2.0 Animasjon av et spear-phising angrep (Departement of Homeland security & the Federal Bureau of Investigation, 2016:2)..... 42
Figur 3.0 Aktører innen russisk spionasje i det digitale rom (Välisluureamet, 2018:55). 44
Figur 4.0 Forebyggende sikkerhet (Elgsaas & Heireng, 2014:10)..... 49
Figur 5.0 Hvilken type hendelse norske virksomheter har vært utsatt for (Næringslivet sikkerhetsråd, 2016:11). 50
Figur 6.0 Endringer i organisasjonen som følge av hendelsen (Næringslivets sikkerhetsråd, 2016:21). 51
Figur 7.0 viser til utfyllende informasjon om alias, oppstartperiode, taktikk, teknikk og prosedyrer (TTPs) vedrørende cyberangrep og etterretningsmål for APT28 og APT29 (Muller, Gjesvik & Friis, 2018:17). 59
Figur 8.0 Kritisk infrastruktur og kritiske samfunnsfunksjoner (Norges offentlige utredninger, 2006:16). 64
Figur 9.0 Befolkningens sikkerhet basert på samfunnsfunksjonen IKT-sikkerhet med kapabiliteter (Direktoratet for samfunnssikkerhet og beredskap, 2016:63). 78
Figur 10.0 Forsvarets nasjonale operasjoner i henhold til de kategoriserte konfliktnivå (Forsvaret, 2014;66). 79

1 Introduksjon

Introduksjonskapittelet redegjør for oppgavens konseptuelle rammer. Kapittelet utdyper bakgrunn for oppgaven og redegjør for resiliens som et sentralt begrep. Videre utdypes valg av problemstilling, etterfulgt av en redegjørelse av den akademiske debatten med tidligere og pågående forskningsprosjekt av relevans, før denne oppgaven plasseres i henhold til relevante studier. Videre utdypes oppgavens relevans og avgrensning spesifiseres for å underbygge nødvendigheten av økt fokus på forskningsområdet. Avslutningsvis redegjøres det for oppgavens fem resterende kapitler.

1.1 Bakgrunn for oppgaven

Denne oppgaven omhandler totalforsvaret og digitale sårbarheter som forårsaker digitale sikkerhetsutfordringer. Oppgaven tar sikte på å undersøke totalforsvarskonseptets relevans i en tid preget av en ny trusseldimensjon. Totalforsvaret er et produkt av etterkrigstiden, hvor datidens totalforsvar vektla sterk samhandling mellom det militære og sivile samfunn, for å sikre og ivareta nasjonale verdier, landets selvstendighet, territorium og det øvrige samfunn. I tråd med samfunnsutviklingen ble totalforsvarskonseptet modernisert og omfatter i dag gjensidig støtte mellom forsvar og det sivile samfunn i forbindelse med forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering. En av Forsvarets eksplisitte oppgaver er å bidra til ivaretagelse av samfunnssikkerhet, derav skal Forsvaret i større grad enn tidligere yte støtte til det sivile samfunn i fredstidskriser (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2015:12). Det moderniserte totalforsvaret forblir aktuelt, ettersom forsvarssektoren er avhengig av sivil infrastruktur og tjenesteproduksjon for å kunne løse Forsvarets oppgaver som er tuftet på en operasjonalisering av de forsvarspolitiske målene (Forsvarsdepartementet, 2016:46). Den sivile støtten til Forsvaret baseres i stor grad på kommersielle ordninger og samarbeid med sivil sektor som forsterker et ytterligere behov for samarbeid. Tilførselen av kompetanse, varer, teknologi og tjenester har i større grad integrert Forsvaret i det sivile samfunn (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2015:10). På bakgrunn av det ytterligere behovet for sivilt-militært samarbeid er Forsvarets avhengig av at det sivile samfunnet til enhver tid er i en normaltilstand, uavhengig av den sikkerhetspolitiske situasjonen. Herunder spesifiseres to forhold, henholdsvis den spesifikke sivile støtten til

Forsvaret, samt støtten gjennom kommersielle ordninger. Disse to forholdene er grunnleggende for den gjensidige avhengigheten mellom Forsvaret og det sivile samfunn (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2015:27). Det moderne totalforsvaret er relevant i hele krisespekteret fra fred, via sikkerhetspolitiske krise til væpnet konflikt.[1]

Til tross for et modernisert totalforsvar viser Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Etterretningstjenesten (E-tjenesten) til nedslående informasjon om økt risiko for tilsiktede uønskede handlinger rettet mot den norske stat og den øvrige befolkningen (Trusselvurdering 2018, Risiko 2018, Helhetlig IKT-risikobilde 2017 og Fokus 2018).[2] NSM har i en årrekke rapportert om at gjennomføringen av sårbarhetsreduserende tiltak ikke forekommer i samme takt som utviklingen av trusselbildet, da sikkerhetstilstanden i Norge ikke er på et tilfredsstillende nivå (Nasjonal sikkerhetsmyndighet, 2010:3).[3] Gjennomgående i NSMs årlige utgivelser rettes det kritikk mot mangelfull effekt av forebyggende sikkerhetsarbeid.

Den digitale utviklingen har ført til en rekke faktorer som fremmer digitale sikkerhetsutfordringer, fra mangelfull sikring og teknologisk utvikling til sikkerhetspolitiske endringer og nye trusler fra målrettede trusselaktører. Trusler i det digitale rom er omfattende og truslene sprer seg raskt mot privatpersoner, næringsvirksomhet og offentlige institusjoner (Forsvarsdepartementet, 2012a:24). Digitaliseringen har ført til etableringen av et nytt handlingsrom i internasjonal politikk, som preges av en ny trusseldimensjon og digitale sikkerhetsutfordringer. Den nye trusseldimensjonen som blir adressert i denne oppgaven er av den art at truslene i stor grad kan svekke sentrale samfunnsstrukturers funksjonsdyktighet, samt svekke Norges sikkerhetspolitiske handlingsrom. Det digitale rom åpner for nye og alvorlige grenseoverskridende trusler, samt innebærer avhengighet av informasjons- og kommunikasjonsteknologi (IKT) et mer uoversiktlig og komplekst risikobilde. Dette

[1] Stortinget sluttet seg i Innst. S. nr. 234 (2003-2004) til St. prp. nr. 42 (2003-2004)) og Innst. S. nr. 49 (2004-2005) til St. meld. Nr. 39 (2003-2004) til en utvidelse og modernisering av totalforsvarskonseptet (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2015:12).

[2] NSM publiserer i løpet av et kalenderår en rekke rapporter og vurderinger, herunder kvartals- og halvårsrapporter, årsrapporter, årlige risikorapporter og helhetlig IKT-risikobilde, hvor denne oppgaven fokuserer på de to siste.

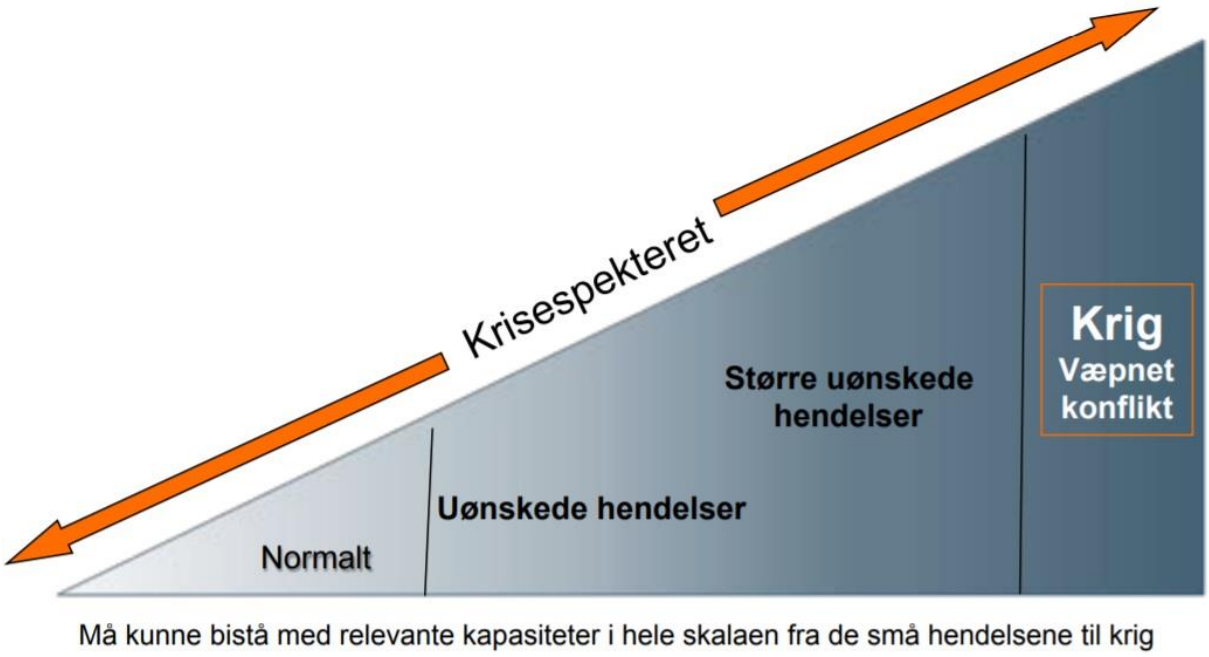
[3] I NSMs rapport av 2010 (Sikkerhetstilstanden 2010) rapporteres det at gapet mellom trusselaktørenes kapasiteter og mottiltakene i aktuelle virksomheter har økt og sikkerhetstilstanden i Norge dermed forverres. De to påfølgende årene, 2011 og 2012, rapporterte NSM at sikkerhetstilstanden i Norge blir stadig svekket, samt at sikkerhetsarbeidet i norske virksomheter utvikles ikke tilstrekkelig for å møte et stadig mer komplekst risikobilde (Nasjonal sikkerhetsmyndighet, 2011:4; 2012:3).

resulterer i økt interesse for fremmed etterretningsvirksomhet rettet mot Norges nasjonale interesser.[4]

Norske myndigheter har opplevd en mer aggressiv og målrettet etterretningsvirksomhet mot nasjonale interesse i nyere tid. Russiske aktører har rettet vedvarende etterretningsaktiviteter mot norske virksomheter, borgere og myndigheter. I kjølevannet av dette vurderer PST russisk etterretningskapasitet til å inneha størst skadepotensial overfor norske interesser (Politiets sikkerhetstjeneste, 2018:7). I følge E-tjenesten er etterretning i det digitale rom den mest alvorlige trusselen mot Norge, hvor russiske påvirkningsoperasjoner mot vestlige land er trappet opp (Etterretningstjenesten, 2018:32). NSM viser til etterretningsoperajoner som en fremtredende trussel, på bakgrunn av fremmede staters etterretningsvirksomheter har ved gjentatte anledninger forsøkt å etablere digital kontroll og innhente sensitiv informasjon fra norske virksomheter som forvalter viktig og til dels kritiske samfunnsfunksjoner (Nasjonal sikkerhetsmyndighet, 2018:9). Digitaliseringen av samfunnet og den stadige økende avhengigheten a IKT har resultert i en sterk konsentrasjon av sensitiv informasjon i det digitale rom. Sensitiv informasjon som er av stor interesse for fremmede staters etterretningstjenester omhandler politiske, militære og høyteknologiske forhold. Trusselaktørenes metoder er i stadig endring noe som utfordrer nasjonale deteksjonsmekanismer i henhold til å forebygge, oppdage og håndtere cyberoperasjoner som kan resultere i samfunnsmessige konsekvenser, spesielt alvorlige IKT-sikkerhetshendelser (Nasjonal sikkerhetsmyndighet, 2017a:8). Russisk etterretningsvirksomhet, i form av omfattende informasjonsinnhenting og kartlegging av sentrale samfunnsfunksjoner, kan benyttes som et strategisk fortrinn for nasjonal militærdisposisjon dersom det forekommer en eventuell endring i den sikkerhetspolitiske situasjonen. Cyberoperasjoner som en defensiv aktivitet omhandler å sikre handlefrihet, hvor cyberoperasjoner som en offensiv aktivitet styrker situasjonsforståelse og redusere eller hindre en potensiell motstanders cyberoperasjoner. I eventuelle fremtidige konflikter, vil dermed både defensive- og offensive cyberoperasjoner være av stor betydning da dette har blitt en etablert tilleggsdimensjon ved militære operasjoner (Forsvarsdepartementet, 2012a:102).

[4] Se *Vedlegg 2* og *Vedlegg 3.*

Fra sentrale hold er evnen til å håndtere IKT-hendelser også under press da et dagsaktuelt aktør- og trusselbilde er komplekst, noe som har ført til at regjeringen i 2017 lanserte *Internasjonal cyberstrategi for Norge*. Regjeringens internasjonale cyberstrategi gjør rede for de styrende prinsipper og strategiske prioriteringer i det digitale rom. Grunnet sterk korrelasjon mellom samfunnets økende avhengighet av det digitale rom og betydelig økning av digitale sikkerhetsutfordringer og digitale sårbarheter, har regjeringen rettet fokus på robusthet vedrørende Norges cyberstrategi.



*Figur 1.0 Krisespekteret (*Daae, 2017:7).

1.1.1 Resiliens

Resiliens (*resilience*) er begrepet som betegner samfunnets evne til å håndtere og gjenopprette normaltilstanden etter forstyrrende hendelser, og om nødvendig tilpasses til endrede forutsetninger. Begrepet fremmer en aksept av risiko for at et angrep vil finne sted, ettersom erkjennelse av risiko er en forutsetning for å kunne forebygge, redusere og håndtere risikoen videre (Ravndal, Johansen, Kjeksrud og Broen, 2014:6). Innarbeidet resiliens vil kunne bidra til å forhindre, oppdage og absorbere effekten av cyberoperasjoner. Innenfor cybersikkerhetsrelatert litteratur brukes resiliens, motstandsdyktighet og robusthet om hverandre, hvor resiliens-begrepet som oftest benyttes som et samlebegrep om robuste og

motstandsdyktige systemer. Dette er også tilfellet i rapporter og dokumenter fra beslutningsmyndigheter.[5]

Systemer i institusjoner og virksomheter med betydelig grad av resiliens legger til rette for en sikker og stabil tilstand som kan absorberer forstyrrelser. Resiliente-systemer innehar:

1. Evnen systemer har til å håndtere mindre hendelser, som utstyrssvikt, uten at selve systemet svekkes. Hverdagslige utfordringer som håndteres automatisk og sikrer systemers pålitelighet.

2. Evnen systemer har til å gjenopprette normaltilstanden etter større hendelser, som et digitalt angrep, i løpet av relativt kort tid. Herunder inkluderes et primært tiltak for sikring i kjølevannet av et angrep, sekundært initieres gjenoppbyggelse (The European Network and Information Security Agency, 2011:16).[6]

De overnevnte egenskapene er vitale ved strategier for å inneha resilens i sentrale systemer, ettersom gjennomføringen av sårbarhetsreduserende tiltak ikke forekommer i samme takt som utviklingen av trusselbildet. Den stadige digitaliseringen av samfunnet danner nye verdier og utviklingsmuligheter, samtidig utvides sårbarhetsflaten. Kompleksiteten som det digitale paradigme medbringer virker å øke overraskelsespotensialet i systemer, overfor sårbarheter (Demchak, 2012:264). Dette resulterer i at potensielle mottiltak og evnen til å beregne risiko og utføre forebyggende sikkerhetstiltak svekkes, da tiltak som reduserer sårbarhetene ikke holder tritt med et stadig mer komplekst risikobilde.

1.2 Valg av problemstilling

I en tid preget av økt informasjonsteknologi og informasjonsflyt hvor kompetente trusselaktører har en reell mulighet til å tilegne seg kritisk og sensitiv informasjon vedrørende norske interesser, vil resiliens og cybersikkerhet være av strategisk interesse for å opprettholde et ønskelig politisk- og militært strategisk handlingsrom. Dagens trusselbilde

[5] Meld. St. 37 (2014-2015) *Globale sikkerhetsutfordringer i utenrikspolitikken – Terrorisme, Organisert kriminalitet, Privatvirksomhet og Sikkerhetsutfordringer i det digitale rom*, Meld. St. 5 (2016-2017) *Nordisk samarbeid* og Meld. St. 10. (2016-2017) *Risiko i et trygt samfunn*, samt Prop. 151 S (2015-2016). Proposisjon til Stortinget (forslag til stortingsvedtak). *Kampkraft og bærekraft – langtidsplan for forsvarssektoren* og Prop. 153 L (2016-2017). Proposisjon til Stortinget (forslag om lovvedtak). *Lov om nasjonal sikkerhet (sikkerhetsloven)*.
[6] The European Network and Information Security Agency (ENISA).

krever et utviklet sivilt- militært samarbeid for å styrke resiliens som et tiltak innen forebyggende sikkerhet i interne strukturer. Trender innenfor norske samfunnsstrukturer viser allikevel til at samfunnet har blitt mer sårbart som følge av sentralisering, spesialisering og avhengigheten av informasjons- og kommunikasjonsteknologi overfor vitale samfunnsfunksjoner. En nasjonal akkumulering og sterk konsentrasjon av sensitiv informasjon i digitale rom utgjør en betydelig trussel som forsterker sårbarhetspotensialet, da muligheten til å tilegne denne informasjonen faller innenfor fremmede staters etterretningsarbeid.

Allikevel er det tilstede gjennomgående manglende gjennomføring av sårbarhetsreduserende tiltak som forekommer i samme takt med den dynamiske utviklingen i trusselbildet. Det rettes oppmerksomhet mot evnen til det moderne totalforsvarets grunnlinje om forebygging, beredskapsplanlegging, krisehåndtering samt konsekvenshåndtering, da norske virksomheter, borgere og myndigheter opplever økt etterretningsvirksomhet. Ettersom norske myndigheter har opplevd vedvarende etterretningsvirksomhet mot borgere og nasjonale interesser som: forsvars- og beredskapssektor, politiske beslutningsprosesser, kritisk infrastruktur og teknologiskutvikling er det dermed berettiget å rette oppmerksomhet mot hvordan totalforsvarets operasjonelle evne utfordres av russiske cyberkapabiliteter, da vedvarende russisk etterretning vurderes fortsatt til å ha størst skadepotensialet. Herunder defineres oppgaven problemstilling på følgende måte:

Hvilke digitale sikkerhetsutfordringer står totalforsvaret overfor i fredstid?

Problemstillingen bygger på tre underlagte delspørsmål som underveis i oppgaven skal besvares:

1) *På hvilken måte utgjør digitale sårbarheter en sikkerhetsutfordring for totalforsvaret?*

2) *Tyder vedvarende russisk etterretningsvirksomhet og kartlegging av sentrale norske myndigheter og virksomheter på opprustning i det digitale rom?*

3) *Kan styrket resiliens tilspisse den sikkerhetspolitiske situasjonen mellom Norge og Russland?*

Denne oppgaven skal undersøke dagens sikkerhetspolitiske situasjon.[7] Potensielle mottiltak i form av strategier for å oppnå resiliens, vil være tuftet på aksept av risiko for at cyberoperasjoner vil forekomme. Dynamikken i den nye trusseldimensjonen, resulterer i at defensive kapabiliteter er basert på usikkerhet om hvordan cyberoperasjoner vil kunne svekke virksomhetenes systemer. Kartleggingen av sensitive informasjon benyttes for å gjennomføre målrettede cyberoperasjoner, samt for å etablere bakdører og sikre tilgang til nettverk som kan benyttes som et virkemiddel for å lamme sentrale stats- og samfunnsfunksjoner dersom den sikkerhetspolitiske situasjonen endres.

1.3 Tidligere og pågående forskning

Dette underkapittelet redegjør for tidligere og pågående forskning av relevant tema, før denne oppgaven plasseres i den akademiske debatten.

Beskyttelse av samfunnet (BAS) er et større forskningsprosjekt ledet av Forsvarets forskningsinstitutt (FFI). Moderne BAS-forskning baseres på samfunnssikkerhet, og alvorlige hendelser som kan ramme Norge, og som krever beredskapsplanlegging og krisehåndtering på tvers av sektorer og nivåer, og der det er behov for sivilt-militært og offentlig-privat samarbeid (Endregard, Brattekås, Nystuen, Sandrup & Gerhardsen, 2016;4).

Fra Forsvarets høgskole (FHS) er det i tidsperioden 2011-2016 blant annet skrevet fire masteroppgaver relatert til cybersikkerhet. Ingun. H. Gustavsen skrev en masteroppgave i 2014, med temaet *Sivilt-militært samarbeid i en cyberkrise*. Jens-Aksel Johansen skrev en masteroppgave i 2016, med temaet *Strategisk kompetanseledelse (SKL) i cyberforsvaret*. Silje Nythun skrev en masteroppgave i 2016, med temaet S*amhandling i cyberforsvaret*. Arild Skillinghaug skrev en masteroppgave i 2011, om hvorvidt det *i Norge er ansvarsprinsippet eller helhetlig tilnærming til cybersecurity*.

Norges utenrikspolitiske institutt (NUPI) er en ledende norsk aktør innenfor forskning på internasjonal politikk. Cybersikkerhetssenteret forsker på politiske og sikkerhetspolitiske

[7] Dagens sikkerhetspolitiske situasjon baseres på sikkerhetspolitiske utviklingstrender hvor betydelige utfordringer og potensielle trusler er i en gråsone mellom krig og fred. Oppgavens tidsaspekt er fra oppgavestart (august 2017) satt i en 10 års periode fra cyberoperasjonen mot Estland, og vil ved oppgaveslutt omhandle en tidsperiode på 11 år. Innst. S. nr 9 (2002-2003), Jf. St. Meld. Nr. 17 (2001-2002) påpeker at oppgaven med å ivareta samfunnssikkerhet stadig viktigere grunnet det moderne samfunnets sårbarhet (Forsvarskomiteen & Justiskomiteen, 2003:52).

aspekter av cybersikkerhet. Cybersikkerhetssenteret publiserte tidligere i år (2018) en rapport om cybervåpen i internasjonal politikk, hvor fokuset var politisk motiverte cyberangrep mot oljesektoren, og om norsk petroleumssektor er godt nok rustet mot cyberangrep (Muller, Gjesvik & Friis, 2018).[8]

Denne oppgaven derimot tar sikte på å undersøke hvilke digitale sikkerhetsutfordringer totalforsvaret står overfor i fredstid. Av den tidligere nevnte forskningen, er det mindre fokus på utfordringer relatert til IKT-hendelser mot det sivile samfunn i fredstid, innenfor rammene av totalforsvaret. På bakgrunn av at fremmede staters etterretningsvirksomhet er den mest alvorlige trusselen mot Norge i det digitale rom, krever trusselbildet stadig økende fokus på sivile utfordringer fremfor militære utfordringer. Totalforsvarets relevans overfor sivile utfordringer, forsterkes dermed på bakgrunn oppgaver om forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering i hele krisespekteret. Digitaliseringen har endret sentrale strukturer i samfunnet, som i henhold til trusselbildet, og dermed blitt mer attraktive mål for fremmede staters etterretningsvirksomhet.

Oppgavens målsetting er å bidra med ny og relevant forskning om cybersikkerhet, i henhold til den rådende sikkerhetspolitiske situasjonen og ved anvendelse av *cybersikkerhetsdilemmaet*. Fremtidens trussel- og risikobilde er komplekst, den geopolitiske utviklingen er stadig mer uforutsigbar, noe som visker ut skille mellom det offentlige og private, samt skille mellom krig og fred. Disse implikasjonene på samfunnssikkerheten og den nasjonale sikkerheten resulterer i økt usikkerhet om hvordan cyberoperasjoner skal håndteres. Oppgavens vinkling er videre relevant for gjennomgang av relevante scenarioer, som et verktøy i beredskapsplanlegging og medfører til bedre nasjonal oversikt. Oppgaven innehar et betydelig fokus på resiliens overfor digitale sårbarheter som kan utnyttes av fremmede staters etterretningsvirksomhet. Styrket resiliens er prekært for å unngå statlig handlingslammelse og svekket beslutningskraft, ettersom cyberoperasjoner mot sentrale stats- og samfunnsfunksjoner kan være første steg på at en væpnet konflikt er under oppseiling. Ved anvendelse av *cybersikkerhetsdilemmaet* drøftes det hvorvidt styrket nasjonal resiliens kan resultere i en bilateral konflikt som utspilles i et spent internasjonalt system. Oppgavens vektleggelse av resiliens skiller seg tydelig ut fra tidligere leverte masteroppgaver hvor cybersikkerhet har vært av betydelig interesse.

[8] I rapporten til Muller, Gjesvik og Friis benyttes begrepet cyberangrep, da offensive aktiviteter rettes mot andre staters nettverk.

1.4 Avgrensing og Aktualitet

1.4.1 Cybersikkerhet

Den teknologiske utviklingen gjør det digitaliserte samfunnet stadig mer sårbart for fremmede staters etterretningsvirksomhet. PST, NSM og E-tjenesten advarer mot informasjonsgapet mellom trusselaktørenes kapabiliteter og nødvendige mottiltak av aktuelle virksomheter. Sårbarhetsflatens stadige utvikling innenfor IKT-feltet skyldes et digitalt kappløp, hvor den ene siden bestå av (i) utviklingen av skadevare og leveringsmetoder, og den andre siden omhandler (ii) mekanismer for deteksjon og beskyttelse i form av sårbarhetsreduserende tiltak (Etterretningstjenesten, 2016:82). Sikring av IKT og digital informasjon er en forutsetning får å begrense digitale sårbarheter som følge av digitale sikkerhetsutfordringer, ettersom digitaliseringen av samfunnet har segmentert internett som strukturen resterende infrastruktur er avhengig av. Kritikaliteten av sikre, stabile og robuste digitale nettverk, er herunder betydelig.

Sikringen av IKT og digital informasjon defineres ulikt, avhengig av aktør for definisjonen. *IKT-sikkerhet, informasjonssikkerhet* og *cybersikkerhet* er begreper som har blitt brukt ukritisk om hverandre fra sentrale aktører i Norge, og bidratt til begrepspluralisme på området. I den nasjonale strategien for informasjonssikkerhet av 2012 ble begrepet informasjonssikkerhet anvendt (Departementene, 2012).[9] Norges offentlige utredninger (NOU) sidestilte de to begrepene i utredningen *Digitale sårbarhet – sikkert samfunn*, og definerte IKT-sikkerhet som et synonym til cybersikkerhet (Norges offentlige utredninger, 2015:34). Justis- og beredskapsdepartementet (JD), i likhet med Utenriksdepartementet (UD), har sidestilt de to begrepene som synonymer (Justis- og beredskapsdepartementet, 2016:59).

Forsvarsdepartementets (FD) cyberretningslinjer, i likhet med de overnevnte departement og aktører, benytter samme definisjon til *cybersikkerhet* og *informasjonssikkerhet;* ved unntak av en spesifisering. I FDs cyberretningslinjer etableres *cybersikkerhet* som definisjonsmessig lik begrepet om *informasjonssikkerhet*, men *cybersikkerhet* spesifiseres som et begrep i en digital kontekst (Forsvarsdepartementet, 2014:22).

[9] Strategien ble utarbeidet i samarbeid mellom Fornyings- og administrasjonsdepartementet (Nåværende Fornyings-, administrasjons- og kirkedepartementet), Samferdselsdepartementet, Justis- og beredskapsdepartementet og Forsvarsdepartementet.

Oppgaven vil gjennomgående omtale sikkerhet innenfor det digitale rom som *cybersikkerhet*. Dette valget er tatt på bakgrunn av at sentrale dokumenter fra offentlig hold benytter begreper *cyber* ved tiltalelse av det digitale rom.[10] Norges første internasjonale cyberstrategi fremmer en rekke strategiske prioriteringer, som hver for seg og gjennom en samlet effekt skal styrke landets cybersikkerhet, ved å fremme sikre, stabile og robuste digitale nettverk (Utenriksdepartementet, 2017:7). FDs presisering av *cybersikkerhet* spesifiseres som et begrep i en digital kontekst og er kompatibelt med definisjonen av *cyberspace* som ikke kun omhandler digitalisert informasjon, men også karakteristiske trekk som fremmer presiseringen av sikkerhet i det digitale rom.

> Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies (Kramer, Starr & Wentz, 2009:28).

1.4.2 Cyberoperasjoner/datanettverksoperasjoner

I likhet med cybersikkerhet, benyttes også flere ulike begreper for å betegne cyberoperasjoner/datanettverksoperasjoner hvor mangelen av rigid bruk og definisjon svekker forståelsen av virkemidler i det digitale rom. Cyberangrep, dataangrep, digitale angrep, sabotasjehandlinger via det digitale domenet, IKT-angrep og datanettverksoperasjoner benyttes om hverandre av sentrale aktører. Cyberoperasjoner/datanettverksoperasjoner (Computer network operations, CNO) er samlebetegnelse som videre inndeler i følgende: *Computer network attack* (CNA) Computer network *exploitation* (CNE) og *Computer network defence* (CND). CNA og CNE kategoriseres som offensive aktiviteter og utføres i motstanderes nettverk. Formålet til CNA er å utnytte det digitale rom til egne operasjoner og redusere motstanderes evne. Formålet CNE er å identifisere aktiviteter og informasjon i cyberdomenet som gir situasjonsforståelse, samt tå gjenkjenne trusler. Formålet til CND er å sikre handlefrihet i egen informasjonsinfrastruktur, til tross for gjennomføringen av offensive aktiviteter av en motstander (Forsvarsdepartementet, 2014:5-6).

[10] I *Internasjonal cyberstrategi for Norge 2017*, omtales det digitale rom som cyberdomenet i strategiens forord, av Statsminister Erna Solberg.

Hvor PST og E-tjenesten virker samstemte og betegner tilsiktede uønskede handlinger som datanettverksoperasjoner, benytter NSM cyberangrep.[11]

> «Med cyberangrep menes en cyberoperasjon som er forventet å forårsake død eller skade på personell eller ødeleggelse på objekter» (Forsvaret, 2013:190).[12]

Forsvarsdepartementet har gjennom FDs cyberretningslinjer definert cyberangrep på følgende måte:

> «Handlinger i eller gjennom cyberdomenet med hensikt å skade eller påvirke personell, materiell eller konfidensialitet, integritet, tilgjengelighet eller autensitet til et informasjonssystem» (Forsvarsdepartementet, 2014:5).

Samtidig definerer FD også cyberhendelser på følgende måte:

> Brukes i disse retningslinjene både om situasjoner der IKT-systemer blir utsatt for cyberangrep, og ved utilsiktet svikt forårsaket av ulykker eller uhell. Med alvorlige cyberhendelser menes cyberhendelser som rammer samfunnskritisk infrastruktur, samfunnskritisk informasjon eller samfunnskritiske funksjoner på en likt måte at det får betydning for samfunnets og befolkningens trygghet (Forsvarsdepartementet, 2014:5).

Grunnet oppgavens vinkling og statsvitenskapelige forankring vil FDs definisjon av cyberoperasjoner benyttes gjennomgående, hvor cyberoperasjoner innad i forsvarssektoren benyttes som et synonym til datanettverksoperasjoner (Forsvarsdepartementet, 2014:20). Valget er gjort på bakgrunn av de politiske og militære rammene i oppgaven, hvor det tekniske og detaljerte i henhold til definisjoner av begreper ikke er sentralt.

[11] Heretter referert til som nettverksoperasjoner.
[12] Den generelle definisjonen av angrep gis i punkt 2.2 i manual i krigens folkerett (Forsvaret, 2013:28).

1.4.3 Aktualitet

PST, NSM og E-tjenesten påpeker, gjennom trussel- og risikovurderinger, at cybersoperasjoner har de mest omfattende strategiene som kan utnytte sårbarhetspotensialet overfor norske interesser. I henhold til stats- og samfunnssikkerhetsperspektivet utgjør den største trusselen de aktørene som har ressurser til å gjennomføre handlinger som nasjonale deteksjonsmekanismer ikke evner å oppdage i tide, eller i det hele tatt. Trusselaktører med betraktelige maktressurser kan være statlige aktører som representeres ved sikkerhets- og etterretningstjenester. I lys av de samlede trussel- og risikobilde utgjør digitaliseringen av samfunnet en betydelig styrke multiplikator, hvor informasjonsinnhenting kan utnyttes for å svekke norsk forsvars- og beredskapskapasitet i en eventuell fremtidig endring i den sikkerhetspolitiske situasjonen. Russiske og kinesiske aktører har forsøkt å kartlegge norske datasystemer av interesse, både innenfor virksomheter som forvalter grunnleggende nasjonale verdier og store kommersielle interesser (Politiets sikkerhetstjeneste, 2017:9). Det russiske etterretningstrykket kategoriseres som konstant og høyt, samt utgjør det størst skadepotensial for Norge og norske interesser, etterretningsvirksomheten har i nyere tid blitt aktualisert på en bekymringsfull måte grunnet den overhengende ustabiliteten i det internasjonale samfunnet. Oppgavens fokusområde er rette mot den mest alvorlige trusselen mot Norge i det digitale rom, fremmede staters etterretning. Primært er hensikten i første rekke å innhente strategisk viktig informasjon om tradisjonelle politiske- og militære mål, sekundært er industrispionasje (Etterretningstjenesten, 2018:30).

Oppgavens tema og sikkerhetspolitiske forankring er nødvendig for å sikre staten sterkt politisk handlingsrom, hvor kunnskap om aktiviteter i det digitale rom kan benyttes for å unngå misforståelser. Nettopp dette punktet aktualisert av oppgavens teori i kapittel to. Med den raske utviklingen innenfor digital teknologi understrekes det derfor at relevant lovgivning, regulering og organisering til enhver tid ikke vil forekomme i samme takt som utviklingen.

På bakgrunn av det overnevnte vil oppgaven forankres til relative sikkerhetsaktører og tilsynsmyndigheters trussel- og risikovurdering vedrørende russisk spionasje overfor norske interesser. Til tross for at Russland pr. dags dato ikke utgjør en konkret militær trussel mot Norge, vurderer allikevel E-tjenesten russisk utvikling langsiktig til å representere en betydelig potensiell risiko og utfordring for Norge (Lunde, 2016:7). I henhold til den teoretiske tilnærmingen vil dermed ikke denne oppgaven i betydelig grad diskutere

industrispionasje av kinesisk opphav. Russlands økende militære evne og tydelig maktbruk utgjør den endringen i Norges sikkerhetspolitiske omgivelser av størst betydelse. I den nye trusseldimensjonen har cyberoperasjoner blitt integrert i militære handlingsplaner, som kan lamme Norske myndigheter (Forsvarsdepartementet, 2016:104). Russlands uforutsigbarhet i tråd med den militære utviklingen i nordområdene, har resultert i økt fokus på tradisjonelle- og digitale sikkerhetsutfordringer som aktualiserer totalforsvaret. Oppgavens naturlig Russland fokus er herunder betydelig, og vil fremme en tydeligere statsvitenskapelig forankring grunnet oppgavens foretrukne teoretiske tilnærming. Herunder vektlegges sentrale trekk ved oppgavens teoretiske tilnærming som kompatible med etterretningsvirksomhet relater til cybersikkerhet, ettersom det ikke er de cyberoperasjonene vi kjenner som utgjør det største samfunnsrelaterte problemet, derimot er det de operasjonene vi ikke kjenner.

1.5 Disposisjon av oppgaven

Oppgavens oppbygging er basert på tre hoveddeler bestående av totalt seks kapiteler. Den første hoveddelen består av kapitel en. Følgende avsnitt gir en oversikt over oppgavens videre fremstilling og struktur.

Oppgavens andre del viser til valg av aktuell teoretisk tilnærming og utvalg av relevant forskningslitteratur. Kapittel to går i dybden på relevant teori, hvor det redegjøres for utviklingen av den teoretisk tilnærming. Gjennomgangen av den *realistiske fagtradisjonen* og redegjørelsen av *sikkerhetsdilemmaet* med historisk forankring, gir indikatorer på en utviklingstrend som aktualiserer *cybersikkerhetsdilemmaet*. Videre, fremlegges oppgavens metodiske tilnærming i kapittel tre, og redegjør for oppgavens forskningsopplegg. Kapittel fire viser til relevant empiri som aktualiserer oppgavens problemstilling og teoretiske tilnærming.

Avslutningsvis vil oppgavens funn analyseres og redegjøres for i kapittel fem med forankring i relevant teori som er presenter i kapittel to. I kapittel fem besvares de tre underlagte delspørsmålene til oppgavens problemstilling, med tilhørende delkonklusjoner. I kapittel seks fremlegges oppgavens konklusjon og gir en besvarelse av den definerte problemstilling. Videre, presenteres oppgavens styrker og svakheter for å kunne gi tydelige indikasjoner på om oppgaven har bidratt til videre forskning innenfor relevant tema på en tilfredsstillende måte.

2 Teoretisk tilnærming og utvalg av forskningslitteratur

Dette kapittelet vil danne bakgrunn for den videre diskusjonen i oppgaven med fokus på den teoretiske tilnærming som skal benyttes i analysen for å belyse cybersikkerhet som tema, og avslutningsvis svare på problemstillingen. Dette kapittelet viser innledningsvis til Forsvarets sikkerhets- og forsvarspolitiske mål som operasjonaliseres for å vise Forsvarets oppgaver. Videre vil historiske linjer redegjøres for i form av den *realistiske fagtradisjonen* og *sikkerhetsdilemmaet*, som vil eksemplifiseres med historiske hendelser, som har ledet frem til oppgavens hovedteori som er *cybersikkerhetsdilemmaet*.

2.1 Sikkerhets- og forsvarspolitiske mål

Sikkerhetspolitikkens hovedmål er å ivareta Norges grunnleggende sikkerhetsinteresser og målsettinger. Ivaretagelsen av vår suverenitet, territorielle integritet og politiske handlefrihet er en helt grunnleggende sikkerhetsinteresse, og dette er noe som kommer særlig til uttrykk gjennom Norges satsing i nordområdene. Norges viktigste bidrag til å styrke internasjonal og dermed norsk sikkerhet, er vår deltagelse i de Forente Nasjoner (FN) og i *North Atlantic Treaty Organization* (NATO). Forsvaret er ett av de mest sentrale virkemidlene som norske myndigheter har til rådighet for å understøtte de overordnede sikkerhetspolitiske målene, som er:

- *Å forebygge krig og fremvekst av ulike trusler mot norsk og kollektiv sikkerhet.*
- *Å bidra til fred, stabilitet og videre utvikling av en FN-ledet internasjonal rettsorden.*
- *Å ivareta norsk suverenitet, norske rettigheter, interesser og verdier og beskytte norsk handlefrihet overfor politisk, militært og annet press.*
- *Samme med våre allierte forsvare Norge og NATO mot anslag og angrep.*
- *Å sikre samfunnet mot anslag og angrep fra statlige og ikke-statlige aktører.*

Videre er de forsvarspolitiske målene utredet gjennom Forsvarets sikkerhetspolitiske mål

- *Alene og sammen med allierte sikre norsk suverenitet, norske rettigheter, interesser og verdier samt bevare norsk handlefrihet mot militært og annet press.*

- *Gjennom deltakelse i flernasjonale fredsoperasjoner med utvetydig forankring i FN-pakten og internasjonalt forsvarssamarbeid, bidra til fred, stabilitet, håndhevelse av internasjonal rett og respekt for menneskerettighetene, samt forebygge bruk av makt fra stater og ikke-statlige aktører mot norsk og internasjonal sikkerhet.*

- *Sammen med allierte bidra til kollektivt forsvar av Norge og andre allierte i henhold til våre allianseforpliktelser, og til å møte ulike typer anslag og angrep for å sikre norsk og kollektiv sikkerhet.*

- *Bidra til å ivareta norsk samfunnssikkerhet, redde liv og begrense konsekvenser av ulykker, katastrofer, anslag fra statlige og ikke-statlige aktører* (Forsvarsdepartementet, 2012b:8).

Sikkerhets- og forsvarspolitiske mål må sette Norge i stand til å svare på utfordringer i hele krisespekteret fra episodehåndtering i fred, via sikkerhetspolitiskkrise til væpnet konflikt (Forsvarsdepartementet, 2016:17).

2.1.1 Forsvarets oppgaver

Forsvarets oppgaver er tuftet på en operasjonalisering av de forsvarspolitiske målene. Forsvarsdepartementet definere Forsvarets oppgaver på følgende måte:

1. *Utgjøre en krigsforebyggende terskel med basis i NATO-medlemskapet.*

2. *Forsvare Norge og allierte mot alvorlige trusler, anslag og angrep, innenfor rammen av NATOs kollektive forsvar.*

3. *Avverge og håndtere episoder og sikkerhetspolitiske kriser med nasjonale ressurser, herunder legge til rette for alliert engasjement og nødvendig.*

4. *Sikre et nasjonalt beslutningsgrunnlag gjennom tidsmessig overvåking og etterretning.*

5. *Hevde norsk suverenitet og suverene rettigheter.*

6. *Ivareta myndighetsutøvelse på avgrensede områder.*

7. *Delta i flernasjonal krisehåndtering, herunder fredsstøttende operasjoner.*

8. *Bidra til internasjonalt samarbeid på det forsvars- og sikkerhetspolitiske området.*

9. *Bidra til ivaretakelse av samfunnssikkerhet og andre sentrale samfunnsoppgaver* (Forsvarsdepartementet, 2012b:14-15).

2.2 Den realistiske fagtradisjonen

Realismen som skoleretning i internasjonal politikk, også kalt den *realistiske fagtradisjonen*, kom som et motsvar til idealismen med Edward H. Carr og Hans Morgenthau som sentrale bidragsytere. Den *realistiske fagtradisjonen* er tydelig statssentrert, ved at teorien forutsetter stater som de grunnleggende aktører i internasjonal politikk. Det internasjonale system preges av et tydelig fravær av en overordnet myndighet, noe som resulterer i et permanent sikkerhetsbehov hvor maktforhold definerer maktbalanses som stabilisator i nevnte system (Østerud, 2007:241). I fraværet av en overnasjonal myndighet som kan regulere samhandling mellom stater, etableres et globalt system preget av hierarki og maktkamp. Dette understøttes av teoriens syn på stater som forutsetter en egosentrisk og maktorientert motivering, hvor stater oppfatter andre stater som motiveringsmessige likeartede aktører. En overhengende usikkerhet overfor andre aktørers intensjoner, fremmer realpolitikk hvor den sikkerhetsmaksimerende dimensjonen baseres på gjensidig usikkerhet. Det teoretiske utgangspunktet og selve grunnforutsetningen for den *realistiske fagtradisjonen*, er dermed at aktørenes overlevelse i det hobbesianske anarki i internasjonale forhold drives av snevre nasjonale interesser og kamp for statens videre eksistens. Altså, var *high politics* betydelig preget av nasjonal overlevelse og statsinteresse i fravær av en overordnet myndighet.[13]

Den *realistiske fagtradisjonen* forutsetter at drivkraften til enhver stat er maktmotivet, statene inngår således i et selvhjelpssystem, hvor det utenrikspolitiske siktemålet forblir å konsolidere eller øke statens relative maktposisjon i det internasjonale systemet. Disse nasjonale interessene gjøres gjeldende ved å styrke statens territorielle sikkerhet og politiske uavhengighet. Dette signalisere tydelige skillelinjer mellom stater, hvor plassering i det globale hierarkiet skyldes primært forskjeller i maktressurser. Betydningen av maktressurser medfører til at statlig egeninteresse og sikkerhetsbehov for statens videre eksistens har forrang

[13] Samlebetegnelse for utenriks- og sikkerhetspolitikk (Østerud, 2007:230).

fremfor moralske hensyn. Herunder forutsetter realismen en global maktkamp med fravær av grunnleggende anarkibetingelser hvor militær sikkerhet er det mest vitale for en stats videre eksistens. Tilstedeværelsen av et anarkisk-hierarki tuftet på det hobbesianske hierarki i det internasjonale system, hvor statsinteresse og nasjonal overlevelse er av betydelig interesse, vil gjensidig maktutredning være garanti for videre eksistens (Østerud, 2007:238). Den *realistiske fagtradisjonen* forutsetter at *high politics* er av vital interesse for statens videre eksistens, da ethvert sikkerhetsmaksimerende tiltak nødvendigvis går på bekostning av nasjonalsikkerhet for stater i geografisk nærhet (Hovi & Malnes, 2011:38).

2.3 Sikkerhetsdilemmaet

Sikkerhetsdilemmaet (*The security dilemma*) er en teori som har blitt diskutert ofte i litteratur innenfor internasjonal politikk. Bidragsytere som Robert Jervis, Barry Posen, Ken Booth og Nicholas J. Wheeler er sentrale skikkelser innenfor den aktuelle teorien, samt har Kristian Åtland som norsk bidragsyter fremmet teoriens betydelighet i et dagsaktuelt perspektiv. *Sikkerhetsdilemmaet* betegner en fiendtlig situasjon hvor to aktører er på randen av konflikt, grunnet usikkerhet om motpartens økning av militære evner som danner grunnlag for dilemma. Dersom to stater med defensive intensjoner ender opp i en ond sirkel av uvisshet angående motpartens økning av militære evner, betegner konflikten et sikkerhetsparadoks (Booth & Wheeler, 2008:4-5).

Den kalde krigen danner et empirisk belegg for hvordan *sikkerhetsdilemmaet* tidligere har blitt utspilt i det internasjonale system.

2.3.1 Den kalde krigen

Den kalde krigens hendelsesforløp kan forklares gjennom *sikkerhetsdilemmaet*. Spenningstilstanden oppsto i perioden mellom 1947-1991, og var på sitt mest kritiske under Cubakrisen i 1962 hvor stormaktene USA og Sovjetunionen brakte verden på randen av atomkrig. Sentralt under den kalde var etableringen av militærallianser, opprustning av maktressurser og ideologiske motsetninger mellom stormaktene. Tilstedeværelsen av de ideologiske motsetningene og grunnleggende misnøye mot USA, på bakgrunn av en mislykket invasjon av Grisebukta på Cuba året før ledet av USA, dannet grunnlaget for samarbeid mellom Sovjetunionen og Cuba (Allison, 1969:697). Sovjetunionen plasserte

militært utstyr på Cuba, og begrunnet handlingen som selvforsvar. Amerikansk etterretning avslørte at Sovjetunionen plasserte mellomdistanse- og langdistanseraketter med kjernefysiske sprenghoder, og den kjernefysiske opprustningen var et faktum da USA og Sovjetunionen måtte sørge for egen nasjonal sikkerhet (Buchanan, 2016:16). Det forelå en eksistensiell risiko fremlagt av motpartens atomstrategiske arsenal. Bipolaritet og trusselen om atomutslettelse hadde skapt forholdet for sikkerhetsdilemmaets ytterste relevans. Betydelig innsatsbeslutninger og potensialet for gjensidig utslettelse, begrunnet usikkerhet mellom de to supermaktene under den kalde krigen, spesielt under Cubakrisen som fordret kjernefysisk opprustning og omfattende etterretningsarbeid. Grunnlag for et *worst-case scenario* for begge supermaktene ble lagt. Dette kom tydelig frem i et dokument av, den daværende amerikanske president, Harry S. Truman som bygget opp under tanker om at USA sto i veien for Kremls verdensdominans (Truman, 1950:4).

Allikevel er det John Hertz og Herbert Butterfield som skal tildeles mest oppmerksomhet, da de begge anses som *sikkerhetsdilemmaets* pionerer med sine bidrag om en uløselig usikkerhet innad i det internasjonale system.[14] Hertz var den første teoretikeren til å benytte seg av begrepet i artikkelen *Idealist Internationalism and the security dilemma* (1950), for å identifisere og problematisere det faktumet at staters defensive motivasjon uforutsett kunne skape frykt og potensielt danne grunnlag for konflikt.

Booth og Wheeler bygget videre på de grunnleggende tankene fra Hertz og Butterfield, og definerte deretter *sikkerhetsdilemmaet* på følgende måte:

> The security dilemma is a two-level strategic predicament in relations between states and other actors, with each level consisting of two relates lemmas (or propositions that can be assumed to be valid) which force decisions-makers to choose between them. The first and basic level consist of a dilemma of interpretation about the motives, intentions and capabilities of other; the second derivative level consists of a dilemma of response about the most rational way of responding (Booth & Wheeler, 2008:4).

[14] *Unresolvable uncertainty*, oversatt til uunngåelig usikkerhet: i den forstand at usikkerheten er uunngåelig ved at enkelte stater genererer usikkerhet overfor en motpart med motiver, intensjoner og kapabiliteter, ved forberedelser av maktressurser.

Kjernen i *sikkerhetsdilemmaet* er det anarkiske-hierarkiet i det internasjonale system, hvor såkalte *worst-case* antagelser dominerer det multilaterale forholdet mellom stater (Åtland, 2014:147). Teorien baseres på elementer underlagt den *realistiske fagtradisjonen* noe som er tydelig ved mangelen på en overnasjonal institusjon eller autoritet som kan håndheve internasjonale lover i større grad enn i dagens internasjonale samfunn. Dette resulterer i at usikkerheten virker uunngåelig. *Sikkerhetsdilemmaet* forutsetter at denne overhengende usikkerheten er en eksistensiell betingelse i det anarkiske hierarkiet.

Booth og Wheelers nivåer fremkommer som to problematiserende forhold i form av to dilemmaer. Innledningsvis, i det primære nivået, oppstår et dilemma av et fortolkningsspørsmål som er problematiserende overfor aktuelle beslutningsmyndigheter vedrørende spørsmål om sikkerhet. Dilemma om tolkning baseres på et valg mellom to betydelige eller uønskede alternativer om militær politikk og politisk stilling fra andre aktører, herunder stater. Tolkningen skal på best mulig måte redegjøre for om den oppfattede militære utviklingen til en fremmed stat skyldes utelukkende defensiv eller offensiv hensikt i form av økte kapabiliteter og informasjonskartlegging. Dersom en aktør akkumulerer makt i form av nasjonale sikkerhetstiltak, utgjør denne konsentrasjonen av maktmidler en kilde til usikkerhet overfor andre aktuelle stater, som resulterer i redusert sikkerhet for nettopp de aktuelle statene.

Ved det sekundære nivået, omhandler dilemmaet respons som følge av en redegjørelse av fortolkningsspørsmålet. Aktuelle beslutningsmyndigheter må på bakgrunn av dilemmaet i det foregående nivået, beslutte om responsen skal være av avskrekkende eller beroligende karakter. Herunder er det kritisk for den videre sikkerhetspolitiske situasjonen at dilemmaet i dette nivået baseres på troverdig innhentet informasjon, heller enn ukorrekte antagelser om potensielle motiver og intensjoner overfor aktuelle stater. Dilemmaet i det andre nivået betegnes av storpolitiske svingninger, hvor sikkerhetstilstanden kontinuerlig påvirkes. Dersom aktuelle beslutningsmyndigheter beslutter at dilemmaet skal løses med avskrekkende respons kan dette føre til en spiral av gjensidig fiendtlighet.

Teoriens bakteppe er nettopp ved at slike antagelser medfører til at stater er sikkerhetssøkende. Hvor frykt og usikkerhet underbygger den videre dynamikken i teorien og utspiller en betydelig rolle i det internasjonale system. Tilstedeværelsen til den uunngåelige usikkerheten i det internasjonal system, dannet grunnlaget for dilemmaet ved beslutningsmyndighetenes forståelse av andre staters adferd. Våpen er teoriens materielle

tilskudd, grunnet symboleffekten som er knyttet til våpen som maktmiddel. Stater i det internasjonale systemet er selv ansvarlig for å opprettholde og verne over nasjonal sikkerhet og suverenitet. States adferd fremsto som strategisk fiendtlig grunnet usikkerhet og frykt, og ikke grunnet aggressive eller predatoriske intensjoner (Butterfield, 1951:21). Den paradoksale situasjonen hvor individer er venner og fiender på en og samme tid, betegnet et dualistisk forhold i individets sosiale liv som teorien om *sikkerhetsdilemmaet* er tuftet på (Hertz, 1950:3).

2.3.2 Operasjon misforståelse

Amerikansk etterretningsarbeid avslørte russisk atomopprustning på Cuba og risikoen for gjensidig utslettelse mellom de to supermaktene var reell. Tolkningsdilemmaet var vitalt ved ytterligere to isolerte hendelser under den kalde krigen. 27 oktober 1962 foretok et amerikansk etterretningsfly av typen U-2 et defensivt militært oppdrag hvor målet var å innhente strategisk informasjon om Sovjetisk atomkapabiliteter. Menneskelig svikt hos den amerikanske piloten ledet etterretningsflyet inn i sovjetisk luftrom, og Sovjetunionen svarte på krenkelsen av eget territorium med å klargjøre luftstyrker. Den sikkerhetspolitiske situasjonen var allerede kritisk under Cubakrisen mellom de to supermakten. Sovjetunionens territorium var krenket av et amerikansk fly som opptrådde aggressivt, og trusselen virket reell om at et amerikansk atomangrep var underveis. Til tross for den alvorlige tilstanden seint oktober 1962, deeskalerte situasjonen ved at det amerikanske etterretningsflyet forlot sovjetisk luftrom (Buchanan, 2016:15-16).

1 september 1983 krenket Korean Air Lines Flight 007 på vei fra New York til Seoul sovjetisk luftrom, men resultater forble et helt annet enn ved det amerikanske etterretningsflyet 21 år tidligere. Korean Air Lines Flight 007 fløy over et prøveområde for sovjetiske atomraketter, et område av signifikant interesse for USA og var ofte kartlagt av amerikanske etterretnigsfly. Sovjetisk motsvar på det ukjente luftfartøyets krenkelse av luftrommet medførte til fatale følger og passasjerflyet med 269 mennesker ombord ble skutt ned, hvorav ingen overlevde angrepet. Sovjetunionens handling var begrunnet med sterk amerikansk interesse i det samme området, som medførte til en effekt av økt mistillit og mistanke (Buchana, 2016:27).

Lærdommen av den kalde krigen vektlegger sentrale element som: det betydelige maktdrevende perspektivet i det internasjonale system, nødvendigheten for stater å opparbeide militær kapabiliteter og bedrive etterretningsarbeid, samt tilstedeværelsen av risikoen av misforståelse og eskalering. Disse sentrale elementene gjør seg gjeldende også i *cybersikkerhetsdilemmaet*.

2.4 Cybersikkerhetsdilemmaet

Konseptet om *cybersikkerhetsdilemmet* bygger videre på det tradisjonelle tankegodset og anerkjente teorien *sikkerhetsdilemmaet* innenfor internasjonal politikk.[15] Ben Buchanan lanserte *cybersikkerhetsdilemmaet* i boken *The Cybersecurity Dilemma: hacking, trust and fear between nations* (2016), ettersom det problematiserende forholdet hvor en nasjon styrker nasjonal sikkerhet, truer andre staters sikkerhet grunnet usikkerhet. Dette strukturelle problemet kan fører til en eskalering av den sikkerhetspolitiske situasjonen, hvor maktressurser forskyves og konsentreres, og tilrettelegger for stormaktsrivalisering og tradisjonell geopolitikk. Herunder er teoriens kjernepunkt ufravikelig, da etterretningsarbeid som i hovedsak kun skal innhente informasjon som en defensiv tilnærming, kan misforstås og oppfattes som om et angrep er nært forekommende. *Cybersikkerhetsdilemmaet* identifiserer stater som sentrale aktører, noe som medfører til at teorien føyer seg i rekken av anerkjente teorier innen studie av internasjonal politikk med samme utgangspunkt. Et betydelig fokus på stater som sentrale aktører korresponderer med dagens sikkerhetspolitiske utfordringer. Til tross for at ikke-statlige aktører er bidragsytere i utviklingen av cyberoperasjoner, viser allikevel relevant empiri til at sofistikerte angrep er av statlig opphav. Ikke-statlige aktører som handler på vegne av en gitt stat, som et ledd i en utenrikspolitisk strategi, er en trend som forekommer i det internasjonale system (Buchanan, 2016:11). Statlige aktørers beslutningsapparat innehar kommunikasjonskanaler som er av vital interesse for fremmede staters etterretningsarbeid, og dermed også av betydelig interesse for hver stat å forhindre betydelig etterretningsarbeid mot statshemmeligheter og kritisk informasjon. Strategisk viktige nettverk, herunder kritisk infrastruktur og kritiske samfunnsfunksjoner, er av betydelig interesse for en trusselaktør, da disse strategisk viktige nettverkene er sentrale for en stats

[15] *Cybersecurity Dilemma*, oversatt grunnet oppgavens språkform. Oversettelsen begrunnes med at det pr. i dag ikke er definert en anerkjent norsk oversettelse, som det er for *Sikkerhetsdilemmaet*. *Sikkerhetsdilemmaet* i det digitale domenet er dagsaktuelt og en helt norsk betegnelse på teorien er dermed nødvendig.

funksjonalitet. Altså, et mål som overskrider en terskel av strategisk betydning for en motpart, er et ønskelig etterretningsmål.[16] *Cybersikkerhetsdilemma* betegner med andre ord, prosessen før en eventuell konflikt finner sted.

Cybersikkerhetsdilemmaet definerer to muligheter for at nevnte terskel overskrides. Den definerte forskjellen baseres på: (i) uautorisert innhenting av informasjon fra et datanettverk, og (ii) angrep med formål om å destruere eller manipulere informasjon fra et datanettverk (Buchanan, 2016:12). Løpende etterretningsarbeid med hensikt om å innhente informasjon vedrørende andre stater, av strategisk nyttig informasjon forekommer i det internasjonale system og er nødvendig i et system tuftet på et anarkisk hierarki. I forsøket på å utbedre egen nasjonal sikkerhet, stimuleres frykt overfor potensielle og betydelige motparter. Dette utløser et hendelsesforløp, hvor den potensielle motparten risikerer å svekke egne kapabiliteter, dersom staten ignorerer den andre statens sikkerhetstiltak. Effekten av å ikke følge opp motpartens sikkerhetstiltak kan være utslagsgivende i en skjerpet sikkerhetspolitiske situasjon eller konflikt. Dette er en risiko stater i det anarkiske systemet ikke villig til å ta, ettersom stater i all hovedsak er sikkerhetssøkende. Hendelsesforløpet betegnes som *the race to the bottom*, da den dynamiske utviklingen er av eskalerende karakter, og kan resultere i uante konsekvenser grunnet de komplekse truslene i en allerede usikker sikkerhetspolitisk situasjon (Buchanan, 2016:29).

Teoriens natur baseres på den sikkerhetsmaksimerende dimensjonen som er tydelig i teorien om *sikkerhetsdilemmaet* og i den *realistiske fagtradisjonen*, som definerer et sett med operasjonelle insentiver som pådrivere for *cybersikkerhetsdilemmaet*. Dersom en stat har utviklet offensive kapabiliteter preventivt, har staten et insentiv til å benytte de offensive kapabilitetene før det er sikkerhetspolitiske hensiktsmessig og nødvendig. Denne grunnleggende egenskapen er sentral innenfor cybersikkerhet, med særlig fokus på cyberoperasjoner rettet mot uautorisert innhenting av sensitiv informasjon. Teorien fremlegger fire relaterte intensjoner som fremmer inntrengning og informasjonsinnhenting i datanettverk, cyberoperasjoner, preventivt av en konflikt eller økt sikkerhetspolitisk spenning: (i) cyberoperasjoner varierer stegvis i hastighet; (ii) operasjonelle steg er lineære, men uten tydelig momentum; (iii) sterk utholdenhet, (iiii) og deler av cyberoperasjoner kan forberedes

[16] *Threshold of importance,* oversatt til terskel. Et strategisk viktig mål er ikke utelukkende rettet mot en regjering eller infrastruktur. Allikevel, gir etterretningsmål er av dyp strategisk viktighet største utnytte av ønskelig informasjon (Buchanan, 2016:12).

på forhånd. Disse operasjonelle insentivene av cybersoperasjoner med fokus på informasjonsinnhenting legger tydelige føringer for teoriens holdepunkt, ettersom stater kan finne det hensiktsmessig å utvikle offensive kapabiliteter før de er nødvendige i en sikkerhetspolitisk situasjon (Buchanan, 2016:41).

Tilstedeværelsen av de operasjonelle insentivene danner grunnlag for teoriens første grunnpilar. Stater som søker etter å øke den relative maktposisjonen gjennom cyberoperasjoner og nyttiggjørelse av det digitale rom, må handle offensivt for at cyberoperasjoner skal kunne nå maksimal nytteeffekt. Herunder vil tradisjonell kapasitetsbygging samt cyberoperasjoner med fokus på innhenting av sensitiv informasjon om en stats indre anliggende være aktuelt. Ettersom dette vil i henhold til det teoretiske utgangspunktet medføre til at ethvert sikkerhetsmaksimerende tiltak gjennomført av en stat, vil gå på bekostning av den nasjonale sikkerhet til en stat i geografisk nærhet (Buchanan, 2016:48).

Teoriens andre grunnpilar baseres på at stater har genuine defensive tilnærminger for å iverksette cyberoperasjoner ved inntrengning og innhenting av interessant informasjon fra andre stater. Langsiktig er dette et mål, da eventuelle fremtidige risikoer kan bli oppdaget og avverget. I en skjerpet sikkerhetspolitisk situasjon hvor usikkerheten overfor nasjonal sikkerhet er betydelig, vil informasjonsinnhenting av defensive tilnærming være ønskelig. En lignende defensiv tilnærming hvor målet kun er strategisk informasjonsinnhenting gjennom etterretningsarbeid, poserer ingen direkte trussel. Allikevel er teoriens kjernepunkt ufravikelig i den forstand, da etterretningsarbeid som i hovedsak kun skal innhente informasjon som en defensiv tilnærming, kan misforstås og oppfattes som om et angrep er nært forekommende. *Sikkerhetsdilemmaet* i det digitale rom er dermed tilstede, og fremkommer i gråsone som medbringer betydelig usikkerhet. Etterretningsarbeid i form av tradisjonell informasjonsinnhenting, kan tolkes truende i en tid hvor den sikkerhetspolitiske situasjonen er preget av usikkerhet, uavhengig om etterretningsarbeidet er i form av cyberoperasjoner av defensiv karakter eller ikke (Buchanan, 2016:72-73). Allikevel er den potensielle nytteverdien ved informasjonsinnhentingen uvurderlig og gir en stat muligheter til å kartlegge og innhente kritisk informasjon som kan benyttes når den sikkerhetspolitiske situasjonen er mer tilspisset, i henhold til teoriens grunnlinje om sikkerhetsmaksimering.

I likhet med *sikkerhetsdilemmaet*, vektlegger også *cybersikkerhetsdilemmaet* at dilemma om tolkning, når en stat oppdager det pågående etterretningsarbeidet mot egen stats nasjonale interesser. Tolkningsdilemmaet er teoriens tredje grunnpilar, hvor cyberoperasjoner rettes mot strategisk vital informasjon vil tolkes som truende mot den angrepenes stats indre anliggende. Dersom det hersker tvil om hvorvidt etterretningsarbeidet er av potensielt betydelig skadelig karakter eller som en etterretningsoperasjon av defensiv tilnærming vil fremdeles teoriens grunnlinje være avgjørende, derav det sikkerhetsmaksimerende aspektet i en ustabil sikkerhetspolitisk situasjon (Buchanan, 2016:96).

Teoriens grunnlinje, hvor stater opptrer som sikkerhetssøkende aktører i det internasjonale system, baseres på teoriens kjernekonsept om at frykt og usikkerhet resultere i en betydelig eskalering av statens sikkerhetspolitiske situasjon. Eskaleringen er fremtredende i *cyber-sikkerhetsdilemmaet* så vel som i *sikkerhetsdilemmaet*, og forblir på den internasjonale politiske agendaen grunnet utviklingen av nye våpen, utplasseringen av militære styrker, kompleksiteten vedrørende tolkningsspørsmålet av potensielle trusler av nasjonal sikkerhet, og betydelig etterretningsvirksomhet. Herunder påvirkes alvorlighetsgraden og tolkningsdilemmaet av benyttet teknologi, geografi og relaterte stater. Kompleksiteten og alvorlighetsgraden av eskaleringen er på det mest kritiske dersom stater med betydelige maktressurser er inkludert i dilemmaet. Stater med betydelige maktressurser søker etter å svekke det politiske handlingsrommet til en motpart, som senere kan utnyttes av staten med betydelig maktressurser dersom den sikkerhetspolitiske situasjonen skjerpes. Potensielt kan tilstedeværelsen av stater med betydelige maktressurser øke de allerede eksiterende fallgruvene, da fraværet av troverdig informasjon, komplekse trusler og tolkningsdilemmaet problematiseres av utfordringen av å definere trusler som tilsiktede eller utilsiktede. Det anarkiske internasjonale systemet dikterer at stater må forsvare seg, det endelige resultatet danner grobunn for teoriens kjernekonsept, nemlig overhengende frykt og usikkerhet (Buchanan, 2016:187).

I det anarkiske system som foreligger og forutsettes i *cybersikkerhetsdilemmaet*, vil det være berettiget for stater å inneha en viss skeptisk holdning overfor andre stater i det internasjonale system, grunnet den sikkerhetspolitiske dynamikken. Noe som medfører til teoriens relevans i det internasjonale system, hvor trusselbildet er betydelig sammensatt gjennom dynamiske trusler som forekommer som tidseffektive og som en kombinasjon av en rekke ulike virkemidler medfører til at potensielt eskalerende dynamikk. Enhver stat er avhengig av å

kunne opprettholde samfunnets grunnleggende funksjoner uavhengig av hvilken ekstern påvirkning staten utsettes for. Resultatet av eskaleringen er fremtredende, da cyberoperasjoner kan forekomme uten at det utartes en militær konflikt. Kompleksitet som er tilstede, betyr at skillelinjen fra normaltilstanden til en mer alvorlig sikkerhetspolitisk situasjon er av svak natur, ettersom tolkningsdilemmaet er av stor betydning.

3 Metode

Dette kapittelet skal redegjøre for metoden som ligger til grunne for oppgaven. Innledningsvis i kapittelet redegjøres det for valg av forskningsdesign. Deretter redegjøres det for prosessen ved datainnsamlingen før selve innsamlingen av datamaterialet analyseres. Avslutningsvis drøftes valget av forskningsdesign og innsamlingen i henhold til validitet og reliabilitet. Metode kan defineres på følgende måte «En metode er en framgangsmåte, et middel til å løse problemer og komme fram til ny kunnskap. Et hvilket som helst middel som tjener dette formålet, hører med arsenalet av metoder» (Hellevik, 2003:12).

3.1 Valg av forskningsdesign

Statsvitenskap er det systematiske studie av politikk (Østerud, 2007:22). I henhold til denne oppgaven vil det systematiske element i hovedsak representeres i form av russisk uforutsigbarhet, samt en ny trusseldimensjon, som vil svekke den nasjonale sikkerhetstilstand. For å besvare oppgavens problemstilling, vil det vitenskapelig være hensiktsmessig å velge et passende forskningsdesign, ettersom bevisst og kritisk refleksjon over valg av metoder er viktig for å sikre godt vitenskapelig arbeid (King, Keohane & Verba, 1994:25).

Oppgaven vil primært anvende allerede foreliggende data, basert på oppgavens avgrensning og relevans.[17] PST, NSM og E-tjenesten vil være essensielle for utarbeidelse av foreliggende data i denne oppgaven. Dokumentbasert undersøkelse som valgte forskningsdesign benyttes for å kunne gjennomgå og analysere aktuelle dokumenter og strategier i henhold til problemstillingen. Dokumentbasert undersøkelse er en noe mindre allmenn benyttet form for et forskningsdesign, noe som kan understøttes med at dokumentbasert undersøkelse ikke er en like tydelig disiplin som andre mer benyttete forskningsdesign (Scott, 2006:84). En noe mer udefinert og uklar definisjonsmessig form for forskningsdesignet, settes i tydelig kontrast til det faktumet at bruken av dokumenter er en av hovedkildene innenfor samfunnsvitenskapelig forskning. I det samfunnsvitenskapelige benyttes dokumentbasert undersøkelse til å undersøke hvordan statsvitenskapelig forskning forholder seg til tekst, samt på hvilken måte tilnærmingen benyttes til å undersøke empirisk materialet. På denne måten tilrettelegger dokumentbasert undersøkelse for systematisk gjennomgang av aktuelle dokumenter, som

[17] Se *1.4 Avgrensing og aktualitet*.

gjennom tolkning fremmer forståelsen og utvikler empirisk kunnskap relatert til problemstillingen. Videre kan dokumenter defineres som "Documents may be regarded as physically embodied text, where the containment of the text is the primary purpose of the physical medium" (Scott, 2006:15). Vurderingen av det foreliggende materialet gjennomføres ved bruken av fire kriterier hvor dokumentene vurderes i henhold til autensitet, troverdighet, representativitet og tolkning. Alle de fire kriteriene er gjensidig avhengige av hverandre som spiller ut over den samlede vurderingen, som i utgangspunktet vektlegger tolkningskriteriet som er i konstant behov for revidering (Scott, 2006:39.40).

På den andre siden presiseres utgiverne av datamaterialet. PST, NSM og E-tjenesten er alle underlagt offentlige myndigheter, og fremmer det samme vurderingen av trusselbildet ved at cyberoperasjoner er den største trusselen i det digitale rom, hvor Russland utgjør den av de aktive aktørene som fremmer største skadepotensialet i Norge, samt at sårbarhetspotensialet er betydelig større enn sårbarhetsreduserende tiltak vedrørende cybersikkerhet. Tolkningen av det foreliggende materialet ses i betydelig sammenheng til å omhandle samme aktør og sårbarheter underlagt den nye trusseldimensjonen. Gitt at foreliggende materialet er et produkt av offentlige myndigheter som gjennom flere samarbeidsfora koordinerer styrker, støtter dette det foreliggende materialets autensitet, troverdighet og representativitet.

I denne oppgaven benyttes kvalitativ innholdsanalyse av overnevnte dokumenter, for å få et presist innblikk i undersøkelsesforholdet til relevante dokumenter ettersom analyseformen vektlegger hvordan de ulike elementene i dokumentene kan forstås i sammenheng (Grønmo, 2004:120). I den faglitterære debatten har både kvalitativ- og kvantitativ tilnærming til innholdsanalyse vært oppe til diskusjon, allikevel har kvalitativ metodisktilnærming fått betydelig mindre oppmerksomhet. Dette har resultert i at den kvantitative tilnærmingen har blitt definert som tilhørende innholdsanalyse (Scott, 2006:135-136).

Til tross for normaliseringen av kvantitativ innholdsanalyse, vil denne oppgaven benytte kvalitativ innholdsanalyse ettersom denne tilnærmingen i større grad fremmer sentrale aspekter av intensjonene bak dokumentene på et gitt tidspunkt, enn standardiserte kvantitative tilnærmingen (Scott, 2006:135). Gjennom kvalitativ innholdsanalyse vil derfor indikatorene i større grad være passende for oppgaven og resultere i mer produktiv informasjon, enn ved kvantitativ innholdsanalyse (Scott, 2006:141). Innholdsanalyse som analyseform dekker dermed essensen av dokumentene som undersøkes, samt gir den underliggende ambisjonen om å trekke slutninger til forhold utenfor tekstene (Bratberg, 2014:85). Slutninger til forhold

utenfor tekstene kan gi en overordnet forståelse og bidra til å kunne besvare den foreliggende problemstillingen. Herunder vektlegges innsamlingen av valide estimater av intensjonen og underliggende meninger i dokumenter, som i henhold til denne oppgaven vil fremme en tydeligere samlet vurdering av de aktuelle digitale sikkerhetsutfordringene som totalforsvaret står overfor i fredstid (Scott, 2006:151).

3.2 Datainnsamling

Oppgavens primærkilder består av offentlig publiserte og ugraderte trussel- og risikovurderinger. Utredninger, stortingsmeldinger og proposisjoner til Stortinget vil benyttes for å tilføre oppgaven mer faglig dybde. Dokumentene danner grunnlaget for datainnsamlingen, ettersom skrevne tekster utgjør det sentrale datatilfanget ved benyttelse av kvalitativ innholdsanalyse (Hellevik, 2003:176)

Formålet med analysen er å fremskaffe en bedre forståelse av totalforsvarskonseptets relative betydning i et digitalisert samfunn. Av hensyn til oppgavens struktur er kvalitativ analyse valgt, i form av et intensivt opplegg, for å kunne gå i dybden i en dagsaktuell kontekst. Den valgte analyseformen fremmer i tydelig grad detaljkunnskap om cybersikkerhet som tema, samt er analyseformen dekkende for å kunne danne et helhetsperspektiv (Hellevik, 2003:98).

PSTs *Trusselvurdering 2018*, E-tjenestens *Fokus 2018* og NSMs *Risiko 2018* samt *Helhetlige IKT-risikobilde 2017*, er alle aktørenes vurderinger som representerer dagens sikkerhetspolitiske situasjon, og representerer dermed dokumenter som betegner økt risiko for tilsiktede uønskede handlinger rette mot den norske stat og den øvrige befolkningen, grunnet kontinuerlig digitalisering av samfunnet. NSM påpeker at gjennomføringen av sårbarhetsreduserende tiltak ikke forekommer i samme takt som utviklingen av trusselbildet, hvor Norske myndigheter opplever stadig mer aggressiv og målrettet etterretningsvirksomhet mot nasjonale interesser. PST vurderer russisk etterretningskapasitet til å inneha størst skadepotensial overfor norske interesser, samt kategoriseres fremmede staters etterretningsvirksomhet som den mest alvorlige trusselen mot Norge i det digitale rom.

De overnevnte dokumentene utgjør Norges sikkerhetstilstand vurdert ut ifra sentrale sikkerhetsaktører og tilsynsmyndigheter relatert til oppgavens tema og problemstilling.[18] Oppgavens kvalitative innholdsanalyse ledsages av oppgavens valgte hovedteori *cybersikkerhetsdilemmaet* som ligger til grunne for å diskutere oppgavens problemstilling, samt de tre underliggende delspørsmålene.[19]

3.3 Validitet og reabilitet

Validitet og reliabilitet er kriterier for vurderinger av styrker og svakheter vedrørende metode i samfunnsvitenskapelig forskning. Presisjon i overgangen mellom teoriplanet og empiriplanet fremme fruktbar forskning, til tross for at det er umulig å oppnå perfekt validitet i empirisk forskning, kun tilnærmet høy validitet (Lund, 2002:86). Oppgavens datainnsamling og operasjonelle definisjon tilrettelegger for undersøkelsens reliabilitet, som videre er en nødvendig forutsetning for at den innsamlede data skal ha høy grad av validitet (Hellevik, 2003:53).

3.3.1 Validitet

Cook og Cambells validitetssystem omfatter fire kvalitetskrav av validitet i forbindelse med kausale undersøkelser, herunder statistisk validitet, indre validitet, begrepsvaliditet og ytre validitet (Lund, 2002:105). Validitet representerer et forskningsmessigutrykk for hvor godt datamaterialet svarer til forskerens intensjoner med undersøkelsesopplegget og datainnsamlingen (Grønmo, 2004:426). Denne oppgaven vil gjennomgående forholde seg til begrepsvaliditet.

Operasjonelle definisjoner anvendes for innen forskning i spranget fra teoretisk diskusjon til empirisk studie, for å gjøre et fenomen målbart ved å kunne redegjøre om et empirisk fenomen faller inn under begrepet (Hellevik, 2003:51). I henhold til oppgaven og den fremlagte problemstillingen vil det av naturlige årsaker bidra utelukkende forskningsmessig positivt å operasjonalisere resiliens.

[18] Se *1.2 Valg av problemstilling*.
[19] Se *2.4 Cybersikkerhetsdilemmaet*.

Resiliens omhandler skadebegrensende tiltak, herunder forberedende og planlegge konsekvensreduserende tiltak, samt aksept av risiko for at et angrep vil finne sted, ettersom erkjennelse av risiko er en forutsetning for å kunne forebygge, redusere og håndtere risikoen videre.[20] Høy grad av resiliens vil si at sentrale funksjoner har betydelig evne til å raskt gjenopprette normaltilstanden, dersom det forekommer en situasjon hvor deler av eller hele funksjonen blir påvirket av en hendelse (Norges offentlige utredninger, 2016:258).

Vedrørende operasjonaliseringen av resiliens så kan operasjonaliseringen forekomme på flere måter. Primært, vil fokuset rettes mot tiltak som øker resiliens for kritiske samfunnsfunksjoner i et forsøk på å redusere sårbarheten. En kombinasjon av flere tiltak eller implementering av flere enheter eller delsystemer som på sikt bidrar til opprettholdelse av resiliens er to måter på å gjøre begrepet målbart. Etableringen av Sentralt totalforsvarsforum, Cyber Forsvaret (CYFOR), Cyberkoordineringsgruppen (CKG), Norsk senter for informasjonssikring (NorSIS), Varslingssystem for digital infrastruktur (VDI) og *Center for Cyber and Information Service* (CCIS) er alle enheter som på kortsiktig- og langsiktig basis fremmer resiliens for kritiske samfunnsfunksjoner og generelt i samfunnet.

Allikevel gir ikke nødvendigvis lignende operasjonalisering begreper preget av høy grad av begrepsvaliditet. Styrket resiliens som sårbarhetsreduserende tiltak er ikke direkte overførbart til et samfunn som i større grad raskt og effektivt vender tilbake til en tilnærmet normaltilstand i ettertid av en større cyberoperasjon. En operasjonell variabel kan representere eller måle tre komponenttyper: det relevante begrep, irrelevante begreper og usystematiske feil, hvor de to siste alternativene representerer trusler mot begrepsvaliditet (Lund, 2002:120). Dersom operasjonaliseringen av resiliens omhandler tiltak som øker resiliens utelukkende gjennom kombinasjon av tiltak og opprettelse av enheter eller delsystemer, representerer dette et irrelevant begrepet, ettersom begrepsvaliditet omfatter generalisering vedrørende begreper på årsaks- og effektsiden (Lund, 2002:106). Hovedsakelig vil resiliente samfunn, i en sikkerhetspolitisk kontekst, indikeres av forebyggende tiltak for å redusere tidsperioden hvor normaltilstanden ikke er et faktum. En ønsket effekt av styrket resiliens vil være å minimere

[20] I 2004 understreket regjeringen viktigheten av forebyggendearbeid vedrørende samfunnssikkerhet, slik at dersom uønskede hendelser inntraff så ville konsekvensene minimeres. Regjeringens fokus på grunnberedskap for hyppig forekommende hendelser gir også god beredskap når samfunnet står overfor ekstraordinære hendelser (Justis- og beredskapsdepartementet, 2004:6). Regjeringens betydelige fokus på forebyggende arbeid vedrørende samfunnssikkerhet i en tid hvor regjeringen (2004) selv vurderte trusselen mot statens som lav, understøtter poenget om utbedret forebyggende arbeid og nødvendigheten av innarbeidet resiliens gjennomgående ved sentrale institusjoner.

risikoen for effekten av cyberoperasjoner, ettersom eksistensen av den nye trusseldimensjonen er vanskeligere å motarbeide. Dette støttes av NSM, som vurderer økningen i alvorlige cyberoperasjoner, kompromittering av nettverk i mindre virksomheter, bruk av cyberoperasjoner og stjålet informasjon til påvirkning av flere økonomisk motiverte hendelser (Nasjonal sikkerhetsmyndighet, 2017b:8-9). PST fremmer lignende prediksjoner vedrørende fremmede staters etterretningsvirksomheter, som forventes å gjennomføre cyberoperasjoner mot virksomheter innen forsvars- og beredskapssektoren, statsforvaltningen, forskning og utvikling samt kritisk infrastruktur, da interessen for disse områdende har vist seg å være vedvarende (Politiets sikkerhetstjeneste, 2018:7).

På bakgrunn av det overnevnte vil en operasjonalisering av resiliens være med fruktbar i henhold til oppgavens problemstilling dersom det målbare er: fraværet av IKT-hendelser som i en lengre tidsperiode undergraver normaltilstanden. Denne operasjonaliseringen måler i større grad effekten av sårbarhetsreduserende tiltak i form av styrket resiliens, i motsetning til opprettelse av enheter eller delsystemer som er tiltak hvor det tilrettelegges for styrket resiliens, men ikke gir tydelige indikatorer på effekten av tiltakene. Oppgaven tar dermed utgangspunkt i den redegjorte operasjonaliseringen vedrørende resiliens, da begrepet i forskningsspørsmålet operasjonaliseres slik at det gis grunnlag for begrepsvaliditet, altså i hvilken grad begrepene har god validitet (Lund, 2002:89).

3.3.2 Reliabilitet

Høy reliabilitet er en nødvendig forutsetning for at data skal inneha høy validitet. For å kunne besvare oppgavens valgte problemstilling er det prekært at de relevante slutningene ikke bare innehar høy validitet, men også høy grad av reliabilitet. Reliabilitet kan defineres som nøyaktighet med fravær av målefeil. Samsvar mellom den operasjonelle definisjonen og teoretiske definisjonen avgjør definisjonsmessige validiteten, som videre har betydning overfor oppgavens gjennomførelse og graden av validitet. Reliabilitet gjenspeiles i overgangen mellom den operasjonelle definisjonen og de faktiske data, og om resultatet hadde vært det samme dersom undersøkelsen ble gjennomført på nytt (Hellevik, 2003:52-53). Etterprøvbarhet er med det, et viktig krav for å oppnå høy reliabilitet i en forskningsstudie. I henhold til oppgavens tema og problemstilling er det problematisk å gjennomføre en reliabilitetstest som stabilitetstest, hvor det gjennomføres målinger på ulike tidspunkt for å se om resultat samstemmer, ettersom cybersikkerhet, digitale sikkerhetsutfordringer og

sårbarhetsreduserende tiltak alle er dynamiske aspekter av Norges sikkerhetspolitiske forhold (Hellevik, 2003:184). Det vil dermed ikke gi fruktbare eller relevante målinger dersom en stabilitetstest blir gjennomført i denne oppgaven. Til tross for at en stabilitetstest er velegnet til undersøkelsesopplegg som benytter foreliggende materiale som innholdsanalyse, vil gjennomføringen ikke bidra til å kunne svare på den definerte problemstillingen ettersom tidsaspektet mellom målingene ikke er relevante for oppgaven. Endringen som har forekommet i form av den nye trusseldimensjonen grunnet digitaliseringen av samfunnet er ikke videre relevant for denne oppgaven.

Oppgavens funn av den metodologiske tolkningen som skal svare på den definerte problemstillingen, baseres dermed på innhenting av det foreliggende materialet i form av datainnsamlingen og behandlingen av dette materialet. Kvalitativ forskning baseres i betydelig grad på forskerens tolkning av datamaterialet, noe som kan svekke oppgavens reliabilitet og dermed også validiteten, ettersom undersøkelsen må sannsynliggjøre funnene på en troverdig måte for å styrke reliabiliteten (Gentikow, 2005:59).

Allikevel er det gjennomført tiltak for å kunne styrke oppgavens reliabilitet i form av undersøkelsesopplegget. Begrepspluralisme innenfor det digitale rom svekker reliabiliteten i henhold til oppgavens tema, ettersom forskere og relevante myndigheter vektlegger begreper ulikt, samt at ved flere sentrale begreper innenfor tema finnes utallig versjoner av samme begrep. Derav oppgavens innledende redegjørelse og konsekvente valg om å gjennomgående benytte et begrep i redegjørelse av fenomen, for å styrke oppgavens samlede reliabilitet. Det foreliggende materialet som ble innhentet ved datainnsamlingen og som benyttes til oppgaven er offentlig, ugradert og tilgjengelig informasjon som i stor grad er etterprøvbar. Studie av dokumenter som stabile objekter medfører til uforandrede dokumenter uten utslag av påvirkning, som styrker undersøkelsers etterprøvbarhet. Oppgavens betydelige fokus på et tydelig avgrenset datamateriale som er observerbart, styrker valget av innholdsanalyse som forskningsmetode ettersom det fremmer teknikken for å trekke realiserbare og valide slutninger fra data til kontekst (Krippendorf, 2012:21).

4 Empiri

Dette kapittelet redegjør for faktiske hendelser av betydelig relevans for cybersikker, digitale sårbarheter, digitale sikkerhetsutfordringer og resiliens på strategisk og operativt nivå. I kapittel to ble det redegjort for teoretiske tilnærminger som kan tolke staters utenrikspolitiske adferd. I dette kapittelet tillegges oppgaven empirisk tygde. Statlig etterretning har i den nye trusseldimensjonen etablert en rekke nye virkemidler som potensielt kan svekke en annen stats handlingsrom, som alvorlige IKT-sikkerhetshendelser eller cyberoperasjoner mot myndighetene, sentrale virksomheter og befolkningen. Dette kapittelet viser til den historiske utviklingen av cyberoperasjoner med eksempler fra både russisk etterretningsvirksomhet og cyberoperasjoner mot norske institusjoner. Dette kapittelet vil i likhet med kapittel to tilrettelegge for den kommende analysen.

4.1 Den nye trusseldimensjonen

Sjefen for E-tjenesten, generalløytnant Morten Haga Lunde, har beskrevet dagens sikkerhetspolitiske situasjon på følgende måte «I dagens tryggingspolitiske klima kan enkeltepisodar få alvorlege konsekvensar som ingen av partane i utgangspunktet ønskjer eller er tente med» (Etterretningstjenesten, 2017:22). Utsagnet må tolkes i lys av den nye trusseldimensjonen, hvor kombinasjonene av tradisjonelle maktmidler og mer subtile virkemidler utgjør statlige strategier for å nå politiske og militære strategiske mål. Dette innebærer eksempelvis å videreutvikle operasjonelle kapabiliteter for sabotasjeformål rettet mot digitale sårbarheter som ligger i grenseflaten mellom digital informasjonsbehandling, digital kommunikasjon og digital styring. Den økende betydningen av digitale systemer, utvikler parallelt og systematisk fremmede staters etterretningsvirksomheter interesse for samme digitale systemer. Digitaliseringens følger overfor fysiske grenser og den strukturelle maktbalansen, baseres på at maktutøvelse i det digitale rom utfordrer det tradisjonelle synet på makt som en funksjon av tilgjengelige ressurser. Trusler i det digitale rom rettes mot digitale sårbarheter og menneskelige svakheter gjennom etterretnings- påvirknings- og sabotasjeoperasjoner i det digitale rom (Etterretningstjenesten, 2018:32).[21]

[21] Digital sabotasje benyttes som et virkemiddel i et overordnet konsept som ellers omfatter desinformasjon, manipulasjon, aggressiv propaganda og stimulering sosial uro (Etterretningstjenesten, 2017:34).

Utfordringer i det digitale rom er grenseoverskridende på tvers av land, sektorer og virksomheter, og utvikles kontinuerlig. Den nye trusseldimensjonen utfordrer det tradisjonelle skillet mellom fred og krig, samtidig utfordres den tradisjonelle ansvarsplasseringen mellom sivil og militær sektor. Dette kapitlet skal gi en oversikt over relevant strategisk viktige hendelser som har forekommet relatert til cybersikkerhet og Norges sikkerhetspolitiske situasjon.

4.1.1 Politisk motivert cyberoperasjon mot Estland

Høsten 2007 ble Estland utsatt for en politisk motivert cyberoperasjon, hvor sentrale finansinstitusjoner og statlige organer ble lammet. Daværende utenriksminister for Estland, Urmas Paet, hevdet umiddelbart at Russland sto bak handlingen (Singer & Friedman, 2014:110).[22] Cyberoperasjonen varte i om lag tre uker hadde som formål å svekke den estiske stats funksjon, og fremme en digital kollaps i en betydelig digitalisert stat. I løpet av de tre ukene ble det utført målrettede angrep mot presidentskapet og parlamentet, departementene, politiske partier, det sentrale nasjonale kringkastingsbyrået, finansinstitusjoner, samt større kommunikasjonsfirmaer (Kramer *et al*, 2009:475).

Representanter fra verken NATO eller EU anklaget Russland formelt for cyberoperasjonen, til tross for at det ble identifisert spesifikke internettadresser tilknyttet Russland, samt enkelte tilfeller hvor tilknytningen var til russiske institusjoner. Russiske myndigheter tok avstand fra anklagene (Kramer *et al*, 2009:475). Spekulasjoner om russisk involvering i cyberoperasjonen mot estiske stats- og samfunnsfunksjoner, var basert på en disputt mellom de to statene. Estland hadde planlagt en relokalisering av et Sovjetisk minnesmerke fra Tallin og denne handlingen svekket det politiske forholdet mellom de to statene.[23] Tidspunktet da cyberoperasjonen inntraff og effekten som ble generert, indikerer utnyttelse av digitale sårbarheter på bakgrunn av omfattende etterretningsvirksomhet orkestrert av Kreml (Connell & Vogler, 2017:14). Operasjonen hadde russiske koblinger gjennom såkalte patriotiske hackere, hvor ikke-statlige aktører handler på vegne av en stat, mens ledende

[22] *Distributed Denial of Services* (DDoS).
[23] *The Bronze Soldier of Tallin*, et Sovjetisk minnesmerke fra andre verdenskrig.

beslutningsorgan i en stat innehar en mer subtil rolle som allikevel orkestrerer handlingen for å sikre effektivitet (Singer & Friedman, 2019:111).[24]

Cyberoperasjonen mot Estland i 2007 markerte en milepæl innenfor forsvars- og sikkerhetspolitikk, da et helt samfunn ble destabilisert av en cyber-blokade. Hendelsen i 2007 var første gang Russland koordinerte bruken av cyberdomenet til å påvirke et strategisk utfall i en nabostat (Connell & Vogler, 2017:13). Russlands handling plasserte cybersikkerhet for alvor på den internasjonale dagsordenen.

4.1.2 Russlands posisjon: Georgia og Ukraina

I august 2008 ble *femdagerskrigen* utspilt mellom Russland og Georgia. Russland demonstrerte tydelig evne til å utføre større og kompliserte operasjoner, til tross for marginal militær investering på 1990-tallet (Heier & Kjølberg, 2015:86-87). Den russiske luftkampanjen møtte sterkest motstand i form av georgisk luftvern, til tross for betydelige forskjeller i luftstyrker til fordel for Russland. Den digitale krigføringen rettet mot georgiske statsfunksjoner innehadde elementer som minnet om cyberoperasjonen som Estland ble utsatt for et år i forveien. Til tross for at den georgiske regjeringens nettside og e-poster ble rammet av en russisk cyberoperasjon under krigen i 2008, ble ikke georgiske styrkers forsvarsevne redusert i betydelig grad (Heier & Kjølberg, 2015:88). Tjenestenektangrepet var rettet mot å svekke den georgiske regjeringens kommunikasjonsevne overfor befolkningen.[25] I likhet med cyberoperasjonen mot Estland, ble et subtilt virkemiddel benyttet av russiske myndigheter. Fremgangsmåten på operasjonen rette mot den Georgiske stat var slående lik operasjonen i Estland, ikke-statlige aktører handlet på vegne av et beslutningsorgan i en stat, hvor myndighetene innehadde en mer subtil rolle.

Intervensjonen i Ukraina og spesielt annekteringen av Krimhalvøya i februar 2014 derimot, viste en dominerende militærmakt som benyttet flere virkemidler målrettet for å øke nasjonalt handlingsrom. Russlands utenrikspolitiske strategi fremmet en større usikkerhet som lammet det internasjonale samfunnet etter annektering av Krimhalvøya. Hendelsesforløpet er en påminnelse om den kontinuerlige utviklingen av den nye trusseldimensjonen og moderne krigføring (Matlary & Heier, 2016:239). Numerisk overlegenhet, tungt materiell og overlegen

[24] *Patriotic hacking*, en handling som omhandler involvering av borgere eller grupper i en stat sammen utfører cyberangrep mot en oppfattet fiende av egen stat.
[25] *Denial of Services* (DoS).

ildkraft var blitt erstattet av mobile, hurtige og manøvrerende styrker i tospann med lokale støttespillere i form av russiske minoriteter (Heier & Kjølberg, 2015:88). Gjennom ikke-lineær krigføring, ble det rettet press mot en vital funksjon i et samfunn og hvor fokuset er å nøytralisere statens vitale funksjonalitet (Schnaufer, 2017:21). Denne strategien var synlig, da Russland strategisk plasserte nasjonale styrker langs grensen mot Ukraina, hvor ukrainske styrker måtte mobiliseres til grensen i frykt for en invasjon av Øst-Ukraina. Russland svekket Ukrainas handlingsrom, ettersom Ukraina ikke hadde militære styrker å avse til å forsvare Krim (Heier & Kjølberg, 2015:89). Russland utnyttet usikkerheten i situasjonen ved å deployere styrker, små grønne menn.[26] De isolerte tilstedeværende ukrainske styrker i kombinasjon med at russiske myndigheter utøvde strategisk press gjennom flere virkemidler, deriblant: informasjon, militært, økonomi, var utslagsgivende (Matlary & Heier, 2016:37, 181).

Utviklingen fra krigen med Georgia til intervensjonen i Ukraina var betydelig. Ettersom den georgiske utenrikspolitikken hadde gradvis blitt mer positiv overfor Vesten, demonstrerte Russlands militære evne og vilje til for å nå utenrikspolitiske mål (Connell & Vogler, 2017:17). Cyberoperasjonen satte regjeringens nettsteder ute av spill i en mindre periode, allikevel utgjorde ikke følgene av dette en betydelig svekkelse av den georgiske regjeringens handlingsrom (Heier & Kjølberg, 2015:88). Intervensjonen i Ukraina bar tydelig preg av at Russlands væpnede styrker hadde gjennomgått en omfattende reform- og moderniseringsprosess, med utgangspunkt i lærdommen fra krigen mot Georgia. Materiellparken, strategisk trening, konsepter og doktrine ble tilpasset en ny tid, bidro til å undergrave legitimiteten og autoriteten til ukrainske militære og politiske institusjoner (Connell & Vogler, 2017:19). Samspillet mellom cyberoperasjoner og konvensjonelle militære operasjoner er en betydelig og markant forskjell mellom krigen i Georgia og intervensjonen i Ukraina seks år senere (Heier & Kjølberg, 2015:88). Russlands krig med Georgia og intervensjonen i Ukraina, viser statens militære evne og politiske vilje til å utføre uforutsigbar og folkerettsstridig maktpolitikk utenfor eget territorium. Geopolitiske maktforstyrrelser setter institusjonelle rammeverk under press, og Russlands sofistikerte offensive cyberkapabiliteter kan utnytte digitale sårbarheter for å lamme sentrale stats- og samfunnsfunksjoner i en stat. Disse to forholdene viser Russlands militære utvikling innenfor det digitale rom, og aktualiserer behovet for sårbarhetsreduserende tiltak.

[26] Soldater uten emblem/kjennemerker i anonymiserte styrker.

4.1.3 Stuxnet

I januar 2010 forårsaket Stuxnet-ormen fysisk ødeleggelse på et av Irans atomanlegg. Cyberoperasjonen mot det spesifikke atomanlegget er av interesse for andre internasjonale aktører, ettersom atomanlegget var mistenkt som en sentral del av Irans ulovlige atomvåpenprogram. Stuxnet var en svært sofistikert dataorm som målrettet angrep strategiske kontrollenheter for å ødelegge atomsentrifuger ved det iranske atomanlegget, lokalisert i Natanz. Stuxnet-ormen utnyttet fire nulldagssårbarheter[27] og oppdaget de relevante Windows maskinene i atomanleggets kontrollenhet, før et program anvendt i *Siemens Programmable Logic Controllers* ble angrepet (Singer & Friedman, 2014:116). [28]

Stuxnet-ormen skulle redusere Irans produksjon av anriket uran, hvor raffinert uranbrensel anvendes i atomreaktorer i kjernekraftverk. Motivet for cyberoperasjonen danner grobunn for mistanke om at en eller flere stater står bak, dette støttes opp under med tanke på de enorme ressursene som har vært nødvendig i henhold til etterretningsarbeidet (Langer, 2013:10). I tiden etter Stuxnet har det kommet indikasjoner på at det trolig var USA og Israel som sto bak cyberoperasjonen (Singer & Friedman, 2014:118). Stuxnet-ormen utnyttet en betydelig sårbarhetsflate da en av det iranske atomanleggets egne sikkerhetsventiler mistet sin primære operative funksjon. *Air-gap* skal minske muligheten for en operasjon i det digitale rom ved å danne et komplett skille mellom sensitive systemer i en virksomhet og offentlige nettverk. Denne funksjonen ble utspilt, da mottaksmekanismen ble infiltrert gjennom iranske atomforskeres egne digitale enheter og minnepinner som hadde vært tilkoblet både offentlige nettverk og atomanleggets sensitive system. Før Stuxnet-ormen benyttet seg av en selvdestruerende funksjon i 2012, påførte ormen betydelig skade på reaktorene i atomanlegget. Stuxnet hindret ikke bare atomanleggets produksjon, i tillegg skjulte ormen effekten av det synkende produksjonsnivået. Systemet i atomanlegget ga informasjon om optimal funksjonalitet til de iranske ingeniørene, selv om sentrifugene kollapset en etter en. Dermed resulterte Stuxnet i en betydelig reduksjon i Irans atomprogram, samt dyrket ormen usikkerhet og den psykologiske effekten svekket ingeniørenes og iranske myndigheters tro på programmet (Singer & Friedman, 2014:117).

[27] Ukjente sårbarheter som ofte oppdages etter en gjennomført cyberoperasjon.
[28] Mer utfyllende, WinCC/PCS 7 Supervisory Control and Data Acquisition (SCADA).

Stuxnet illustrerer hvordan cyberoperasjoner kan få alvorlige konsekvenser utenfor det digitale rom. Stater som opplever uautorisert innhenting av informasjon opplever ikke bare frykt for at den sikkerhetspolitiske situasjonen skal endre, men også for at informasjonsinnhentingen er begynnelsen på en større sikkerhetspolitisk utfordring (Buchanan, 2016:77).

4.1.4 NotPetya

I 2017 ble en rekke virksomheter globalt utsatt for en større cyberoperasjon. I første rekke var det sentrale ukrainske virksomheter som ble tilsynelatende utsatt for et løsepengevirus-angrep.[29] Dette var et målrettet angrep hvor deler av virksomhetenes data ble kryptert og dermed utilgjengelig, hvor hackerne som sto bak krevde løsepenger for å frigjøre dataen. Fremgangsmåten var slående lik tidligere løsepengevirus-angrep, allikevel var det en betydelig forskjell; betalingsmåten var ikke gjennomførbar.[30] Til tross for at NotPetya fremsto som et løsepengevirus-angrep var det i realiteten en dataorm som infiltrerte sentrale virksomheters kontrollenheter for så å slette data fra harddiskene til de infiltrerte datamaskinene (Muller, Gjesvik & Friis, 2018:24). Cyberoperasjon spredte seg hovedsakelig gjennom regnskapsprogramvaren *MeDoc*, som i henhold til Ukrainsk lov er ett av to programmer som skal benyttes av virksomheter som opererer innenfor ukrainske grenser (Muller *et al*, 2018:25). Dette medførte til rask og effektiv spredning av ormen til sentrale ukrainske virksomheter og andre relevante offentlige etater.

NotPetya tilfellet viser hvor sofistikerte cyberoperasjoner kan være, samt problemene ved å attribuere og respondere trusselaktører (Muller *et al*, 2018:26). Det tilsynelatende løsepengeviruset illustrer også kompleksiteten av digitale sikkerhetsutfordringer med samhandling mellom tjenester, systemer og infrastrukturer mellom virksomheter. NotPetya viste hvordan trusselaktører kan, gjennom ulike metoder, spre et feilaktig budskap i et forsøk på å undergrave tilliten til det offentlige. Den nasjonale sårbarhetsflaten øker ved at digitale sårbarheter, i tråd med feil, forplantes raskt mellom leddene i verdikjedene og digitaliseringen tilrettelegger for strukturell samfunnsmessig sårbarhet som trusselaktører kan utnytte.

[29] Ransomware.
[30] Non-functional, derav navnet på cyberangrepet.

4.2 Statlig etterretning

Den geopolitiske utviklingen og stadig hardere globale konkurransen for å skape økonomisk vekst, ressurstilgang og teknologisk utvikling, gir grunnlag for etterretningsvirksomhet mot Norge. Målrettet innhenting og bearbeiding av informasjon i en kompleks, uoversiktlig og usikker sikkerhetspolitisk situasjon, styrker beslutningstøtten for politiske myndigheter som har iverksatt omfattende etterretningsarbeid. I nyere tid har norske myndigheter opplevd mer aggressivt og målrettet etterretningsvirksomhet, hvor særlig russiske aktører har rettet vedvarende aktiviteter mot sentrale myndigheter og virksomheter. Norge har ikke et sikkerhetspolitisk samarbeid med hverken Kina eller Russland, som gjennom PST og E-tjenestens årlige trusselvurderinger blir fremstilt som de to statene som utgjør de mest alvorligste truslene mot norske digitale systemer (Politiets sikkerhetstjeneste, 2018:7 & Etterretningstjenesten, 2015:84). Det pågående og omfattende etterretningsarbeidet i og mot Norge, tar sikte på å få tilgang til sensitiv og skjermingsverdig informasjon, i tillegg til å påvirke politiske, økonomiske og forvaltningsmessige beslutninger. Informasjon som har kritisk nytteverdi, fremkommer som interessant for en stat som har som formål å sabotere kritisk infrastruktur eller kritiske samfunnsfunksjoner ved en eventuell fremtidig konflikt. Offentlig og aggressiv etterretning styrker nasjonale interesser på bekostning av andre stater. Norge er av ulike årsaker interessant for fremmede staters etterretningstjenester, grunnet bestanddeler av store høyteknologiske forsvarsleverandører og mindre leverandører av nisjeteknologi innen norsk industri. Offensiv etterretningsvirksomhet mot norske virksomheter innen teknologi og innovasjon, møter dermed målrettede angrep utført av aktører med store ressurser på søken etter informasjon som kan gi statens egne nasjonale selskap konkurransefortrinn. I enkelte stater er det tette koblinger mellom privat industri, staten og forsvaret, som igjen styrker deres etterretningsressurser. Etterretningstrusselen fremstår dermed som forsøk på, i det digitale rom, å infiltrere norske IKT-systemer, norsk industri og myndighetsapparat.

4.2.1 Alle piler peker mot Russland

I PSTs trusselvurdering fra 2015 ble Russland, i likhet med Kina, for første gang omtalt som stater som bedriver etterretningsvirksomhet mot Norge (Politiets sikkerhetstjeneste, 2015:11). Etterretningstjenester fra stater med tette kobling mellom industri, staten og forsvar betegner den russiske etterretningen mot Norge, i et allerede betydelig asymmetrisk sikkerhetspolitisk

forhold. Et betydelig skille mellom øst og vest, her representert ved henholdsvis Russland og Norge, er forståelsen av maktfordelingen mellom stat og borgere. Anerkjent politisk stabilitet og økonomisk produktivitet baseres på en reell motmakt til statlige myndigheter i Norge og Vesten generelt. I Russland derimot, anses fragmentering av makt, fremfor sterk konsentrasjon, som mulige kilder til sosial- og politisk uro (Heier & Kjølberg, 2015:41).

Russland har vist evne til å unngå en direkte konfrontasjon med NATO, parallelt med at det arbeides for å styrke landet rolle utenfor egne nærområder. Ved at staten har påberopt seg retten til å foreta humanitær intervensjon, som ved konflikten med Georgia, samt handlinger i Krim og Donetsk, har russiske myndigheter styrket nærværet i nasjonale interesseområder gjennom vestlige demokratiske forankrede verdier (Matlary & Heier, 2016:37). Kreml benytter informasjon, kultur og økonomi mot Vesten for å danne splittelse i Vesten, samt innad i NATO-alliansen, og undergrave vestlige institusjoner (Pomerantsev & Weiss, 2014:14) Russiske myndigheters propaganda-apparat består av påvirkningskampanjer innen: politikk, økonomi, korrupsjon, energi, militære, cyber, minoriteter, kultur og *soft power*, som benyttes for å fremme russiske interesser (Matlary & Heier, 2016:199).[31] Russlands operasjonelle konsept i det digitale rom tydeliggjøres av artikkel 4 i *Convention On International Information Security* (The Ministry of Foreign Affairs of the Russian Federation, 2011:3). Artikkel 4 omhandler de mest sentrale truslene mot internasjonal fred og sikkerhet i det digitale rom. Herunder artikkel 4.4, hvor handlinger i det digitale rom tar sikte på å undergrave det politiske, økonomiske og sosiale system overfor en annen regjering. Videre rettes psykologiske kampanjer mot statens befolkning for å destabiliseres samfunnet. Spesielt artikkel 4.11, som omhandler informasjon ekspansjon; altså et siktemål om å overta kontroll over andre nasjoners informasjons ressurser, understreker kritikalitet av den nye trusseldimensjonen.

Russland markerer seg stadig sterkere i det asymmetriske sikkerhetspolitiske forholdet med Norge. I et allerede spent forhold mellom Russland og Vesten, videreutvikles russiske offensive cyberkapabiliteter i tråd med at landets posisjon utenfor egne nærområder.

[31] *Soft force*, er et bedre uttrykk ettersom Russlands tolkning av *Soft power* skiller seg betraktelig fra den vestlige tolkningen av begrepet. Den russiske tolkningen vektlegger bruken av tvangsmakt og destabilisering gjennom ikke-militære midler. Styrkebidrag som demonstrering av militær styrke, cyberangrep og ikke minst påvirkning mot energiavhengighet (Matlary & Heier, 2016:183).

4.2.2 Russiske simulerte angrep mot norske mål

Sjefen i E-tjenesten, Generalløytnant Morten Haga Lunde, presenterte i Mars 2018 radar-utskrifter av russiske kampfly som ved flere anledninger trente på å angripe norske mål. Generalløytnant Lunde viser til tre simulerte angrep mot norske mål og mål tilknyttet Norges NATO-medlemskap. [32]

i. 24. mars 2017. Russiske bombefly fløy i taktisk formasjon mot E-tjenestens installasjon på Vårberget, Vardø. Bombeflyene, med eskorte, gjennomførte flyaktivitet i taktiske profiler (Lunde, 2018).

ii. 22. mai 2017. Nordvest for Senja i Troms fløy russiske bombefly i taktisk formasjon mot en NATO-flåtestyrke som opererte i Norskehavet. Også ved denne anledningen gjennomførte bombeflyene, med eskorte, aktivitet i taktiske profiler. Den russiske styrkevisningen signaliserte motstand mot norsk og alliert øvelse (Lunde, 2018).

iii. 27. mai 2017. Norge ledet en større alliert luftforsvarsøvelse i samarbeid med Sverige og Finland. Russisk misnøye ble signalisert med et tilsvarende tokt, som det som fant sted fem dager tidligere, rettet mot militære installasjoner i nærområdet tilhørende Bodø (Lunde, 2018).

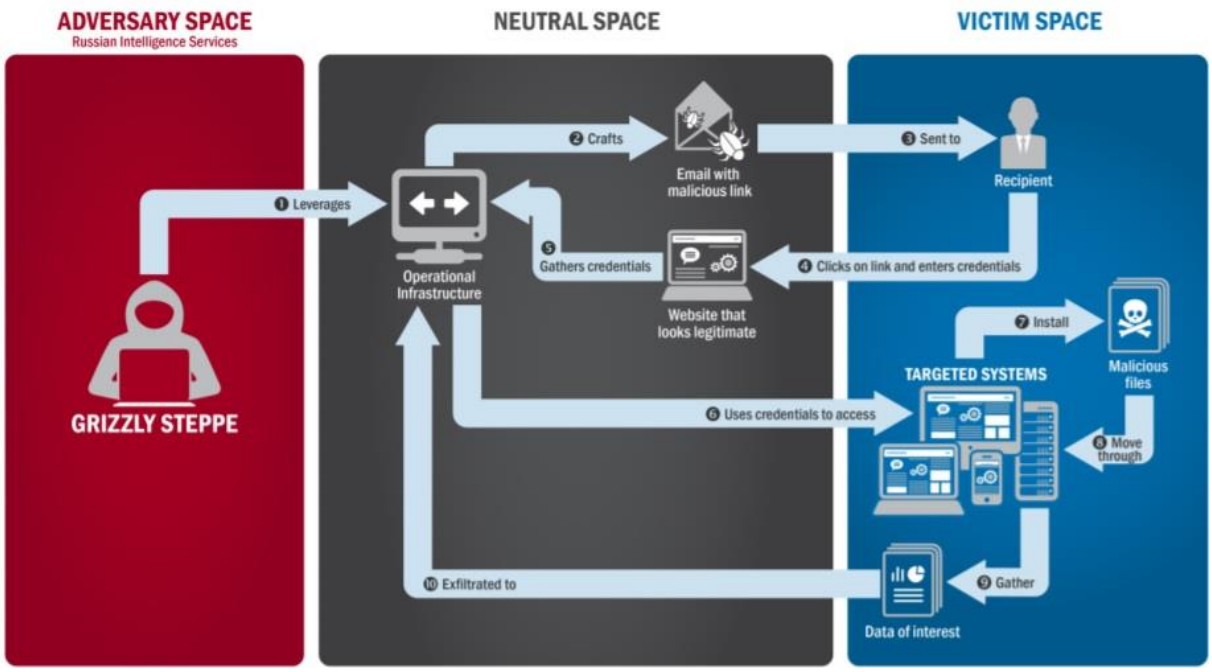
Disse tre militærøvelsene viser en stadig mer offensiv russisk adferd i nordområdene, med høy militær aktivitet. Militærøvelsene understreker at Russland styrker posisjon utenfor eget territorium, hvor uanmeldte militærøvelser kan medføre til økt usikkerhet vedrørende Russlands maktpolitikk.

[32] I sitt årlige foredrag for Oslo Militære Samfund i forbindelse med utgivelsen av E-tjenestens årlige åpne vurdering av aktuelle sikkerhetsutfordringer.

4.2.3 Cyberoperasjon mot Norge

Telenor

Metodikken som ofte blir benyttet vedrørende cyberoperasjoner forekommer gjennom målrettet og troverdig utformet e-post, såkalte *phising*, og *spear-phising* hvor enkeltindivider i bedrifter av interesse for fremmede etterretningstjenester blir utvalgt som etterretningsmål grunnet individets posisjon i organisasjonen. *Spear-phising* var metoden som ble tatt i bruk mot Telenor, da virksomheten i 2013 ble utsatt for en omfattende cyberoperasjon. Personlige og troverdige utformede e-poster ble sendt til sentrale individer i Telenor. E-postene inneholdt skadevare som krevde at mottakere foretok en handling, i form av å åpne en lenke, før avsenderen av e-posten hadde tilgang til sensitiv informasjon i Telenor, som vist i figur 2.0. Cyberoperasjonen mot Telenor i 2013 var ett av flere angrep mot virksomheter innenfor et bredt spekter av potensielle mål, og var ett ledd i en omfattende industrispionasje fra ikke-statlige aktører basert i India. Skadevaren som ble plantet i e-postene hadde som formål å gi avsender tilgang til forretningshemmeligheter og annen sensitiv informasjon, til tross for at Telenor, *Telenor Security Operations Center* (TSOC), oppdaget angrepet lykkes den ikke-statlige aktøren med å tappe Telenor for sensitiv informasjon (Fagerland *et al*, 2013).

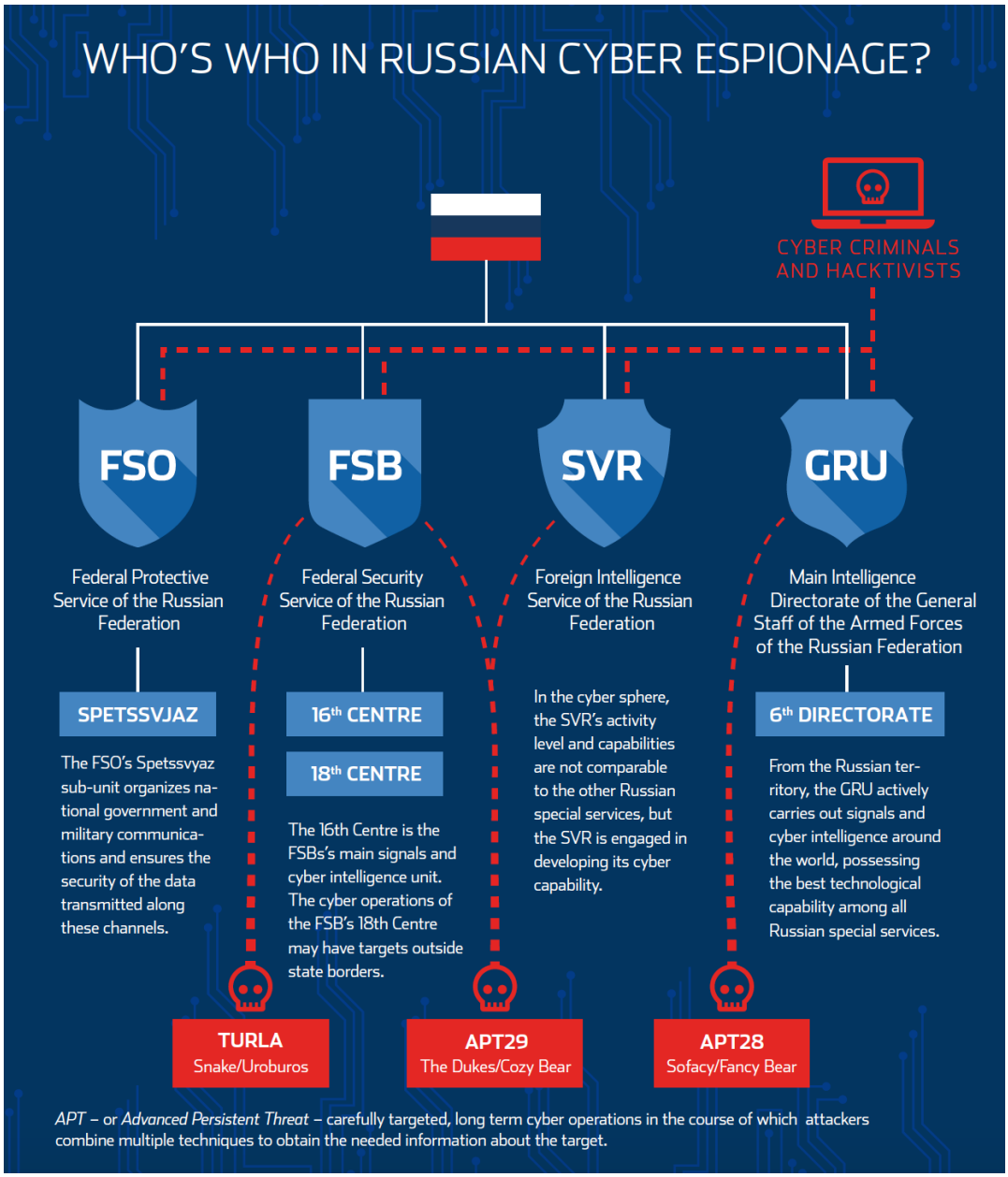


Figur 2.0 Animasjon av et *spear-phising* angrep (Departement of Homeland security & the Federal Bureau of Investigation, 2016:2)

En omfattende cyberoperasjon mot flere norske institusjoner

I februar 2017 kom nyheten om at flere norske institusjoner utsatt for en omfattende cyberoperasjon. Russiske målrettede og langsiktige cyberoperasjoner baseres på flere teknikker for optimal funksjonalitet, *advanced persistent threat* (APT) (Välisluureamet, 2018:52).[33] PST stadfester at, i likhet med cyberoperasjonen mot Telenor, forekom også denne operasjonen gjennom ondsinnet e-post, *spear-phising*, som inneholdt skadevare. PST, gjennom Seksjonssjef Arne Christian Haugstøy, påpeker at denne spesifikke cyberoperasjonen kan konkret attribueres til trusselaktøren APT29, som videre knyttes til russiske myndigheter (TV2, 2017).[34] APT29 gjennomførte cyberoperasjonen ved å målrettet sendte ondsinnet e-post til ni konkrete e-postadresser ved Aps Stortingsgruppe, Forsvaret, UD, Statens Strålevern (NRPA), en høyskole og til PST.[35] Ved samtlige institusjoner var nettverksangrepet rettet mot åpne og ugraderte e-postadresser (TV2, 2017). APT29 som aktør er sentral i russiske påvirkningskampanjer samt bistår ved etterretnings- og sabotasjehandlinger og benyttes som et virkemiddel av *Federal Security Service of the Russian Federation* (FSB) og *Foreign Intelligence Service of the Russian Federation* (SVR) (Välisluureamet, 2018:53), som belyst i figur 3.0.

[33] Avanserte vedvarende trusler.
[34] Alternativt, *Cozy Bear* (Välisluureamet,2018), cybersikkerhets firmaene Fireeye og F-Secure refererer til grupperingen som henholdsvis *APT29* og *The Dukes.*
[35] National Radiation Protection Authority.



Figur 3.0 Aktører innen russisk spionasje i det digitale rom (Välisluureamet, 2018:55).

Helse Sør-Øst

I januar 2018 ble datasystemene til Helse Sør-Øst utsatt for en cyberoperasjon. Regionen Helse Sør-Øst er den største av de totalt fire helseregionene i Norge og omfatter pasienter i fylkene Østfold, Akershus, Oslo, Hedmark, Oppland, Buskerud, Vestfold, Telemark, Aust-Agder og Vest-Agder, noe som utgjør pasientinformasjon for 2,9 millioner mennesker (Helse Sør-Øst,2018). Helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet (HelseCERT) rapporterte om unormal aktivitet i datasystemene til Helse Sør-Øst

(Helsedirektoratet, 2018).[36] Cyberoperasjonen er under etterforskning (mars 2018), hvor partene i Felles Cyberkoordineringssenter (FCKS) tar del i håndteringen av hendelsen. Aktuelle parter er NSM, E-tjenesten, PST og Kripos, etter koordinering av Helsedirektoratet og NSM (Norsk senter for informasjonssikkerhet, 2018).[37] Cyberoperasjonen etterforskes som mulig brudd på straffeloven § 121 *Etterretningsvirksomhet mot statshemmeligheter* (Straffeloven, 2005, § 121), ettersom forholdet kan være informasjonsinnhenting med utgangspunkt i å skade grunnleggende nasjonale interesser, herunder samfunnets infrastruktur i henhold til opplysninger om helseberedskap (Politiets sikkerhetstjeneste, 2018).

Empirisk, har etterretningsaktivitet vært rettet mot tradisjonelle politiske og militære mål, som utenrikstjenesten og Forsvaret. Øvrige mål for fremmed etterretningsvirksomhet har vært statsforvaltningen, akademiske institusjoner, kraftselskap og bedrifter i industrien (Etterretningstjenesten, 2018:30). Cyberoperasjonen mot Helse Sør-Øst tydeliggjør at etterretningsvirksomhet mot Norge ikke er begrenset til tradisjonelle politiske og militære mål, men at sivile mål også er utsatt for fremmede staters etterretningsvirksomhet. Innbruddet i datasystemene til Helse Sør-Øst tyder på at fremmede staters etterretningsvirksomhet forsøker å innhente sensitiv informasjon om nasjonal helseberedskap, Norges grunnleggende interesser. Informasjonen kan videre benyttes til å tilpasse cyberoperasjoner etter individuelle profiler, og utforme troverdig e-post som sendes til strategisk viktige enkeltindiver for å spre skadevare. Cyberoperasjonen viser til interesse og fremgangsmåte som samsvarer med en fremmed stat eller statsstøttet aktør (Lunde, 2018).

4.2.4 Internasjonale trender

E-tjenesten har fremlagt tre sentrale områder knyttet til økt etterretningsvirksomhet på grunnlag av internasjonale trender, hvor det ene punktet gjør seg gjeldende for det sivile samfunn og enkeltindividet. E-tjenesten advarer mot en økende interesse for personopplysninger, ettersom tilgang på personopplysninger, passbilder og biometrisk data simplifiserer fremmede staters genuine mulighet til å tilpasse etterretningsoperasjoner etter enkeltindivider (Etterretningstjenesten, 2016:82).

[36] Computer Emergency Rescue Team.
[37] NorSIS.

Det teknologiske paradigme-skiftet innen sikkerhets- og forsvarspolitikk har resultert i en utvikling av sofistikerte virkemidler innen staters utenrikspolitiske arsenal. Stuxnet, cyberoperasjonen mot Estland, Russlands sofistikerte cyberkapabiliteter, samt evne til å benytte flere virkemidler før å øke nasjonalt handlingsrom, har plassert cybersikkerhet på den politiske agenda i det internasjonale system. NotPetya understreker kompleksiteten av digitale sikkerhetsutfordringer med samhandling mellom virksomheter og øker den nasjonale sårbarhetsflaten.

I en norsk kontekst har Russlands uforutsigbarhet plassert cybersikkerhet og sårbarhetsreduserende tiltak på den politiske dagsordenen, gjennom en vedvarende etterretningstrussel og nye digitale sikkerhetsutfordringer som kan svekke norske myndigheters handlingsrom og utnyttes dersom den sikkerhetspolitiske situasjonen endres. Den omfattende cyberoperasjonen mot sentrale norske institusjoner samt de simulerte angrep mot Norge, tydeliggjør Russlands uforutsigbarhet og den betydelige usikkerheten som forsterkes i det sikkerhetspolitiske forholdet ved enkeltstående handlinger. Cyberoperasjonen mot Helse Sør-Øst understreker at etterretningsvirksomhet mot Norge ikke er begrenset til tradisjonelle politiske og militære mål, men at sivile mål også er utsatt for fremmede staters etterretningsvirksomhet.

Vedvarende russisk etterretningsvirksomhet mot Norge og norske interesser gjennom det digitale rom har forplantet seg som en overhengende trussel mot kritisk infrastruktur og kritiske samfunnsfunksjoner. Ved å avdekke sårbarheter i sentrale virksomheter eller institusjoner, samt å infiltrere enkeltindividers mobile enheter kan etterretningsaktiviteten kartlegg kritisk infrastruktur og kritiske samfunnsfunksjoner for egen utnyttelse. Russland har etablert en egenart innenfor arbeidsmetode ved informasjonsinnhenting som statens *modus operandi* innenfor det digitale rom som tar siktemål på å svekke Norges politiske handlingsrom, mens grunnlaget for et størst mulig russisk handlingsrom er dannet for å kunne vise makt i en eventuell fremtidig konflikt eller endret sikkerhetspolitisk situasjon. I lys av det samlede trussel- og risikobildet er behovet for støtte av håndtering av IKT-hendelser av betydelig omfang, allikevel forekommer gjennomføringen av sårbarhetsreduserende tiltak ikke i takt med utviklingen av trusselbildet.

5 Analyse

I følgende kapittel analyseres totalforsvarets rolle preget av den nye trusseldimensjonen og digitale sårbarheter som forårsaker digitale sikkerhetsutfordringer. Analysen vil benytte *cybersikkerhetsdilemmaet* for å redegjøre for hvilke digitale sikkerhetsutfordringer totalforsvaret står overfor i fredstid, samt potensielle implikasjoner av å redusere digitale sårbarheter. *Cybersikkerhetsdilemmaets* tre grunnpilarer vil tolkes i en sikkerhetspolitisk kontekst om forholdet mellom Norge og Russland. Analysen vil svare på problemstillingens tre underlagte spørsmål, med tilhørende delkonklusjoner. Analysen forekommer på bakgrunn av at norske myndigheter har opplevd mer aggressivt og målrettet etterretningsvirksomhet mot nasjonale interesser i nyere tid. På bakgrunn av vedvarende russisk etterretningsvirksomhet vurderer PST russisk etterretningskapasitet til å inneha størst skadepotensial overfor norske interesser. E-tjenesten viser til etterretning i det digitale rom som den mest alvorlige trusselen mot Norge (Etterretningstjenesten, 2018:32), samt at russiske påvirkningskampanjer mot Vesten har trappet opp. NSM viser til etterretningsoperasjoner som en fremtredende trussel, da forsøk på å etablere digital kontroll og innhente sensitiv informasjon fra norske virksomheter og institusjoner som forvalter nasjonale grunnleggende interesser, kritisk infrastruktur og kritiske samfunnsfunksjoner.

5.1 Ny Normaltilstand

Norges sikkerhetspolitiske situasjon og potensielle utfordringer relatert til krisehåndtering har tradisjonelt omhandlet Russland grunnet geografiske omstendigheter, Norges medlemskap til NATO og vedvarende interesse for Nordområdene og Arktis. Tradisjonelt har det eksistert en tverrpolitisk enighet om norsk beroligelse og avskrekkelse overfor Russland, først og fremst overfor Sovjetunionen under den kalde krigen, av stabiliserende årsaker (Heier & Kjølberg, 2015:32). Til tross for tilstedeværelsen av latente interessemotsetninger i det bilaterale sikkerhetspolitiske forholdet, har beroligelsesaspektet forgrenet seg overfor en bredere kontaktflate som medfører til at avskrekking og NATO-medlemskap fortsatt er hjørnesteinen i norsk sikkerhetspolitikk (Heier & Kjølberg, 2015:38). Dualiteten har vært tydelig i relevant politikkutforming som omhandler Nordområdene, som er Norges viktigste forsvars- og sikkerhetspolitiske interesseområde.

Allikevel så formes det sikkerhetspolitiske forholdet av en ny normaltilstand hvor asymmetrien består. Norge, Vesten og stater som tidligere var underlagt Sovjetunionen må forholde seg til et stadig mer uforutsigbart Russland som søker å utvide nasjonal innflytelse og posisjon i det internasjonale samfunnet. Norske virksomheter, borgere og myndigheter opplever dette ved at russiske aktører har opprettholdt et vedvarende etterretningspress. Etterretning i det digitale rom er den mest alvorlige trusselen mot Norge, hvor russiske etterretningsoperasjoner vurderes til å inneha størst skadepotensial ettersom Russland har etablert funksjonsdyktige offensive cyberkapabiliteter som utfordrer Norges deteksjonsmekanismer. Cyberoperasjoner har de mest alvorligste og omfattende strategiene som kan utnytte sårbarhetspotensialet for hele spekteret av norske interesser, hvor alvorlige IKT-sikkerhetshendelser vil kunne svekke Norges politiske handlingsrom. Slike potensielle hendelser, i henhold til stats- og samfunnssikkerhetsperspektivet, utgjør den største trusselen av de aktørene som har ressurser til å gjennomføre handlinger som nasjonale deteksjonsmekanismer ikke evner å oppdage. Trusselaktører med betraktelige maktressurser kan være statlige aktører representert som fremmede staters sikkerhets- og etterretningstjenester. Aktiviteter rettet mot øvrige deler av statsforvaltningen, akademia, kraftselskaper og industri kan på bakgrunn av målvalg og metode knyttes til hemmelige russiske tjenester med betydelige maktressurser (Etterretningstjenesten, 2018:30). Empirisk, har aktører med bånd til hemmelige russiske tjenester handlet på vegne av Kreml, som ved handlingene mot Estland, Ukraina og cyberoperasjoner mot flere sentrale norske institusjoner.

5.1.1 Sikkerhetstilstanden

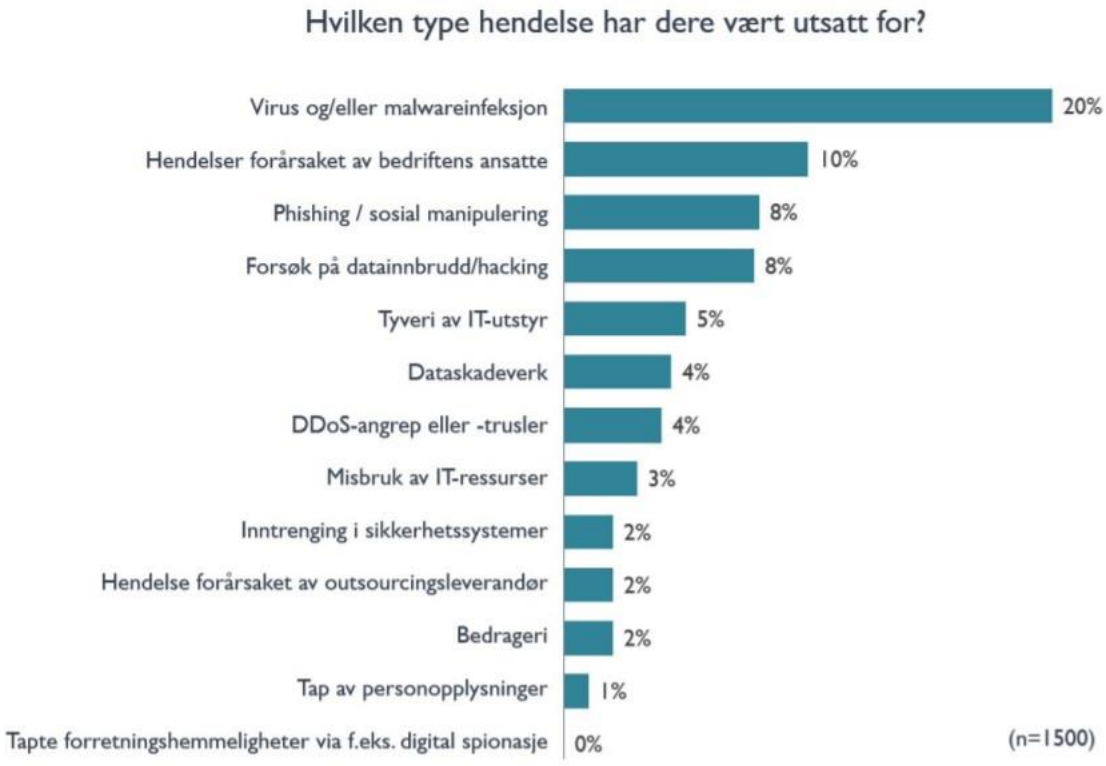
Sikkerhetstilstanden fastsettes av det aktuelle risikobildet med påfølgende forebyggende sikkerhet, hvor risikobildet hovedsakelig påvirkes av eksterne årsaker og forebyggende sikkerhet hovedsakelig påvirkes av interne årsaker. I henhold til denne oppgavens fokus på resiliens, vektlegges dermed forebyggende sikkerhet, ettersom dette er kontrollerbart overfor norske virksomheter og den øvrige befolkningen.

Figur 4.0 Forebyggende sikkerhet (Elgsaas & Heireng, 2014:10)

Figur 4.0 belyser den tredelte sammensetningen av forebyggende sikkerhet, herunder menneskelige-, organisatoriske- og teknologiske tiltak, som samlet har en effekt overfor forebyggende sikkerhetsarbeid. Sammensetningen belyser at tiltakene er gjensidig avhengige av hverandre for å opprettholde et nødvendig nivå av forebyggende sikkerhet overfor sikkerhetstilstanden. Av de ovennevnte tiltakene er menneskelige tiltak utfordrende overfor sikkerhetstilstanden, ettersom digitaliseringen av samfunnet utfordrer risikoaksepten ved at kunnskap og mulighet for å gjennomføre manuelle rutiner forvitrer. Videre medfører denne utviklingen til et stadig økende gap mellom tilgjengelighet og behov for sikkerhetskompetanse, som på et nasjonal plan utgjør en betydelig sårbarhet (Nasjonal sikkerhetsmyndighet, 2017a:8). Mangelen på nødvendig kompetanse har over tid medført at gjennomføringen av sårbarhetsreduserende tiltak ikke forekommer i takt med utviklingen av trusselbildet, og det etableres et betydelig informasjonsgap mellom trusselaktørenes kapabiliteter og nødvendige mottiltak.

NSM, PST og E-tjenesten vurderer cyberoperasjoner fra fremmede stater som den høyeste IKT-risikoen tradisjonelt rettet mot offentlig forvaltning. Samtlige, av de nevnte, sikkerhetsaktørene og tilsynsmyndigheten kategoriserer målrettede og troverdig utformede e-post, *spear-phising*, med skadevare som den mest benyttede metoden for å infiltrere nettverk tilknyttet norske virksomheter og enkeltindivider. Målrettede og troverdige utformede e-poster tappet Telenor for sensitiv informasjon, tilt tross for at organisasjonen har et betydelig sikkerhetsapparat. I sum vil det vedvarende etterretningspresset mot Norge øke samfunnsmessige konsekvenser, og potensielt utløse alvorlige IKT-sikkerhetshendelser. PST, NSM og E-tjenestens vurderinger av cyberoperasjoner anerkjennes av JD, som erkjenner at

behovet for støtte til håndteringen av IKT-hendelser er mer omfattende enn hva NSM og NorCERT har kapasitet til (Justis- og beredskapsdepartementet, 2016:66). Utbedring av resiliens svekkes av et stadig økende forbedringspotensial hos en rekke virksomheter med hensyn til digital hendelseshåndtering på et nasjonalt plan (Justis- og beredskapsdepartementet, 2016:68). I følge en undersøkelse utført av Næringslivets sikkerhetsråd (NSR) publisert i 2016, hadde over en fjerdedel av norske virksomheter, 27%, opplevd uønskede sikkerhetshendelser i perioden fra 2015-2016 (NSR, 2016:3). [38]



Figur 5.0 Hvilken type hendelse norske virksomheter har vært utsatt for (Næringslivet sikkerhetsråd, 2016:11).

Figur 5.0 viser hvilke typer hendelser aktuelle bedrifter har vært utsatt for. *Virus og/eller malwareinfeksjon*, *Hendelser forårsaket av bedriftens ansatte*, *Phising/sosial manipulering* og *Forsøk på datainnbrudd/hacking* representerer de kategorien med størst oppslutning. Felles for tre av de fire kategoriene med størst prosentandel, *Virus og/eller malwareinfeksjon*; *Hendelser forårsaket av bedriftens ansatte* og *Phising/sosial manipulering*, er at disse hendelsene kommer som et resultat av menneskelige feil. Trusselaktører vil systematisk

[38] I den gjennomførte undersøkelsen, Mørketallsundersøkelsen 2016, var totalt 1500 virksomheter deltagende. 412 av 1500 virksomheter har opplev uønsket sikkerhetshendelser i perioden. Undersøkelsen ble gjennomført av Opinion på vegnen av NSR, hvor fokuset omhandlet oppdagelse og håndtering av hendelser, på bakgrunn av alvorlige hendelser.

utnytte aktuelle virksomhets svakeste ledd, som en del av cyberoperasjonene. Digitale sårbarheter, i henhold til tre av de fire kategoriene med størst prosentandel, kan utnyttes da menneskelige feil representerer en betydelig risikofaktor i henholdt til virksomheters sikkerhet.

I samme undersøkelse vises det til gjennomførte endringer i organisasjonen som resultat av hendelser som virksomhetene ble utsatt for. I de 412 rammede virksomhetene ble endringer gjennomført på flere nivåer i et forsøk på å endre virksomhetens sikkerhetskultur og styrke virksomhetens resiliens. Figur 6.0 viser til at det ved kun 3% av de rammede virksomhetene medførte, endringer i organisasjon på bakgrunn av den gjennomførte hendelsen, til at flere kompetente individer ble ansatt. Til tross for at majoriteten av hendelsene mot de 412 aktuelle virksomhetene forekom på bakgrunn av menneskelig feil, medførte hendelsene til at kun 3% av virksomhetene har *Ansatt flere kompetente mennesker*. Figur 6.0 viser til at aktuelle virksomheter i større grad *Investerer i sikkerhetsutstyr*, 25% av virksomhetene, fremfor å *Investere i opplæringsprogram for de ansatte*, 10% av virksomhetene. Av figur 6.0. kan det trekkes slutninger om at i enkelte virksomheter ble en vurdering foretatt om at det var mer prekært å oppgradere sikkerhetsutstyr, hvor de ansatte potensielt ikke har kunnskap om å benytte det oppgraderte sikkerhetsutstyret på en optimal måte.

Figur 6.0 Endringer i organisasjonen som følge av hendelsen (Næringslivets sikkerhetsråd, 2016:21).

Figur 5.0 og 6.0 understreker det betydelige forbedringspotensialet som JD, i samme år, påpekte vedrørende informasjonsgapet mellom trusselaktører og sårbarhetsreduserende tiltak. Det etablerte informasjonsgapet utvider den nasjonale sårbarhetsflaten i det digitale rom. Utviklingen har vært tydelig i det nasjonale deteksjonsarbeidet mot alvorlige IKT-

sikkerhetshendelser. NorCERT registrerte en relativ nedgang i detekterte alvorlige cyberoperasjoner fra 2014 til 2015, hvor en av årsakene til nedgangen skyldes at metodene til trusselaktørene har blitt mer sofistikerte og avanserte og dermed vanskeligere å detektere (NSR, 2016:6). Videre understrekes informasjonsgapet mellom trusselaktørene og eventuelle sårbarhetsreduserende tiltak ytterligere ved at den samme undersøkelsen utført av NSR viser til at ved 46% av tilfellene, hvor virksomheter ble utsatt for hendelser, ble hendelsen oppdaget ved en tilfeldighet (NSR, 2016:18). Den dynamiske utviklingen av risikobildet og det noe mer statiske arbeidet relatert til forebyggende sikkerhet, med virksomheters økte fokus på sikringstiltak av verdier og skjermeverdig informasjon resulterer i at trusselaktører tilpasser egne metoder i henhold til andre sårbarheter. Av disse grunner vurderes risikobildet til å forverres, samt forventes det en vedvarende økning av samfunnskonsekvenser som følge av IKT-hendelser (Nasjonal sikkerhetsmyndighet, 2017a:8).

5.1.2 Etablering av bakdører – fremmede staters etterretningsvirksomhet fremlagt av PST, NSM og E-tjenesten

Vedvarende etterretning mot sentrale virksomheter, departement og den øvrige forvaltningen gir trusselaktørene et godt grunnlag for å kartlegge aktuelle etterretningsmåls sårbarheter blant personell og organisering eller i nettverk. Kartleggingen av sårbarheter kan forårsake feil i etterretningsmålenes nettverk, samt kan trusselaktørene utnytte de digitale sårbarhetene som er tilstede. Ved etablering av bakdører sikrer trusselaktørene varig tilgang til aktuelle virksomheters nettverk, samt etableres kontroll over nettverket i tiden før eventuelle større cyberoperasjoner inntreffer. Etableringen av bakdører er et ledd i cyberoperasjoner hvor aktuelle virksomheters nettverk infiltreres med skadevare som gir angriperen uautorisert tilgang til nettverket, samt mulighet til å kontrollere nettverket.

Trusselaktører som gjennomfører cyberoperasjoner basert på vedvarende og målrettede angrep på systemer med formål om å etablere bakdører, plante og spre skadevare for å samle inn kritisk informasjon, har store ressurser tilgjengelige og opererer i et langsiktig tidsperspektiv. PST, NSM og E-tjenesten slår alle fast at cyberoperasjoner som et virkemiddel av fremmede staters etterretningsvirksomhet utgjør den mest alvorlige trusselen mot Norge i det digitale rom. En stadig økende trussel hvor alvorligheten tydelig presiseres i PSTs trusselvurdering for 2018. I trusselvurdering for 2018 tildeles nær halvparten av spalteplassen sikkerhetspolitiske utfordringer og trusler knyttet til fremmede staters etterretningsvirksomhet

mot Norge i det digitale rom. Rekruttering av kilder og agenter danner grunnlag for innside trusselen, dessuten vektlegges kartlegging av kritisk infrastruktur som potensielle hendelser som kan aktualisere en alvorlig IKT-sikkerhetshendelse. Gjennomgående omhandler vurderingene fra PST, NSM og E-tjenesten tre områder av interesse: (i) fremmede staters etterretningsvirksomhet i det digitale rom som en økende trussel mot nasjonale myndigheter og virksomheter, (ii) cyberoperasjoner hvor det etableres bakdører ved de aktuelle etterretningsmålene, (ii) samt at majoriteten av målrettede digitale spionasjeoperasjoner fra fremmede staters etterretningsvirksomhet mot norske mål forekommer gjennom bruken av *spear-phising*. Den stadige økende forekomsten av cyberoperasjoner vikles inn mot norsk industri, tradisjonelle etterretningsmål herunder militære- og politiske mål, og den øvrige befolkningen som en ny trend underlagt den nye trusseldimensjonen.

E-tjenestens vurdering distanserer seg markant fra PST og NSMs vurdering ved at Russland spesifikt nevnes hyppig og kategoriseres som en betydelig sikkerhetspolitisk trussel overfor Norge i det digitale rom. PST og NSM derimot, viser til bånd mellom Russland og trusselaktører. Til tross for at PST i trusselvurdering for 2018 konstaterer at russisk etterretningsvirksomhet vurderes til å ha størst skadepotensial på Norge, er det tydelig at i de årlige trusselvurderingene etter Russlands annektering av Krim så har PST endret toneskiftet vedørende Russland. I trusselvurdering av 2015, året etter Russlands annektering av Krim, ble Russland for første gang nevnt som en stat som bedriver etterretningsarbeid i Norge. E-tjenesten har tradisjonelt gjennom de årlige ugraderte vurderingene viet betydelig plass til å redegjøre for Russlands posisjon og adferd i henhold til norsk sikkerhetspolitikk.

I tiden etter flere sentrale norske institusjoner ble utsatt for omfattende cyberoperasjoner har PST være sparsommelig med informasjon om hvordan sikkerhetstjenesten selv ble utsatt for en cyberoperasjon, dette til tross for at åpenhet er et styrende prinsipp i *Internasjonal cyberstrategi for Norge* (Utenriksdepartementet, 2017:7).[39] Åpenhet danner kunnskap og fremmer samfunnsdebatten om hvorvidt digitale sårbarheter kan utnyttes i andre virksomheter og i individers personlige sfære. For å redusere samfunnets og individets sårbarhet er det prekært at informasjon vedrørende cyberoperasjoner på norske institusjoner fremlegges. Gjennom åpenhet og offentliggjøring av hendelser tilrettelegges det for nasjonal resiliens ved

[39] Se *4.2.4 Cyberoperasjon mot Norge*.

at aksept og forståelse for kompleksiteten og utfordringen rundt den nye trusseldimensjonen, samt vitaliteten av cybersikkerhet i samfunnet.

I likhet med PSTs årlige vurderinger, er ikke NSMs årlige vurderinger, *Risiko* eller *Helthetlig IKT-risikobildet*, like tydelig på å spesifikt nevne Russland eller andre stater som kan fremme en alvorlig IKT-sikkerhetshendelse mot norske myndigheter og virksomheter. I NSMs rapporten *Helhetlig IKT-risikobilde 2017*, eksemplifiseres dette ved at formuleringer som «Målrettede digitale spionoperasjoner fra fremmede stater mot norske virksomheter» (Nasjonal sikkerhetsmyndighet, 2017a:7). NSMs vurderinger derimot benytter et mer teknisk språk og vektlegger etatens posisjon, i likhet med NorCERT, vedrørende det stadig økende informasjonsgapet mellom trusselaktørene og sårbarhetsreduserende tiltak.

PST, NSM og E-tjenesten fremlegger informasjon om trusler mot norske myndigheter, virksomheter og borgere, virkemidler av den nye trusseldimensjonen og aktuelle etterretningsmål. Gjennom årlige utgivelser av *Fokus*, er E-tjenesten den sikkerhetsmyndigheten som utelukkende omtaler Russland i størst grad, og de potensielle utfordringene russiske myndigheter kan påføre norske myndigheter, virksomheter og borgere. Samlet viser sikkerhets- og tilsynsmyndighetene til en endring i Russlands adferdsmønster i de studerte vurderingene, som ved Russlands utvikling av konvensjonelle militære styrker og utviklede militærdoktrine overfor militær kapasitet i det digitale rom. Hvorfor PST, NSM og E-tjenesten varierer i å attribuere Russlands som en relevant rammefaktor ved utformingen av norsk sikkerhets- og forsvarspolitikk ved fokus på hendelser i det digitale rom, kommer ikke tydelig fram i vurderingene. Det kan allikevel tolkes som at PST, NSM og E-tjenesten er alle underlagt departementer og arbeider for norsk sikkerhet og norske interesser. I henhold til det tradisjonelle asymmetriske sikkerhetspolitiske forholdet mellom Norge og Russland som fra norsk side har vært tuftet på avskrekkelse og beroligelse, følger PST, NSM og E-tjenesten denne strategien videre. Ved at PST og NSM ikke kategoriserer Russland på lignende måte slik E-tjenesten har for vane å gjøre, er ikke det totale inntrykket av innholdet i de tre vurderingene like bastant. Dersom det samlede inntrykket av vurderingene i betydelig grad hadde fremmet Russlands som en hovedaktør som forverret Norges sikkerhetstilstand, enn hva som faktisk fremkommer kunne dette svekket Norges sikkerhetspolitiske handlingsrom. Ettersom det å kategorisere en annen stat som en direkte sikkerhetsutfordrer, kan medføre til økt spenning i det sikkerhetspolitiske forholdet mellom to stater (Snyder, 1984:468).

Allikevel kan PST, NSM og E-tjenestens vurderinger tolkes på følgende måte, det er underforstått at fremmede staters etterretningsvirksomhet forekommer i betydelig grad som i all hovedsak omhandler russisk etterretningsvirksomhet. Vurderingene fra PST, NSM og E-tjenesten omhandler tre områder av interesse som legger føringer mot å attribuere Russland som trusselaktør: (i) fremmede staters etterretningsvirksomhet i det digitale rom som en økende trussel mot nasjonale myndigheter og virksomheter, (ii) cyberoperasjoner hvor det etableres bakdører ved de aktuelle etterretningsmålene, (ii) samt at majoriteten av målrettede digitale spionasjeoperasjoner fra fremmede staters etterretningsvirksomhet mot norske mål forekommer gjennom bruken av *spear-phising.*

5.1.3 Første delkonklusjon

På hvilken måte utgjør digitale sårbarheter en sikkerhetsutfordring for totalforsvaret?

Digitale sikkerhetsutfordringer er et resultat av den strukturelle samfunnsmessige sårbarheten. Et stadig økende behov for samhandling mellom tjenester, systemer og infrastrukturer mellom virksomheter tilrettelegger for overførsel og forplanting av feil og skadevare. Betydelig samhandling på følgende måte øker den totale sårbarhetsflaten som trusselaktører vil systematisk utnytte, ved målrettede cyberoperasjoner mot aktuelle virksomhets svakeste ledd. Trusselaktørenes metoder er i stadig endring noe som problematiserer deteksjonsarbeidet og evne til å forebygge hendelser for virksomhetene og nasjonale tilsynsmyndigheter. Ettersom det foreligger et betydelig informasjonsgap mellom trusselaktører, utsatte virksomheter og nasjonale sikkerhetsaktører, da gjennomføringen av sårbarhetsreduserende tiltak ikke forekommer i takt med utviklingen av trusselbildet.

Et nasjonalt behov for styrket resiliens er dermed nødvendig for å redusere den stadig økende sårbarhetsflaten. Cyberoperasjoners natur omfatter stadig endrede strategier for å kunne utnytte det nasjonale sårbarhetspotensielt for et bredt spekter av nasjonale interesser, hvor alvorlige IKT-sikkerhetshendelser vil kunne svekke Norges politiske handlingsrom. Da det er svært tidkrevende å attribuere trusselaktører for omfattende cyberoperasjoner fremkommer en total styrkelse av nasjonal resiliens som et nødvendig mottiltak, ettersom behovet for støtte til håndtering av betydelige IKT-hendelser er mer omfattende enn det behovet NSM og NorCERT skal kunne dekke.

Optimal effekt av sårbarhetsreduserende tiltak som reduserer digitale sikkerhetsutfordringer vil være fraværet av IKT-hendelser som i en lengre tidsperiode undergraver normaltilstanden.[40] Som tidligere diskutert, dersom trusselaktører etablerer bakdører vil dette resultere i sikret tilgang til et ønsket nettverk ved en senere anledning. Dermed vil sårbarhetsreduserende tiltak som resulterer i fraværet av IKT-hendelser som i en lengre tidsperiode undergraver normaltilstanden, ikke gi korrekte indikasjoner da en cyberoperasjon likevel kan være nært forekommende.

Allikevel, viser dagens situasjon til at manglende resiliens er betydelig overfor virksomheter tilknyttet tradisjonelle politiske- og militære mål, øvrige deler av statsforvaltningen, akademia, kraftselskaper, industri og enkeltindivider. Digitale sikkerhetsutfordringer utfordrer totalforsvarets beskyttende rolle overfor det sivile samfunn, dog vil etableringen av enklere og mer sømløs informasjonsflyt mellom virksomheter og relevante myndigheter og/eller organisasjoner redusere nevnte sikkerhetsutfordringer i dagens totalforsvar. Gjennom etableringen av bedret informasjonsflyt kan aktører i det sivile samfunn etablere evnen systemer har til å håndtere mindre hendelser for å sikre systemets pålitelighet, samt evnen systemer har til å gjenopprette normaltilstanden etter større hendelser. Langsiktig, vil dette kunne redusere den stadig økende sårbarhetsflaten gjennom etableringen av sårbarhetsreduserende tiltak som medfører til fravær av IKT-hendelser som kan undergrave normaltilstanden over lengre tid. Fundamental avhengighet av IKT, med påfølgende svak resiliens gjennomgående i styrende systemer, innebærer et mer uoversiktlig og komplekst risikobilde som stadig gir fremmede staters etterretningsvirksomheter nye muligheter overfor kartleggelse av Norges nasjonale interesser. Kritikaliteten av dette understrekes ved at NSM vurderer at risikobildet forverres, i tillegg forventes det at samfunnskonsekvensene av IKT-hendelser vil øke.

[40] Se *3.3.1 Validitet*.

5.2 Etterretningsmål

Forsvarssjef, admiral Haakon Bruun-Hanssen, presiserte i april 2018 viktigheten av operasjoner innen overvåking ved fremleggelsen av *Forsvarets årsrapport 2017*, på følgende måte «Daglige operasjoner innen overvåking, suverenitetshevdelse og myndighetsutøvelse er alltid en prioritet i Forsvaret» (Hanssen, 2018). Etterretningsarbeidet som Forsvarssjefen vektlegger viktigheten av skal understøtte norske myndigheter med informasjon og vurderinger om utenriks-, sikkerhets- og forsvarspolitiske forhold. Etterretningsarbeidet fremskaffer informasjons og varsler om forhold som kan true Norge eller norske interesser, da analyse av ny informasjon raskt kan endre trusselbildet. Forsvaret skal gjennom etterretning og overvåking sikre et nasjonalt beslutningsgrunnlag. I henhold til de sikkerhets- og interessebaserte politiske rammene, og tilstedeværelsen av betydelige russiske strategiske militære styrker i våre nordområder, utgjør dette et betydelig behov for etterretning i nordområdene (Heier & Kjølberg, 2015:125). Etterretningsarbeidet skal danne et tilfredsstillende bilde for norsk evne til suverenitetshevdelse og myndighetsutøvelse som tilrettelegger for et målrettet samfunnssikkerhetsarbeid, ettersom dette arbeidet forutsetter at samfunnet har et klart bilde av hvilke funksjoner, virksomheter og leveranser det er prekært å sikre. Etterretningsarbeidet spiller inn på det sivil-militære samarbeidet innen totalforsvarskonseptet, ettersom samarbeidet omhandler gjensidig støtte mellom Forsvaret og det sivile samfunnet om forebygging, beredskapsforberedelser og operativ håndtering i alvorlige situasjoner. Et velfungerende samspill i det sivil-militære samarbeidet tilrettelegger for et resilient samfunn overfor cyberoperasjoner som kan fremkomme gjennom digitale sabotasje som virkemiddel i et overordnet konsept som ellers omfatter desinformasjon, manipulasjon, aggressiv propaganda og stimulering av sosial uro. Stabilitet i norske områder av sikkerhetspolitisk interesse for Russland, er et resultat av evnen til å minimere usikkerhet gjennom vedvarende og betydelig etterretning i regionen. Tilstedeværelsen av betydelig etterretningsaktivitet fra norske myndigheter er av strategisk betydning og uavhengig av hvor tilspisset den sikkerhetspolitiske situasjonen er på et gitt tidspunkt, noe som Forsvarssjefen, admiral Haakon Bruun-Hanssen, påpekte i 2015 «Intensiverer ikke vi vår overvåking og tilstedeværelse i takt med økningen i aktivitet, vil en senere økning kunne bli tolket som en eskalering i en hendelse/krise» (Hanssen, 2015). Lignende minimering av usikkerhet er dog problematisk vedrørende sikkerhetspolitiske utfordringer relatert til den nye trusseldimensjonen.

Fremmede staters etterretningsvirksomhet har tradisjonelt rettet etterretningsaktivitet med hensikt å fremskaffe innsikt i nasjonale forhandlingsstrategier, sensitive økonomiske og sikkerhetspolitiske spørsmål. Utbredt etterretningsaktivitet hvor etterretningsvirksomheter benyttes som et virkemiddel for å posisjonere statens næringsutvikling og konkurranseevne, er stadig mer tydelig på bakgrunn av de valgte etterretningsmålene (Justis- og beredskapsdepartementet, 2016:92). Innhenting av strategisk viktig informasjon om tradisjonelle politiske- og militære mål er videreutviklet til å rette etterretningsaktivitet mot øvrige deler av statsforvaltningen, akademia, kraftselskaper og industri som på bakgrunn av målvalg og metode kan attribueres til russiske etterretningstjenester. Utviklingen muliggjøres av den stadige økende digitaliseringen som parallelt øker risikoen for at sentrale stats- og samfunnsfunksjoner blir utsatt for sikkerhetstruende virksomhet i form av alvorlige IKT-sikkerhetshendelser. Vedvarende risiko for at trusselaktører tar sikte på å utnytte digitale sårbarheter maksimerer den nasjonale digitale sårbarhetsflaten. Større cyberoperasjon som en rekke sentrale institusjoner ble utsatt for i 2017 grunnet metodevalget, *spear-phising*, indikerte at APT29 systematisk søkte etter å identifisere og utnytte det sikkerhetsmessige svakeste leddet i de aktuelle etterretningsmålene.

Ytterligere problematiseres deteksjonsarbeidet, utbedringen av nasjonal resiliens og etableringen av sårbarhetsreduserende tiltak for å redusere den nasjonale sårbarhetsflaten ved stadig utvikling i metodevalget til trusselaktørene. Empirisk, rettes cyberoperasjoner mot tradisjonelle etterretningsmål, som ved tilfellet da blant annet Forsvaret og UD ble forsøkt infiltrert, samt viser internasjonale trender til målrettede operasjoner mot underleverandører og kontraktører. Mindre virksomheter har generelt svakere sikkerhetsmekanismer som utnyttes av trusselaktører for å få tilgang til hovedmålets nettverk (Nasjonal sikkerhetsmyndighet, 2018:11). Den stadige økende bruken av tredjepartstjenester, tjenesteutsetting eller utkontraktering, medfører til en mer kompleks samarbeidsstruktur, hvor usikkerheten øker i takt med digitale sårbarheter. Konstant påføring av nye enheter, tredjepartstjenester eller en generell økning i organisasjonen, tilknyttet et nettverk resulterer i en stadig mer uoversiktlig digital verdikjede. Den nasjonale sårbarhetsflaten øker ved at digitale sårbarheter, i tråd med feil, forplantes raskt mellom leddene i verdikjedene og digitaliseringen tilrettelegger for strukturell samfunnsmessig sårbarhet som trusselaktører kan utnytte (Nasjonal sikkerhetsmyndighet, 2018:9). Et uromoment ved bruken av tredjepartstjenester er hvorvidt informasjonen som går ut av virksomhetene til tredjepartstjenester går til korrekt mottaker, samt til hvilken grad den aktuelle informasjonen

videre blir beskyttet. Et resultat av utstrakte digitale verdikjeder med flere ledd, resulterer i at virksomheter har redusert oversikt overfor egne sårbarheter (Norges offentlige utredninger, 2015:15).

5.2.1 Metode og målvalg

Den stadige økende forekomsten av cyberoperasjoner retter etterretningsaktivitet mot tradisjonelle politiske og militære mål, som utenrikstjenesten og Forsvaret. Øvrige mål for fremmed etterretningsvirksomhet har vært øvrige deler av statsforvaltningen, akademiske institusjoner, kraftselskap og bedrifter i industrien av interesse for en fremmed stat. Herunder påpekes de omfattende cyberoperasjonene mot sentrale norske institusjoner, hvor målrettede *spear-phising* angrep var rettet mot individer posisjonert i Aps Stortingsgruppe, UD, Forsvaret, PST, NRPA og ved en høyskole. Figur 7.0 viser til taktikk, teknikk og prosedyre samt etterretningsmål som kjennetegner APT29.

	Aliases	**Active since**	**TTPs**	**Targeted sectors**
APT28 (Tsar Team)	Fancy Bear, Sofacy, Pawn Storm	2008	Spear-Phishing, custom malware. Zero-day vulnerabilities, watering holes, credential collection, data theft	Government, defence, media, hospitality, construction, non-profit, technology
APT29	Dukes, Crazy Bear	2008	Spear-Phishing, watering holes, custom malware, zero-day vulnerabilities, high operational security, data theft	Government, think thank/NGOs, hospitality, finance, pharmaceutical, legal

Figur 7.0 viser til utfyllende informasjon om alias, oppstartperiode, taktikk, teknikk og prosedyrer (TTPs) vedrørende cyberangrep og etterretningsmål for APT28 og APT29 (Muller, Gjesvik & Friis, 2018:17).

Informasjonen som fremkommer av figur 7.0 korrelerer sterkt med de omfattende cyberoperasjonene mot norske institusjoner. APT29 angriper konsekvent enheter relatert til utenriks- og sikkerhetspolitikk som tradisjonelle etterretningsmål, noe som understøtter mistanke om at grupperingen har tette bånd til Kreml og russiske myndigheter.[41] Annet enn

[41] Herunder, kan fremgangsmåten ved å benytte APT29 styrke Russlands eskaleringsdominans. Russlands tradisjonelt betydelige styrkemessige overlegenhet gjør seg gjeldende i det digitale rom, hvor det sofistikerte videreutviklede konseptet vil kunne styrke statens handlingsrom om nødvendig.

angrepene rettet mot UD, Forsvaret og PST, var andre etterretningsmål høyt profilerte mål i omfattende angrep, noe som tyder på at APT29 som trusselaktør innehar større mengder ressurser i form av offensive kapabiliteter i det digitale rom. Betydelige mengder maktressurser er nok en indikator på at APT29 utfører etterretningsvirksomhet på vegne av en fremmed stats etterretningsvirksomhet, hvor etterretningsmålene indikerer et tydelig bånd med grupperingen og russiske myndigheter. APT29s betydelige maktressurser gjør at grupperingen kan omstille og innrette metoder etter forbedringer av digital sikring i form av resiliens. APT29s målrettede cyberoperasjoner på profilerte mål, enheter i statsforvaltningen som tradisjonelt omhandler utenriks- og sikkerhetspolitikk, indikerer at grupperingen raskt kan endre metode og videre angripe andre digitale sårbarheter ved ønsket mål. Normaliteten bygger på at små skala angrep er inkludert i normaltilstanden av digitale sikkerhetsutfordringer, men til tross for at trusselaktører innehar tekniske kapabiliteter mangler den finansiell motivasjon til å gjennomføre angrep av stor skala (Kramer *et al*, 2009:205). Denne indikatoren understøttes av PST og E-tjenesten som peker på at cyberoperasjonenes metode og målvalg tyder på at trusselaktøren har russisk tilhørighet eller bånd til russiske myndigheter. Majoriteten av cyberoperasjoner utført av APT29 finner sted mellom 06:00-16:00 UTC+0, noe som korrelerer med arbeidstid mellom 09:00-19:00 UTC+3 som er tidssonen, *Moscow Standard Time*, som dekker betydelige mengder av vest Russland, blant annet Moskva og St. Petersburg (Raiu, Soumenkov, Baumgartner & Kamluk, 2013:17; F-Secure, 2015:26; Fireeye, 2015:5).

5.2.2 Digital sabotasje

Vedvarende russisk etterretningsvirksomhet har empirisk vist at informasjon som etterretningen har som mål å avdekke omhandler gradert og sensitiv informasjon om norsk forsvar, sikkerhet og beredskap. På bakgrunn av de omfattende cyberoperasjonene mot en rekke sentrale norske institusjoner så forblir departementer, offentlige virksomheter, institusjoner og bedrifter som håndterer informasjon om kritisk infrastruktur eller kritiske samfunnsfunksjoner, eller forhold som omhandler politikk, økonomi og militære (Justis- og beredskapsdepartementet, 2016:92) av interesse for russiske myndigheter. I avsnitt *5.1.1 Sikkerhetstilstanden*, *5.1.2 Etablering av bakdører* og *5.2.1 Metoder og målvalg* er det redegjort for etterretningsvirksomheten og de potensielle følger mot sentrale stats- og samfunnsfunksjoner og den øvrige forvaltning. Det er vist til at etterretningen tilrettelegger

for cyberoperasjoner av stor skala ved et senere tidspunkt, gjennom å etablere bakdører og dermed sikret permanent tilgang til ønskelige nettverk av strategisk og operativ interesse.

Russland har videreutviklet konseptet for offensive operasjoner mot infrastrukturer og kritiske system, noe som begrunner frykten for at Russland kan benytte digital sabotasje som et virkemiddel for å svekke norske myndigheters handlingsrom. Vedvarende interesse for industri relatert til petroleum- og energiselskapers styringssystemers indikerer en betydelig russisk ambisjon om å kunne sabotere infrastruktur (Etterretningstjenesten, 2018:30). Digital sabotasje er bare en av tre kategorier for digitale trusler som E-tjenesten viser til, hvor de resterende kategoriene omhandler etterretning og påvirkning. Tilstedeværelsen av Russlands militære evne fortsetter å øke i norske nærområder i tråd med aktivitetsmønsteret i nordområdet (Lunde, 2018). Forholdet mellom Russland og Vesten i dagens sikkerhetspolitiske situasjon er på sitt kaldeste siden den kalde krigen, som spiller utover Norge som NATOs yttergrense mot nettopp Russland. Ettersom det sikkerhetspolitiske forholdet mellom Russland og Norge er indirekte betinget av Norges NATO-medlemskap. Den rådende sikkerhetspolitiske situasjonen er i betydelig grad tuftet på en grunnleggende usikkerhet. I tråd med Russlands videreutvikling av offensive cyberkapabiliteter som et konsept, viser faktiske gjennomførte omfattende cyberoperasjoner mot sentrale norske institusjoner- og myndigheter til at Russland vil påføre sentrale norske institusjoner digitale sikkerhetsutfordringer. Virkemidlene kategorisert som spionasje og sabotasje vil kunne destabilisere kritiske funksjoner og svekke statens funksjonalitet, som kan resultere i en lammet og pasifisert stat. Effekten av kommende og allerede gjennomførte cyberoperasjoner mot norske myndigheter er en utbredt usikkerhet hos beslutningstakerne og den øvrige forvaltningen.

Allikevel, basert på den rådende sikkerhetspolitiske situasjonen utnytter russiske myndigheter muligheten som er tilstede, i tråd med tradisjonelt nullsum-spill, ved gjennomføringen av cyberoperasjoner ved sofistikerte offensive cyberkapabiliteter.[42] I henhold til *cybersikkerhetsdilemmaet* har staten et betydelig insentiv til å benytte de utviklede offensive cyberkapabiliteter preventivt, før det er sikkerhetspolitisk hensiktsmessig. Den grunnleggende sikkerhetsmaksimerende dimensjonen er tuftet på tilstedeværelsen av gjennomgående usikkerhet i det internasjonale system. Empirisk, viser utviklingen av sofistikerte offensive

[42] Se *4.2.4 Cyberoperasjon mot Norge*.

cyberkapabiliteter til at uautorisert innhenting av sensitiv informasjon er en vedvarende digital sikkerhetsutfordring.

Tilstedeværelsen av Russlands anspente forhold til Vesten, Norge og stater som tidligere var underlagt Sovjetunionen har resultert i at et stadig mer uforutsigbart Russland som søker etter å utvide nasjonal innflytelse og posisjon i det internasjonale samfunnet. I henhold til *cybersikkerhetsdilemmaets* første grunnpilar, må stater handle offensivt for at både cyberoperasjoner skal kunne nå maksimal nytteeffekt fra angripende stats side, samt for å øke statens relative maktposisjon. Russiske myndigheters tydelige utenrikspolitiske ambisjon om å gjenopprette Russland som stormakt, baseres på et sikkerhetspolitisk grunnlag om militær troverdighet i henhold til regional og global strategisk avskrekkingsevne gjennom kjernefysiske våpen og betydelig konvensjonell militærmakt (Forsvarsdepartementet, 2016:29). Alvorlige IKT-sikkerhetshendelser rettet mot å svekke en stats funksjonalitet er underlagt russisk militær operativ strategi, da informasjonsinfrastrukturen betraktes som et strategisk mål. Empirisk, har Russland testet europeiske staters cyberkapabiliteter, hvor motivasjonen ligger i at cyberoperasjoner rettet mot sentrale stats- og samfunnsfunksjoner kan gi strategiske fordeler utenfor det digitale rom. De omfattende cyberoperasjonene rette mot blant annet Forsvaret, PST og UD indikerer at Russland kartlegger norske myndigheter i søket etter sårbarheter som kan utnyttes, med mulighet for etablering av bakdører til sentrale nettverk eller tradisjonell etterretning mot forsvars- og beredskapssektorer. Kartleggelsen av blant annet Forsvaret, PST og UD faller inn under tradisjonell kapasitetsbygging hvor de forekommende cyberoperasjonene har fokus på innhenting av sensitiv informasjon om norske myndigheter og sentrale institusjoner. I henhold til *cybersikkerhetsdilemmaet* vil ethvert sikkerhetsmaksimerende tiltak gjennomført av Russland, gå på bekostning av Norges nasjonale sikkerhet.

5.2.3 Kritisk infrastruktur og kritiske samfunnsfunksjoner

Digital sabotasje er kun et av flere virkemidler Russland har videreutviklet som konsept av offensive cyberkapabiliteter, hvor målrettede cyberoperasjoner tar sikte på å innhente sensitiv og skjermingsverdig informasjon. I henhold til tilstedeværelsen av de fire relaterte intensjonene som fremmet inntrengning og informasjonshenting i datanettverk, cyberoperasjoner, preventivt av en konflikt ved økt sikkerhetspolitisk spenning, kan insentivet om den fjerde av de fire relaterte intensjonene, som omhandler at deler av en cyberoperasjon

kan forberedes på forhånd, begrunne vedvarende russisk etterretning mot norske myndigheter og sentrale institusjoner.[43] Det stadige kjøligere forholdet mellom Vesten og Russland understøtter russiske myndigheters insentiv om at det er hensiktsmessig å utvikle offensive kapabiliteter og benytte disse før de er nødvendige i en sikkerhetspolitisk situasjon.

Cyberoperasjonene mot Estland, Ukraina og de omfattende cyberoperasjonene mot en rekke sentrale norske institusjoner er alle attribuerte til russiske myndigheter og trusselaktører med bånd til russiske etterretningsvirksomheter, hvor APT29 sto bak de målrettede angrepene mot norske institusjoner. Felles for målene er at de er av strategisk betydning for den angripende stat, i henhold til statens videre funksjonalitet. Altså, har en terskel av strategisk betydning blitt overskredet i en alvorlig cyberhendelse hvor følgene i Estland og Ukraina kan kategoriseres som alvorlige IKT-sikkerhetshendelser, men cyberoperasjonen mot sentrale institusjoner i Norge har hatt uante konsekvenser, ettersom PST kategoriske ikke opplyser hvor vellykket cyberoperasjonene var. Allikevel, er det berettiget å karakterisere cyberoperasjonen mot Forsvaret, UD, PST, Aps Stortingsgruppe, NRPS og en høyskole som alvorlige IKT-sikkerhetshendelse, ettersom det var reelle uønskede tilsiktede hendelser i det digitale rom rettet mot kritisk infrastruktur og kritiske samfunnsfunksjoner.

Sårbarhetspotensialet ved kritisk infrastruktur og kritiske samfunnsfunksjoner

Vedvarende etterretningsvirksomhet mot norske myndigheter i dagens digitale samfunn problematiserer sårbarhetspotensialet og utvider sårbarhetsflaten på et politisk nivå tilknyttet kritisk infrastruktur og kritiske samfunnsfunksjoner. En kontinuerlig trussel har forplantet seg i det digitale rom overfor norske myndigheter-, borgere- og virksomheter, hvor sabotasje handlinger via det digitale rom innehar evne til å skade, ødelegge, forstyrre eller undertrykke administrasjons- og ledelsessystemer sivilt og militært (Etterretningstjenesten, 2016:82). Hendelsesforløpet av det vedvarende etterretningspresset fremstår som et ledd i en større vurdering av operasjonell kapabilitet for sabotasjeformål rettede aktiviteter. Disse aktivitetene bygger på omfattende informasjonsinnhenting hvor relevante aktører kartlegger kritisk infrastruktur og kritiske samfunnsfunksjoner i fredstid, som kan benyttes som et strategisk fortrinn i en mer tilspisset sikkerhetspolitisk situasjon.

[43] Se *2.4 Cybersikkerhetsdilemma*.

Kritisk infrastruktur og kritiske samfunnsfunksjoner. Utvalget har ikke eksplisitt vurdert de kritiske samfunnsfunksjonene som står i kursiv

Kritisk infrastruktur	Kritiske samfunnsfunksjoner
Elektrisk kraft	Bank og finans
Elektronisk kommunikasjon	Matforsyning
Vann og avløp	Helse-, sosial- og trygdetjenester
Transport	Politi
Olje og gass	Nød- og redningstjeneste
Satellittbasert infrastruktur	Kriseledelse
	Storting og Regjering
	Domstolene
	Forsvar
	Miljøovervåkning
	Renovasjon

Figur 8.0 Kritisk infrastruktur og kritiske samfunnsfunksjoner (*Norges offentlige utredninger*, 2006:16).

Figur 8.0 viset at både kritisk infrastruktur og kritiske samfunnsfunksjoner er bærebjelkene i dagens samfunn og sikrer befolkningen med nødvendige behov i en normaltilstand, dessuten skal behovene også kunne dekkes dersom samfunnet utsettes for påfallende påkjenninger. Kritisk infrastruktur og kritiske samfunnsfunksjoner innehar dermed et betydelig sårbarhetspotensial, og forblir et ønsket etterretningsmål for fremmede staters etterretningsvirksomhet. Samfunnets funksjonsdyktighet er svært avhengig av en rekke fysiske og teknologiske infrastrukturer som muliggjør leveranser av varer og tjenester som befolkningen er avhengig av. Kritisk infrastruktur og kritiske samfunnsfunksjoner understøtter rikets sikkerhet, landets vitale interesser og befolkningens trygghet. Kompleksitet mellom kritisk infrastruktur og kritiske samfunnsfunksjoner er at de er gjensidige avhengige av hverandre. Altså, et betydelig sårbarhetspotensial ved svikt som fremkommer som sektorovergripende.

Russiske virkemidler tilrettelegger for mulige digitale sabotasjehandlinger hvor formålet er å svekke norsk handlingsrom og samtidig styrke eget handlingsrom, som videre kan benyttes som et pressmiddel dersom den sikkerhetspolitiske situasjonen tilspisses. I

cybersikkerhetsdilemmaet defineres to muligheter for å overskride terskelen av strategisk betydning: (i) uautorisert innhenting av informasjon fra et datanettverk, og (ii) angrep med formål om å destruere eller manipulere informasjon fra et datanettverk. Empirisk basert på Russlands militære evne og vilje til å benytte maktressurser for å nå utenrikspolitiske mål, tjener punkt (i) uautorisert innhenting av informasjon fra et datanettverk som et primært grunnlag av *cybersikkerhetsdilemmaets* andre grunnpilar. Defensiv tilnærming representerer *cybersikkerhetsdilemmaets* andre grunnpilar, hvor den uautoriserte inntrengningen via cyberoperasjoner gjennomføres for å innhente strategisk informasjon som skal kunne øke Russlands nasjonale sikkerhet. Da uautorisert innhenting av sensitiv informasjon vedrørende militære og utenrikspolitisk karakter potensielt kan redusere en mulig risiko mot Russland. Herunder understrekes den defensive tilnærmingen ved at cyberoperasjonene var rettet mot blant annet Forsvaret, UD og PST. Tradisjonell etterretningsaktivitet rettet, som tidligere redegjort for, mot forsvars- og beredskapssektoren i henhold til politiske- og militære mål, forekommer på bakgrunn av det stadig kjøligere forholdet mellom Russland og Vesten. Vedvarende russisk etterretningsvirksomhet og gjennomførte cyberoperasjoner baseres på, fra russisk side, at NATO styrker alliansens militære evne ved utviklingen av missilforsvaret, i Russlands interessesfære, som tolkes som en trussel (Etterretningstjenesten, 2018:18). Ettersom Russlands har utviklet sofistikerte cyberkapabiliteter, benyttes disse kapabilitetene til å styrke landets posisjon i det internasjonale samfunnet slik at Vesten må forholde seg til Kreml i spørsmål av sikkerhetspolitisk karakter. Russlands defensive tilnærming overfor cyberkapabiliteten til rådighet og den utstrakte og vedvarende etterretningsvirksomhet, styrker Kremls posisjon til å motarbeide EU-ekspansjon og NATO-utvidelse til russiske nærområder.

Allikevel, tjener argumentet om målrettede cyberoperasjoner mot blant annet Forsvaret, UD og PST for utelukkende defensiv informasjonsinnhenting for å styrke Russlands nasjonale sikkerhet, svært så formålsvennlig dersom argumentet benyttes for å markere usikkerheten dette påfører sikkerhetstilstanden i Norge. De målrettede cyberoperasjonene mot sentrale norske institusjoner indikerer at russiske myndigheter søker etter sårbarheter som kan svekke Norges stats- og samfunnsfunksjonalitet. Den rådende sikkerhetspolitiske situasjonen viser et stadig mer offensiv og opportunistisk Russland i henhold til den utøvde utenrikspolitikken. Grunnet Russlands sterke interesser i nord og overfor sentrale institusjoner som kan svekke den norske stats- og samfunnsfunksjonaliteten, ønsker myndighetene å signalisere, gjennom å vise frem konvensjonelle militære- samt sofistikerte cyberkapabiliteter, misnøye med norsk sikkerhetspolitikk. De tre simulerte angrepene rette mot norske mål som Russland

gjennomførte i underkant av en måned våren 2017 understreker dette.[44] I kjølevannet av de gjennomførte handlingene, gjennom uautorisert inntrengning overfor norske myndigheter eller sentrale institusjoner, eller forsøk på å etablere bakdører og dermed sikret permanent russisk tilstedeværelse i norske strategisk viktige nettverk, kan dermed ikke kategoriseres som en defensiv handling i henhold til *cybersikkerhetsdilemmaet*. Herunder er teoriens kjernepunkt ufravikelig, da etterretningsarbeid som i hovedsak kun skal innhente informasjon som en defensiv tilnærming, kan misforstås og oppfattes som om et angrep er nært forekommende.

Sårbarhetspotensialet som er tilstede ved kritisk infrastruktur og kritiske samfunnsfunksjoner utfordres av russiske myndigheters evne og vilje til å rette vedvarende etterretningsaktivitet mot nettverk av strategisk betydning for Norges stats- og samfunnsfunksjonalitet. I henhold til de to definerte muligheter for å overskride terskelen av strategisk betydning, (i) uautorisert innhenting av informasjon fra et datanettverk, og (ii) angrep med formål om å destruere eller manipulere informasjon fra et datanettverk, vil den primære hendelsen, (i), kunne tilrettelegge for den sekundære hendelsen, (ii), i henhold til et kommende angrep som kan svekke norsk handlingsrom i en eventuell endring i den sikkerhetspolitiske situasjonen. Russiske offensive cyberkapabiliteter innehar evne til å skade, ødelegge eller forstyrre, samt undertrykke administrasjons- og ledelsessystemer sivilt eller militært, noe som aktualiserer behovet for styrket resiliens nasjonalt og i virksomheter tilknyttet forsvars- og beredskapssektoren.

Uavhengig av Russlands intensjon, representerer uautorisert innhenting av sensitiv informasjon og etablering av bakdører i form av cyberoperasjoner russisk tilstedeværelse i nettverk av strategisk betydning for norske myndigheter. Basert på målvalg, metode og Russlands betydelige ønske om at Vesten i større grad må forholde seg til Kreml vedrørende utvikling i det internasjonale system, fremstår Russlands defensive tilnærming om cyberoperasjoner og vedvarende etterretning som hendelser i ledd av å sondere operasjonelle kapabiliteter for sabotasjeformål. Ved å kartlegge kritisk infrastruktur og kritiske samfunnsfunksjoner i fredstid, styrkes Russlands handlingsrom for å utnytte den innhentede informasjonen dersom den sikkerhetspolitiske situasjonen endres. Kritikaliteten av å kunne svekke kartleggelsen som kan fremme sabotasjeformål er dermed betydelig.

[44] Se *4.2.2 Russiske simulerte angrep mot Norge*.

Til tross for vedvarende etterretning mot forsvar og beredskap, politiske beslutningsprosesser og kritisk infrastruktur og kritiske samfunnsfunksjoner, er Forsvarets evne til å håndtere de mest alvorligste sikkerhetspolitiske utfordringene svekket (Forsvaret, 2015:8). Behovet for samordning og koordinering av tiltak som forsvarssektoren utøver i det digitale rom, ble understreket i Forsvarets langtidsplan for 2016 (Forsvarsdepartementet, 2016:36). I det sivile samfunn forekommer ikke gjennomføringen av sårbarhetsreduserende tiltak med utviklingen av trusselbildet. Informasjonsgapet mellom trusselaktørenes kapabiliteter og nødvendigheten av styrket resilines og mottiltak medfører til en stadig økende sårbarhetsflate i det sivile samfunn. Innenfor det militære aspektet av totalforsvaret, vil dagens informasjonsinfrastruktur problematisere E-tjenestens virke og deteksjonsarbeid vedrørende alvorlige trusler mot Norge og norske interesser. Den nye trusseldimensjonen har medført betydelige endringer i trusselbildet. En kraftig eskalering av cybertrusler innenfor det digitale rom, aktualiserer økt omfang av cybersikkerhet grunnet cybertruslers stadige økning i volum og kompleksitet. Den nye trusseldimensjonens skifte fra satellitt-basert koordinering til nettbasert koordinering, resulterer i at E-tjenesten pr. dags dato ikke har tilgang til trusselaktørenes kommunikasjonskanaler og etterretningskapasiteten svekkes betydelig (Lysne II-utvalget, 2016:11). Lysne II-utvalget har slått fast at E-tjenestens evne til levere etterretning om Norge og norske interesser problematiseres av mangelfull aksess til trusselaktørenes kommunikasjonskanaler.[45] Kompleksiteten i de digitale verdikjedene er som kjent av interesse for fremmede staters etterretningstjenester, da sensitiv informasjon kartlegges da dette kan utnyttes ved en senere anledning for å øke nasjonalt handlingsrom.

5.2.4 Andre delkonklusjon

Tyder vedvarende russisk etterretningsvirksomhet og kartlegging av sentrale norske myndigheter og virksomheter på opprustning i det digitale rom?

Russlands velorganiserte og videreutviklede arsenal innenfor offensive cyberkapabiliteter og uforutsigbare utøvelse av maktpolitikk vil resultert i betydelig digitale sikkerhetsutfordringer

[45] Et utvalg ledet av Olav Lysne, med mandat for å utrede sentrale problemstillinger knytte til E-tjenestens aksess til elektronisk informasjon som går inn og ut av Norge gjennom fiberoptiske kabler.

for totalforsvaret, dersom etterretningsvirksomheten tydet på opprustning i det digitale rom. For å etablere styrket resiliens overfor myndigheter, virksomheter og befolkningen på tvers av samfunnet er det nødvendig å forstå hva hver enkelt skal beskytte seg mot, da målet er å styrke beredskap og redusere samfunnets digitale sårbarheter. På bakgrunn av dette vektlegges det hvorvidt vedvarende etterretning og kartlegging av sentrale norske myndigheter og virksomheter tyder på russisk opprustning i det digitale rom. De identifiserte sikkerhetsutfordringene som er etablert grunnet digitale sårbarheter i totalforsvaret, aktualiserer behovet for å styrke samfunnets resiliens som et tiltak innenfor forebyggende sikkerhet. Ettersom sikkerhetstilstanden fastsettes av det aktuelle risikobildet med påfølgende forebyggende sikkerhet vurderes derfor de potensielle følger av russisk etterretning og kartlegging. Herunder vektlegges mulig russisk opprustning overfor sikkerhetstilstanden.

Cyberoperasjoner mot blant annet Forsvaret, UD og PST for utelukkende defensiv informasjonsinnhenting for å styrke russisk nasjonal sikkerhet, påfører usikkerhet overfor den nasjonale sikkerheten i Norge. Den rådende sikkerhetspolitiske situasjonen viser et stadig mer offensiv og opportunistisk Russland. I henhold til *cybersikkerhetsdilemmaets* første og andre grunnpilar, styrker utenrikspolitikken utelukkende de defensive ambisjoner overfor Russlands sikkerhet. Preventivt av en tilspisset sikkerhetspolitisk situasjon, vil det være hensiktsmessig å utvikle samt benytte offensive kapabiliteter, for at den innsamlede informasjonen om Norges funksjonalitet skal kunne gi optimal effekt dersom russiske myndigheter finner det nødvendig. Insentivet om å styrke nasjonal sikkerhet ved å gjennomføre uautorisert inntrengning med formål om å innhente sensitiv informasjon, tjener russiske interesser samtidig som Norges sikkerhet svekkes.

Uavhengig av Russlands intensjon, representerer uautorisert innhenting av sensitiv informasjon og etablering av bakdører russisk tilstedeværelse i nettverk av strategisk betydning for norske myndigheter. Etterretningsvirksomheten og cyberoperasjonene er rettet mot øvrige deler av statsforvaltningen, akademia, kraftselskaper og industri, dette understreker russiske ambisjoner om å svekke den norske stats funksjonalitet dersom myndighetene finner det hensiktsmessig for å etablere et strategisk fortrinn. Herunder kan russisk tilstedeværelse kategorisere som etableringsforsøk for å styrke kontroll og kapabiliteter. De omfattende cyberoperasjonene mot Estland og Ukraina understreker russiske ambisjoner om å kunne gjennomføre større cyberoperasjoner med sabotasjeformål. I den

omfattende cyberoperasjonen mot en rekke sentrale norske institusjoner i 2016 testet Russlands nasjonale offensive cyberkapabiliteter på Norge som NATOs yttergrense.

Til tross, for at Russland ikke utgjør en direkte militær trussel mot Norge i dagens sikkerhetspolitiske klima, understrekes Russlands uforutsigbarhet, militære modernisering og det kjølige forholdet til Vesten som grunnlaget for en ny normaltilstand. Russland vil utvide nasjonens innflytelse overfor verdenssamfunnet. Kremls markeringsbehov vises i norske nærområder konvensjonelt og overfor etterretningsmål med sensitiv informasjon om forsvar og beredskap, politiske beslutningsprosesser og kritisk infrastruktur i det digitale rom. PST, NSM og E-tjenestens vurderinger om at cyberoperasjoner utgjør de mest alvorlige utfordringene tilknyttet fremmede staters etterretningsvirksomhet, med PSTs presisering på at russisk etterretningsvirksomhet vurderes til å ha størst skadepotensial – understreker kritikaliteten en enkelt hendelse kan resultere i overfor den rådende sikkerhetspolitiske situasjonen.

5.3 Realpolitikk i det digitale rom?

Empirisk, har Norges forhold til Russland vært preget av en tydelig dualitet. Bilateralt samarbeid finner sted, til tross for trusselen som Russland poserer som utestående til NATO og et tradisjonelt sikkerhetsfellesskap, tydeliggjør utformingen av norsk sikkerhetspolitikk.[46] Det anstrengte sikkerhetspolitiske forholdet mellom Russland og Vesten skaper et behov for etterretning om det norske forsvarets installasjoner, virksomheter og personell som NATOs yttergrense mot Russland i nord, da det er av strategisk interesse for Russland. Herunder, omfattes militære anlegg og installasjoner tilknyttet NATO- samarbeid, norsk sjømakt, Forsvarets øvingsvirksomhet og norske etterretningsinstallasjoner (Politiets sikkerhetstjeneste, 2018:11). Samtidig, er en betydelig andel av russiske maktressurser konsentrert strategisk nær NATOs yttergrense mot Russland i nord.

Ved besvarelse av oppgavens to første underlagte delspørsmål av problemstillingen, vises det til i første- og andre delkonklusjon om betydelige sårbarhetsflater som fremmede stater kan utnytte dersom den politiske motivasjonen tilser det. Digitale sikkerhetsutfordringer er et resultat av den strukturelle samfunnsmessige sårbarheten, hvor stadig økende samhandling

[46] Bilaterale relasjoner fremmer forutsigbarhet i felles interesseområder, Nordområdene, gjennom etablert kontakt mellom militære styrker og kontroll av fiske i Barentshavet (Heier & Kjølberg,2015:38).

mellom tjenester, systemer og infrastrukturer mellom virksomheter resulterer i overførsel og forplanting av feil. Koordinert handling og nyttiggjørelse mot identifiserte sårbarheter kobles med en politisk ambisjon om å destabilisere et annet land uten at den sikkerhetspolitiske situasjonen eskaleres til en konflikt. Empirisk, viser Russland gjennom sin utenrikspolitiske egenart at staten har blitt mer uforutsigbar og i større grad er villig til å bruke militære maktmidler for å nå politiske mål.[47] Geopolitikk og sikkerhet er fortsatt det dominerende narrativ innenfor russisk utenrikspolitisk tenkning, og realpolitikk er det grunnleggende elementet i politikken (Trenin, 2011:84). Vedvarende russisk etterretningsvirksomhet mot Norge og Vesten, har kommet som en følge av Vestens sanksjoner mot Russland for den folkerettsstridige anneksjonen av Krim halvøya. Alternative metoder innenfor utstrakt etterretning har blitt benyttet av russiske aktører i et forsøk på å tilegne vestlig teknologi (Etterretningstjenesten, 2016:82). Russlands grunnleggende mangel av respekt overfor andre staters suverenitet og territorielle integritet er synlig etter folkerettsbrudd og en revitalisering om statens tilknytningsform til NATO (Kjølberg & Heier, 2015:85). Dette grunnleggende empiriske belegget om at Russland har politisk vilje og militær makt inngår i et betydelig skadepotensial i egne nærområder, sett i sammenheng med en gråsone mellom krig og fred for maktmidler som kan anvendes innenfor det digitale rom, som aktualiserer en overhengende usikkerhet vedrørende Russlands neste militære trekk. Ustabiliteten i den sikkerhetspolitiske situasjonen kombinert med økt etterretningsvirksomhet mot den norske stat i sanntiden, aktualiserer totalforsvarsbegrepet i det digitale rom.

Det russiske etterretningstrykket kategoriseres som konstant og har i nyere tid blitt aktualisert på en bekymringsfull måte grunnet den overhengende ustabiliteten i det internasjonale samfunnet. PST fastslår at Russisk etterretningsvirksomhet vil kunne true Norges territorielle kontroll og sentrale samfunnsinteresser, ettersom det foreligger en kontinuerlig kartlegging av kapasitetene til Forsvars, sikkerhets- og beredskapsmessige forhold i Norge. Det vedvarende og konstante etterretningspresset fra Russland har som formål å tilrettelegge for det russiske militære i en eventuell endret sikkerhetspolitisk situasjon, hvor norske myndigheters politiske handlingsrom svekkes og grunnlaget for et størst mulig russisk handlingsrom legges (Politiets

[47] Russlands annektering av Krim-halvøya og destabiliseringen av Øst-Ukraina har vist at russiske myndigheter har vilje til å bruke militær makt for å nå sine politiske mål, hvor Putins regime demonstrert at internasjonale rettsregler ikke nødvendigvis blir respektert, særlig i de tilfeller nasjonal interesse ikke er forenlig med prinsippene om nasjoners territorielle ukrenkelighet, slik de er nedfelt i folkeretten.

sikkerhetstjeneste, 2017:7-9). Risikobildet forverres og samfunnskonsekvensene av IKT-hendelser vil øke da alvorlig trusler kommer innenfra egne systemer, iverksatt av en trusselaktør med betydelige maktressurser. APT29s omfattende cyberoperasjoner mot flere sentrale norske institusjoner var rettet mot profilerte mål, til tross for at konsekvensene av de gjennomførte handlingene ikke hat blitt fremlagt i offentligheten, er det berettiget å vise til cyberoperasjonenes formål om å hemme Norges funksjonalitet grunnet ATP29s målvalg. Avsnitt *5.2 Etterretningsmål* redegjorde for bakgrunnen av målvalg og metode, dermed fremstår ikke vedvarende russisk etterretningsvirksomhet som en handling med utelukkende etterretningsinnhentingsformål, men i kombinasjon med å teste sårbarheter i sentrale norske systemer. Dette utfordrer deteksjonsmekanismene i det sivile samfunn og dermed Forsvaret, ettersom det ikke er de angrepene vi kjenner som utgjør det største samfunnsrelaterte problemet, det er de angrepene vi ikke kjenner.

5.3.1 Kanarifugl i kullgruve

Russland viser økt evne og vilje til å bruke et bredt spekter av virkemidler for å nå sine politiske mål. Til tross for innenrikspolitiske tilstramninger og svak økonomisk vekst innad, fremstår russisk utenrikspolitikk som mer offensiv overfor landene i Russlands interessesfære. De siste årene har et stadig mer selvsikkert Russland vist seg villig til å ta i bruk konvensjonelle- og ukonvensjonelle tvangsmidler. Det sofistikerte angrepet NotPetya viser kompleksiteten ved deteksjonsarbeid og resiliente-systemer overfor lignende operasjoner som kan attribueres til aktører tilknyttet russiske myndigheter. Et i øyenfallende løsepengevirus-angrep var i realiteten en dataorm som infiltrerte sentrale virksomheters kontrollenheter og slettet data fra harddiskene til de infiltrerte datamaskinene. Strukturelle samfunnsmessige sårbarheter ble utnyttet, på bakgrunn av samhandling mellom tjenester, systemer og infrastrukturer mellom virksomheter. Dette resulterte i rask og effektiv spredning av ormen til sentrale ukrainske virksomheter og andre relevante offentlige etater. Det anstrengte forholdet mellom Vesten og Russland understøtter et nytt fokus på avskrekking i Norge og NATO, allikevel har ikke Russlands stadig mer sofistikerte og forstyrrende cyberoperasjoner blitt avverget uten at sensitiv informasjon delvis har blitt innhentet gjennom russisk etterretning.

Spionasje i det digitale rom er blitt en integrert del av fremmede sikkerhets- og etterretningstjenesters arbeid og utføres i stort omfang mot Norge og norske interesser. Spionasje i det digitale rom har et høyt etterretningsutbytte tilknyttet cyberspionasje, samt

innenfor cybersabotasje kan cyberoperasjoner kompromittere og skade vitale nasjonale interesser, ved virksomheter med mangelfull sikkerhetskultur og kompetanse som bidrar til at sårbarheten er vedvarende. Gjennom cyberoperasjoner kan fremmede staters etterretningstjenester uten forvarsel dermed ramme kritisk infrastruktur eller kritiske samfunnsfunksjoner, med et betydelig skadepotensial for samfunnet og staten. Den betydelige sårbarhetsflaten gjennom kritisk infrastruktur og kritiske samfunnsfunksjoner som er etterretningsmål for russisk etterretningsvirksomhet i Norge, fremkommer som en alvorlig trussel mot Norges indre anliggende og befolkningens trygghet. Trusler kan realiseres som et virkemiddel i form av skadeverk og kriminalitet i det digitale rom og er en betydelig utfordring for samfunnet, ettersom økonomiske- eller politiske motiverte aktører benytter en kombinasjon av sosial manipulering i forbindelse med inntrengning i informasjonssystemer. Sårbarheten økes gjennom dynamiske- og grenseløse trusler, da det stadig etableres et større informasjons gap mellom trusler og nødvendige mottiltak. Den teknologiske utviklingen gjør samfunnet stadig mer sårbart for fremmede staters etterretning.

Totalforsvarskonseptet har som grunnleggende ansvar å bidra til ivaretagelse av samfunnssikkerheten, og dermed beskytte det sivile samfunnet i hele krisespekteret. Digitaliseringen av samfunnet har resultert i betydelige endringer i samfunnets strukturer hvor trusselbildet omhandler stadige økende tematisering av sivile utfordringer, fremfor militære utfordringer. Det teknologiske paradigme skifte innen sikkerhets- og forsvarspolitikk har simplifisert fremmede staters etterretningsvirksomhet i det digitale rom. Den digitale sårbarheten er betydelig overfor enkeltindivider grunnet økende interesse for personopplysninger. Tilgangen på personopplysninger, passbilder og biometrisk data simplifiserer fremmede staters genuine mulighet til å tilpasse etterretningsoperasjoner mot enkeltindivider, som et ledd i omfattende cyberoperasjoner for å svekke statens funksjonalitet. Sofistikerte cyberoperasjoner hvor troverdige e-poster som innehar skadevare blir sendt til utvalgte individer kan sikre trusselaktører tilgang til etterretningsmålets nettverk hvor det kan etableres bakdører og dermed varig tilgang til nettverket. Totalforsvarets rolle i det digitale samfunnet er prekært for å bedre samlet resiliens på tvers av samfunnssektorene, da det påbegynte og meget omfattende etterretningsarbeidet av russisk karakter kan fremstå som en kanarifugl i en kullgruve – i det øyeblikket betydelige cyberoperasjoner mot norsk kritisk infrastruktur og kritiske samfunnsfunksjoner finner sted, vil eventuelle mottiltak av norske

defensive cyberkapabiliteter være nytteløse.[48] Over lengre tid har russiske myndigheter vist betydelig interesse for energiselskaper og industrielle styringssystemer. Omfattende kompromittering med mål om å tilegne seg erfaringer og kunnskap om sabotasjeoperasjoner i tråd med interessen for energiselskaper og industrielle styringssystemer, indikerer tydelige ambisjoner om å kunne sabotere kraftinfrastruktur for å styrke russisk handlingsrom som igjen kan utnyttes dersom den politiske motivasjonen er tilstede. Langsiktig vil erfaringer fra hendelsene i Estland, Ukraina og annekteringen av Krimhalvøya, NotPetya angrepet og de omfattende cyberoperasjonene mot en rekke norske institusjoner, gjøre Russland i stand til å gjennomføre omfattende cyberoperasjoner. Digitale sabotasjehandlinger kan rettes mot kritisk infrastruktur eller kritiske samfunnsfunksjoner som strømforsyninger og transport, samt forstyrre militære styrker i en mulig militær konflikt (Etterretningstjenesten, 2018:31).

Sikkerhetstruende etterretningsvirksomhet er tydelig i både den offentlige- og private sektor hvor virksomheter og enkeltindivider kan være mål for fremmede staters etterretningsvirksomheter. Skadepotensialet er av betydelig størrelse dersom sårbarhetsflaten er tydelig, hvor forekommende etterretningsaktiviteter i enkelte tilfeller og gjennom en samlet effekt vil kunne påføre det norske stat og norske interesser betydelig skade. Fremmede staters etterretningstjenesters rekruttering av kilder og agenter, cyberoperasjoner, kartlegging av norsk infrastruktur og tiltak for å påvirke norske beslutningsprosesser, vil være en vedvarende utfordring for den norske stat. Herunder informasjonsinnhenting som kan utnyttes for å svekke norsk forsvars- og beredskapsevne i en eventuell fremtidig krisesituasjon, spesielt utsatt er statsforvaltningen og forsvars- og beredskapssektoren. Hvorvidt den vedvarende russiske etterretningsvirksomheten og de forekommende cyberoperasjonene mot en rekke sentrale norske institusjoner skal tolkes i en militær kontekst, legger føringer for oppgavens videre diskusjon.

5.3.2 Sårbarhetsreduserende tiltak

Avsnitt *5.1 Ny normaltilstand, 5.2 Etterretningsmål* og *5.3 Realpolitikk i det digitale rom?* med tilhørende underavsnitt, understreker kritikaliteten av en tydelig situasjonsforståelse overfor den rådende sikkerhetspolitiske situasjonen. Behovet for styrket resiliens

[48] Ordtrykk som omhandler en indikasjon om at noe er på ferde. Gruvearbeidere som arbeidet i kullgruver hadde med kanarifugler ned i gruvene for å få en indikasjon om når avgassene var på et farlig høyt nivå. Dersom kanarifuglene døde underveis var dette en indikasjon på at avgassene var på et helseskadelig nivå.

gjennomgående i samfunnet og i samfunnets informasjonsinfrastrukturer er betydelig, da økningen av digitale sikkerhetsutfordringer og digitale sårbarheter stiger i takt med digitaliseringen og avhengigheten av det digitale rom. Nevnte behov anerkjennes av *Internasjonal cyberstrategi for Norge* av 2017 og *Nasjonal strategi for informasjonssikkerhet* av 2012 hvor det vises til, henholdsvis robusthet (Utenriksdepartementet, 2017:6) samt deteksjonsmekanismer for å oppdage, varsle og håndtere uønskede IKT-hendelser (Departementene, 2012:21). Situasjonsforståelse og sikringstiltak vil i henhold til den asymmetriske utviklingen av cyberoperasjoner inneha redusert effekt, i forhold til den potensielle effekten av cyberoperasjoner uavhengig av offensiv eller defensiv tilnærmelse. Frafallet av geopolitikkens betydning for gjennomførelse av cyberoperasjoner i det digitale rom gir trusselaktørene betydelige fordeler da de står fritt til å bevege seg og utføre handlinger innenfor nettverk av strategisk betydning ved stater av interesse. Oppbyggingen av det digitale rom tilrettelegger for inntrengning av nettverk og gjennomførsel av cyberoperasjoner. Trusselaktører sikrer tilgang til nettverk gjennom målrettede cyberoperasjoner eller gjennom utnyttelse av digitale sårbarheter, gjennom (i) nulldagssårbarheter, eller (ii) kjente sårbarheter som ikke er utbedret (Buchana, 2016:106-107). Det strategisk utbytte gir en bedre effekt dersom den anvendes offensivt fremfor defensivt (Buchanan, 2016:85). Gjennomførelsen av cyberoperasjoner på et gitt tidspunkt, kan på bakgrunn av den innsamlede strategisk viktige informasjonen, påvirke hvordan potensielt fremtidige konflikter vil utartes.

5.3.3 En mulig trussel

Lærdommen av Stuxnet ormen er at inntrengning i nettverk av strategisk betydning kan tilrettelegge for omfattende cyberoperasjoner med siktemål om å svekke staters strategiske datasystem, som igjen svekker en stats handlingsrom samtidig som handlingsrommet til staten som gjennomfører cyberoperasjoner styrkes. For å kunne danne resiliente-systemer og styrke den nasjonale sikkerhetskulturen må de ytre rammene for hva som påvirker trusselbildet etableres. Avsnitt *5.2 Etterretningsmål* med påfølgende underavsnitt attribuerer de omfattende cyberoperasjonene mot sentrale norske institusjoner til APT29 og russiske myndigheter. I henhold til tolkningsdilemmaet, *cybersikkerhetsdilemmaets* tredje grunnpilar, dersom det detekteres pågående og omfattende etterretningsarbeid i form av cyberoperasjoner mot Norges nasjonale interesser eller rettet mot nettverk av strategisk betydning for statens funksjonalitet, vil hendelsene tolkes som offensive cyberoperasjoner med formål om å styrke russisk politisk handlingsrom samt svekke Norges politiske handlingsrom, som kan utnyttes

dersom den sikkerhetspolitiske situasjonen tilspisses. Det problematiserende aspektet, omhandler usikkerheten om hvorvidt russiske cyberoperasjoner har utelukkende etterretningsinnhentingsformål eller om formålet er å teste sårbarheter i strategisk viktige nettverk. Dersom det hersker tvil om hvorvidt etterretningsarbeidet var av potensielt betydelig skadelig karakter eller som en etterretningsoperasjon av defensiv tilnærming, vil fremdeles *cybersikkerhetsdilemmaets* grunnlinje være avgjørende, derav det sikkerhetsmaksimerende aspektet preget i en ustabil sikkerhetspolitisk situasjon. Den rådende sikkerhetspolitiske situasjonen er i stor grad preget av usikkerhet grunnet den iboende uforutsigbarhet som er tilstede i russisk politikk og samfunnsliv (Heier & Kjølberg, 2015:13). Retorikken og russisk politisk motivasjon motarbeider en potensiell defensiv tilnærming og begrunnelse av russisk cyberoperasjoner mot Norge, og aktualiserer teoriens kjernekonsept om at frykt og usikkerhet resulterer i en betydelig eskalering av den sikkerhetspolitiske situasjon.

Norges kapasiteter i form av avskrekkelse og resiliens har åpenbare begrensninger. Dersom avskrekkelsesstrategi anvendes i etterkant av en trusselaktørs inntrengning i et nettverk av strategiske betydning, fremfor benyttelse av offensive kapabiliteter i form av angrep, kan behovet for en troverdig respons fremme eskalering (Buchana, 2016:97-98).[49] En troverdig respons rettet mot Russland i dagens sikkerhetspolitiske situasjon preget av vesentlig usikkerhet basert på det kjølige forholdet mellom Vesten og Russland, kan resultere i at enkeltepisoder får mer alvorlige konsekvenser enn hva de aktuelle partene er tjent med.

Allikevel, *cybersikkerhetsdilemmaets* grunnlinje om sikkerhetsmaksimering samt det problematiserende forholdet hvor en nasjon styrker nasjonal sikkerhet svekker andre staters sikkerhet grunnet usikkerhet, plasserer innsatsen i form av statens sikkerhet på et betydelig nivå. Eskaleringen er berettiget i et anarkisk system dersom statens sikkerhet er truet, noe som begrunner *cybersikkerhetsdilemmaets* alvorlighet (Buchanan, 2016:99). Utviklingen av NATOs missilforsvar i russiske nærområder betraktes som en hovedtrussel for Russland. Kremls hovedmål om å motarbeide EU og NATO-utvidelse, medfører til at russiske myndigheter arbeider for å styrke posisjonen utenfor landets nærområder, hvor anvendelse av militærmakt aktivt signaliserer politiske standpunkter. Russlands strategiske fordel av videreutviklede og sofistikerte offensive cyberkapabiliteter, underbygges av at det er mindre

[49] Warszawa 2016, på et NATO toppmøte ble det vedtatt at det digitale rom skulle etableres som et operasjonelt domene. I henhold til alliansens kjerneartikkel, Art. 5, skal handlinger i det digitale rom oppfattes på lik linje som handlinger i de andre operasjonelle domenene (North Atlantic Treaty Organization, 2018).

krevende å angripe en stat enn å forsvare en stat i det digitale rom. Målrettede cyberoperasjoner rettet mot profilerte mål for å teste offensive kapabiliteter for sabotasjeformål i det digitale rom, samtidig som sensitiv informasjon blir innhentet, styrker russiske myndigheters handlingsrom (Buchanan, 2016:103). Uavhengig av videreutviklet samarbeid mellom Russland og Norge på enkelte områder, forblir geopolitikk og sikkerhet dominerende narrativ innenfor russisk utenrikspolitisk tenkning, med realpolitikk som grunnleggende elementet i politikken. Derav, blir utspill fra norske myndigheter ofte tolket i en realpolitisk og sikkerhetspolitisk kontekst fra russiske myndigheter, noe som problematiserer diplomatisk tilnærming vedrørende spørsmål relatert til cybersikkerhet (Heier & Kjølberg, 2015:19).

5.3.4 En potensiell sikkerhetspolitisk krise?

Innen internasjonal cyberpolitikk arbeider norske myndigheter for å sikre handlefrihet og redusere samfunnets og individets sårbarhet gjennom åpenhet, sikkerhet, robusthet og frihet (Utenriksdepartementet, 2017:6). Gjennom samarbeidsfora fremmer norske myndigheter internasjonalt samarbeid om cybersikkerhet, enighet om statlig oppførsel i det digitale rom samt samarbeid om å styrke evne til å forebygge, oppdage, varsle og håndtere alvorlige cyberhendelser, på viktige arenaer i regi av FN eller NATO, samt Europeiske Union (EU) eller Organisasjonen for sikkerhet og samarbeid i Europa (OSSE) (Utenriksdepartementet, 2017:7).[50] Herunder forankres norsk cybersikkerhet ytterligere i Vesten, basert på den drivende utviklingen av en rettsbasert verdensorden.

På andre siden, handlefriheten norske myndigheter arbeider for, utfordres av Russland som utfører uforutsigbar og folkerettsstridig maktpolitikk utenfor eget territorium. Russlands politiske motivasjon ses i sammenheng med at geopolitiske maktforstyrrelser setter institusjonelle rammeverk under press. Kompleksiteten vedrørende den nye trusseldimensjonen, forsterker gråsonen og svekker dermed skillet mellom krig og fred ytterligere. Russiske myndigheter utnytter den relative fordelen av å være en autoritær stat (Matlary & Heier, 2016:279). Noe som er tydelig i russiske myndigheters operasjonelle konsept i det digitale rom, herunder handlinger i det digitale rom siktet på å undergrave det politiske, økonomiske og sosiale system ved en annen regjering, samt psykologiske

[50] Forkortelsene til FN og NATO er redegjort for under *2.1 Sikkerhets- og forsvarspolitiske mål*.

kampanjer rettet mot den øvrige befolkningen av staten for å destabiliseres samfunnet, samt siktemål om å overta kontroll over andre nasjoners informasjon ressurser.[51] En videreutvikling av subversjonskampanjer, *aktive tiltak*, i det digitale rom med utnyttelse av digitale sårbarheter medfører til at risikoen for å bli rammet av uønskede hendelser øker.

I henhold til *sikkerhetsdilemmaet* påvirkes utfallet av variabelen om hvorvidt våpen og politikk beskytter staten, men tilfører også offensive kapabiliteter for et eventuelt angrep (Jervis, 1978:199). Dette er direkte overførbart til det digitale rom, *cybersikkerhetsdilemma*, i henhold til teoriens tredje hovedpilar om tolkningsdilemma. Ettersom *sikkerhetsdilemmaet* og *cybersikkerhetsdilemmaet* beskriver hendelser i forkant av en konflikt, kan norske myndigheters utbedring av digitale sårbarheter tilspisse den sikkerhetspolitiske situasjonen mellom Norge og Russland, (Buchanan, 2016:130). Norske myndigheter arbeider for å redusere sårbarhetspotensialet i samfunnet ved å danne resiliente samfunnsstrukturer, hvor arbeidet videre fremmes i det internasjonale system. *Cybersikkerhetsdilemmaets* grunnlinje, hvor stater opptrer som sikkerhetssøkende aktører i det internasjonale system, baseres på teoriens kjernekonsept om at frykt og usikkerhet resulterer i en betydelig eskalering av statens sikkerhetspolitiske situasjon. I henhold til Kremls hovedmål om å motarbeide EU og NATO, samt å styrke egen posisjon i det internasjonale system, motstrides vestlige tiltak for å utbedre cybersikkerheten. Ettersom tilstedeværelsene av digitale sårbarheter i strategisk viktige nettverk styrker russiske myndigheters spillerom ved utnyttelse, definerer dette innenfor tradisjonelt nullsum-spill et område som kan styrke egen stats sikkerhet og svekke en annen stats sikkerhet. Eskaleringspotensialet i den rådende sikkerhetspolitiske situasjonen preges ikke av et politisk vakuum, dog er det etablert tydelige interessemotsetninger. Herunder kan en sikkerhetspolitisk krise oppstå dersom et initiativ eller en enkeltstående hendelse utfordrer nasjonale interesser (Heier & Kjølberg, 2013:24). Altså, er det et betydelig eskaleringspotensial tilstede i det norsk-russiske forholdet, som kan trigges av at Norge gjennom NATO-samarbeid utfordrer russiske nasjonale interesser ytterligere.

5.3.5 Sivilt- militært samarbeid

Utbedringen av resiliens, fraværet av IKT-hendelser som i en lengre tidsperiode undergraver normaltilstanden, vil i en sikkerhetspolitisk kontekst øke nasjonal sikkerhet i Norge. Effekten

[51] Se *4.2.2 Russland*.

av å styrke defensive kapabiliteter reduserer muligheten for trusselaktører å fremme en trussel, som på sikt reduserer antall trusselaktører og problematikken vedrørende å attribuere, som igjen svekker kompleksiteten av områder for beslutningstakere (Buchanan, 2016:162). De omfattende russiske cyberoperasjonene rettet mot sentrale institusjoner i Norge rammet Norges grunnleggende nasjonale interesser, herunder forsvars-, sikkerhets- og beredskapsmessige forhold; de øverste statsorganenes virksomhet, sikkerhet eller handlefrihet; forhold til andre stater; samt samfunnets infrastrukturer, så som mat-, vann- og energiforsyninger, samferdsel og telekommunikasjon, helseberedskap eller bank- og pengevesen (Straffeloven, 2005, §121). [52]

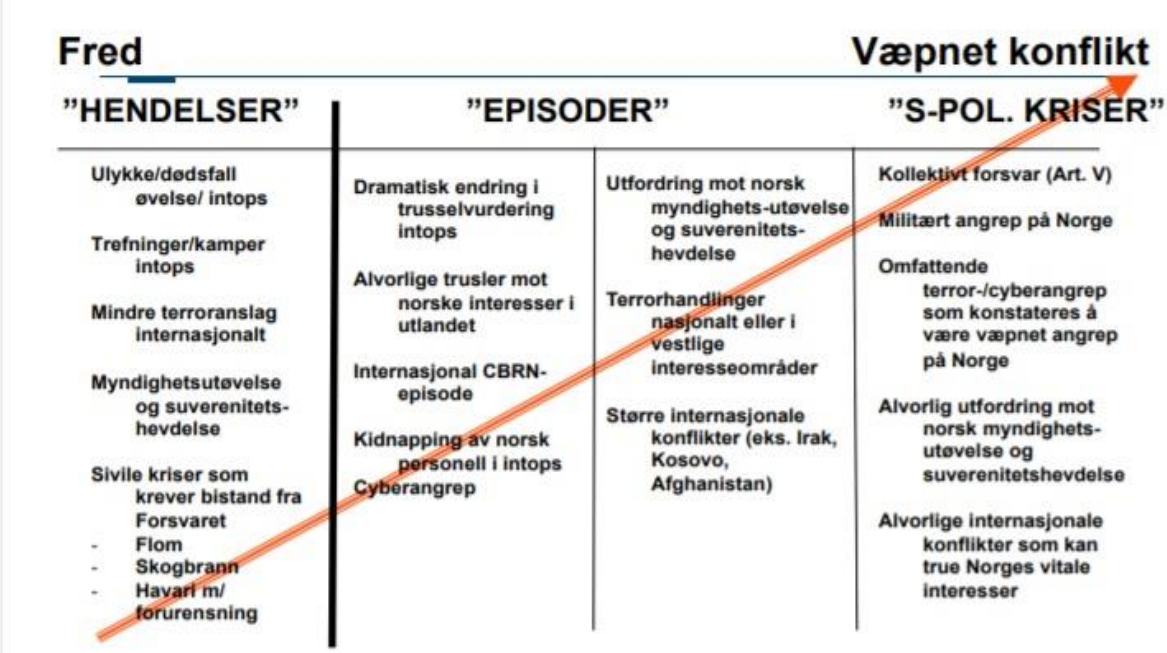
Figur 9.0 Befolkningens sikkerhet basert på samfunnsfunksjonen IKT-sikkerhet med kapabiliteter (Direktoratet for samfunnssikkerhet og beredskap, 2016:63).[53]

Figur 9.0 viser ulike områder av befolkningens sikkerhet og samfunnsfunksjonen *IKT-sikkerhet*, som i sivil sektor involverer samfunnskritisk informasjon lagret i sivile databaser, samt systemer, funksjoner og tjenester relatert til oppdatering og/eller tilgjengeliggjøring av informasjon til aktuelle registre eller og databaser (Direktoratet for samfunnssikkerhet og beredskap, 2016:63). Sterk konsentrasjon av kritisk informasjon om statens funksjonalitet eller sensitive personopplysninger kan utnyttes, ved kartlegging av nøkkelpersoner som gjennom *spear-phising* angrep kan etablere trusselaktørers tilgang til ønsket nettverk.

[52] Norges grunnleggende nasjonale interesser er omtalt i Straffeloven kapittel 17 §121, se vedlegg. Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) tolker de grunnleggende nasjonale interessene er underlagt nasjonens sikkerhet, se vedlegg.

[53]DSB benytter begrepet *IKT-sikkerhet* gjennomgående i vurderingen *Samfunnets kritiske funksjoner – hvilken funksjonsevne må samfunnet opprettholde til enhver tid* hvor denne figuren er hentet fra, i den videre teksten vil *cybersikkerhet* benyttes som begrep, se *1.4.1 Cybersikkerhet*.

Cyberoperasjonen rettet mot Helse Sør-øst har målrettet bedrevet informasjonsinnhenting med utgangspunkt i å skade grunnleggende nasjonale interesser, herunder samfunnets infrastruktur i henhold til opplysninger om helseberedskap. Norske myndigheter arbeider for internasjonal cyberpolitikk for å fremme nasjonal handlefrihet, allikevel forblir samfunnets- og individet sikkerhet i det digitale rom sårbar og eksponert.



Figur 10.0 Forsvarets nasjonale operasjoner i henhold til de kategoriserte konfliktnivå (Forsvaret, 2014;66).

Figur 10 viser ulike operasjoner Forsvaret må gjennomføre i henhold til det aktuelle stadiet av krisespekteret. *Cyberangrep* er plassert mellom fred og væpnet konflikt, som kan eskaleres til en sikkerhetspolitisk krise. Krisehåndtering omhandler balansen i et dikotomisert forhold mellom to henholdsvis motstridende objekter; herunder (i) å ivareta eller beskytte interessen eller verdien som oppfattes truet, og (ii) å hindre at forholdet til den aktuelle motparten forverres og krisen eskaleres (Heier & Kjølberg, 2013:166). Vedvarende russisk etterretningsvirksomhet, grunnet spesifikke og profilerte målvalg, indikerer at russiske myndigheter søker å innhente kritisk informasjon som kan utnyttes, dersom den sikkerhetspolitiske situasjonen tilspisses. Russiske myndigheters politiske motivasjon til rette strategiske cyberoperasjoner mot sentrale norske institusjoner utfordrer Norges sikkerhets- og forsvarspolitiske mål, ved at samfunnssikkerheten reduseres og vanskeliggjør Forsvarets mål om å sikre samfunnet mot anslag fra statlige og ikke-statlige aktører.[54] Samt, utfordres

[54] Se *2.1 Sikkerhets- og forsvarspolitiske mål.*

Forsvarets oppgave om å bidra til ivaretagelse av samfunnssikkerhet og andre sentrale samfunnsoppgaver, av russiske offensive cyberkapabiliteter gjennom etablering av bakdører i aktuelle mål tilknyttet tradisjonelle politiske- og militære mål, øvrige deler av statsforvaltningen, akademia eller deler av kritisk infrastruktur og kritiske samfunnsfunksjoner.[55] Styrket resiliens vil kunne danne en sterkere digital grunnberedskap, hvor håndteringsevnen ville redusert muligheten til fravær av normaltilstand blant virksomheter. Styrket resiliens vil fremme beskyttelsen av interesser samt verne nasjonale verdier, som på sikt vil forhindre at en mulig trussel medfører til en eskalering i den sikkerhetspolitiske situasjonen (Heier & Kjølberg, 2013:164).

Til tross for at totalforsvarskonseptet er tydelig, forekommer håndteringen av IKT-hendelser mot det sivile samfunn i fredstid på et ikke tilfredsstillende nivå. I avsnittene *5.1.1 Sikkerhetstilstanden* og *5.1.2 Etablering av bakdører* ble det redegjort for at mangelen på nødvendig kompetanse over tid har medført til at gjennomføringen av sårbarhetsreduserende tiltak ikke forekommer i takt med utviklingen av trusselbildet, og det etableres et betydelig informasjonsgap mellom trusselaktørenes kapabiliteter og nødvendige mottiltak. Samfunnet blir stadig mer sårbart, ettersom den totale nasjonale sårbarhetsflaten øker. Digitale sårbarheter og feil forplantes mellom leddene i verdikjedene og digitaliseringen tilrettelegger for strukturell samfunnsmessig sårbarhet som trusselaktører kan utnytte, altså betydelig risiko overfor dagens IKT-systemer at trusselaktører får innsyn i sensitiv informasjon, som har økt i takt med digitaliseringen (Norges offentlige utredninger, 2015:31). Herunder digitale sårbarheter i grenseflatene mellom digital informasjonsbehandling, digital kommunikasjon og digital styring. Ettersom sårbarhetene er skjulte og akkumulert i komplekse verdikjeder tilknyttet sektorprinsippet, er det utfordrende å kartlegge de reelle digitale sårbarhetene i sentrale funksjoner. Faren med en eksponert og kjent sårbarhetsflate, er at trusselaktørenes metoder er i stadig endring noe som problematiserer deteksjonsarbeidet og evne til å forebygge hendelser for virksomhetene og nasjonale tilsynsmyndigheter. I henhold til den rådende sikkerhetspolitiske situasjonen, har det blitt presisert fra norske myndigheter at de samlede ressurser innenfor sivil beredskap, politi og Forsvaret skal sikre at samfunnet er rustet til å møte moderne utfordringer, samt at gråsoner defineres ved akutte situasjoner (Forsvarskomiteen & Justiskomiteen, 2003:40). Det moderniserte totalforsvarskonseptet vektlegger i større grad enn tidligere Forsvarets støtte til det sivile samfunn. Det militære skal

[55] Se *2.1.1 Forsvarets oppgaver*.

yte bistand til den sivile befolkningen og bidra til samfunnssikkerhet, samt i et digitalisert samfunn hvor enkeltindivider er av betydelig interesse for fremmed staters kontinuerlige etterretningsvirksomhet. Totalforsvaret står overfor et samlet trussel- og risikobilde hvor behovet for støtte til håndtering av digitale hendelser er mer omfattende enn det behovet NSM og NorCERT skal kunne håndtere. I en sikkerhets- og forsvarspolitisk kontekst fremstår det som svært urovekkende at fremmede stater retter cyberoperasjoner mot virksomheter og systemer som ikke forvalter skjermingsverdig informasjon, og som tidligere har vært mindre aktuelle etterretningsmål. Det tradisjonelle skillet mellom stats- og samfunnssikkerhet viskes ut ved bruken av virkemidler underlagt den nye trusseldimensjonen, noe som aktualiserer sivilt-militært samarbeid i det digitale rom for å redusere eskaleringspotensialet som kan tilspisse den sikkerhetspolitiske situasjonen.

5.3.6 Tredje delkonklusjon

Kan styrket resiliens tilspisse den sikkerhetspolitiske situasjonen mellom Norge og Russland?

Digitale sårbarheter i grenseflaten mellom digital informasjonsbehandling, digital kommunikasjon og digital styring, utsettes for koordinerte handlinger og nyttiggjørelsen kobles til en russisk politisk ambisjon om å destabilisere Norge uten at den sikkerhetspolitiske situasjonen eskaleres til en konflikt, på nåværende tidspunkt. Konvensjonelle- og cybertrusler kan undergrave demokratiet og sette vitale samfunnsfunksjoner ut av drift. Den rådende sikkerhetspolitiske situasjonen baseres på et stadig kjøligere forhold mellom Vesten og Russland, hvor enkeltepisoder kan få mer alvorlige konsekvenser enn hva de aktuelle partene er tjent med. Herunder kan en sikkerhetspolitisk krise oppstå dersom et initiativ eller en enkeltstående hendelse utfordrer nasjonale interesser. Resultatet vil da være ytterligere digitale sikkerhetsutfordringer, overfor totalforsvaret, dersom styrket resiliens tilspisser den sikkerhetspolitiske situasjonen. PST, NSM og E-tjenesten påpeker at fremmede staters cyberoperasjoner representerer en alvorlig og stadig økende trussel mot nasjonale myndigheter og virksomheter. Russiske myndigheter har vist politisk vilje og evne til å anvende militærmakt i egne nærområder med virkemidler som er i gråsone mellom krig og fred og anvendes innenfor det digitale rom. De dominerende narrativ, geopolitikk og sikkerhet, i russisk utenrikspolitikk, samt realpolitikk som et grunnleggende element i politikkutformingen aktualiserer en overhengende usikkerhet vedrørende Russlands neste maktpolitiske trekk. I henhold til *cybersikkerhetsdilemmaets* tredje grunnpilar vedrørende

tolkning, vil hendelser tolkes som offensive cyberoperasjoner med formål om å styrke russisk politisk handlingsrom samt svekke Norges politiske handlingsrom, dersom cyberoperasjonen detekteres. *Cybersikkerhetsdilemmaets* grunnlinje vil være avgjørende, dersom det hersker tvil om hvorvidt etterretningsarbeidet var av potensielt betydelig skadelig karakter eller om en cyberoperasjons hadde utelukkende etterretningsformål. *Cybersikkerhetsdilemmaets* grunnlinje, det sikkerhets maksimerende aspektet i en ustabil sikkerhetspolitiske situasjon, er basert på usikkerheten om hvorvidt russiske cyberoperasjoner har utelukkende etterretningsinnhentingsformål eller om formålet er å teste sårbarheter i strategisk viktige nettverk. Usikkerheten påvirkes av utfallet av variabelen om hvorvidt våpen og politikk beskytter staten, men tilfører også offensive kapabiliteter for et eventuelt angrep. Ustabiliteten i den rådende sikkerhetspolitiske situasjonen kombinert med økt etterretningsvirksomhet mot norske myndigheter, aktualiserer totalforsvarsbegrepet i det digitale rom.

Allikevel, formålet til det vedvarende etterretningspresset fra russiske myndigheter er å tilrettelegge for det russiske militæret dersom det forekommer en endring i den sikkerhetspolitiske situasjonen. Herunder svekkes norske myndigheters politiske handlingsrom. Russlands sofistikerte og videreutviklede offensive cyberkapabiliteter kan omstille og innrette metoder etter forbedringer vedrørende digital sikring i form av resiliens. Utover de tradisjonelle politiske- og militære mål, rettes russiske etterretningsvirksomhet mot øvrige deler av statsforvaltningen, akademia, aktører tilknyttet kritisk infrastruktur og kritiske samfunnsfunksjoner, samt den øvrige befolkningen som en ny trend underlagt den nye trusseldimensjonen. I en sikkerhets- og forsvarspolitisk kontekst utfordres samfunnssikkerheten ved at fremmede stater retter cyberoperasjoner mot virksomheter og systemer som ikke forvalter skjermingsverdig informasjon, og som tidligere har vært mindre aktuelle etterretningsmål. Ettersom, dette forverrer risikobildet og utvider trusselbildet ved at samfunnskonsekvensene av IKT-hendelser vil øke, da alvorlig trusler kommer innenfra egne systemer, iverksatt av en trusselaktør med betydelige maktressurser. Norske myndigheters motsvar er tuftet på defensive cyberkapabiliteter innad i informasjonsinfrastrukturen, samt en utbredelse av robusthet og sikkerhet for å fremme internasjonalt samarbeid om cybersikkerhet, enighet om statlig oppførsel i det digitale rom samt styrke evnen til å forebygge, oppdage, varsle og håndtere alvorlige cyberhendelser. En gjennomgående utbedring av internasjonal cybersikkerhet fremkommer som en form for avskrekkelse i etterkant av russiske myndigheters inntrengning i nettverk av strategiske betydning, fremfor benyttelse av offensive kapabiliteter i form av angrep, kan behovet for en troverdig respons

fremme eskalering. En troverdig respons rettet mot Russland i dagens sikkerhetspolitiske situasjon preget av vesentlig usikkerhet basert på det kjølige forholdet mellom Vesten og Russland, kan resultere i at enkeltepisoder får mer alvorlige konsekvenser enn hva de aktuelle partene er tjent med, ettersom *cybersikkerhetsdilemmaet* er et selvødeleggende aspekt i søket etter sikkerhet og vil resultere i en opprustningsspiral (Jervis, 1978:78).

Den rådende sikkerhetspolitiske situasjonen herunder kan betegnes som livsløpet til en kanarifugl i en kullgruve; i det øyeblikket større cyberoperasjoner mot norske stats- og samfunnsfunksjoner finner sted, vil eventuelle mottiltak være nytteløse. Norske myndigheter risikerer å svekke egne kapabiliteter dersom staten ignorerer Russlands sikkerhetstiltak som kan vise seg å være utslagsgivende i en skjerpet sikkerhetspolitisk situasjon. Vedvarende russisk etterretningsvirksomhet fremstår ikke som en handling med utelukkende etterretningsinnhentingsformål, men som i kombinasjon med å teste sårbarheter i sentrale norske systemer. Dette utfordrer deteksjonsmekanismene i det sivile samfunn og dermed Forsvaret, ettersom det ikke er de angrepene vi kjenner som utgjør det største samfunnsrelaterte problemet, men de angrepene vi ikke kjenner.

6 Konklusjon

Formålet til dette oppgaven har vært å undersøke totalforsvarets relevans i en tid preget av en ny trusseldimensjon, i henhold til digitale sikkerhetsutfordringer i fredstid. For å etablere et godt kunnskapsgrunnlag for sivilt- militært samarbeid, rettes det i oppgaven fokus på hvordan totalforsvarets utfordres av russiske cyberkapabiliteter i henhold til forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering. Oppgavens problemstilling er som følgende:

Hvilke digitale sikkerhetsutfordringer står totalforsvaret overfor i fredstid?

Problemstillingen bygger på tre underlagte delspørsmål som underveis i oppgaven skal besvares:

1) *På hvilken måte utgjør digitale sårbarheter en sikkerhetsutfordring for totalforsvaret?*
2) *Tyder vedvarende russisk etterretningsvirksomhet og kartlegging av sentrale norske myndigheter og virksomheter på opprustning i det digitale rom?*
3) *Kan styrket resiliens tilspisse den sikkerhetspolitiske situasjonen mellom Norge og Russland?*

Problemstillingen har blitt besvart i sin helhet gjennom tre steg ved delkonklusjonene til de underlagte delspørsmålene. Gjennom oppgavens tre delspørsmål har digitale sikkerhetsutfordringer på bakgrunn av digitale sårbarheter i totalforsvaret blitt identifisert. På bakgrunn av at russisk etterretningsvirksomhet vurderes til å ha størst skadepotensiale overfor norske interesser, diskuteres det hvordan russisk etterretning kan utnytte de redegjorte sikkerhetsutfordringene som følge av digitale sårbarheter i totalforsvaret. For å utarbeide og styrke totalforsvarets evne innen forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering, er det diskutert hvorvidt vedvarende etterretning og kartlegging av sentrale norske myndigheter og virksomheter tyder på russisk opprustning i det digitale rom. Diskusjonen til delspørsmål nummer to er begrunnet med at det er prekært for norske myndigheter, virksomheter og befolkningen å forstå hva de skal beskytte seg mot, for å kunne styrke beredskap og redusere samfunnets digitale sårbarheter. Basert på det overnevnte, diskuteres det avslutningsvis hvorvidt styrket resiliens kan tilspisse den sikkerhetspolitiske situasjonen mellom Norge og Russland.

6.1 Oppgavens funn

Digitaliseringen av samfunnet har resultert i betydelige endringer i samfunnets strukturer hvor trusselbildet omhandler stadige økende tematisering av sivile utfordringer, fremfor militære utfordringer. Uten nødvendige og sårbarhetsreduserende tiltak øker risikoen for at virksomheter, myndigheter og den øvrige befolkningen blir rammet av uønskede hendelser grunnet digitale sårbarheter. Samfunnet blir stadig mer sårbart ettersom den totale nasjonale sårbarhetsflaten øker, hvor digitale sårbarhet og feil forplantes mellom tjenester, systemer, virksomheter og infrastrukturer som ledd i verdikjedene og muliggjør strukturelle samfunnsmessige sårbarheter som trusselaktører videre kan utnytte. En stadig økende sårbarhetsflate forenkler fremmede staters etterretningsvirksomhet mot tradisjonelle politiske- og militære mål, øvrige deler av statsforvaltningen, akademia, kraftselskaper og industri. Virksomheter og systemer som ikke forvalter skjermingsverdig informasjon, og som tidligere har vært mindre aktuelle etterretningsmål opplever et stadig økende etterretningspress. Resultat er et utvidet risiko- og trusselbilde ved at de totale samfunnskonsekvensene av IKT-hendelser vil øke ettersom alvorlig trusler kommer innenfra egne systemer, iverksatt av en trusselaktør med betydelige maktressurser. Internasjonale trender viser også til økende interesse for personopplysninger, da tilgangen på personopplysninger, passbilder og biometrisk data forenkler mulighet til å tilpasse etterretningsoperasjoner mot enkeltindivider, med siktemål om å sikre tilgang til nettverk av strategisk betydning.

Gjennom kvalitativ innholdsanalyse vises det til trussel- og risikovurderinger fra PST, NSM og E-tjenesten gjennomgående omhandler tre områder: (i) fremmede staters etterretningsvirksomhet i det digitale rom som en økende trussel mot nasjonale myndigheter og virksomheter, (ii) cyberoperasjoner hvor det etableres bakdører ved de aktuelle etterretningsmålene, (ii) samt at majoriteten av målrettede digitale spionasjeoperasjoner fra fremmede staters etterretningsvirksomhet mot norske mål forekommer gjennom bruken av *spear-phising*. Norske myndigheter, JD, erkjenner at behovet for støtte til håndtering av betydelige IKT-hendelser er mer omfattende enn det behovet NSM og NorCERT skal kunne dekke. Digitale sikkerhetsutfordringer for totalforsvar etableres og utvikles da sårbarhetsreduserende tiltak ikke forekommer i samme takt som utviklingen av trusselbildet, og et stadig økende informasjonsgap mellom trusselaktørenes kapabiliteter og nødvendige mottiltak av aktuelle virksomheter. Digitale sikkerhetsutfordringer utfordrer totalforsvarets beskyttende rolle overfor det sivile samfunn.

For videre å analysere de potensielle implikasjonene digitale sikkerhetsutfordringer påfører totalforsvaret som følge av digitale sårbarheter, anvendes *cybersikkerhetsdilemmaet.* Russland forblir sentral som rammefaktor ved utforming av norsk sikkerhets- og forsvarspolitikk, som gjenspeiles ved at PST vurderer russisk etterretningsvirksomhet til å inneha størst skadepotensiale. Russlands uforutsigbare utøvelse av maktpolitikk og vedvarende etterretningsvirksomhet tolkes, på bakgrunn av *cybersikkerhetsdilemmaets* første og andre grunnpilar, som utelukkende defensive ambisjoner om å styrke nasjonal sikkerhet. Allikevel grunnet metode og målvalg fremstår ikke vedvarende russisk etterretningsvirksomhet som en handling med utelukkende etterretningsinnhentingsformål, men som i kombinasjon med å teste sårbarheter i sentrale norske systemer. Ved å kartlegge tradisjonelle militære- og politiske mål, kritisk infrastruktur og kritiske samfunnsfunksjoner i fredstid, styrkes Russlands handlingsrom for å utnytte den innhentede informasjonen dersom den sikkerhetspolitiske situasjonen endres. Insentivet om å styrke nasjonal sikkerhet ved å gjennomføre uautorisert inntrengning med formål om å innhente sensitiv informasjon, tjener russiske interesser samtidig som Norges handlingsrom og sikkerhet svekkes.

Den rådende sikkerhetspolitiske situasjon er basert på det kjølige forholdet mellom Vesten og Russland, hvor enkeltepisoder får mer alvorlige konsekvenser enn hva de aktuelle partene er tjent med. Ettersom den stadig økende usikkerheten påvirkes av utfallet av variabelen om hvorvidt våpen og politikk beskytter staten, allikevel tilføres offensive kapabiliteter for et eventuelt angrep. I henhold til *cybersikkerhetsdilemmaets* tredje grunnpilar vedrørende tolkning, vil allikevel alvorlige IKT-sikkerhetshendelser tolkes som offensive cyberoperasjoner med formål om å styrke russisk politisk handlingsrom samt svekke Norges politiske handlingsrom, dersom disse cyberoperasjonen detekteres. Norske myndigheters etableringsforsøk av resiliens og enighet om statlig oppførsel i det digitale rom i det internasjonale system, kategoriseres som et forsøk på å styrke nasjonal sikkerhet. Ettersom forsvar mot digitale trusler ikke skaper sikkerhet alene, tar Norges internasjonale cyberstrategi utgangspunkt i å håndtere de bakenforliggende årsakene til trusler. I henhold til den tredje grunnpilaren, på bakgrunn av geopolitikk og sikkerhet som dominerende narrativ i russisk utenrikspolitikk, kan et forsøk på styrke nasjonalt handlingsrom trigge en troverdig respons og fremme eskaleringspotensialet. På bakgrunn av de latente interessemotsetninger i det asymmetriske forholdet kan den rådende sikkerhetspolitiske situasjonen betegnes som livsløpet til en kanarifugl i en kullgruve, i det øyeblikket betydelige cyberoperasjoner finner sted vil eventuelle mottiltak av norsk defensive cyberkapabiliteter være nytteløse.

Cybersikkerhetsdilemmaet fremstår herunder som et selvødeleggende aspekt i søket etter sikkerhet og vil resultere i en opprustningsspiral.

Basert på det overnevnte da *cybersikkerhetsdilemma* omhandler prosessen før en eventuell konflikt, er sårbarhetspotensialet betydelig ved de digitale sikkerhetsutfordringene totalforsvaret står overfor i fredstid. I det moderne totalforsvaret baseres sivil støtte til Forsvaret i stor grad på kommersielle ordninger og samarbeid med sivil beredskap. Forsvarssektoren er avhengig av sivil infrastruktur og tjenesteproduksjon for å løse forsvarets oppgaver tuftet på en operasjonalisering av de forsvarspolitiske målene. Dermed er forsvaret avhengige av at det sivile samfunn til enhver tid er i en normaltilstand, uavhengig av den sikkerhetspolitiske situasjonen.

Samfunnets totale sårbarhetsflate øker, hvor digitale sårbarheter og feil forplantes mellom tjenester, systemer, virksomheter og infrastrukturer som resulterer i strukturelle samfunnsmessige sårbarheter. Disse forholdene resulterer i digitale sikkerhetsutfordringer, som mangelfull sikring og teknologisk utvikling til sikkerhetspolitiske endringer og nye trusler fra målrettede trusselaktører. Herunder, cyberoperasjoner rettes mot å skade, ødelegge eller forstyrre, samt undertrykke administrasjons- og ledelsessystemer sivilt eller militært. Samfunnets digitale sikkerhetsutfordringer som følge av digitale sårbarheter i totalforsvaret, resulterer i svikt vedrørende oppgaver om forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering i hele krisespekteret fra fred via sikkerhetspolitisk krise til væpnet konflikt. Den sivile støtten angripes og dermed trues befolkningens sikkerhet, da interessen for sensitiv informasjon om enkeltindivider er stadig økende blant fremmede staters etterretningsvirksomheter. Personvernopplysninger forenkler målrettede cyberoperasjoner mot enkeltindivider gjennom skreddersydde e-post med skadevare. Gjennom målrettet og troverdig utformet e-post som inneholder skadevare kan trusselaktører etablere bakdører og sikre varig tilgang til aktuelle virksomheters nettverk, samt etablere kontroll over nettverket i tiden før en eventuelt større cyberoperasjon inntreffer. I Norges sikkerhets- og forsvarspolitiske kontekst utfordres samfunnssikkerheten ved at fremmede stater retter cyberoperasjoner mot virksomheter og systemer som ikke forvalter skjermingsverdig informasjon, samt som tidligere har vært mindre aktuelle etterretningsmål. Resultatet er et forverret risikobilde og utvidet trusselbilde da samfunnskonsekvensene av IKT-hendelser vil øke når alvorlige trusler kan komme innenfra egne systemer, iverksatt av en trusselaktør med betydelige maktressurser.

Konklusjonen beror på svikt i totalforsvaret ved forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering av digitale sikkerhetsutfordringer som følge av digitale sårbarheter i egen struktur. I henhold til stats- og samfunnssikkerhetsperspektivet utgjør den største trusselen de aktørene som har ressurser til å gjennomføre handlinger som nasjonale deteksjonsmekanismer ikke evner å oppdage i tide, eller i det hele tatt. Dette utfordrer deteksjonsmekanismene i det sivile samfunn og i Forsvaret, ettersom det ikke er de angrepene vi kjenner som utgjør det største samfunnsrelaterte problemet, det er de angrepene vi ikke kjenner. Dagens situasjon byr på utfordringer knyttet til usikkerhet og utilstrekkelig koordinering mellom myndighetene, som aktualiserer sivilt- militært samarbeid i det digitale rom. Ettersom nasjonal sikkerhet forutsetter høy sikkerhet innad i aktuelle virksomheter, samt samarbeid mellom myndigheter og private aktører for å styrke resiliens på tvers av samfunnssektorene.

I møte med digitale sikkerhetsutfordringer vil et videreutviklet sivilt-militært samarbeid innenfor rammene av totalforsvarskonseptet, lette koordineringsproblematikken. En potensiell etablering av mindre avansert og mer sømløs informasjonsflyt mellom virksomheter og relevante myndigheter vil delvis kunne redusere digitale sikkerhetsutfordringer. Kortsiktig vil dette styrket evnen blant virksomheter til å håndtere mindre hendelser for å sikre systemets pålitelighet, samt gjenopprette normaltilstanden etter større hendelser. Langsiktig reduseres sårbarhetsflaten som gir rom for utvikling av sårbarhetsreduserende tiltak som medfører til fravær av IKT-hendelser som kan undergrave normaltilstanden over lengre tid. Forsvar mot cyberoperasjoner blir stadig viktigere, men forsvar alene skaper ikke sikkerhet. Styrket resiliens i en ny normaltilstand vil kunne danne en sterkere digital grunnberedskap, hvor håndteringsevnen ville redusert muligheten til fravær av normaltilstand som følge av IKT-hendelser blant virksomheter og sentrale institusjoner. Styrket resiliens vil øke beskyttelsen av interesser samt verne nasjonale verdier, som på sikt vil forhindre at en mulig trussel medfører til en eskalering i den sikkerhetspolitiske situasjonen.

6.2 Kritikk og forslag til videre forskning

En betydelig utfordring med denne oppgaven har vært å arbeide med begrenset informasjon relatert til Norsk forsvars-, beredskaps- og sikkerhetspolitikk. Mye av den offentlig tilgjengelige informasjonen er ugradert, hvor enkelte kilder opptrer som vage. Informasjon som utvilsomt ville spisset oppgavens relevans og i større grad besvar problemstillingen er unnlatt offentligheten, det vises til at PST ikke opplyser hvor vellykket cyberoperasjonene mot sentrale norske institusjoner var. Dette begrunner derfor de metodiske valgene ved å benytte dokumentbasert undersøkelse som forskningsdesign, med kvalitativ innholdsanalyse som analyseform har vært hensiktsmessig for å kunne forstå sammenheng ved PST, NSM og E-tjenestens trussel- og risikovurderinger, og videre tolke trusselbildet. Bruken av kvalitativ innholdsanalyse har muliggjort en underliggende ambisjon om å trekke slutninger utenfor tekstene som utelukkende gir oppgaven et større spillerom i henhold til *cybersikkerhetsdilemmaet* som valgte teori.

Innholdsanalysens underliggende ambisjon om å trekke slutninger utenfor tekstene, fordrer at forskeren unnlater at det subjektive overskrider oppgavens objektivitet. Uavhengig av tematisk vinkling, er det tilstede fallgruver vedrørende oppgaver som omhandler Russland eller russisk aktiviteter i det internasjonale samfunnet. Nevnte fallgruver kan kategoriseres som *Russland-fella*, hvor objektiviteten til forskere utfordres kraftig av subjektiviteten da Russland omtales i et negativt lys i påvente av en større sikkerhetspolitisk handling. Kvalitativ forskning baseres på forskerens tolkning noe som fordrer gjennomgående arbeid med oppgavens reliabilitet for etterprøvbarhet og som en nødvendig forutsetning for validitet. Aktuelle hendelser fremstår som støy og kan fremme forskeres subjektive formening gjennomgående i forskningsarbeidet. Arbeidet med denne oppgaven har i stor grad foregått mens saken om den pensjonerte grenseinspektøren, Frode Berg, har vært i nyhetsbildet. Frode Berg ble i desember 2017 pågrepet av den russiske sikkerhetstjenesten FSB i Moskva og er siktet for spionasje. Samt, fant Giftangrepet i Salisbury, England, sted i denne oppgavens avsluttende fase. Norge sto sammen med Storbritannia, allierte, partnere og naboland. Giftangrepet ble fordømt av den vestlige verden og resulterte gjensidige utvisninger av diplomater i respektive land. Aktuelle hendelser som er plassert på dagsordenen av media medfører til støy som kan øke subjektiviteten ubevist i det som produseres. Ved at Russland omtales i et negativt lys i påvente av en større sikkerhetspolitisk handling, kan dermed

overskride de faktiske forhold om at Russland pr. nå ikke utgjør en militær trussel mot Norge, samt at NATO er konvensjonelt overlegen Russland.

Cybersikkerhetsdilemmaet som valgte teori for oppgaven, har gjennom de tre grunnpilarene belyst digitale sikkerhetsutfordringer i totalforsvaret. Gjennom innholdsanalysens underliggende ambisjon om å trekke slutninger utenfor dokumentene, vises det til at vedvarende russisk etterretningsvirksomhet ikke fremstår som en handling med utelukkende etterretningsinnhentingsformål, men som i kombinasjon med å teste sårbarheter i sentrale norske systemer. *Cybersikkerhetsdilemmaets* tredje grunnpilar, tolkningsdilemmaet, understreker dette ved å vise til sikkerhetsmaksimering som teoriens grunnlinje. Sikkerhetsmaksimering legger føringer for en opprustningsspiral grunnet den betydelige usikkerheten i det internasjonale system.

Gjennom latente interessemotsetninger i det bilaterale forholdet mellom Norge og Russland, kan norske handlinger bli tolket i en realpolitisk og sikkerhetspolitiske kontekst, grunnet geopolitikk og sikkerhetspolitikk som dominerende narrative innenfor russisk utenrikspolitikk. Teorigrunnlaget er i betydelig grad kompatibel med tradisjonelt nullsum-spill, og oppgaven har videre begrunnet en overhengende trussel som russiske cyberkapabiliteter kan ha overfor stats- og samfunnsfunksjoner og den øvrige befolkningen. En trussel som kan eskalere til en sikkerhetspolitisk krise, belyst av forsvarssjefen, admiral Haakon Bruun-Hanssen, ved å påpeke at en senere økning i norske styrkeforhold kan bli tolket som en eskalering.

Til tross for at forhold mellom Vesten og Russland er på sitt kjøligste siden den kalde krigen, er det tvilsomt om *cybersikkerhetsdilemmaet* i denne konteksten bidrar til fruktbar forskning. Opprustningsspiralen som vil kunne oppstå vil bestå av, på russisk side, sofistikerte og videreutviklede cyberkapabiliteter, mens på norske side vil styrket resiliens medføre til økt motstandsdyktighet. Den rådende sikkerhetspolitiske situasjonen vil på bakgrunn av dette kunne tilspisse, men en større eskalering i tråd med stegene i *cybersikkerhetsdilemmaet* er mindre aktuelt. Allikevel skal det påpekes at gjennomgang av ulike scenarioer er prekært for forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering, noe denne oppgaven har bidratt med ved å belyse usikkerhetsmoment og betydelige utfordringer.

I forlengelse av studie om oppgavens tema, ville det være hensiktsmessig å avvente for å se på effekten av Norges internasjonale cyberstrategi, da den fremdeles er relativt ny. Samt er det er pågående arbeidet med det åttende prosjektet i serien om Beskyttelse av samfunnet (BAS), BAS 8 omhandler sivilt-militær krisehåndtering og beredskap. Prosjektet skal bidra til bedre sivilt-militært samarbeid innenfor rammene av totalforsvaret i alvorlige kriser, med målsetning om å bedre utnyttelsen av tverrsektorielle kriseøvelser (Forsvarets Forskningsinstitutt, 2017).

Et av oppgavens formål har vært å rette fokus på hvilke digitale sikkerhetsutfordringer totalforsvaret står overfor i fredstid, da den nye trusseldimensjonen består av at IKT-hendelser rettes mot den sivile befolkningen. Dette vil tilrettelegge for videre forskning for å etablere et godt kunnskapsgrunnlag for utvikling av krisehåndtering og beredskap. Ny forskning på området vil kunne være tjent med en annen operasjonalisering av resiliens, da dette kan gi indikasjoner på om flere gjennomførte tiltak har reduserte sårbarheter og styrket forebyggende sikkerhetsarbeid.

Litteraturliste

Allison, T, G. (1969). Conceptual Models and the Cuban Missile Crisis. *The American Political Science Review*. Vol 63. Pp 689-718.

Booth, K. & Wheeler,J. N. (2008). *The Security Dilemma: Fear, Cooperation and Trust in World Politics*. New York: Palgrave Macmillan.

Bratberg, Ø. (2014). *Tekstanalyse for samfunnsvitere*. Oslo: Cappelen Damm Akademisk.

Buchanan, B. (2016) *The Cybersecurity Dilemma: hacking, trust, and fear between nations*. London: Hurst & Company.

Butterfield, H. (1951). *History and Human Relations*. London: Collins.

Connell, M. & Vogler, S. (2017). *Russia's Approach to Cyber Warfare*. Hentet fra https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf

Daae, C. (2017). *Totalforsvaret: Beredskap for en ny tid?* Paper presenter på konferanse om totalforsvaret ved Oslo Militære Samfund på vegne av DSB. Hentet fra https://www.oslomilsamfund.no/wp-content/uploads/2017/02/Totalforsvaret-beredskap-for-en-ny-tid_Oslo-millit%C3%A6re-samfunn_45-min_27022017_Cecilie.pdf

Demchak, C, C. (2012). Resilience and Cyberspace: Reconizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI). *Journal of Comparative Policy Analysis: Research and Practice*. 14(3), 254-269.

Departement of Homeland Security & the Federal Bureau of Investigation. (2016). *Grizzly Steppe – Russian Malicious Cyber Activity*. Hentet fra https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

Departementene (2012). *Nasjonal strategi for informasjonssikkerhet*. Hentet fra https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf

Direktoratet for samfunnssikkerhet og beredskap. (2016). *Samfunnets kritiske funksjoner: Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* Hentet fra https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Elgsaas, M, I. & Heireng, S, H. (2014). *Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet*. FFI-rapport 2014/00948.

Endregard, M., Brattekås, K., Nystuen, K. O., Sandrup, T. og Gerhardsen, W. (2016). *Viten /2016 Beskyttelse av samfunnet i en ny tid*. FFI-rapport 2015/02472

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

Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste. (2016). *Dokument 16 (2015-2016) Rapport til Stortinget fra Evalueringsutvalget, for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget).* Hentet fra https://www.stortinget.no/globalassets/pdf/dokumentserien/2015-2016/dok16-201516.pdf

Fagerland, S., Kråkvik, M. & Camp, J. (2013). *Operations Hangover: Unveiling an Indian Cyberattack Infrastructure.* Hentet fra https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/NS-Unveiling-an-Indian-Cyberattack-Infrastructure_FINAL_Web.pdf

Fireeye. (2015). *HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group*. Hentet fra https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf

Forsvaret. (2013). *Manual i Krigens Folkerett*. Hentet fra https://brage.bibsys.no/xmlui/bitstream/id/201436/manual_krigens_folkerett.pdf

Forsvaret. (2014). *Forsvarets fellesoperative doktrine*. Hentet fra https://brage.bibsys.no/xmlui/bitstream/id/317149/FFOD%202014.pdf

Forsvaret. (2015). *Et forsvar i endring: Forsvarssjefens fagmilitære råd*. Hentet fra https://forsvaret.no/fakta_/ForsvaretDocuments/EtForsvariEndring-Nett.pdf

Forsvarets Forskningsinstitutt. (2017). *BAS 8 – Sivil-militær krisehåndtering og beredskap.* Hentet fra https://www.ffi.no/no/Forskningen/totalforsvar/BAS/bas8/Sider/BAS8.aspx

Forsvarsdepartementet. (2004). *Den videre moderniseringen av Forsvaret i perioden 2005-2008*. (Prop. 42 2003-2004). Hentet fra

https://www.regjeringen.no/contentassets/4648088bb28649bc8458f1484d9cbe06/no/pdfs/stp200320040042000dddpdfs.pdf

Forsvarsdepartementet. (2012a). *Et forsvar for vår tid.* (Prop. 73 S 2011-2012). Hentet fra https://www.regjeringen.no/contentassets/e6b0d7ef3c26457ab6ef177cd75b5d32/no/pdfs/prp201120120073000dddpdfs.pdf

Forsvarsdepartementet. (2012b). *Fakta om Forsvaret*. Hentet fra https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fakta2012_norsk_nettutgave.pdf

Forsvarsdepartementet. (2014). *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren. «FDs cyberretningslinjer»*. Hentet fra https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf

Forsvarsdepartementet. (2016). *Kampkraft og bærekraft – langtidsplan for forsvarssektoren.* (Prop. 151 S 2015-2016). Hentet fra https://www.regjeringen.no/contentassets/a712fb233b2542af8df07e2628b3386d/no/pdfs/prp201520160151000dddpdfs.pdf

Forsvarsdepartementet. (2017). *Lov om nasjonal sikkerhet (sikkerhetsloven).* (Prop. 153 L 2016-2017). Hentet fra https://www.regjeringen.no/contentassets/0fcee45affd24280896b88b5413a00aa/no/pdfs/prp201620170153000dddpdfs.pdf

Forsvarsdepartementet & Justis- og beredskapsdepartementet. (2015). *Støtte og samarbeid: en beskrivelse av totalforsvaret i dag*. Hentet fra https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/rapporter-og-regelverk/fd_stotte-samarbeid_web_april.pdf

Forsvarskomiteen og justiskomiteen. (2003). *Innstilling fra forsvarskomiteen og justiskomiteen om samfunnssikkerhet – Veien til et mindre sårbart samfunn*. (Innst. S. nr. 9 2002-2003). Hentet fra https://www.stortinget.no/globalassets/pdf/innstillinger/stortinget/2002-2003/inns-200203-009.pdf

F-Secure. (2015). *The Dukes – 7 Years of Russian cyberespionage*. Hentet fra https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Gentikow, B. (2005). *Hvordan utforsker man medieerfaringer? Kvantitativ metode*. Revidert utgave. Kristiansand: Høyskoleforlaget.

Grønmo, S. (2004). *Samfunnsvitenskapelige metoder*. Bergen: Fagbokforlaget.

Hanssen, B, H. (2015). *Forsvarssjefens tale i OMS 12. januar 2015*. Oslo Militære Samfund.

Hanssen, B, H. (2018). *Leders beretning 2017*. Hentet fra https://forsvaret.no/fakta/undersokelser-og-rapporter/aarsrapport/leders-beretning-2017

Heier, T. & Kjølberg, A. (red.). (2013). *Mellom Fred og Krig: Norsk militær krisehåndtering*. Oslo: Universitetsforlaget.

Heier, T. & Kjølberg, A. (red.). (2015). *Norge og Russland: Sikkerhetspolitiske utfordringer i Nordområdene*. Oslo: Universitetsforlaget.

Hellevik, O. (2003). *Forskningsmetode i sosiologi og statsvitenskap*. Oslo: Universitetsforlaget.

Helsedirektoratet. (2018). *Innbrudd i datasystemene til Helse Sør-Øst.* Hentet fra https://helsedirektoratet.no/nyheter/innbrudd-i-datasystemene-i-helse-sor-ost

Helse Sør-Øst. (2018). *Om oss*. Hentet fra https://www.helse-sorost.no/om-oss#om-helse-s%C3%B8r-%C3%B8st-rhf

Hertz, H., J. (1950). Idealist Internationalism and the Security Dilemma. *World Politics*. 2 (2), 157-180.

Hovi, J. & Malnes, R. (Red.). (2011). *Anarki, Makt og Normer – Innføring i internasjonal politikk*. Abstrakt forlag: Oslo.

Justis- og beredskapsdepartementet. (2002). *Samfunnssikkerhet: veien til et mindre sårbart samfunn* (Meld. St. 17 2001-2002). Hentet fra https://www.regjeringen.no/contentassets/ee63e1dd1a16409fa0bb737bfda9279a/no/pdfa/stm200120020017000dddpdfa.pdf

Justis- og beredskapsdepartementet. (2004). *Samfunnssikkerhet og sivilt-militært samarbeid.* (Meld. St. 39 2003-2004). Hentet fra https://www.regjeringen.no/contentassets/5f624a82750b4b14b3a7717e6bdb3516/no/pdfs/stm200320040039000dddpdfs.pdf

Justis- og beredskapsdepartementet. (2011). *Fullføring av utbygging og drift av Nødnett i hele fastlands- Norge*. (Prop. 100 S 2010-2011). Hentet fra https://www.regjeringen.no/contentassets/431d2e2892734472a36ed705dbf381da/no/pdfs/prp201020110100000dddpdfs.pdf

Justis- og beredskapsdepartementet. (2016). *Risiko i et trygt samfunn - samfunnssikkerhet.* (Meld. St. 10. 2016-2017). Hentet fra https://www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/no/pdfs/stm201620170010000dddpdfs.pdf

Justis- og beredskapsdepartementet. (2017). *IKT-sikkerhet et felles ansvar*. (Meld. St. 38 2016-2017). Hentet fra https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf

King, G., Keohane, O., R., & Verba, S. (1994). *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton: Princeton University Press.

Kramer, D, F., Starr, H, S & Wentz, K, L. (2009). *Cyberpower and National Security*. Washington, D.C: Potomac Books.

Krippendorf, K. (2012). *Content Analysis: An Introduction to Its Methodology*. 3 utgave. London: Sage.

Langer, R. (2013). *Stuxnet's Secret Twin: The real program to sabotage Iran's nuclear facilities was far more sophisticated than anyone realized*. Hentet fra https://www.rexsresources.com/uploads/6/5/2/1/6521405/stuxnet%E2%80%99s_secret_twin_%7C_foreign_policy.pdf

Lund, T. (2002). *Innføring i forskningsmetodikk*. Oslo: Unipub forlag.

Lunde, H, M. (2016). *Etterretningstjenestens Fokus 2016*. Paper presentert på foredrag om Etterretningstjenestens åpne vurdering av aktuelle sikkerhets utfordringer 2016 ved Oslo Militære Samfund, Oslo. Hentet fra https://forsvaret.no/fakta_/ForsvaretDocuments/Etterretningssjefens%20foredrag%2014.%20mars%202016.pdf

Lunde, H, M. (2018) *Etterretningssjefens årstale 2018*. Hentet fra https://forsvaret.no/etjenesten/etterretningssjefens-aarlige-tale

Lysne II -utvalget. (2016). *Digitalt grenseforsvar (DGF)*. Hentet fra https://www.regjeringen.no/contentassets/ca1f705dbebd48cb9a61889d4cfee6bf/digitalt-grenseforsvar-lysne-ii-utvalget.pdf

Matlary, H, J. & Heier, T. (2016). *Ukraine and beyond: Russia's strategic security challenge to Europe*. Palgrave macmillan: London.

Muller, P, L., Gjesvik, L & Friis, K. (2018). *Cyber-weapons in International Politics – possible sabotage against the Norwegian petroleum sector*. NUPI rapport 3/18. Hentet

fra https://brage.bibsys.no/xmlui/bitstream/handle/11250/2486814/NUPI_Report_2018-3.pdf?sequence=1&isAllowed=y

Nasjonal sikkerhetsmyndighet. (2010). *Rapport om sikkerhetstilstanden 2010*. Hentet fra https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/rst_2010.pdf

Nasjonal sikkerhetsmyndighet. (2011). *Rapport om sikkerhetstilstanden 2011*. Hentet fra https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/rst_2011.pdf

Nasjonal sikkerhetsmyndighet. (2012). *Rapport om sikkerhetstilstanden 2012*. Hentet fra https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/rst_2012.pdf

Nasjonal sikkerhetsmyndighet. (2016). *Håndbok: Risikovurdering for sikring*. Hentet fra https://www.nsm.stat.no/globalassets/dokumenter/handboker/risikovurdering_nsm_handbok_mars2016.pdf

Nasjonal sikkerhetsmyndighet. (2017a). *Helhetlig IKT-risikobilde 2017*. Hentet fra https://www.nsm.stat.no/globalassets/helhetlig_ikt-risikobilde_2017_orig_low.pdf

Nasjonal sikkerhetsmyndighet. (2017b). *Risiko 2017: Risiko og sårbarheter i en ny tid – En vurdering av sårbarheter og risiko i Norge*. Hentet fra https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2017_lr_0404_enkelts_v3.pdf

Nasjonal sikkerhetsmyndighet. (2018). *Risiko 2018: verdifulle individer, verdifulle virksomheter, verdifull infrastruktur*. Hentet fra https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2018_web.pdf

Norges offentlige utredning. (2000). *Et sårbart samfunn: utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.* Justis- og beredskapsdepartementet (NOU rapport 2000:24). Hentet fra https://www.regjeringen.no/contentassets/1c557161b3884335b4f9b89bbd32b27e/no/pdfa/nou200020000024000dddpdfa.pdf

Norges offentlige utredning. (2006). *Når sikkerhet er viktigst: beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Justis- og beredskapsdepartementet (NOU rapport 2006:6). Hentet fra https://www.regjeringen.no/contentassets/c8b710be1a284bab8aea8fd955b39fa0/no/pdfs/nou200620060006000dddpdfs.pdf

Norges offentlige utredning. (2015). *Digitale sårbarheter – sikkert samfunn: beskytte enkeltmennesket og samfunnet i en digitalisert verden*. Justis- og beredskapsdepartementet (NOU rapport 2015:13). Hentet fra https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

Norges offentlige utredning. (2016). *Samhandling for sikkerhet: beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*. Forsvarsdepartementet (NOU rapport 2016:19). Hentet fra https://www.regjeringen.no/contentassets/03960058f3f94fbe9d290593bee22c1a/no/pdfs/nou201620160019000dddpdfs.pdf

Norsk senter for informasjonssikring. (2018). *Hacking av Helse Sør-Øst – Oppsummering*. Hentet fra https://norsis.no/hackingen-helse-sor-ost-oppsummering/

North Atlantic Treaty Organization. (2018). *NATO cyber defence: Factsheet*. Hentet fra https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-en.pdf

Næringslivets sikkerhetsråd. (2016). *Mørketallsundersøkelsen 2016 – informasjonssikkerhet, personvern og datakriminalitet*. Oslo: Næringslivets sikkerhetsråd.

Politiets sikkerhetstjeneste. (2015). *Trusselvurdering 2015*. Hentet fra https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2015/

Politiets sikkerhetstjeneste. (2017). *Trusselvurdering 2017*. Hentet fra https://www.pst.no/trusselvurdering-2017/

Politiets sikkerhetstjeneste. (2018). *Trusselvurdering 2018*. Hentet fra https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2018.pdf

Politiets sikkerhetstjeneste. (2018). *Mandag 14. januar 2018 iverksatte PST etterforskning av nettverksangrep mot datasystemene til Helse Sør-Øst*. Hentet fra https://pst.no/alle-artikler/pressemeldinger/etterforsking-av-nettverksangrep-mot-datasystemene-til-helse-sor-ost/

Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet, Politiet & Næringslivets sikkerhetsråd. (2017). *Sikkerhet ved ansettelsesforhold – før, under og ved avvikling*. Hentet fra https://www.pst.no/globalassets/artikler/utgivelser/sikkerhet_ved_ansettelsesforhold_2017_utskrift.pdf

Pomerantsev, P. & Weiss, M. (2014). *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. A Special Report presented by The Interpreter, a project of the institute of Modern Russia. Hentet fra http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf

Pynnöniemi, K & Rácz, A. (eds.) (nd). Fog of Falsehood. *Russian Strategy of Deception and the Conflict in Ukraine*. FIIA report 45. Helsinki: The finish institute of international affairs.

Raiu, C., Soumenkov, I., Baumgartner, K, & Kamluk, V. (2013). *The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor (or "how many cool words can you fit into on title")*. Hentet fra https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/themysteryofthepdf0-dayassemblermicrobackdoor.pdf

Ravndal, A. J., Johansen, T. S., Kjeksrud, S., Broen, T. (2014) *Resilience methodology – multinational experiment 7*. FFI-rapport 2014/00973.

Schnaufer, A, T. (2017). Redefining Hybrid Warfare: Russia's Non-linear War against the West. *Journal of Strategic Security*, 10(1), 17-31. DOI: http://doi.org/10.5038/1944-0472.10.1.1538

Scott, J. (2006). *Documentary Research*. Vol. 1. London: Sage.

Straffeloven. (2005). Lov om straff av 20 mai 2005 nr. 28. Hentet fra https://lovdata.no/dokument/NL/lov/2005-05-20-28

Sikkerhetsloven. (1998). Lov om forebyggende sikkerhetstjeneste av 20 mars 1998 nr. 10. Hentet fra https://lovdata.no/dokument/NL/lov/1998-03-20-10?q=sikkerhetsloven

Singer, W, P. & Friedman, A. (2014) *Cybersecurity and Cyberwar: what everyone needs to know*. Oxford University Press: New York

Snyder, G, H. (1984). The Security Dilemma in Alliance Politics. *World Politics*, 26 (04), 461-495.

The European Network and Information Security Agency. (2011). *Inter-X: Resilience of the Internet Interconnection Ecosystem*. Full Report – April 2011.

The Ministry of Foreign Affairs of the Russian Federation. (2011). *Convention on International Information Security* (Concept). Hentet fra

http://carnegieendowment.org/files/RUSSIAN-DRAFT-CONVENTION-ON-INTERNATIONAL-INFORMATION-SECURITY.pdf

Trenin, D. (2011). *Post-Imperium: A Eurasian Story*. Carnegie Endowment for International peace: Washington, DC.

Truman, S, H. (1950). A Report to the National Security Council – NSC 68. *President's Secretary's File, Truman papers*.

TV2. (2017). *PST bekrefter omfattende hackerangrep mot Norge*. Hentet fra https://www.tv2.no/a/8903847/

Utenriksdepartementet. (2015). *Globale sikkerhetsutfordringer i utenrikspolitikken – Terrorisme, Organisert kriminalitet, Privatvirksomhet og Sikkerhetsutfordringer i det digitale rom.* (Meld. St. 37 2014-2015). Hentet fra https://www.regjeringen.no/contentassets/bdf4bd40d57d4dc79409de87419a2217/no/pdfs/stm201420150037000dddpdfs.pdf

Utenriksdepartementet. (2017). *Nordisk samarbeid.* (Meld. St. 5 2016-2017). Hentet fra https://www.regjeringen.no/contentassets/73a448d464a04fb0a2dbfb135f87af89/no/pdfs/stm201720180005000dddpdfs.pdf

Välisluureamet. Estonian Foreign Intelligence Service (EFIS). (2018). *International Security and Estonia 2018*. Hentet fra https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf

Østerud, Ø. (2007). *Statsvitenskap – innføring i politisk analyse*. Universitetsforlaget: Oslo.

Åtland, K. (2014). Interstate Relations in the Arctic: An Emerging Security Dilemma? *Comparative Strategy*. 33 (2): 145-166.

Vedlegg

Vedlegg 1

Begrepsforklaringer.

Aktive tiltak (*Active measures*/*aktivinyye meropriyatiya*):

> *Subversjonskampanjer benyttet av KGB i stor grad under den kalde krigen, hvor målet var å påvirke oppførsel og handlinger innad i en fremmed stat, med påfølgende virkemidler rette mot sentrale funksjoner innad i en fremmed stat:*
>
> *a) Påvirke regjeringspolitikken.*
>
> *b) Undergrave tilliten til beslutningstakere og institusjoner.*
>
> *c) Forstyrre forholdet mellom andre stater.*
>
> d) *Diskreditere og svekke statlige og ikke-statlige motstandere* (Pynnöniemi & Rácz, nd:48).

Alvorlige IKT-sikkerhetshendelser:

> *Reelle uønskede tilsiktede hendelser eller trusler om slike hendelser i det digitale rom som er rettet mot kritisk infrastruktur og/eller kritiske samfunnsfunksjoner* (Nasjonal sikkerhetsmyndighet, 2017a:52).

Autentisitet:

> *"Ekthet"* (Forsvarsdepartementet,2014:21).

Cyberoperasjoner/Datanettverksoperasjoner

> *Samlebegrep som tilsvarer det engelske begrepet Computer Network Operations (CNO). CNOs formål er å påvirke motstanderens datanett og beskytte eget nett. Samlebegrepet består videre av:*

Computer Network Defence (CND)

Tiltak for å opprettholde militær handlefrihet i en militær operasjon ved å overvåke, detektere, analysere og iverksette defensive mottiltak i egne informasjonssystemer ved CNA eller CNE mot egne informasjonssystemer.

Computer Network Attack (CNA)

Angrep på motstanderens datasystem med sikte på å forstyrre, manipulere eller ødelegge som støtte til en militær operasjon.

Computer Network Exploitation (CNE)

Tiltak for å oppnå adgang til motstanderens datasystem, tappe det for informasjon og utnytte denne informasjonen (uten at motstanderen er klar over det) som støtte til en militær operasjon (Forsvarsdepartementet, 2014:5).

Cybersikkerhet:

Samme definisjon som informasjonssikkerhet, men i en digital kontekst (Forsvarsdepartementet, 2014:22).

Trussel:

Mulig uønsket handling som kan gi negativ konsekvens for en entitets sikkerhet (Nasjonal sikkerhetsmyndighet, 2016:25).

Digital sårbarhet:

Utfordringer ved sikring av IKT og digital informasjon, digitale trender som påvirker sårbarhetsbildet, og tilsiktede og utilsiktede hendelser (Norges offentlige utredninger (Norges offentlige utredninger) 2015:21).

Forsvarssektoren:

Samlebetegnelse for Forsvarsdepartementet (FD), Forsvaret, Forsvarets forskningsinstitutt (FFI), Forsvarsbygg (FB) og Nasjonal sikkerhetsmyndighet (NSM) (Forsvarsdepartementet, 2014:22).

Informasjon:

> *Enhver form for opplysninger i materiell eller immateriell form* (Forsvarsdepartementet, 2014:23).

Informasjonssikkerhet:

> *Sikkerhetstiltak for i nødvendig grad å oppnå konfidensialitet, integritet, tilgjengelighet og autentisitet ved behandling av informasjon i alle situasjoner, uavhengig av verktøy og metoder. Cyberretningslinjene er innrettet mot håndtering av digital informasjon og informasjonssystemer. Informasjonssikkerhet omfatter både etablering av barrierer, deteksjon av sikkerhetstruende hendelser og reaksjon på slike med tanke på gjenoppretting av sikker tilstand for informasjon og systemer. Defensive datanettverksoperasjoner (CND) omfattes av begrepet informasjonssikkerhet, men utføres i en operativ kontekst* (Forsvarsdepartementet, 2014:23).

Informasjonssystem:

> *En organisert samling av periferiutrustning, programvare, datamaskiner og kommunikasjonsnett som knytter dem sammen* (Forsvarsdepartementet, 2014:23).

Innsider:

> *En nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt autorisert tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap* (Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet, Politiet & Næringslivet sikkerhetsråd, 2017:18)

Integritet:

> *Sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter* (Forsvarsdepartementet, 2014:23).

Konfidensialitet:

> *Sikkerhet for at nærmere angitt informasjon ikke avsløres for uvedkommende, og at kun autoriserte personer får tilgang til denne* (Forsvarsdepartementet, 2014:23).

Kritisk infrastruktur:

> *De anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse* (Norges offentlige utredninger, 2006:31).

Kritisk samfunnsfunksjoner:

> *De funksjoner som er nødvendige for å dekke samfunnets grunnleggende behov og befolkningens trygghetsfølelse* (Direktoratet for samfunnssikkerhet og beredskap, 2016:106).[56]

Tilgjengelighet:

> *Sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov* (Forsvarsdepartementet, 2014:23).

Nødnett:

> *Betegnelsen på et nytt digitalt radiosamband for nød- og beredskapsetatene i Norgebasert på TETRA-standard (Terrestrial Trunked Radio). Nødnettet gir mulighet til å kommunisere sømløst på tvers av organisatoriske og geografiske grenser, samtidig som det er mulig for en gruppe å snakke uforstyrret på nettet uten at andre nødnettbrukere har adgang til informasjonene (*Justis- og beredskapsdepartementet, 2011:8).

Resiliens:

> *Aksept av risiko for at et angrep vil finne sted, og legge vekt på å øke evnen til å forhindre, oppdage og absorbere cyberangrep vektlegges, samt evnen til å gjenopprette normaltilstanden etter angrepet* (Ravndal *et al*, 2014:6)

[56] Vurderingen er ikke helt konsekvent i hvordan kritiske samfunnsfunksjoner defineres. «En samfunnsfunksjon er kritisk hvis den er absolutt nødvendig for å ivareta samfunnets og befolkningens grunnleggende behov» er en definisjon som også benyttes.

Phising:

> *En trusselaktørs handling ved å kamuflere et digitalt angrep gjennom en e-post med en tulsynelatende legitim avsenderadresse og tilpasse innholdet til mottakeren, hvor skadevaren skjule som et vedlegg eller lenke i e-posten. Den tilsynelatende legitime e-posten krever en form for handling av mottaker for å aktivisere skadevaren* (Singer & Friedman, 2014:40).

Sabotasje handlinger via det digitale domenet:

> *Offensive digitale verktøy, benyttes av en trusselaktør, som innehar evne til å skade, ødelegge, forstyrre eller undertrykke administrasjons- og ledelsessystemer sivilt eller militært* (Etterretningstjenesten, 2016:82).

Samfunnssikkerhet:

> *Samfunnets evne til å verne seg mot 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* (Justis- og beredskapsdepartementet, 2016:9).

Sikkerhet:

> *Innebærer beskyttelse mot fravær av trusler som kan forårsake uønskede hendelser* (Norges offentlige utredninger 2015:34)

Sikkerhetstilstanden:

> *Et sammensatt begrep som består av to hovedkomponenter: risikobildet og forebyggende sikkerhet.*
>
> *Risikobildet* kan videre defineres som, *tidsbegrenset beskrivelse av entitets risiko.* Samt kan *forebyggende sikkerhet* tilknyttes risikobildet gjennom sikkerhetslovens definisjon av forebyggende sikkerhetstjeneste, *planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet* (Elgsaas & Heireng, 2014:7-8).

Sikkerhetstruende virksomhet:

> I lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) kapittel 1 § 3 nr. 2 defineres sikkerhetstruende virksomhet som *forberedelser, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandling, samt medvirkning til slik virksomhet* (Sikkerhetsloven, 1998, § 3).

Spear-phising:

> *Mer utfordrende og sofistikert en tradisjonell phising, ettersom det skjulte digitale angrepet er i større grad er spesialtilpasset et enkeltindivid som mål. Spesial angrep i denne sjangere forutsetter i større grad at relevant informasjon er innhente i forkant av et angrep, for at forespørselen om handling for mottaker fremstår mest mulig troverdig* (Singer & Friedman, 2014:41).

Sårbarhet:

> *Et utrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet. Sårbarhet er knyttet opp til mulig tap av verdi. System kan i denne sammenhengen for eksempel være en stat, den nasjonale kraftforsyningen, en bedrift eller et enkeltstående datasystem. I stor grad er sårbarhet selvforskyldt. Det går an å påvirke sårbarheten, begrense og redusere den* (Norges offentlige utredninger 2000:18).

Trusselaktør:

> *En aktør som ønsker å utføre en handling eller påvirke andre på en måte som er i strid med norske sikkerhetsinteresser eller en bestemt virksomhets interesser* (Politiets sikkerhetstjeneste *et al*, 2017:18).

Totalforsvar:

> *Totalforsvarskonseptet omfatter den gjensidige støtte om samarbeid mellom Forsvaret og det sivile samfunn i hele krisespekteret fra fred via sikkerhetspolitisk krise til krig.*

Begrepet totalforsvar ble utviklet etter slutten av den andre verdenskrig, hvor konseptet la vekt på sterk samhandling mellom militære og det sivile samfunn for på best mulig måte forsvare nasjonale verdier, landets selvstendighet, territorium og den sivile befolkningen. Det moderniserte totalforsvarskonseptet omfatter gjensidig støtte mellom Forsvar og det sivile samfunn i forbindelse med forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering i hele krisespekteret fra fred via sikkerhetspolitiske krise til væpnet konflikt (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2015:12).

Nulldagssårbarheter (Zero day):

Ukjente sårbarheter som oppdages som oftest i ettertid av et angrep, hvor det på det aktuelle tidspunktet ikke eksisterer reparasjon mot sårbarheten (Norges offentlige utredninger 2015:37).

Vedlegg 2

Grunnleggende nasjonale interesser:

Omtalt i straffeloven kapittel 17 i lovens §121 om etterretningsvirksomhet mot statshemmeligheter, er grunnleggende nasjonale interesser beskrevet i bokstav a-f (Straffeloven, 2005, §121):

a) Forsvars-, sikkerhets- og beredskapsmessige forhold,

b) de øverste statsorganenes virksomhet, sikkerhet eller handlefrihet,

c) forholdet til andre stater,

d) sikkerhetsopplegg for fremmede staters representasjon og ved større nasjonale og internasjonale arrangementer,

e) samfunnets infrastruktur, så som mat-, vann- og energiforsyninger, samferdsel og telekommunikasjon, helseberedskap eller bank- og pengevesen eller,

f) norske naturressurser[57].

[57] Tilføyd ved lov 7 mars 2008 nr. 4.

Vedlegg 3

I evalueringsutvalget for Stortingets kontroll utvalg for etterretnings-, overvåkings- og sikkerhetstjenestes rapport til Stortinget om nasjonal sikkerhet heter det:

> Rikets eller nasjonens sikkerhet omfatter flere felt. For det første nasjonal suverenitet og herredømme over landets territorium til lands, til sjøs og i luften. Et annet viktig felt er vern av det politiske styresettet, altså Norges demokratiske system og institusjoner. I tillegg kommer beskyttelse av andre viktige fysiske og digitale samfunnsstrukturer. Disse beskyttelsesverdige interessene er blant annet vernet gjennom straffelovens bestemmelser om vern av Norges selvstendighet og andre grunnleggende nasjonale interesser, samt bestemmelsene om straff for terrorhandlinger og terrorrelaterte handlinger (Evalueringsutvalget for Stortingets kontroll utvalg for etterretnings-, overvåkings- og sikkerhetstjeneste, 2016:33).