Russisk cybersabotasje -
Forsmak på fremtidens cyberkrig?

Per Einar Kroghrud

MASTEROPPGAVE

Institutt for sammenliknende politikk
Universitetet i Bergen
MAI 2019

Sammendrag

Denne oppgaven ser på hvordan russisk cybersabotasje har blitt gjennomført de siste 12 årene og i hvilken grad vi kan si at dette er en forsmak på fremtidens cyberkrigføring eller kjente aktive tiltak i nye rammer. Temaet er svært relevant for Norge på grunn av vår nærhet til Russland og at PST har sagt offentlig at andre lands etterretningstjenester har kartlagt norsk kritisk infrastruktur. Inter-statlige cyberkonflikter er fortsatt et relativt nytt fenomen og det er en pågående mellom forskere som mener cyberkrig aldri vil finne sted, og flere sikkerhetseksperter som mener verden kan vente seg et cyber-Pearl Harbour. Denne oppgaven redegjør for de to motstridende synspunktene gjennom å se på hvordan klassisk militærteori kan benyttes for å forstå cyberkrigføring. Her beskrives krig som enten 1) En voldelig, instrumentell handling med politisk målsetting eller 2) Som en utmattelseskrig hvor man kan oppnå sine politiske målsettinger gjennom andre midler enn militær makt. Sistnevnte er mer gjenkjennbart i hvordan konflikter har utspilt seg etter andre verdenskrig. Cyberoperasjoner og andre ikke-militære maktmidler er idag foretrukket da det er liten risiko og gode muligheter til å oppnå politiske målsettinger. Oppgaven viser hvordan dette synet samstemmer med russisk nasjonal sikkerhetsstrategi.

Videre gjennomgår oppgaven åtte caser med russisk cybersabotasje de siste 12 årene. Analysen av de åtte casene viser hvordan russisk cybersabotasje har gjennomgått en evolusjon. De første årene brukte Russland cybersabotasje som et virkemiddel eller avstraffelse i kanonbåtdiplomati. De siste 5 årene viser casene at russisk cybersabotasje har blitt mer avansert, målrettet og har hatt større konsekvenser enn tidligere. Til tross for dette så har syv av de åtte casene blitt gjennomført i Russlands nærområder, noe som indikerer at bruken av cybersabotasje ikke bryter med uttalt russisk sikkerhetsstrategi. Dette støtter delvis synspunktet til de som mener at cybersabotasje best forstås som tradisjonelle aktive tiltak som spionasje, sabotasje og påvirkning i ny form, noe Russland alltid har drevet med.

På den andre siden så blir en snever definisjon av krig som en voldelig, instrumentell og politisk handling analytisk begrensende og lite gjenkjennbart i hvordan konflikter har utspilt seg etter andre verdenskrig. Det er en evolusjon som viser stadig mer alvorlig russisk cybersabotasje og det er fortsatt manglende internasjonale normer og avtaler som regulerer

bruken av cyberoperasjoner. Cyberoperasjoner er derfor et effektivt virkemiddel for å destabilisere og redusere motstanderens politiske handlingsrom, samtidig som aktivitetene er under en terskel som rettferdiggjør NATO artikkel fem eller annen gjengjeldelse. Russisk cybersabotasje frem til nå gir derfor en pekepinn på hvordan russisk maktbruk i cyberdomenet vil bli utført i en fremtidig tilspisset konflikt.

Innholdsfortegnelse

1. Forkortelser

Attribusjon – Å fastslå identiteten og lokasjonen til angriperen eller angriperens mellommann

Cyberoperasjoner - bruken av cyberkapabiliteter med primærhensikt å oppnå målsettinger i eller ved bruk av cyberspace (CCDCOE 2017).

Cybersabotasje – et angrep via *cyberspace* som forårsaker skade, ødeleggelse eller forstyrrelser på informasjonsystemer og/eller digital og fysiske infrastruktur (Etterretningstjenesten 2019).

Cyberspionasje – aktivitet hvis formål er å innhente digitalt lagret, men ellers utilgjengelig informasjon (Etterretningstjenesten 2018).

Distributed Denial of Service Attack (DDoS) – Distribuert tjenestenekt angrep – et målrettet angrep mot et nettverk hvor det bombarderes med datapakker slik at legitim trafikk ikke slipper til. Slike tjenestenektangrep tar ofte i bruk tusenvis av infiserte datamaskiner eller enheter som er tilkoblet internett.

Påvirkningsoperasjoner – bruken av sosiale medier og nyhetsmedier til å undertrykke og manipulere virkelighetsoppfatningen gjennom fornektelse, villedning og desinformasjon (Etterretningstjenesten 2018).

Skadevare («*malware*») - benytter tekniske sårbarheter for å oppnå uautorisert tilgang og rettigheter til utstyret eller dataen den infiserer. Skadevare kan klassifiseres etter spredningsform, som virus, orm, bakdør eller trojansk hest. De kan også klassifiseres ut fra intensjon, som, løspengevirus, spionprogramvare og logiske bomber. Sistnevnte er skadevare som utløses ved en forhåndsbestemt hendelse i systemet eller på et bestemt tidspunkt (Lysne 2015).

2. Innledning

Denne oppgaven ser på hvordan russisk cybersabotasje har blitt gjennomført de siste 12 årene og i hvilken grad vi kan si at dette er en forsmak på fremtidens cyberkrigføring eller kjente aktive tiltak i nye rammer.

> "To immobilize a nation, to render it incapable of defending itself, attackers no longer need military, kinetic weapons. Nor do these same weapons offer us defence. Today this holds true theoretically. Nations continue to buy tanks and rockets, but there have been enough tabletop cyber conflict exercises as well as real incidents to know what is possible already now" (Ilves 2014).

Sitatet kommer fra en tale Toomas Hendrik Ilves, presidenten av Estland, holdt på München sikkerhetskonferanse 31. januar 2014. Ilves var også president da Estland i 2007 ble utsatt for et av de mest omfattende cyberangrepene verden da hadde sett. Hackere mistenkt å være tilknyttet russiske myndigheter stengte ned nettsidene til en rekke institusjoner som parlamentet, banker, departementer og aviser. Cyberangrepet mot Estland er et av mange eksempler på cyberoperasjoner hvor statlige aktører mistenkes for å stå bak. Statlige cyberoperasjoner har siden den gang utviklet seg til å være et strategisk virkemiddel. Dette ble eksemplifisert da dataviruset Stuxnet klarte å fysisk ødelegge Irans uransentrifuger for å sinke deres atomprogram og avsløringer vinteren 2017 om at amerikanske myndigheter skal ha gjennomført lignende operasjoner mot missilprogrammet til Nord-Korea (Sanger 2017). Samtidig har Russland de siste fem årene ført en mer aggressiv utenrikspolitikk og etter den russiske annekteringen av Krim og støtte til Assad i Syria, har blant annet FNs general-sekretær uttalt at vi er i en ny kald krig (Guterrres 2018). Operasjoner i cyberdomenet er blant de fremste asymmetriske maktmidlene Russland har tatt i bruk mot Vesten. Teknologi og kunnskap ment for å binde mennesker sammen og opplyse har blitt militarisert.

I løpet av de siste årene har det vært flere hendelser av cybersabotasje knyttet til Russland. Etterretningstjenesten skriver i sin årlige strategiske trusselvurdering at:

> "De siste årene er det observert flere tilfeller der digital sabotasje er testet i operasjoner mot europeiske land. Denne utprøvingen gjør metodene mer målrettede og anvendelige for framtidige operasjoner. Konsekvensene av denne typen angrep kan spenne fra mindre forstyrrelser til sammenbrudd av samfunnsviktige tjenester. Terskelen for å gjennom-føre dyptgripende, digital sabotasje er høy, fordi en slik operasjon kan oppfattes som en krigshandling, men veien fra evne til faktisk bruk har blitt kortere" (Etterretningstjenesten 2019:17).

For Norges del så er det spesielt frykten for at russisk cybersabotasje skal ramme kritisk infrastruktur. Utover at slike angrep kan påføre staten enorme økonomiske omkostninger og varige skader hos grunnleggende nasjonale interesser kan de også føre til tap av liv og helse på lik linje som et fysisk bombeangrep.

2.1. Oppgavens formål og problemstilling

Norske myndigheter har i økende grad satt fokus på de problemstillingene som oppstår etter hvert som vi stadig blir et mer digitalisert samfunn. Samtidig ser vi at stadig flere statlige aktører utvikler sine kapabiliteter til å drive både spionasje, sabotasje og påvirkning gjennom cyberdomenet. Inter-statlige cyberkonflikter er et relativt nytt fenomen og det er en pågående debatt mellom forskere og sikkerhetseksperter om i hvor stor grad operasjoner i det digitale rom endrer forutsetninger for krig og konflikt. På den ene siden har man de som venter på en cyberkrig og mener cyberoperasjoner kan revolusjonere måten stater bedriver krigføring på og at verden må forberede seg på at det vil komme et cyber-Pearl Harbor (Clarke og Knake 2012).

På den andre siden er det de som mener begrepet cyberkrig er unøyaktig og at vi aldri vil se en cyberkrig som andre har advart mot i en årrekke. Spørsmålet denne oppgaven skal svare på er:
I hvilken grad er 12 år med russisk cybersabotasje en forsmak på fremtidens cyberkrigføring?

Kjente hendelser av russisk cybersabotasje kan gi en pekepinn på hva som kan ramme norsk kritisk infrastruktur ved en fremtidig sikkerhetspolitisk krise. Oppgaven vil definere hva som

legges i begrepet cybersabotasje. Deretter hvordan cybersabotasje henger sammen med krigføring som definert i klassisk militærteori. Oppgaven vil deretter drøfte lover, normer og avtaler for å regulere cyberdomenet for å se om internasjonalt arbeid bidrar til å begrense bruk av cybersabotasje. Deretter gjennomgås hva russisk sikkerhetsstrategi og doktriner sier om bruk av cyberoperasjoner før åtte caser med russisk cybersabotasje vil gjennomgås. Til slutt identifiseres fellestrekk ved de åtte casene for å se om russisk cybersabotasje representerer noe nytt eller om det er i tråd med hvordan andre maktmidler brukes. Disse funnene vil til slutt bli drøftet opp mot de teoretiske funnene for å se om cybersabotasje er virkemiddel som viser ouverturene av hvordan fremtidens konflikter vil utspille seg.

2.2. Avgrensinger

Oppgaven avgrenser seg til cybersabotasje gjennomført av Russland eller statlig styrte russisktilknyttede grupperinger. Oppgaven vil ikke behandle påvirkningsoperasjoner som sabotasjeoperasjoner. Etterretningstjenesten beskriver påvirkningsoperasjoner som evnen til å bruke sosiale medier og nyhetsmedier til å manipulere virkelighetsoppfatningen gjennom fornektelse og desinformasjon. Målet er å diskreditere en stats myndigheter, forvirre befolkningen og eventuelt demoralisere militært personell. Den overordnede hensikten er å forme det strategiske handlingsrommet til egen fordel (Etterretningstjenesten 2018:32).

Påvirkningsoperasjoner kan grense opp mot sabotasje da det det saboterer politiske prosesser og tillit ved å enten plante og formidle falske historier til større befolkningsgrupper eller gjennomføre ensidige lekkasjer mot uønskede kandidater. Dagens teknologi gjør at stater kan konstruere alternative virkeligheter for aktører, publikum eller media. Overvåking av sosiale medier gjør at effekt kan måles og justeres i sanntid (Waltzman 2017). Russiske påvirkningsoperasjoner har vist seg spesielt effektive ved å kombinere manipulasjon av sosiale medier med strategiske utnyttelse av informasjon innhentet gjennom cyberspionasje. De russiske lekkasjene mot det demokratiske partiet før det amerikanske valget i 2016 er et godt eksempel på slik påvirkning. Således ligger påvirkningsoperasjoner tett opp mot spionasje da det er en mer indirekte tilnærming for å utforme en stats strategiske handlingsrom. Det er også et mykere maktinstrument enn direkte sabotasje av

informasjonssystemer eller kritiske samfunnsfunksjoner for å tvinge gjennom ønsket politikk. Påvirkningsoperasjoner vil derfor falle utenfor rammene rundt problemstillingen.

3. Cyberoperasjoner som virkemiddel

Oppgaven vil i dette kapittelet gjennomgå hva som legges i begrepet cyberoperasjoner, herunder hva det betyr, hvem gjennomfører det og en generisk beskrivelse av hvordan de gjennomføres. Grunnen til dette er at forståelsen, og derav begrepsbruken rundt cyberoperasjoner tidvis er upresis i media, blant forskere og blant politikere. Et datainnbrudd i en bedrift med svært dårlig cybersikkerhet hvor hensikten er å hente ut sensitiv informasjon blir beskrevet som et cyberangrep. En avansert skadevare som tok over to år å utvikle, hvis hensikt var å fysisk ødelegge sentrifuger brukt til uranutvinning blir også rapportert som cyberangrep. Disse to hendelsene blir sidestilt, selv om det er svært stor forskjell i kompleksitet, hensikt og ressurser bak operasjonene. Utredningen av begrepet cyberoperasjoner er derfor inkludert i litteraturgjennomgangen da det er et helt sentralt begrep for oppgaven. Det oppleves også at temaer rundt cyber enten er teknisk skrevet med tanke på et publikum utdannet i informasjonssikkerhet eller veldig abstraherte og skrevet for samfunnsvitere og et ikke-teknisk publikum. Begrepet cyberoperasjoner blir derfor utdypet for å skape en bedre grunnforståelse for resten av oppgaven og i større grad gjøre den mer lesbar for lesere med ikke-teknisk bakgrunn.

3.1. Hva er cyberoperasjoner?

I Williams Gibsons sci-fi klassiker Neuromancer beskrev han cyberspace som:

> "Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data" (1995:294).

Det er en betydelig overlapp i litteraturen om trusler i det digitale domenet. Direktoratet for Samfunnssikkerhet- og Beredskap utga i 2014 en risikoanalyse av cyberangrep mot EKOM-infrastruktur (2014). Lysne-utvalgets NOU-rapport fra 2015, Digital Sårbarhet - sikkert samfunn bruker begrepet IKT-trusler (2015) og Forsvarets Etterretningstjeneste bruker begrepet digitale trusler (2018). Denne oppgaven vil benytte begrepet cyber. Cyberbegrepet er mer internasjonalt og favner bedre bredden på tematikken, herunder nærliggende spørsmål av folkerettslig natur eller knyttet til normsetting og internasjonale avtaler (SOU 2015:23).

Begrepet cyberangrep er den mest brukte benevnelsen når stater eller kriminelle bryter seg inn i nettverk. Tallinn-manualene, som er det mest omfattende forsøket på å finne ut av hvordan dagens internasjonale lovverk bør appliseres til cyberoperasjoner beskriver cyberangrep som:

> "A cyber attack is a cyber operation, whether offensive or defensive that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (2013:415).

En systemsentrisk tilnærming definerer tre typer cyberangrep. De tre angrepene tar utgangspunkt i en grunnprinsipp i informasjonssikkerhet som kalles CIA-triaden (Confidentiality, Integrity, Availability) og mener at alle cyberangrep kan utledes basert på disse tre (Winterfeld og Andress 2012).

Konfidensialitet kan sidestilles med informasjonsvern. De fleste bedrifter og statlige etater har sensitiv informasjon som ikke bør være tilgjengelig for uvedkommende. Cyberangrep som kompromitterer konfidensialiteten knyttes vanligvis opp mot spionasje. Eksempelvis ble det internasjonale advokatfirmaet Mossack Fonseca utsatt for et datainnbrudd hvor over 11 millioner dokumenter ble lekket til flere utvalgte gravejournalister. Dokumentene viste hvordan et hundretalls politiske, økonomiske eliter rundt om i verden brukte offshore banker for å unngå skatt og skjule formuer (Harding 2016).

Integritet er tillit, nøyaktighet og et konsistent system. Har man automatiserte prosesser og algoritmer må man ha tillit til at svarene man får er riktige. Angrep mot integritet kan være

manipulasjon av data eller algoritmer og er ofte forbundet med sabotasje. Stuxnet-angrepet på Iran er et eksempel på hvordan manipulasjon av frekvenser på uraniumsentrifuger antageligvis satte det iranske atomprogrammet flere år tilbake (Zetter 2011).

Tilgjengelighet vil si at systemene, både hardware og software alltid er tilgjengelig. Et angrep mot tilgjengeligheten betyr at en angriper nekter brukeren tilgang til systemet, for eksempel via et DDoS-angrep (Perrin 2008) . Flere av casene gjennomgått i denne oppgaven er eksempel på hvordan sabotasje blir gjennomført ved å påvirke tilgjengeligheten til en eller flere systemer, som for eksempel Tv-kanalene til TV5 Monde som er et av casene denne oppgaven vil gjennomgå.

En systemsentrisk tilnærming er begrensende da den sier lite om trusselaktørens målsetting mot systemet som blir angrepet. Begrepet cyberoperasjoner passer derfor bedre som en overordnet kategori for å beskrive bruken av cybervirkemidler hvis hensikt er å oppnå målsettinger i det digitale rom. Forsvarets etterretningstjeneste deler digitale trusler inn i de tre kategoriene etterretningsoperasjoner (spionasje), påvirkningsoperasjoner og sabotasjeoperasjoner (Etterretningstjenesten 2019).

Etterretningsoperasjoner har til formål å innhente digitalt lagret, men ellers utilgjengelig informasjon, og utnytte denne i en systematisk bearbeidings-prosess. Etterretningsoperasjoner er i høy grad rettet mot politiske, militære, teknologiske og økonomiske mål i samsvar med nasjonalstatlige interesser. Påvirkningsoperasjoner vil si å bruke sosiale medier og nyhetsmedier til å undertrykke og manipulere virkelighetsoppfatningen gjennom fornektelse og desinformasjon. Målet vil være å diskreditere en stats myndigheter, forvirre befolkningen og eventuelt demoralisere militært personell. Den overordnede hensikten er å forme det strategiske handlingsrommet til egen fordel. Den russiske innblandingen i det amerikanske valget høsten 2016 er et eksempel på en påvirkningsoperasjon og ikke en sabotasjeoperasjon. Sabotasjeoperasjoner omfatter skade, ødeleggelse og forstyrrelser. Norge kan settes under press og tvang ved at fremmede stater retter trusler mot sivile mål som infrastruktur for elektrisk kraft, telekommunikasjon, transport og banktjenester. NUPI har blant annet gjennomgått hvordan norsk petroleumssektor kan utsettes for cybersabotasje av Russland

(Friis, Muller og Gjesvik 2018). På det militære området kan det rettes sabotasjehandlinger mot systemer for kommando og kontroll, kommunikasjon, navigasjon og overvåkning. Med dette som utgangspunkt blir begrepet cyberoperasjoner et sekkebegrep for å snakke generelt om trusler i det digitale rom og begrepene etterretningsoperasjoner, påvirkningsoperasjoner og sabotasjeoperasjoner for å beskrive aktørens aktivitet og hensikt. Disse begrepene gir en mer presis beskrivelse av aktiviteten som blir gjennomført og er et bedre rammeverk for å knytte det til geopolitiske interesser.

3.2. Hvem gjennomfører cyberoperasjoner?

Aktører som opererer i det digitale rom har økt kraftig de siste årene. De mest avanserte er de statlige aktørene, vanligvis tilknyttet staters etterretningstjenester. Statlige aktører har betydelige personell- og teknologiske ressurser og understøtter statens geopolitiske interesser og oppdrag som å forhindre trusler utenfra, støtte til militære operasjoner og spionasje. Russland er blant statene som har drevet lengst med cyberoperasjoner. Allerede i 1996 avdekket amerikanske FBI omfattende spionasje mot flere titalls organisasjoner inkludert forsvarssektoren, energisektoren og teknologiselskaper. Etterforskningen til FBI fikk navnet Moonlight Maze og ble attribuert til russiske styresmakter (Rid 2016). De siste årene har graderte dokumenter fra Moonlight Maze blitt sluppet og det er gjenfunnet kode fra Moonlight Maze-kampanjen til en fortsatt aktiv russisk cyberspionasjekampanje kalt Turla (Guerrero-Saade, Raiu, Moore og Rid 2017).

Man har også de ikke-statlige aktørene som kan være individer, grupper eller organisasjoner. Disse gjennomfører også politisk motiverte cyberoperasjoner, enten i samsvar med, eller mot statens geopolitiske interesser. Eksempler på ikke-statlige aktører kan være individuelle hackere som ser etter utfordringer, anarkistgrupper som Anonymous, patriotiske cyberkriminelle eller større kriminelle organisasjoner (Sigholm 2013). Denne oppgaven tar primært for seg statlige aktører, men vil også ta for seg statligstøttede eller statlig sponsede aktører, det vil si organiserte kriminelle som gjennomfører finansiell kriminalitet, men også hjelper sin respektive stat med cyberoperasjoner som spionasje og sabotasje (Geary 2017).

3.3. Hvordan gjennomføres en datainntrengning?

Blant faktorene som skiller cyberoperasjoner fra vanlige konvensjonelle militære eller etterretningsoperasjoner er det potensielle fraværet av tid og rom. En cyberoperasjon kan gjennomføres mot mål fra hele verden og det skjer i i løpet av millisekunder. En cyber operasjon består vanligvis syv faser (Hutchins, Cloppert og Amin 2011).

Reconnaissance – her blir det gjort undersøkelser for å identifisere og velge mål ved å for eksempel saumfare e-postlister, sosiale medier eller informasjon om spesielle teknologier.
Weaponization – Beskriver hvordan angriperen finner hvilken skadevare som skal brukes og finne ut hvordan den skal leveres, for eksempel gjennom et e-post vedlegg.
Delivery – beskriver hvordan skadevaren skal leveres, f.eks. gjennom en e-post, en nettside eller USB-minnepinne.
Exploitation – etter at skadevaren er levert til offeret blir den ondsinnede koden eksekvert på operativsystemet.
Installation – Når bakdøren eller fjerntilgangen er opprettet har angriperen nå mulighet til å ha fotfeste i systemet
Command and Control (C2) – Dette er infrastrukturen som den nå infiserte datamaskinen snakker med og tillater angriperen å ha 'hånden på keyboardet' i den infiserte klienten.
Actions on Objective – Det er her angriperen endelig kan oppnå sine mål. Videre handlinger kan være å bevege seg dypere inn i systemet for mer tilganger, data uthenting, manipulasjon av systemer eller ødeleggelse.

Disse stegene beskriver et datainnbrudd og enkelte av disse stegene kan ta sekunder, timer, uker, måneder eller år avhengig av hvor godt sikret nettverket de forsøker å bryte seg inn i er. Et annet moment er at helt frem til 'actions on objective' så kan det være svært vanskelig å skille en spionasje- og sabotasjeoperasjon.

3.4. Cybersabotasje

Cybersabotasje har til hensikt å skade, ødelegge, manipulere eller forstyrre et system, en prosess, infrastruktur eller fysiske komponenter. Problemstillingen spør om i hvilken grad 12

år med russisk cybersabotasje er en forsmak på fremtidens cyberkrigføring? Cybersabotasje er det som ligger nærmest krigshandlinger i form av ødeleggelser. En vellykket sabotasjeoperasjon kan ha logiske konsekvenser, som tap eller manipulasjon av data og verdier eller nedetid på systemer. Cybersabotasje kan også ha fysiske konsekvenser, som tap av strøm og ødeleggelse av utstyr og infrastruktur. Direktoratet for Samfunnssikkerhet og Beredskap anslo at cybersabotasje mot transportnettet til Telenor kan føre til minst 50 tapte liv og et direkte tap på flere titalls milliarder kroner (DSB 2014). Selv tjenestenektangrep mot betalingstjenester eller statlige nettsider begrenset til bare timer kan føre til økonomiske tap i millionklassen (Neustar 2015). Den mest kjente cybersabotasjen er Stuxnet. I 2010 ble det kjent at Irans atomprogram støtte på problemer. Et stort antall av deres sentrifuger ble ødelagt av en skadevare som ble kalt Stuxnet. Skadevaren gikk målrettet på det industrielle styringssystemet og endret frekvenshastigheten for sentrifugene som gjorde at de ble fysisk skadet. I etterkant har det kommet frem at Stuxnet ble utviklet av Israel og USA for å forsinke Irans atomprogram. Stuxnet er fortsatt en av de mest avanserte skadevarene som er oppdaget (Zetter 2011).

Sabotasjeoperasjoner varierer i kompleksitet og konsekvenser. Kompleksitet kan vurderes ut i fra faktorer som om operasjonen krever at man evner å bryte seg inn i systemene man skal ramme eller om man simpelthen forsøker å begrense tilgjengeligheten til tjenester som har et grensesnitt mot internett. Videre må det vurderes hvor skreddersydd en skadevare er til oppdraget den skal gjennomføre, og bruken av nulldagssårbarheter (tekniske sårbarheter i programvare som gir uautorisert aksess og som ikke er oppdaget av andre). Stuxnet tok anslagsvis 2-3 år å utvikle og skaperen måtte ha detaljkunnskap om Siemens industrielle styringssystemer som Iran brukte til å kontrollere sentrifugene sine (Lindsay 2013:380). Hvorvidt et angrep er sofistikert eller ikke avhenger av en rekke faktorer som om skadevaren er kjøpt eller lagd selv, nettverket de bruker til å kommunisere med, testing før operasjonen, hvor vedvarende den er og operasjonssikkerhet. Bruken av sofistikerte verktøy er alltid en avveiing mellom kostnader, effektivitet og hvor rettidig den er. Det er ikke noe poeng å bruke statens mest avanserte verktøy hvis det holder med å bruke noe som allerede er tilgjengelig på det åpne markedet (Buchanan 2017).

Distribuerte tjenestenektangrep er mindre komplekse, og skadeomfanget er i større grad midlertidig. Hensikten med et tjenestenektangrep er å forstyrre tilgjengeligheten til det gitte systemet i perioden hvor DDoS-angrepet foregår. DDoS var sabotasjemetoden for flere av casene som blir gjennomgått senere. For at angrepet skal være kraftig nok kreves det som oftest flere tusen infiserte datamaskiner. I dag er det profesjonelle kriminelle som livnærer seg av å selge slike tjenester. Crime-as-a-service har de siste årene tatt et kvantesprang og blitt høyst profesjonalisert. Personer kan kjøpe spionprogramvare eller DDoS mot en nettsiden man selv spesifiserer med standardiserte timepriser for hvor lenge det skal vedvare (Manky 2013).

Oppgaven har nå sett på hva som ligger i begrepet cyberoperasjoner, hvordan det gjennomføres og hva som kjennetegner en cybersabotasje. Videre har nyansene rundt forskjellige typer sabotasje og deres kompleksitet blitt belyst. Neste kapittel vil se på hvordan cybersabotasje henger sammen med cyberkrigføring.

4. Cyberkrigføring og klassisk militærteori

Problemstillingen til oppgaven er i hvilken grad 12 år med russisk cybersabotasje er en forsmak på fremtidens cyberkrigføring. For å svare på problemstillingen må det redegjøres hvordan cyberoperasjoner forstås gjennom klassisk militærteori og forståelsen av krig i det 21 århundre. Dette er nødvendig da det hersker uenig både i akademia og blant eksperter om hvordan cybersabotasje bør forstås. Potensialet i cyberkrigføring har vært gjenstand for debatt i lengre tid. Flere amerikanske offisielle tjenestemenn har advart mot et cyber Pearl Harbour, et omfattende cyberangrep mot amerikansk infrastruktur og kommunikasjonssystemer (Stone 2013). NATO har uttalt at cyberdomenet er et operasjonsdomene de kan krige i på lik linje med land, sjø og luft. Videre har NATO stadfestet at Cyberforsvar er en av kjerneoppgavene i det kollektive forsvaret og et omfattende cyberangrep kan utløse artikkel fem (NATO 2016).

Blant de som mener cyber revolusjonerer krigføring er det spesielt tre momenter som trekkes frem. For det første så reduserer cyberdomenet viktigheten av nasjonal territorium og grensekrysning. For det andre kan angrep skje umiddelbart og mot mål i hele verden. Til slutt

er målene for digitale trusler i større grad sivile enn det er for konvensjonelle maktmidler (Nye 2010). Andre går lengre og sammenligner potensiale i cyberkrigføring med utviklingen av atombomben, men der hvor stater idag har forutsigbare doktriner for bruk av atombomben, så mangler dette i cyberdomenet da staters faktiske kapasitet er gradert og hemmeligholdt. Doktriner og uttalelser til stormakter som USA, Russland og Kina er tvetydige på bruk av cyberkrigføring. Det gjør det vanskelig for motstandere på den internasjonale arenaen å kalkulere under hvilke omstendigheter slike kapabiliteter vil bli tatt i bruk og øker risikoen for strategiske feilvurderinger (Clarke et al. 2012).

4.1. Argument mot cyberkrig

På den andre siden er det de som mener cyberkrigføring ikke bringer noe nytt til bordet. De mener cyberkrigføring er et nytt strategisk virkemiddel med mange applikasjoner, men på ingen måte revolusjonerende (Mitchell 2013). Blant annet mangler det empiri på at cyberkrigføring endrer grunnleggende teorier om krigføring (Gray 2013). Blant de mer fremtrendende kritikerne er akademikeren Thomas Rid som i sin bok *'Cyberwar will not take place'* argumenterer for at begrepet cyberkrig har vært hemmende for en konstruktiv debatt om virkemidler i cyberdomenet. Han argumenterer for at vi sannsynligvis aldri vil se en reell cyberkrig. Han baserer denne påstanden på Clausewitz tre krav til krig: Det må innebære voldsbruk, handlingen må være instrumentell og det siste kravet er at krig støtter oppunder en politisk sluttilstand. Han er også fast på hendelser i cyberdomenet frem til boken ble skrevet i 2013 såvidt oppfylte ett av disse kravene og at det derfor ikke finnes empiri på at en cyberkrig som oppfyller alle tre kravene har skjedd i dag. Rid hevder videre at vi må slutte å bruke begrepet cyberkrig og heller snakke om cyberoperasjoner i rammen av det han kaller staters aktive tiltak, som er spionasje, sabotasje og subversjon (Rid 2013).

4.2.Clausewitz og cyberkrig

Clausewitz definerer krig som "War therefore is an act of violence intended to compel our opponent to fulfil our will" (Clausewitz 1982). Det er to perspektiver for hvordan Clausewitz beskriver krig, og som også legger føringer for hvordan man forstår cyberkrig. I den første tolkningen, som Rid legger til grunn, defineres krig som en voldelig handling, en krig er

instrumentell og en krig har en politisk målsetting. Clausewitz bruker begrepet treenigheten for å beskrive krigen som et samspill mellom hat og vold som en naturkraft, krigens sjansespill og krig som et politisk instrument som gir det fornuft. Det første aspektet omhandler folket hvis lidenskap og sinne må blusse opp i krig. Det andre aspektet er for generalen og hærstyrkene, mens det siste aspektet angår styresmaktene. Det finnes flere veier å nå målsettingen på, men Clausewitz er klar på at krig handler om å bruke fysisk makt for å tvinge motstanderen til sin vilje. Det er flere veier man kan bruke for å nå det politiske målet, men det eneste virkemiddelet er militære kamper for å frata motstanderen evnen til motstand og dermed også motstanderens politiske vilje. I overført betydning så vil cyberkrig i den første tolkningen forstås som handlinger som medfører død, bruken er instrumentell mot fiendens militære styrker og den understøtter politiske målsettinger (Clausewitz 1982).

Clausewitz trakk sine erfaringer fra landkriger på begynnelsen av 1800-tallet. På 1920-tallet argumenterte den italienske generalen Giulio Douhet for at luftmakt vil revolusjonere krig. Han mente at offensive luftoperasjoner kan fly forbi hærstyrkene og direkte angripe sivil infrastruktur. Douhet beskrev et hypotetisk fremtidsscenario:

> "How many bombing units would be needed to cut all rail communications between Piedmont and Liguria, and the rest of Italy, in a single day? How many bombing units would be needed to cut Rome off from all rail, telegraph, telephone, and radio communication, and to plunge the city itself into terror and confusion by the destruction of governing bodies, banks, and other public services in a single day" (2014)?

Douhet argumenterte med at ved å bombe infrastruktur bryter du ned befolkningens moral og de forsvarende myndigheter vil bli anklagd for angripernes luftangrep som igjen fører til populært opprør og politiske konsesjoner. Det er en gjenkjennbarhet i Douhets profetier om luftmakt og de som advarer om et cyber Pearl Harbour. Douhet tok feil om mye, spesielt hans spådommer om utviklingen av luftforsvar, men hans bok "Command of the Air" var en hjørnestein i Vestlig bruk av luftmakt de neste 50-60 årene, senest i amerikanske

bombekampanjer under Vietnamkrigen. Luftmakt erstattet ikke krig i andre domener, men det hadde stor påvirkning på hvordan krig gjennomføres idag.

Det har per dags dato ikke blitt gjennomført cybersabotasje som oppfyller de tre kravene til krig som Clausewitz legger til grunn. På den andre siden har det blitt oppdaget skadevare i kritisk infrastruktur. Et eksempel på slik hendelse er Triton som ble oppdaget i 2017. Triton er en antatt russisk skadevare utviklet av myndighetene som ble funnet i et petrokjemisk anlegg i Saudi-Arabia (FireEye 2018). Skadevaren forsøkte å manipulere sikkerhetsmekanismer for å enten tvinge anlegget til å stenge eller fysisk ødelegge det (Dragos 2017). Dette viser at cybersabotasje med en intensjon om å ramme infrastruktur for å påvirke politisk handlingsrom er mer enn bare en teoretisk mulighet. Slike hendelser resonnerer med hvordan Douhet så for seg at luftangrep kan ramme folket for å oppnå politiske målsettinger.

Det andre perspektivet ser på krig som en handling hvor man skaper forhold som bryter ned militærets, styresmaktens eller folkets vilje til å gjøre motstand. Clausewitz skisserer to strategier for å seire: Tilintetgjørelseskrig og utmattelseskrig. I en tilintetgjørelseskrig vil militær makt være eneste virkemiddelet man bruker, mens i en utmattelseskrig kan man oppnå sine politiske målsettinger med andre veier enn militær makt. Ved å svekke motstanderens vilje så vil de oppgi sin politiske sluttilstand uten kamp. Clausewitz beskrivelser av utmattelseskrig er mer gjenkjennbart i hvordan konflikter har utspilt seg etter andre verdenskrig. Utmattelsesstrategi slekter til en viss grad til det mange idag kaller hybridkrig, definert som evnen til å også benytte ikke-militær makt mot andre stater for å oppnå politiske målsettinger.

Det er to viktige grunner til at maktbruk med ikke-militære virkemidler har blitt mer fremtredende. For det første har det i løpet av tiår skjedd en endring i folkets apetitt for militære ødeleggelser og tap av liv.

> “Det vesentlige poeng er at det har inntruffet en endring i synet ikke bare på represalier overfor sivile og beskyttelse av ikke-stridende, men på aksepten for krigens

> materielle ødeleggelser og tap av liv generelt. Dette gjelder først og fremst den vestlige verden, men også i mer autoritære land gjør den samme trenden seg gjeldende" (Diesen 2018:14).

En konsekvens av en slik holdningsendring er at prisen styresmakter betaler for militær maktanvendelse er potensielt høy i form av folkelig støtte. Det fører til at maktbruk i større grad benytter seg av ikke-militære maktmidler for å oppnå politiske målsettinger. Med dette så har ett av beinene blitt snudd på hodet i Clausewitz treenighet om krig som et samspill mellom folket, militæret og styresmakter. Clausewitz beskrev folket som en pådriver for bruk av maktanvendelse mot statens motstandere, men idag er folket en begrensende faktor for bruk av militæret for å oppnå politiske målsettinger. Krig må derfor utkjempes, ikke bare på en instrumentell måte for å oppnå politiske målsettinger, men også på en begrensende måte for å sikre fortsatt politisk legitimitet i folket.

For det andre er begrepet krig utfordret sett opp mot hvordan nåtidens konflikter blir utkjempet.

> "While the West is largely stuck in an instrumentalist, technicist, battle-centric and kinetic understanding of war, its opponents have been busy redefining war. The lack of conceptual clarity is a problem for HW, but so is the lack of agreement on what war is, how its character is evolving, and what this means for distinctions between peace, conflict and war (Reichborn-Kjennerud og Cullen 2016).

Ved å erkjenne at NATO og USA er militært overlegne så har Russland forskjøvet hele konseptet krig og dermed endret premissene for hvordan man kan påføre motstanderen sin vilje. Clausewitz og kriteriet om voldsbruk i krig er derfor et lite hensiktsmessig rammeverk for å forstå cyberkrig og er utdatert, både på bakgrunn av hvordan konflikter utkjempes idag og ikke minst at NATO har sagt at et cyberangrep kan utløse artikkel fem.

For å konkludere så er det to perspektiver på cyberkrig. Det første perspektivet definerer krig som en voldelig og instrumentell handling med en politisk målsetting. Legger man en slik

definisjon til grunn har forskere som Thomas Rid rett i at cyberkrig enda ikke har funnet sted. På den andre siden så er slik bruk av cybersabotasje mer enn bare et teoretisk mulighetsrom. Cyberoperasjoner i et slik perspektiv kan sammenlignes med hvordan Douhet beskrev fremtidens luftmakt. Det tilførte krig en helt ny dimensjon, men det fjernet på ingen måte viktigheten av sjø og hærstyrker. Man kan derfor tenke seg at cyberoperasjoner også vil tilføre krig en ny dimensjon i større grad enn man har observert til nå. Cyberoperasjoner kan for eksempel være 'åpningsilden' i fremtidens krig hvor represaliene ikke nødvendigvis kommer i cyberdomenet.

Det andre perspektivet utfordrer definisjonen av krig som en voldelig, instrumentell handling med politisk målsetting. I Clausewitz mindre utviklede teorier finner man beskrivelsene av det Clausewitz kaller utmattelseskrig som er er mer gjenkjennbart i hvordan konflikter har utspilt seg etter andre verdenskrig. Utmattelseskrig slekter til en viss grad til det mange idag kaller hybridkrig, definert som evnen til å utøve militær, politisk og økonomisk makt synkronisert i tid mot andre stater for å oppnå politiske målsettinger. Dette har blant annet sammenheng med at befolkningens aksept for død og ødeleggelse er mindre enn den har vært tidligere, også i autoritære stater. Krig må derfor utkjempes på en begrensende måte så politisk ledelse ikke får folket i mot seg. Cyberoperasjoner og andre ikke-militære maktmidler er derfor foretrukket da det er liten risiko og gode muligheter til å oppnå politiske målsettinger.

4.3. Lover, normer og avtaler

De foregående kapitlene har sett på hvordan cybersabotasje defineres og hvordan det kan tolkes i Clausewitz teori om krig. Dette kapittelet skal se hvordan internasjonale lover, normsetting og eventuelt avtaler har regulert bruken av cyberoperasjoner. De første atombombene ble tatt i bruk mot Japan i 1945, men det var ikke før på 1960-tallet at 'Mutual Assured Destruction (MAD)'-doktrinen ble innført og skapte en maktbalanse mellom USA og Sovjetunionen. Perioden mellom 1945 og 1960-tallet kan sammenlignes med slik verden er i dag. Både de teoretiske og praktiske mulighetene i cyberkrigføring har blitt belyst, men det er fortsatt ikke etablert internasjonale normer for bruk av cybersabotasje. Det juridiske rammeverket for cyberoperasjoner er i stor grad uprøvd og kampen om hva som skal være

normen i cyberdomenet og hvordan nettet skal vernes er tilsynelatende fastlåst (Giles og Monaghan 2014).

På en side har man en Euro-Atlantisk konsensus gjennom NATO og EU, inkludert cybermakter som USA og Storbritannia. I denne blokken er det bred enighet om hva som bryter forbudet for maktbruk i internasjonale relasjoner og hva som utløser en stats rett til selvforsvar i væpnet konflikt. Det er også enighet rundt en rekke andre cyberhendelser som ikke når opp til terskelen om maktbruk og væpnet konflikt og legale standarder for attribusjon (CCDCOE 2017). Denne konsensusen reflekteres blant annet i begge utgavene av Tallinn-manualene, to akademisk ikke-bindende studier som samlet ledende juridiske forskere og eksperter for å se på hvordan eksisterende internasjonalt lovverk kan overføres til cyberoperasjoner. Tallinn-manualene har blitt akseptert av mange land, men fraværet av spesielt land som Russland og Kina bidrar til å svekke dokumentets kraft (Giles et al. 2014).

Russland ønsker ikke å slutte seg til dokumentet av flere grunner; for det første var det et initiativ fra NATO. Russland har uttalt at de ønsker å jobbe med regulering av cyberdomenet gjennom overgripende internasjonale organisasjoner som FN. Russland mener at dagens lovverk ikke holder mål. De øsnker blant annet å forby cyberkrig og ikke bare tolke handlinger i cyberdomenet i analogier gjennom folkeretten og FN-pakten. Russland mener det trengs en helt ny traktat for å gjennomføre dette. Vesten mener på sin side at eksisterende pakter, traktater og lovverk er tilfredsstillende for å regulere statlig aktivitet i cyberdomenet. For det andre så var det uenighet om innholdet. Russland ser på internett som primært et sikkerhetsanliggende og sekundært et verktøy for ytringsfrihet og økonomisk vekst. Som en konsekvens vurderer Russland ny teknologi og rollen til sosiale medier som en potensiell nasjonal sikkerhetstrussel. Dette er diametralt motsatt av Vesten hvor tilgang til internett anses som en grunnleggende menneskerett og en grunnmur for økonomisk vekst og velstand (Giles et al. 2014).

Til tross for uenigheter og stillstand rundt lovregulering av staters atferd i cyberdomenet, har arbeidet med å etablere normer kommet lengre. I 2015 kom andre konsensus-rapport fra FN hvor det enes om en rekke prinsipper vedrørende bruk av cybervirkemidler. Gruppen består av

15 medlemmer, inkludert nøkkelaktører i cyberdomenet og alle de permanente medlemmene fra FNs sikkerhetsråd som USA, Kina, Russland og England. Rapporten enes om at internasjonal lov som FN-pakten og internasjonal humanitærrett også gjelder i cyberdomenet. Videre enes det om noen 'kjøreregler' for bruk av offensive cybervirkemidler. Rapporten uttaler blant annet at land skal ikke angripe et annet lands kritiske infrastruktur og heller ikke nasjonale CERTer (Computer Emergency Response Teams). Rapporten definerer derimot ikke hva som kan betegnes som kritisk infrastruktur. I tillegg blir det beskrevet hva som skal til for å offisielt anklage en annen stat for cyberoperasjoner. Rapporten bemerker at bare det faktum at aktivitet ble utført eller kommer fra en stats territorium eller infrastruktur i seg selv ikke er nok til å attribuere den aktiviteten til staten. I forlengelse ble det også beskrevet at anklager om organisering eller implementering av ondsinnede handlinger mot stater må begrunnes (Minárik 2015).

Kjørereglene som har kommet ut av UN GGE arbeidet er ment å være norm-skapende, men er ikke bindende. UN GGE blir presset mellom to verdenssyn hvor USA, EU og fler argumenterer for et fortsatt fritt og åpent internett, mens den andre blokken med blant annet Kina og Russland ønsker sterkere grad av statlig kontroll. Som en konsekvens er det ingen reelle utsikter for å oppnå stormaktskonsensus om regulering av cyberdomenet.

> “Furthermore, the fact that the UN GGE has come to promote voluntary norms of behavior, testifies of no real prospect of consensus. Moscow likely regards the norms process as a stepping stone towards treaty negotiations, while for all countries with operational interests voluntary norms comfortably mean no meaningful restraint in the exercise of their ambitions”
> (Tikk og Kerttunen 2018).

På den ene siden har Russland vært en pådriver for å starte arbeidet med et nytt internasjonalt lovverk inkludert et forbud mot cyberkrig. Russland var også primus motor for konsensus-rapporten til UN GGE vedrørende normer i cyberdomenet. De premissgivende russiske cyberdoktrinene har vist hensyn til internasjonale lover og normer og Russland har alltid insistert på at internasjonale kriser skal håndteres av FNs sikkerhetsråd og være i tråd med

internasjonal lov, ikke fordi Russland alltid følger internasjonal lov, men som en svakere stormakt har de veto i rådet. Russland frykter også at USA kan handle på egenhånd utenfor FN-systemet i en unipolar verden. Russland har i alle år sett på sosiale medier og internetteknologi gjennom linsen til nasjonal sikkerhet og det er et poeng som stadig blir aktualisert. Russiske cyberdoktriner, innvendinger mot blant annet Tallinn-manualen og deres innspill til tidlige utkast av UN GGE konsensus-rapporten viser forsøk på å adressere dette innenrikshensynet og advart mot den potensielt destabiliserende effekten teknologi og mobilisering gjennom sosiale medier kan ha (Giles et al. 2014).

På den andre siden så viser empirien at statlig utviklet skadevare med hensikt å ødelegge hovedsakelig har russisk opphav. Det er observert flere brudd på de russiske forpliktelsene i rammen av UN GGE. Det er blant annet observert mulige russiske cyberoperasjoner som retter seg mot CERT-miljøer i blant annet Ukraina. Mulige årsaker er at myndighetene enten ignorer arbeidet som blir gjort i rammen av FN eller så er det en manglende grad av kontroll på statlige cyberoperasjoner (Labs 2017). Paradoksalt nok er det Russland gjennom sine påvirkningsoperasjoner mot blant annet det amerikanske valget i 2016 og franske valget i 2017 som har vist hvordan sosiale medier og plattformer som Twitter kan bli 'weaponized' for politiske målsettinger. I sum er det svært lite enighet om hvordan cyberdomenet skal reguleres og de få kjøreregelene man tilsynelatende har blitt enige om har blitt brutt ved flere tilfeller. Russiske myndigheter har i dag svært få juridiske eller normative begrensninger for å gjennomføre cybersabotasje (D'incau 2017).

5. Forskningsdesign og metode

Denne oppgaven er en kvalitativ studie som bruker triangulering og flercasestudie design for å se hva som kjennetegner russisk cybersabotasje og i hvilken grad det kan si noe om hvordan fremtidens krigføring vil se ut. Oppgaven har først avklart begrep og forståelsen rundt cyberoperasjoner som et statlig maktmiddel, og hvordan cyberkrig kan forstås gjennom Clausewitz militærteori (se Kap 4). Nå vil oppgaven se på hva russisk sikkerhetsstrategi sier om bruk av cyberoperasjoner. Oppgaven gjennomgår åtte caser av russisk cybersabotasje og sammenligner karakteristikkene geografi, metode og mål, antatt målsetting og konsekvenser.

Til slutt sammenlignes funnene med uttalt russisk sikkerhetsstrategi for å se om cybersabotasje blir brukt i forutsigbare rammer eller om det følger andre spilleregler.

5.1. Datainnsamling

Russiske cyberoperasjoner hvis formål er sabotasje og ødeleggelse er et fenomen som opptrer forholdsvis sjeldent og med stor grad av usikkerhet knyttet til attribusjon rundt de aktuelle hendelsene. I datainnsamlingen for oppgaven er det vektlagt bruk av kildetriangulering som kan defineres som bruken av flere kilder i kvalitativ forskning for å utvikle en helhetlig forståelse av et fenomen (Patton 1999). Kildetriangulering brukes for å oppnå en dypere forståelse for det aktuelle fenomenet som i dette tilfelle er russisk cybersabotasje. Det er ikke et verktøy eller en strategi for å validere data, men et alternativ til validering (Flick 2007:41). Kildetriangulering kan gjøres ved å sammenligne informasjon samlet inn med forskjellige metoder og på forskjellige tidspunkter (Denzin 2012). I denne oppgaven har for eksempel tekniske attribusjonsrapporter blitt sammenlignet med uttalelser fra myndigheter. Kildetriangulering er spesielt viktig når man ser på case studier da bruken av flere og varierte kilder skaper dybde og kvalitet i casene som gjennomgås (Creswell 1998).

Oppgaven har samlet inn data fra primært fire kilder; akademiske bøker og artikler, offisielle myndighetsdokumenter og avtaler, tekniske attribusjonsrapporter fra cybersikkerhetsselskaper og til slutt nyhetsartikler. Offisielle dokumenter og etterretningsrapporter brukes for å analysere staters offisielle standpunkt til bruk av maktmidler i cyberdomenet, status på internasjonale reguleringer av slike maktmidler og attribusjon knyttet til destruktive cyberangrep. Nyhetsartikler har blitt benyttet for flere formål. For det første har mye informasjon om de valgte casene kun vært tilgjengelige gjennom nyhetsartikler, og uttalelser fra politikere, forskere og sikkerhetseksperter har kun vært tilgjengelig gjennom media. Tekniske attribusjonsrapporter har blitt brukt for peke på hvilke aktører som har stått bak flere av angrepene i casestudiene. Disse rapportene gir nok åpen informasjon som gjør at man med større grad av sikkerhet kan vurdere empirien bak anklager mot stater som har gjennomført cybersabotasje. Tekniske attribusjonsrapporter er et godt supplement til myndighetsrapporter og nyhetsartikler da de presenterer betydelig mer empiri på hvorfor en gitt aktør sannsynligvis står bak cyberoperasjoner.

5.2.Kildekritikk

Det er viktig å være bevisst på skillet mellom førstehånds- og annenhåndskilder. En førstehåndskilde er originaldokumenter eller beskrivelser av noen som selv har sett eller hørt noe. En annenhåndskilde er beretninger om hva andre har sett eller hørt. Oppgaven behandler flere annenhåndskilder som primærkilder. Andre kilder som oppgaven bruker er private kilder, offentlige kilder og institusjonelle kilder. Hvilken kildetyper som blir brukt har betydning for kildens pålitelighet (Repstad 2007). Dokumentene brukt i denne oppgaven vurderes utifra fire kriterier; autensitet, troverdighet, representativitet og tolkning. Autensitet handler om hvorvidt man kan garantere at dokumentet er hva det utgir seg for å være, at det ikke er forfalsket eller plagiert. Troverdighet sier noe om vi kan stole på kilden som beretning. Dette er spesielt gjeldende for denne oppgaven da den har omfattende bruk av nyhetsartikler hvor journalistene har benyttet seg av konfidensielle kilder. Statlige operasjoner - både i og utenfor cyberdomenet er stort sett preget av hemmelighold og anonyme kilders beretninger er ofte eneste informasjonsgrunnlag i slike saker. Representativitet beskriver hvorvidt dokumentene brukt er dekkende for det oppgaven skal undersøke. Dette er spesielt relevant der hvor det referer til meningsbærende artikler og offisielle dokumenter som tar for seg temaer som nasjonal eller internasjonal regulering.

Til slutt vurderes kildene utifra tolkning. Med tolkning menes om dokumentet forstås i konteksten den er brukt. For eksempel er kildens opphav av betydning. Lover, forskrifter og NOUer kan ofte være normative kilder hvor forfatterens holdninger, intensjoner, krav og retningslinjer kommer til syne. Normative kilder er ikke rene beskrivelser av hvordan forholdene er eller var, men av kildens opphav. På den andre siden har man kognitive kilder hvor tekster er mer beskrivende og dermed gir et bedre innblikk i hvordan forholdene faktisk var. Det ene utelukker ikke det andre og flere kilder inneholder både normative og kognitive. I denne oppgaven vil for eksempel hendelse- og attribusjonsrapporter være mer beskrivende, mens NOUer og offisielle dokumenter være normative (Repstad 2007).

5.3.Case studie som metode

Robert K. Yin (Yin 2013:74) definerer casestudie som en empirisk undersøkelse om et kontemporært fenomen innenfor konteksten av pågående aktiviteter, og spesielt der hvor grensene mellom fenomen og kontekst ikke er klart. Yin med flere argumenterer for at casestudie og flercasestudie opererer under samme metodiske rammeverk og handler mer om hvilke type forskningsdesign du velger på oppgaven. I tillegg kan det argumenteres med at forskjellen på en singel casestudie og en flercasestudie er graden av dybde på undersøkelsene (Gerring 2007). Flercasestudie kan ofte gi en mer robust analyse ved å belyse likheter og begrensede ulikheter. Det styrker også den ytre validiteten på studien (Stavros og Westberg 2009).

Det er en generell oppfatning om at casestudier har begrenset verdi når hensikten er å generalisere og forklare. Flere mener casestudier kan mangle ytre validitet, det vil si i hvilken grad resultater fra studie er representative for en større populasjon (Gerring 2007:43). Dette gjelder spesielt empirisk representativitet. Teoretisk representativitet derimot bygger på overbevisende argumentasjon om hvordan empiriske hovedsammenhenger kan ses på som representative for begreper og forklaringsmekanismer (Andersen 2013:14).
Casestudiers største styrker er at slike studier oppnår en høy grad av indre validitet, det vil si i hvilken grad funnene stemmer med den teoretiske definisjonen. Indre validitet dreier seg om kvalitet og troverdigheten på studien. Kildetriangulering er en måte å sikre høy grad av indre validitet (Dahlum 2018).

5.4. Valg av Case

I kvantitative studier legges det vekt på at caser bør være tilfeldig utvalgt. I forskning med liten populasjon (n) vil en slik tilfeldig utvelging skape skjevheter og man må derfor benytte seg av ikke-tilfeldige caser (Levy 2008:8). Målsettingen i casevalg er derimot den samme som i tilfeldig utvalg. Det er ønskelig å finne representative utvalg med en nyttig variasjon i dimensjonene innenfor den teoretiske rammen. Det skilles mellom syv ulike casevalgteknikker: typiske, mangfoldige, ekstreme, avvikende, innflytelsesrike, mest lik og mest ulik (Seawright og Gerring 2008). Caseutvelgelsen for denne oppgaven passer til en viss

grad med *diverse case method*. Hensikten er å oppnå maksimal variasjon på relevante dimensjoner (geografi, målsettinger, mål & metode og konsekvenser). Caseutvelgelsen skal representere forskjellige verdier i casene. En slik undersøkelse kan være utforskende (hypotesesøkende) eller bekreftende hvor forskeren er mer opptatt av forholdet mellom verdiene. En slik caseutvelgelse kan også følge forskjellige kausale stier til hva som utløser utfallet man undersøker, i dette tilfelle hvorfor og hvordan ble cybersabotasjen gjennomført (Seawright et al. 2008).

Russisk cybersabotasje er et fenomen som har opptrådt sjeldent, og caseutvalget har derfor vært strategisk utvalgt basert på oppgavens tema, herunder forståelse for hva som utgjør sabotasje og det teoretiske rammeverket (Grønmo 2016:103). Samtlige kjente tilfeller av russisk cybersabotasje de siste 12 årene utgjør caseutvalget. Hva som utgjør cybersabotasje blir godt dekket i oppgaven og styrker derfor den analytiske kontrollen på oppgaven.
En utfordring i caseutvelgelsen for denne oppgaven har vært empirien om det er staten Russland som har gjennomført sabotasjen eller om det grupper uten tilknytning til statlige aktører.

5.5. Attribusjon

En vitenskapelig beskrivelse har minst tre elementer. For det første må man besvare om observasjonene er riktig i den forstand at uttalelser, handlinger og begivenheter som refereres faktisk stemmer. For det andre må man vurdere om det er gjort riktige avgrensninger mellom systematisk og ikke-systematisk variasjon; er observasjonene representative? Til slutt er det spørsmål om man kan trekke pålitelige slutninger fra observerbare til ikke-observerbare forhold (Andersen 2013:161). Casene er valgt utifra én eller flere av følgende kriterier: Hendelser der det er en bred offentlig enighet om hvem som står bak, basert på teknisk attribusjon, respektive lands myndigheter har vært ute og gjort attribusjon eller der den geopolitiske konteksten i stor grad indikerer hvem som står bak. Bakgrunnen for disse valgene knyttes til problemene rundt attribusjon.

Attribusjon har gjennom historien hatt en viktig rolle i store sikkerhetspolitiske hendelser. Fra rollen til den serbiske regjeringen i attentatet mot erkehertug Franz Ferdinand som utløste

første verdenskrig til forgiftningen av Sergei Skripal som førte til skarpe diplomatiske reaksjoner mot Russland. Tradisjonelt har det eksistert tre antagelser om attribusjon i cyberdomenet. For det første antas det at attribusjon i cyberdomenet er betydelig vanskeligere grunnet den underliggende tekniske arkitekturen og internetts geografi. For det andre er det en antagelse om at attribusjon er binært - enten vet man hvem det er eller så vet man ikke. Til slutt er det en antagelse om at utfordringen er å finne bevisene, ikke analysere, berike og presentere det (Rid og Buchanan 2015).
Disse antagelsene er upresise og attribusjon er hva enn stater gjør det til. Å matche en gjerning med en gjerningsmann er en øvelse i å redusere usikkerhet på flere nivåer. På et teknisk nivå handler det om å finne ut hvordan, fra verktøy som ble brukt til IP-adresser knyttet til gjerningen. På et operasjonelt nivå handler det om hva som har skjedd ved å mene mer om angrepets infrastruktur og profilen til gjerningspersonen. Til slutt har man det strategiske målet som er å finne ut hvem gjorde det og hvorfor.

For at casene kan anses som gyldige vitenskaplige beskrivelser må man vite at observasjonene er representative, altså var det russiske statlige eller statssponsede cyberoperasjoner? Casene må være riktig avgrenset - det kan ha vært cybersabotasje, men var det staten Russland som sto bak? Og til slutt om saken belyser en endring i bruk av russiske maktmidler. Casene er valgt ut i fra to argumenter: Det første er at nasjonale myndigheter er best egnet til å gjøre attribusjon. Det andre er hva man definerer som en statlig eller statssponset cyberoperasjon. På den ene siden er myndigheter med godt utviklede etterretningsorganisasjoner ofte bedre rustet til å gjøre attribusjon. Dette kommer av at de vanligvis gjennomfører flerkildeanalyse og kan derfor belyse hendelsen fra flere vinkler utover det tekniske. Tekniske spor og skadevare sier ofte lite om motivasjon, og på et høyere nivå kan andre etterretningskilder som telefonavlytting og menneskebasert innhenting belyse et mer helhetlig bilde. Slike kilder kan i større grad gi svar på hvem som har beordret eller organisert en operasjon. Myndigheter har derfor et mye bedre grunnlag enn selv de beste private cybersikkerhetsorganisasjonene til å attribuere hendelser (Rid et al. 2015).

På den andre siden kan attribusjon bli politisert og brukes for å fremme politiske agendaer. Denne problemstillingen er spesielt relevant da det er svært sjeldent at nasjonale myndigheter

slipper detaljert informasjon om attribusjonsprosessen. Det er flere grunnet til dette; blant annet kan offentliggjøring av informasjon knyttet til attribusjonen avsløre både kilder og metoder. Attribusjon blir derfor ofte formidlet med gyldighetsord, et veletablert begrep hos nasjonale etterretningstjenester for å kommunisere usikkerhet rundt saksomfanget (Rid et al. 2015:30). Det er derimot svært få hendelser hvor myndigheter har blitt tatt i løgn på attribusjon, Tvert om, så viser eksempler med lekkede myndighetsdokumenter troverdige bevis for sine påstander. Et eksempel på dette er hendelsene rundt russiske forsøk på å hacke programvare brukt i stemmetellingsmaskiner. I dette konkrete eksempelet viste en lekket gradert powerpoint hvordan individuelle ansatte i russisk militær etterretning har brukt sine egne telefonnumre og e-post adresser for å teste at falske e-post adresser som igjen blir brukt til såkalt spear-phishing, det vil si forsøk på å lure målene sine til å trykke på en link som leverer skadevare (Cole, Esposito, Biddle og Grim 2017).

Et annet problem er hva som utgjør en statlig cyberoperasjon. De siste årene har det blitt observert russisk-tilknyttede operasjoner fra minst fem aktør-kategorier. Den første kategorien er der hvor statlige etterretningstjenester gjennomfører operasjonene. Et eksempel på slike operasjoner er da antatt russisk militær etterretning sporet ukrainske artillerienheter gjennom en skreddersydd skadevare brukt av artillerioperatører (Crowdstrike 2016). I andre tilfeller er det freelancere eller kontraktører som tar oppdrag for staten (Bing 2017). I Russlands tilfelle vil dets adhockratistiske natur, hvor eliten er definert utifra tjenester de yter til Putin og ikke institusjonelle og sosiale identiteter, føre til at oligarker og maktpersoner kan stå bak cyberoperasjoner og påvirkningsoperasjoner. Slike operasjoner er justert til russiske målsettinger, men organisert utenfor myndighetsapparatet (Galeotti 2017).

Den tredje kategorien er tilfeller hvor Russland har gitt oppgaver til kriminelle som i utgangspunktet gjennomfører vinningskriminalitet til å spionere for Russland (Graff 2017). Slike enkeltstående oppgaver kan også innebære dirigering av tjenestenektangrep for sabotasjeformål. Den fjerde kategorien er der hvor russiske myndigheter ikke utover kontroll, men heller oppfordrer og veileder angrep fra ikke-statlige russiske aktører. I cyberangrepene mot Estland og Georgia (dekket i casene) er det tvil om i hvor stor grad hendelsene var koordinert, og hvor stor grad av kontroll myndighetene hadde på operasjonene. Til slutt er det

hendelser hvor russiske kriminelle og hackere har gjennomført operasjoner som er i tråd med Russisk politikk, men ikke koordinert og utenfor statens kontroll. Disse problemstillingene er gjeldende i caseutvalget til denne oppgaven, spesielt i hendelsene før 2014.

En statlig eller statlig sponset cyberoperasjon defineres som de cyberoperasjonene som har en minimum form av samhandling mellom staten og utøver. Statlige sponset vil derfor inkludere de operasjoner hvor staten utpeker mål eller på andre måte utøver en form for veiledning til de som gjennomfører angrepet. Det som da faller utenfor er cyberoperasjoner hvor det ikke er noen form for kommunikasjon eller samhandling mellom staten og utøver, selv om målene til utøveren samsvarer med statens økonomiske, politiske eller militære mål.

6. Russisk sikkerhetsstrategi

I Russlands nasjonale sikkerhetsstrategi defineres nasjonale interesser og prioriteringer, samt målsettinger og midler. Sentralt i strategien er Russlands behov for å ha en buffersone for å beskytte mot invasjoner eller andre eksterne forhold, spesielt mot Vesten. Dette gjøres ved å enten politisk eller militært kontrollere nærliggende områder og stater hvor de selv sier de har 'privilegerte interesser'. Dette innebærer blant annet Ukraina, Hviterussland, Georgia, Usbekistan og Kirgisistan (Facon 2017:21). Siden den russiske annekteringen av Krim i 2014 har det vært to motstridende syn på russisk sikkerhetsstrategi. Flere mener at Krim-invasjonen kom etter en mangeårig reformering av Russlands væpnede styrker som ble iverksatt etter Georgia-krigen i 2008. En del av denne transformasjonen her også vært å bedre synkronisere statens maktmidler. Krim-annekteringen var til dels en militær operasjon, men like viktig var de ikke-militære virkemidlene som ble tatt i bruk, som informasjonsoperasjoner, cyberoperasjoner og politisk press (Bruusgaard 2014). Russiske aktiviteter mot Ukraina var derfor summen av et Russland som har blitt mer utenrikspolitisk selvsikkert og i bedre stand til å synkronisere alle statens maktmidler, herunder cyberoperasjoner (Giles og Geers 2015).

Videre argumenterer denne siden med at Russland alltid har benyttet seg av ikke-militære virkemidler. Man bør derfor se tilbake i historien for å tolke russiske handlinger. Russiske aktiviteter i cyberdomenet er ikke noe nytt og revolusjonerende, men er det som tradisjonelt er kalt aktive tiltak, men med ny teknologi. Russland, og Sovjetunionen før det har alltid

forsøkt å bruke maktmidler og innflytelse for å forsterke kjente sårbarheter i et samfunn og støtte grupperinger med samsvarende målsettinger som Russland. En del av dette har vært bruk av etterretningstjenestene til å forme utfall i utlandet (McClintock og Radin 2017).

På den andre siden er det de som mener at Russland har operasjonalisert en ny sikkerhetsstrategi som kan beskrives som hybrid krigføring. Hybrid krigføring betegnes som integrasjonen av militære og ikke-militære maktmidler for å gjennomføre politiske målsettinger (Reichborn-Kjennerud et al. 2016). Vestlige eksperter snakker om hybrid krigføring som en doktrine og NATO snakker om det som et konsept de må evne å forsvare seg mot. En slik gråsonekonflikt beveger seg i sømmene mellom væpnet konflikt og fredstid. Gjennom annekteringen av Krim brukte Russland virkemidler som var over det man kan betegne som statlig konkurranse i fredstid, men virkemidlene som påvirkningsoperasjoner for å aktivere russisk nasjonalisme i Øst-Ukraina, 'små grønne menn' og utstedelse av nyvalg skapte nok usikkerhet til at det ikke utløste en stor militær reaksjon fra Ukraina eller NATO (Fitton 2016). Cyberoperasjoner var underordnet de andre virkemidlene, men ble mer synlig senere, noe som case oppgavene vil redegjøre for (Harašta og Míšek 2016).

NATOs generalsekretær Jens Stoltenberg sa i en tale før Warsawa-toppmøtet:

> "[..] Hybrid is the dark reflection of our comprehensive approach. We use a combination of military and non-military means to stabilize countries. Others use it to destabilize them. Of course, hybrid warfare is nothing new. It is as old as the Trojan horse. What is different is that the scale is bigger; the speed and intensity is higher; and that it takes place right at our borders" (Stoltenberg 2015).

Russlands hybride virkemidler har utfordret Vesten og NATO på minst tre områder; for det første skaper det usikkerhet. Russiske handlinger er godt under terskelen for artikkel fem. Det er tvetydighet i hendelsesforløp og hvem som står bak, som gir strategisk usikkerhet og sinker responstid. For det andre så er det vanskelig for NATO å avskrekke og dette reduserer NATOs innflytelse, spesielt i øst-Europa. NATO har ingen god avskrekking for påvirkningsoperasjoner mot befolkningen eller cyberoperasjoner nettopp fordi slike aktiviteter

er godt under terskelen for hva som rettferdiggjør væpnet respons og ikke minst artikkel fem. Til slutt så sliter Vesten med å navigere seg gjennom denne nye normen for krigføring da ledere i liberale demokratier må forholde seg til andre spilleregler enn Putin og russiske ledere som i stor grad kan fritt benytte seg av hardere maktmidler (Fitton 2016).

6.1.Russiske informasjonsoperasjoner

Der Vesten og NATO bruker ordet cyber for å beskrive aktivitet i det digitale rom, bruker Russland konsekvent begrepet informasjonsikkerhet. Russland mener informasjonssikkerhet belyser bredden av informasjon, hvorav cyber er en komponent i dette sammen med flere andre (Godwin III, Kulpim, Rauscher og Yaschenko 2014).
I russiske strategidokumenter påpekes det at informasjonskrigføring har blitt stadig mer intens og truslene mot både sosioøkonomisk utvikling og demokratiske institusjoner er økende. Russland mener selv at flere land er foran Russland i informasjonskrigføring og er eksplisitt i at ledende stater forsøker å dominere informasjonskrigføringen i både det militære, teknologiske og kulturelle domenet. Russisk militær doktrine sier:

> "Military conflict in the information space [voennyi konflikt v informatsionnom prostranstve] is a way to resolve conflicts between or within states by the use of information weapons. An information weapon [informatsionnoe oruzhie] is information technology, means and methods that are used in order to wage information war. Information war [informatsionnaia voina] is a struggle between two or more states in the information space with the goal to damage information systems, processes or resources, critical or other infrastructure, to undermine political, economic and social systems, to destabilise a society and a state by massive psychological influence on the population, and also putting pressure on a state to make decisions that are in the interest of the opponent" (Franke 2015).

Informasjonskrig kan derfor ramme alle sektorer, bade militære og ikke-militære i et samfunn. Videre er det en pågående diskusjon om hva informasjonskrig er og ikke er blant russiske militærteoretikere. Et aspekt de enes om er at informasjonskrigføring pågår kontinuerlig i rommet mellom krig og fred.

I fredstid er Russlands bruk av informasjonskrigføring relatert til sikring av samfunnet og myndighetsapparatet. Informasjonskrigføring blir gjennomført i skjul ved hjelp av etterretning, politikk og psykologiske operasjoner. På inter-statlig nivå involverer dette diplomatiske og økonomiske tiltak. Cyberoperasjoner som bruk av skadevare og datainntrengning er viktig for å kompromittere informasjonssystemer, samt utvikle og teste egne informasjonsvåpen (Heickerö 2010).

Oppsummert så var annekteringen av Krim-halvøya konsekvent med russisk nasjonal sikkerhetsstrategi og uavhengig om det var operasjonaliseringen av en ny doktrine eller en moderniseringen av tidligere doktriner så må det anses som en suksess. Bruken av russiske militære, cybersabotasje, påvirkningsoperasjoner, støtte til opprørerne og hendelser som stengingen av Kertsjstredet er aktiviteter som best forstås gjennom Clausewitz forståelse av utmattelseskrig, hvor Russland gjennom både militære og ikke-militære virkemidler rammer økonomien, befolkningen og styresmakter for å redusere ukrainsk handlingsrom og hindre en dreining mot Vesten. NATO har begynt å tenke nytt på hvordan de skal møte en motstander som setter mindre stater under press med maktmidler som ikke rettferdiggjøre væpnet respons, men som allikevel rammer politisk beslutningtaging. Dette vil være gjeldende så lenge det ikke er etablert konstruktivt internasjonalt samarbeid rundt regulering av cyberoperasjoner, det vil si cyberoperasjoner har per tid ikke hatt konsekvenser for Russland, og andre stater ikke har kommet opp med et effektivt respons for å møte spionasje og sabotasjeoperasjoner.

6.2.Russiske Cyberaktører

Det er fire kjente organisasjoner som gjennomfører cyberoperasjoner. Det er den militære etterretningen (GRU), Den føderale sikkerhetstjenesten (FSB), Den føderale beskyttelsestjenesten (FSO) og den utenlandske etterretningstjenesten (SVR). GRU er tilknyttet forsvarsdepartementet og de tre sistnevnte rapporterer alle til Presidentens kontor (Heickerö 2010).

FSB er den største etterretningsorganisasjonen i Russland, både i antall ansatte og arbeidsoppgaver og det nærmeste man kommer en arvtager til KGB. FSBs primære oppgaver er politisk sikkerhet, anti-terror og håndtering av dissidenter. I utgangspunktet er de en innenrikstjeneste, men har ansvar for noe utenlandsaktivitet i nærområdet og mot spesielle russiske interesser. (Galeotti 2016).

FSB er antatt å være bak kampanjer knyttet til Turla, Snake og Uroburos. De tre navnene representerer samme trusselaktør, men får ulike navn basert på hvilke cybersikkerhetsselskap som har oppdaget konkrete kampanjer de har gjennomført (Alperovitch 2016). Kjente mål er blant annet Vestlige myndigheter og departementer, politiske tenketanker, organisasjoner tilknyttet tsjetsjensk ekstremisme og andre (F-Secure 2015). Aktørens operasjoner er ansett å være både sofistikerte og svært målrettet. Aktøren går langt i å forsøke å skjule seg, blant annet ved omfattende bruk av kryptert trafikk og anti-deteksjonsmekanismer (FireEye 2015). FSB er primært tilknyttet cyberspionasjeoperasjoner. Det vil si de bryter seg inn og henter ut data som senere blir gått gjennom når de er trygt lagret på egne systemer.

SVR har det overordnede ansvaret for Russlands utenlandsetterretning. Primærfunksjonen til SVR er å gi beslutningsstøtte til President Putin og myndighetene gjennom innsamling og analyse av utenlandsetterretning. SVR samler inn på temaer som politikk, økonomi, forsvar, forskning og teknologi. SVR har tradisjonelt drevet menneskebasert innhenting, men har utviklet kapasitet for strategisk signaletterretning og antas å gjennomføre cyberoperasjoner. Aktører som APT29, The Dukes og Cozy Bear er alle knyttet til SVR. Denne organisasjonen gjennomførte senest i vinteren 2017 spionasjeforsøk mot norske mål som Utenriksdepartementet, Forsvaret, Arbeiderpartiet, PST og Statens strålevern (Persen, Talsnes, Østby, Bogen og Sørsdahl 2017). SVR har primært gjennomført spionasje og er ikke kjent for å gjennomføre sabotasjeoperasjoner. (Välisluureamet 2019).

GRU er den militære etterretningen med ansvar for innsamling av informasjon relater til militær-politiske og militær-økonomiske spørsmål. GRU besitter en rekke sensorer for informasjonsinnsamling inkludert cyberoperasjoner. GRU innsamler utenlandsetteretning på lik linje med både SVR og FSB. GRU har tilstedeværelse på de aller fleste russiske

ambassader. Gitt den militære bakgrunnen til GRU betegnes den som mer aggressiv og risikovillig enn FSB og SVR. GRU har en grad av operasjonell autonomi og sjefen kan ofte hendvende seg direkte til Presidenten (Galeotti 2016). I cyberdomenet er GRU kjent som blant annet APT28, Fancybear og Sofacy (NCCIS 2016). GRU har gjennomført cyberoperasjoner mot blant annet det norske Forsvaret, Verdensbanken, EU kommisjonen, Forsvarsministerier i Georgia og Øst-Europa, NATO og OSCE (FireEye 2014).

APT28 og GRU sine cyberoperasjoner ble for alvor kjent da omfanget av russiske datainnbrudd og påfølgende påvirkningsoperasjoner mot det amerikanske presidentvalget i 2016 fikk stor internasjonal mediedekning (Alperovitch 2016). I etterkant av valget utviste USA 35 russiske diplomater for deres rolle i operasjonen. De 35 diplomatene var etterretningspersonell fra GRU og FSB. I tillegg påla USA sanksjoner på de to russiske etterretningstjenestene, samt fire navngitte offiserer i GRU, et tydelig tegn på hvem USA mente var ansvarlig for den russiske innblandingen i valget (Gambino, Siddiqui og Walker 2016). Andre kjente cyberoperasjoner gjennomført av GRU siste året er datainnbruddet og lekkasjene fra anti-dopingsbyrået WADA, tyske bundestag, dissidentgruppen Pussy Riot og TV5Monde i Frankrike (FireEye 2017).

I motsetning til KGB i Sovjet-tiden hvor alle oppgaver var samlet i en organisasjon, har Russland i større grad desentralisert og fragmentert statens sikkerhetsoppgaver. Som en konsekvens har etterretningsbyråene en rekke overlappende ansvarsområder, men mangler samkjøring i oppgaver, samhold og er preget av konkurranse og konflikt. Frykten for å være irrelevant og miste budsjettmidler har ført til at byråene er både aggressive, fantasifulle og viser en stor grad av innovasjon i sine operasjoner (Galeotti 2016). Spesielt GRU som er en del av militæret har vist vilje til aggressive og til dels synlige operasjoner. Siden GRU ble hovedsakelig rammet sanksjonene til USA i etterkant av valginnblandingen, antas det at de var tungt involvert i datainnbruddet til demokratene og de påfølgende lekkasjene. Da det private sikkerhetsselskapet Crowdstrike gjorde analyse av datainnbruddet i DNC-serverne fant de spor av både FSB og GRU. Det var ingenting som tyder på at de visste om hverandre og står som et konkret eksempel på manglende koordinering og innbyrdes konkurranse (Alperovitch 2016).

7. Åtte caser med russisk cybersabotasje

Problemstillingen til oppgaven er *I hvilken grad er 12 år med russisk cybersabotasje en forsmak på fremtidens cyberkrigføring?* Oppgaven har drøftet begrepet cyberoperasjoner og videre hvordan cybersabotasje defineres. Deretter ble det gjennomgått hvordan cybersabotasje kan forstås som en krigshandling gjennom Clausewitz teori om krig. Videre har vi sett på hvordan internasjonale lover, sammen med russisk nasjonal sikkerhetsstrategi og bruk av informasjonsoperasjoner, legger rammene for russisk bruk av cybersabotasje. Til slutt har oppgaven gjennomgått hvilke russiske etterretningsbyråer som gjennomfører cyberoperasjoner.

Dette kapittelet vil gå gjennom åtte caser med russisk cybersabotasje. De åtte casene er de analytiske enhetene som danner grunnlaget for neste kapittel som analyserer fellestrekkene til de åtte casene. Hver case holder samme struktur og går gjennom historisk relasjon mellom den rammede staten og Russland, opptakten til handlingen, gjennomføringen av cybersabotasjen og konsekvensene av handlingene. Utvelgingen av casene er beskrevet i metodekapittelet. I begrepsavklaringen rundt cyberoperasjoner vises det hvorfor russisk innblanding i det amerikanske valget i 2016 ikke inngår i caseutvalget for denne oppgaven. I tillegg er skadevaren kalt Triton ikke tatt med da det hersker for stor usikkerhet rundt hvilken statlig aktør som står bak utviklingen og leveransen av Triton.

7.1. Estland 2007 - Konflikten om krigsminnesmerket

Estland fikk sin uavhengighet fra Russland i 1918, men ble tvunget tilbake til Sovjetunionen i 1940 og frem til 1991 da de fikk sin uavhengighet. Estland har 1.3 millioner innbyggere hvorav ca. 25 prosent er etnisk russere (CIA 2017). Mange i Estland så på den russiske tilstedeværelsen som ulovlig og den medførte vilkårlige henrettelser, massedeportasjoner og tvungne omplasseringer. Russere på sin side mener Sovjetunionen reddet Estland fra Nazi-Tyskland og ser på Estlendere som utakknemlige. Disse spenningene er i stor grad til stede i dag og påvirker personlige forhold og politisk samhandling både internt i Estland, men også i

forholdet mellom Russland og Estland (Vesilind, Tusty og Tusty 2008). I april 2007 bestemte estiske myndigheter at de skulle re-lokalisere et sovjetisk krigsminnesmerke i Tallinn. Den sovjetiske bronsesoldaten hedret sovjetiske soldater som ble drept i andre verdenskrig. Monumentet ble også brukt som et samlingspunkt for etniske russere som ønsket å demonstrere mot styresmakten. Beslutningen fra myndighetene var derfor å plassere monumentet til et sted mindre sjenerende for offentligheten. Beslutningen førte til opptøyer i Tallinn i slutten av april (Davis 2007).

Kort tid etter opptøyene startet, begynte myndighetene å registrere økt ondsinnet cyberaktivitet. Aktiviteten kan deles inn i to kategorier. For det første var det flere tilfeller av 'web defacement', altså skadeverk på nettsidene til myndigheter og media. For det andre ble det gjennomført omfattende DDoS-angrep mot store deler av landets infrastruktur. De største avissidene ble overlastet med trafikk fra botnets og gjort utilgjengelig. Det samme ble banktjenester, myndighetssider, tele- og internettilbydere. Angrepene hadde en betydelig effekt på Estland, et land som da hadde kommet langt i digitaliseringen (Davis 2007). Utenriksministeren har uttalt at angrepene kom fra offisielle IP-adresser knyttet til russiske myndigheter, og rammet mobilnettet og nødnettet som i verste fall kunne kostet liv (Bright 2007). I 2007 var evnen til å gjøre attribusjon umoden i forhold til dagens kapabiliteter. IP-opphav trenger ikke indikere staten som står bak, men på den andre siden kan det være attribusjon som estiske myndigheter ikke ønsker å gå ut med, men som de besitter. I tillegg er evnen til å slå ut nødnett og mobilnett mer avansert enn den gjennomsnittlige patriotiske hacker og kan tyde på at angrepet var til dels koordinert, støttet av russiske myndigheter.

7.2. Litauen 2008 - forbud mot kommunistsymboler

På lik linje med Estland var Litauen en del av Sovjetunionen frem til 1991. Landet består av 2.7 millioner innbyggere og i underkant av fem prosent er etnisk russere (CIA 2016). I motsetning til Latvia og Estland var det svært lite russisk immigrasjon til Litauen. Russland og Litauen hadde også løst sin grenseoppgang i 1999, mens i Latvia og Estland var det fortsatt uenigheter om grenseoppganger. På 2000-tallet var det flere tilfeller av konflikt mellom Litauen og Russland. Blant stridsspørsmålene var russisk kompensasjon til litauiske ofre for

arbeidsleirer, russisk bruk av energi som pressmiddel for politiske formål og Litauen som blokkerte prat om EU-Russland partnerskap.

I juni 2008 ble et litauisk lovforslag godkjent som forbydde bruken av sovjetiske kommunistsymboler. Bare tre dager etterpå ble over 300 websider angrepet. Angrepene var en blanding av DDoS og skadeverk på nettsidene. I forkant av lovforslaget hadde forholdet mellom Litauen og Russland forverret seg. Både nettsidene til regjeringspartiet, etikkrådet og finanstilsynet var blant de som ble rammet (Alexander 2014).

7.3. Georgia 2008 - Russisk invasjon

Georgia fikk sin uavhengighet etter at Sovjetunionen kollapset. Georgia har rundt 3.7 millioner innbyggere. Forholdet mellom Russland og Georgia har vært anspent helt siden rose-revolusjonen i 2003 som så Mikheil Saakasjvili valgt til President. Saakasjvili forsøkte å tilnærme seg Europa og Vesten, samt reintegrere de to utbryterrepublikkene Sør-Ossetia og Abkhazia. De to republikkene er støttet av Russland. Den 7. august 2008 invaderte Russland Sør-Ossetia etter at Georgia ble provosert til å gjennomføre sine egne militære operasjoner. I ukene før hadde Georgia allerede blitt utsatt for DDoS-angrep mot internettinfrastrukturen og nettsidene til Presidenten. Sikkerhetseksperter hadde i forkant av de væpnede kampene sett aktiveringen av minst seks botnet som senere ble brukt da russiske styrker invaderte Georgia (Markoff 2008).

Da kampene pågikk i perioden 7-10 august opplevde Georgia omfattende cybersabotasje i form av skadeverk på nettsider (web defacement) og DDoS-angrep. DDoS-angrepene gjorde finansielle institusjoner, forretninger, utdanningsinstitusjoner, media og myndighetssider utilgjengelige. Da kampene var på sitt mest intensive var myndighetene ute av stand til å kommunisere effektivt med omverden via internett. I tillegg ble serverne til presidentkontoret og utenriksdepartementet bombardert med tusenvis av e-poster og telefonnettet fungerte ikke normalt. I sum ble myndighetene og media i Georgia hindret i å kommunisere effektivt med omverdenen og egen befolkning fikk heller ikke den informasjonen de hadde behov for da russiske bombetokt ble gjennomført i en rekke georgiske byer. Russland hadde bedre kontroll

på informasjonsdomenet og kunne fremme sin versjon av hendelsesforløpet mens de effektivt hindret Georgia i å fortelle sin (Markoff 2008).

Timer etter invasjonen ble det blant annet opprettet en nettside som het StopGeorgia.ru hvor russiske hackere la ut programvare, sårbarheter og instruksjoner for hvordan DDoS kan gjennomføres i tillegg til mållister på nettsider som bør angripes (Economist 2008). Det har også blitt funnet beviser for at botnettene brukt i angrepene er tilknyttet en kriminell organisasjon som kalte seg Russian Business Network (R.B.N.) Gruppen har blitt knyttet til digital kriminalitet som barnepornografi, ID-tyveri, søppelpost og annen skadevare. R.B.N. startet som en internett-tjenesteleverandør (ISP), men er i dag en multinasjonal kriminell organisasjon. R.B.N. får lov å operere av russiske myndigheter da de av og til gjennomfører oppdrag som er i tråd med russiske nasjonale interesser som angrepene mot både Georgia og Kirgisistan (Bradbury 2009). Sikkerhetseksperter som gjennomgikk hendelsene beskriver et klart definert toppstyrt hierarki av profesjonelle hackere som instruerte mållistene og instruksjonene til noviser som gjennomførte de faktiske angrepene (Krebs 2008).

7.4. Kirgisistan 2009 - Kontraktsforlengelse av en amerikansk flybase

Kirgisistan var en del av Sovjetunionen frem til de fikk sin uavhengighet i 1991. Landet består av rundt 5.7 millioner innbyggere hvor av seks prosent er etnisk russere. I 2005 brøt det ut protester mot sittende president Askar Akaev etter parlamentsvalget og han flyktet til Russland i tulipan-revolusjonen (Economist 2005). Politisk uro vedvarte under Kurmanbek Bakijev og de neste fem årene var preget av omfattende protester. Disse protestene vedvarte frem til 2010 da Bakijev ble nødt til å flykte landet sammen med sin familie og levere sin avskjed fra eksil (Collins 2011).

De to siste årene av Bakijevs regime var preget av en betydelig forverring i forholdet mellom Russland og Kirgisistan. Et av de sentrale temaene var kontroll over energiressursene i sentral-Asia. Russland opplevde at kontroll over naturressurser og eksporten gradvis ble dårligere i lys av vestlige og kinesiske investeringer. I tillegg forsøkte flere av de sentral-Asiatiske statene å føre en uavhengig utenrikspolitikk hvor de i større grad balanserte Østen og Vesten. Russland ga lovnader om milliardlån for bygging av en kraftstasjon og for at

Kirgisistan ikke skulle forlenge kontrakten med USA om bruk av flybasen i Manas som ble brukt som transitt- og logistikkbase for operasjonene i Afghanistan (Muzalevsky 2010).

Den amerikanske flybasen i Manas ble opprettet i 2001 som det primære logistikkknutepunktet for amerikanske militære styrker og materiell som roterte inn eller ut av Afghanistan. Kina og Russland var hele tiden ukomfortable med amerikansk tilstedeværelse i Kirgisistan og forsøkte å få Bakijev til å stenge basen (Sershen 2006). I perioden 18. Januar 2009 til månedsskiftet januar/februar ble Kirgisistan rammet av av omfattende distribuert tjenestenektangrep (DDoS) mot landets infrastruktur. Halvparten av landets internettilbydere ble påvirket og enkelte rapporterte at opp til 80 prosent av internettrafikken mot Vesten ble stoppet (Bradbury 2009). I januar 2009 dro Bakijev til Moskva for bilaterale samtaler med daværende President Medvedev.

Den 3. Februar annonserte Bakijev fra Moskva at kontrakten mellom USA og Kirgisistan om leie av flybasen ikke ville bli forlenget. I tillegg fikk Kirgisistan lovnader fra Russland om milliardlån til bygging av en kraftstasjon. Spillet om den amerikanske flybasen i Kirgisistan var et eksempel på Russlands evne til å spille på alle statens maktmidler for å overtale Bakijev til å redusere amerikansk tilstedeværelse i Kirgisistan. Bakijev ble lovet milliardlån for økonomisk utvikling hvis kontrakten med USA ikke ble forlenget. For å understreke dette ble store deler av landets digitale infrastruktur rammet. Hensikten var både vise at Russland har andre virkemidler å spille på, men også undertrykke vestlige informasjonskanaler innad Kirgisistan mens forhandlingene og toppmøtet ble forberedt og pågikk (Wilson III 2008).

7.5. Ukraina - Testområde for cybersabotasje

Ukraina har ca. 42 millioner innbyggere hvorav ca. 17 prosent er av russisk etnisitet. Sentral-, og Vest-Ukraina består hovedsakelig av Ukrainere mens Sør, - og Øst-Ukraina, inkludert Krim består hovedsakelig av Ukrainere med russisk etnisitet (CIA 2014). Forholdet mellom Ukraina og Russland ble drastisk forverret vinteren 2014 da den pro-russiske presidenten Viktor Janukovitsj måtte flykte fra landet etter måneder med massive demonstrasjoner i Kiev. Demonstrasjonene kom som følge av Janukovitsj ønske om å skrinlegge samarbeidsavtalene mellom EU og Ukraina for å heller tilnærme seg Russland.

I februar 2014 okkuperte Russland Krim og erklærte seg uavhengige etter et referendum som gikk gjennom med 98 prosent av stemmene. Samtidig begynte grupper å bevæpne seg i de østlige provinsene Donetsk og Luhansk. I løpet av høsten 2014 var østlige-Ukraina i en borgerkrigslignende tilstand, tungt støttet av russiske militære inkludert høy-teknologisk utstyr som rakettkastere, anti-luftskyts og stridsvogner (Coffey og Kochis 2016). Russiske handlinger på Krim og i Øst-Ukraina dro Russland og Vesten tilbake i noe som ligner på en ny kald krig. Parallelt med disse hendelsene har det vært omfattende aktivitet i cyberdomenet. Allerede i november, før Janukovitsj forlot Ukraina, begynte pro-russiske hackere å undergrave pro-europeiske ukrainere. Aktiviteten besto hovedsakelig av DDoS-angrep mot nettsider kritiske til Janukovitsj-regjeringens forhold til Russland (Maurer og Janz 2014). Det er tre hendelser som utmerket seg spesielt i perioden frem til idag.

7.6. Ukraina 2014 - Villedning knyttet til presidentvalget

I 2013 brøt det ut massive demonstrasjoner i Kiev etter at daværende President Viktor Janukovytsj sa nei til en handelsavtale med EU og heller tilnærmet seg Russland. Janukovytsj signerte en avtale med opposisjonen om nyvalg før han flyktet til Russland. Med Presidenten ute av landet ble det arrangert nytt presidentvalg den 21 mai 2014. I månedene før valget hadde russiske styrker annektert Krim og innledet et væpnet opprør i de østlige ukrainske provinsene. Den uavhengige kandidaten Petro Poroshenko og politikeren Julija Tymosjenko sto frem som de klare favorittene hvor til slutt Poroshenko vant med 54.7 prosent av stemmene.

I forkant av valget klarte hackere å kompromittere den sentrale valgkommisjonens kjernenoder i nettverket. Som en konsekvens tok det 20 timer før programvaren som etter planen skulle gi en sanntidsoppdatering av valgresultatet begynte å fungere igjen. På valgdagen, 12 minutter før stengingen av valglokalene, annonserte hackere på nettsiden til valgkommisjonen at Ukraina Høyre Sektor-leder Dmitry Yarosh hadde vunnet valget, bilder som umiddelbart ble gjengitt på russiske TV-kanaler (Harašta et al. 2016)

7.7. Ukraina 2015 - Cybersabotasje av kraftsektoren

Den 23 desember 2015 rapporterte ukrainske Kyivoblenergo, et regionalt kraftselskap, om et strømbrudd som følge av cybersabotasje. Syv store og 23 mindre kraftstasjoner var frakoblet i rundt tre timer. Cyberoperasjonen skal ha også ha påvirket andre deler av kraftnettet og tvang operatørene til å bytte til manuell modus. Tre kraftselskaper ble rammet og rundt 225.000 kunder mistet strøm da det pågikk. Ukrainske myndigheter beskyldte russiske sikkerhetstjenester for å stå bak angrepet. Ukrainske og amerikanske myndigheter, samt private selskaper gjennomførte analyser for å finne ut av hendelsesforløpet.

Angriperne demonstrerte en rekke avanserte kapabiliteter i angrepet mot kraftinfrastrukturen til Ukraina. Leveransen av første skadevare skjedde allerede i mars 2015 ved å plante en skadevare i office dokumenter som ble levert via e-post til flere ansatte i de tre berørte kraftselskapene. De har dermed hatt fotfeste i systemene i nesten ni måneder før angrepet. Det er sannsynlig at de har brukt tiden på å rekognosere, gjøre seg kjent med infrastrukturen og videre fått tak i mer innloggingsinformasjon for å få tilgang til det industrielle styringssystemet. Under selve angrepet hadde skadevaren blitt modifisert til å angripe nettopp dette styringssystemet på sub-stasjonene. Etter at de hadde deaktivert de fjernstyrte terminalene brukte de et verktøy som heter Killdisk til å slette muligheten til å benytte terminalene.

Samtidig som de iverksatte angrepet, som skjedde samtidig mot tre forskjellige selskaper, skal angriperne ha bombardert minst et av selskapene med tusenvis av telefonsamtaler slik at kunder ikke fikk meldt fra om strømbruddet. En av grunnene til at konsekvensene ikke ble større var at det ikke er veldig lenge siden ukrainsk kraftsektor gikk over til automatiserte sikringsstasjoner slik at gammel kunnskap om bruk fortsatt var tilstede i selskapene. Teknikere ble sendt ut til de rammede kraftstasjonene og operert manuelt.

Skadevaren brukt blir kalt BlackEnergy3. Skadevaren gir full tilgang til det infiserte systemet. Ifølge flere private sikkerhetsselskap er BlackEnergy3 utelukkende brukt av en trusselaktør kalt Sandworm Team (FireEye 2016). Ifølge amerikanske myndigheter er Sandworm Team tilknyttet GRU (NCCIS 2017). Senest i 2017 skal Sandworm Team ha forsøkt å trenge seg inn

i de baltiske kraftnettverkene (Jewkes 2017). Gruppen er også kjent for å bruke nulldagssårbarheter (FireEye 2016). Blant styrkene til gruppen er den langsiktige planleggingen og evnen til å lære seg nettverket før de gjennomførte et synkronisert, cybersabotasjeangrep på flere steder og i flere steg (SANS 2016).

17. desember 2016 ble det gjennomført et ny cybersabotasje mot kraftselskapet Ukrenergo. Denne gangen var det en fjernstyrt terminal enhet som ble frakoblet som førte til sporadiske strømbrudd i Kiev. Strømmen var borte i to timer før den ble gjenopprettet. Denne gangen valgte trusselaktøren kun å deaktivere den fjernstyrte terminale enheten og ikke forsøke å sabotere gjennomopprettingsmulighetene som i 2015-angrepet. Også denne gangen ble BlackEnergy3 brukt. Begge angrepene gikk på den fjernstyrte terminalen. Denne gangen ble kun èn sub-stasjon angrepet versus 30 stykker i 2015 (Williams 2017).

7.8. Ukraina 2017 - NotPetya - spredning av løspengevirus

Den 27 juni 2017 ble en rekke land rammet av det som først ble omtalt som et løsepengevirus kalt NotPetya. Angrepet begynte i Ukraina og rammet en rekke banker, departementer, aviser og kraftselskaper. Russland, Polen, Frankrike, Tyskland, Italia, England, USA og Australia rapporterte om selskaper som hadde blitt rammet. 80 prosent av alle infiserte maskiner befant seg i Ukraina (Wakefield 2017).

Angrepet startet i M.E.Doc, en ukrainsk regnskapsprogramvare brukt av et betydelig antall små og mellomstore bedrifter i Ukraina, samt hos de fleste myndighetsorganer. Programvaren ble kompromittert og sendte ut skadevare isteden for programvareoppdatering. Samtlige av land utenfor Ukraina som ble rammet hadde ukrainske underavdelinger med delt infrastruktur (Cherepanov 2017). Skadevaren baserte seg på ETERNALBLUE, en skadevare utviklet av National Security Agency som våren 2017 ble tilgjengeliggjort av den ukjente personen eller gruppen Shadowbrokers som har lekket flere av verktøyene til NSA (Goodin 2017). Det ble etterhvert kjent at dette ikke var et tradisjonelt løsepengevirus, hvis hensikt er å kryptere filene til offeret for så å kreve penger for å låse de opp igjen. NotPetya hadde ingen mulighet til å låse opp igjen filene, og var i praksis en skadevare for sabotasjeformål (Ivanov og Mamedov 2017).

Kildekoden til NotPetya er tilknyttet gruppen som sto bak sabotasjen mot kraftstasjonene i Ukraina to år tidligere (Cherepanov 2017). I februar 2018 gikk både amerikanske og britiske myndigheter ut og anklagde GRU, russisk militær etterretning for å stå bak angrepet og hevder NotPetya var nok et russisk forsøk på å destabilisere det ukrainske samfunnet (Marsh 2018).

7.9. Frankrike 2015 - Cybersabotasje mot TV5Monde

8.april 2015 gikk samtlige av de 12 kanalene til TV5Monde av lufta. TV5Monde er et av Frankrikes største TV-selskaper. I tillegg til at skjermene gikk i svart ble det postet beskjeder på både Twitter- og Facebook-kontoen til TV5monde hvor angriperen hevdet å være tilknyttet den islamske stats 'Cyber Caliphate' (Corera 2016). Kanalene var nede i over 18 timer og ifølge presidenten for TV-selskapet var angriperne nære å gjøre permanent skade. Noen måneder senere ble det rapportert at både sikkerhetsselskapet som etterforsket hendelsen og myndighetene avskrev IS og rettet oppmerksomheten mot Russland (Frenkel 2015).
Dette var basert på flere indikatorer, som for eksempel at infrastrukturen brukt til å poste IS-meldingene kom fra samme IP-blokk som annen spionasjeaktivitet mot franske aviser. Denne infrastrukturen ble attribuert til APT28, bedre kjent som GRU (Wilson 2015).

Året etter holdt ANSSI, det franske nasjonale cybersikkerhetsbyrået en presentasjon med detaljert gjennomgang av operasjonen. Her sa de blant annet:

> "One of the major takeaways from the investigation is that the attacker, or attack group, conducted reconnaissance inside the TV5Monde network for three months, following its initial access, before launching its sabotage operation. Just a few hours prior to that sabotage, which involved knocking multiple channels offline, the attackers compromised multiple TV5Monde social media accounts. [..] ANSSI says its investigation has concluded that the attackers' goal, from the beginning, was to sabotage TV5Monde's network" (Schwartz 2017).

Gjennomgangen viser hvilke steg angriperen tok for å få full tilgang til nettverket, samt hvordan selve sabotasjen ble gjennomført. Angriperen fikk tilgang via en tredjepartskonto som de brukte til å koble seg på systemene som styrte kameraene, Deretter lagde de en administratorkonto som gjorde at de fikk full tilgang til nettverket. Herfra leste de seg opp på hvordan infrastrukturen var satt sammen og hvilke systemer som snakket sammen, alt tilgjengelig på Tv5Mondes interne wiki. Selve sabotasjen ble gjennomført ved å utføre destruktive kommandoer på kommunikasjonsutstyret til tv-kanalen som gjorde at alt gikk i svart (ANSSI 2017).

Ifølge sjefen for Tv5Monde holdt angriperne på å gjøre permanent skade. De ble reddet av at de samme dag hadde lansert en ny kanal og hadde derfor et knippe teknikere tilstede hvor en av de klarte å fysisk koble fra en server som stoppet angriperne. Alle 12 kanalene kom på lufta løpet av neste dag (Corera 2016). Ingen myndighetsetater har så langt gått offentlig ut med mulig motiv for sabotasjen. Da angrepet ble gjennomført var det ingen kjente diplomatiske kriser eller konflikt mellom Frankrike og Russland. Mulige hypoteser fremmet av media er at Russland testet nye cyberkapabiliteter og valgte en tv-stasjon som var lett å penetrere. Det kan også ha vært konflikter mellom de to landene som ikke har vært kjent i media (Hornak 2016).

8. Analyse

I forrige kapittel gjennomgikk vi de åtte casene av russisk cybersabotasje. Dette kapittelet vil identifisere hvilke fellestrekk de åtte casene har ved å analyse de fem karakteristikkene geografi, metode og mål, målsettinger og konsekvenser på tvers av casene. Kapittelet vil deretter drøfte fellestrekkene opp med de teoretiske funnene i kapittelet om Clausewitz og militærteori.

8.1. Geografi

Av de åtte casene har syv blitt gjennomført i Russlands nærområder. Tre av statene var NATO-medlemer da angrepene ble gjennomført. To av statene (Ukraina og Georgia) har vært i dialog med NATO om MAP-status da angrepene ble gjennomført (Murphy og Mackenzie

2008). Dette indikerer at Russland fortsatt er noe restriktive på bruk av cybersabotasje i land utenfor Russlands regionale interessesfære (stater hvor de mener de har 'privileged interests'). Medlemskap i NATO har også lite innvirkning på Russlands vilje til å gjennomføre cybersabotasje. På den andre siden ble angrepene på NATO-landene gjennomført før NATOs toppmøte i Warszawa i 2016 som erklærte at et cyberangrep kan utløse artikkel fem. Unntaket her er Notpetya - løspengeviruset som russisk militær etterretning brukte mot Ukraina i 2017. Selv om Ukraina var antatt primærmål med 80 prosent av infeksjonene, så spredde viruset seg til flere titalls land, inkludert Russland selv og rammet en rekke sivile virksomheter. Eksempelvis ble det danske shippingselskapet Maersk rammet hardt. NotPetya var sannsynligvis ment å ramme kun Ukraina, men måten viruset ble distribuert på førte til at det rammet betydelig bredere (Greenberg 2018). Angrepet mot TV5Monde i Frankrike er den eneste casen som bryter med forventet russisk handlemåte da det aldri har vært i Russlands regionale interessesfære, er et NATO-land og har et mindre konfliktfylt forhold til Russland enn sine naboer. Som nevnt i case-gjennomgangen, det er fortsatt ukjent hvorfor akkurat Tv5Monde ble angrepet. Det vites ikke om Tv5Monde ble valgt som mål grunnet store sårbarheter i nettverket deres eller om det var en pågående konflikt mellom Frankrike og Russland som ikke var kjent for offentligheten.

8.2. Metode og mål

Det har vært en evolusjon i måten russisk cybersabotasje har blitt gjennomført. I perioden 2007 til 2009 ble de fire angrepene gjennomført på delvis samme måte - omfattende tjenestenektangrep for å ramme tilgjengeligheten for et bredt spekter av nettsider. Nettsidene befant seg innenfor offentlig sektor, finans, media, utdanning og telekom-sektoren for å nevne noen. Med unntak av NotPetya-hendelsen var sabotasjeoperasjonene i 2014-2017 betydelig mer målrettet. De fire hendelsene startet alle med datainnbrudd. Russiske etterretningstjenester tok seg inn i systemene til den ukrainske valgkommisjonen, to kraftselskaper, Linkos Group, og franske Tv5Monde. Disse datainnbruddene var mer kompliserte enn man hadde sett tidligere og det ble brukt lengre tid inne i systemene før de gjennomførte sabotasjen. Da de rammet kraftselskapet i Ukraina kom de seg inn i systemet nesten ni måneder før de skrudde av strømmen. I sabotasjen av Tv5Monde var de inne i tre måneder før skjermene gikk i svart.

Det er et bredt spekter av mål som har blitt rammet. Felles for samtlige mål er at de har primært hatt sivile formål. De generelle angrepene rammet nettsider til banker, finanstilsyn, sivile virksomheter, telekom- og internettleverandører, myndighetssider, media, utdanningsinstitusjoner, tenketanker, kraftselskaper og valgsider. I fem av de åtte casene var målene en blanding av sivile og politiske mål. I de to målrettede angrepene hadde målene utelukkende sivile formål (TV5Monde, Kraftselskapene i Ukraina) Løspengeviruset rammet svært bredt og var trolig myntet på alle sektorer, men det var den sivile sektoren som ble hardest rammet.

8.3. Målsettinger

I tre av hendelsene ble sabotasjen gjennomført i etterkant av en politisk beslutning som var upopulær hos russiske myndigheter. For Estland var det beslutningen om å flytte sovjetiske krigsminnesmerker, for Litauen var det et lovforslag om å forby kommunistsymboler og for Kirgisistan var det avtaleinngåelse med USA om flybaser. For hendelsene i Estland og Litauen ble sabotasjen gjennomført etter at beslutningen var tatt og sabotasjen var derfor en politisk reaksjon eller straff på en upopulær enkeltsak. For Kirgisistan ble cybersabotasjen gjennomført i forkant av et møte mellom de to statslederne og brukt som en pisk for å påvirke en politisk beslutning.

Sabotasjeoperasjonene mot Georgia skiller seg ut fra de syv andre casene. Tjenestenektangrepene mot et bredt spekter av nettsider hos sivile virksomheter og myndighetene skjedde nært opp til russisk invasjon av Sør-Ossetia og videre inn i Georgia. Hensikten med cyberangrepet var å understøtte konvensjonelle militære styrker ved å hindre Georgias politiske ledelse å kommunisere effektivt med egen befolkning.
Cybersabotasje i Ukraina og Frankrike må leses i et annet lys. Russland og Ukraina har siden vinteren 2014 vært en fastlåst konflikt hvor Russland har annektert ukrainske landområder og støtter et opprør øst i landet med personell og materiell. De tre casene fra Ukraina har derfor ikke blitt gjennomført mot politiske enkeltsaker, men er alle virkemidler brukt i en aktiv pågående konflikt. Allikevel hadde angrepet mot nettsiden til valgkommisjonen i 2014 en definert målsetting, som var å understøtte det strategiske narrativet til Russland som var at

ukrainsk politikk hadde blitt kuppet av ytre høyrefløy og nåværende regime besto av nynazister. Ved å gjennomføre et datainnbrudd hos valgkommisjonen og annonsere at en kandidat fra et ytterliggående parti hadde vunnet, så understøttet de det russiske strategiske narrativet. Når det gjelder de to angrepene på ukrainske kraftstasjoner og NotPetya-skadevaren kan det være to overlappende motiver.

For det første kan det ha vært forskning og utvikling fra russiske etterretningstjenester for å se hvor lang tid det tok fra inntrenging til utførelse av selve strømbruddet eller frafallet av kanalene. Hvis man planlegger operasjoner i cyberdomenet ved krig må man allerede ha fått fotfeste og ha skadevare klar hvis man skal ramme for eksempel kritisk infrastruktur. Det krever trening og erfaring i fredstid. For det andre så kan det være et signal til EU og Nord-Amerika. Et argument mange bruker mot cybervåpenets revolusjonerende makt er mangel på empiri om tidligere angrep. Slike "nesten"-hendelser sender en sterk signaleffekt om russisk mulighetsrom uten at det får de store konsekvenser for EU eller NATO. Ukraina er et naturlig sted å gjennomføre slik signalisering da de ikke har en allianse i ryggen, de er i en aktiv konflikt med Russland og de har manglende muligheter til å gjengjelde.

Når det gjelder målsettingen for å slå ut kraftselskapene og å utløse NotPetya-skadevaren kan det forklares med at russiske etterretningstjenester er delvis autonome i beslutninger om hva slags operasjoner de ønsker å gjennomføre. Ukraina er derfor en forsknings- og utviklingsarena for offensive cyberkapabiliteter. Angrepene mot kraftstasjonene ble gjennomført for å se på hvordan cybersabotasje kan ramme kraftsektoren og NotPetya-skadevaren var et eksempel på hvordan man potensielt kan paralysere store deler av den digitale infrastrukturen til andre land.

Angrepet mot TV5Monde er casen det hersker størst usikkerhet rundt målsettinger. En hypotese er at også dette angrepet var "r&d"-preget for å se på mulighetsrommet rundt angrep på tv-kanaler. Britiske myndigheter har også hevdet at GRU tok fullstendig kontroll over den britiske kanalen Islam Channel juli 2015, tre måneder etter angrepet på TV5Monde, men valgte da ikke å ødelegge sendingen eller utstyret (Bond 2018). På den andre siden kan det ha

vært konflikter mellom Frankrike og Russland i 2014 og 2015 som ikke har vært offentlig kjent som utløste cybersabotasje mot Tv5Monde.

8.4. Konsekvenser av russisk sabotasje

De åtte casene viser at russiske sabotasjeoperasjoner har vist en sterk preferanse for å ramme tilgjengeligheten til systemer og nettsider. Sabotasjen i perioden 2007-2009 har vært metodisk enkle, men hatt stort omfang som har evnet å midlertidig redusere tilgjengeligheten til digitale tjenester befolkningen forventer å ha tilgang til. I casen som omhandlet det ukrainske valget var formålet å påvirke integriteten til valget. Felles for alle casene er at det primært har hatt økonomiske konsekvenser, hvor det mest kostbare sannsynligvis er NotPetya-skadevaren som er anslått å ha forårsaket skader for rundt ti milliarder dollar. Angrepene på kraftstasjonene førte til at flere hundre tusen ukrainere mistet strømmen i noen timer, men det er ikke rapportert at det førte til tap av liv eller helse eller at de økonomiske konsekvensene var av betydelig størrelse.

De åtte casene har hatt politiske konsekvenser for de rammede statene. De pågående angrepene mot Ukraina er ment å svekke tilliten til myndighetenes evne til å beskytte egne innbyggere og sivile virksomheter. Det er derimot ukjent i hvilken grad russiske cyberoperasjoner bidrar til å svekke denne tilliten versus andre variabler. Angrepene har også hatt indirekte positive effekter. For Estlands del ble angrepet brukt til å få cybersikkerhet på den politiske agendaen nasjonalt, men også i NATO. Det har blant annet blitt opprettet en NATO-skole for cybersikkerhet i landet.

8.5. Er russisk cybersabotasje en ny form for krigføring?

Russisk cybersabotasje kan deles inn i to distinkte perioder. I perioden 2007 til 2013 kjennetegnes russisk cybersabotasje som en ny form for kanonbåtdiplomati hvor virkemidler i cyberdomenet erstattet eller supplerte tradisjonell bruk av hard makt. De distribuerte tjenestenektangrepene mot Latvia, Litauen og Kirgisistan rammet nasjonalt, men var begrenset i tid og skadeomfang. Cyberoperasjonene mot Georgia derimot understøttet den

konvensjonelle invasjonen. Det var første gang man observerte en grad av synkronisering av konvensjonelle maktmidler og angrep i cyberdomenet.

Den andre perioden fra 2014-2019 kjennetegnes russisk cybersabotasje som målrettede og instrumentelle verktøy brukt i konflikt og med større konsekvenser enn hva man har opplevd tidligere. Forberedelsene var grundige og tidkrevende med skadevare som var skreddersydd konkret for operasjonene de skulle gjennomføre. Det hersker usikkerhet i hvor stor grad målutvelgelsen var politisk styrt eller om russiske etterretningstjenester har fått frie tøyler til å eksperimentere med cyberkapabiliteter. Den militære etterretningstjenesten GRU antas å stå bak brorparten av hendelsene i denne perioden og organisasjonen kjennetegnes som aggressiv, risikovillig og med en grad av operasjonell autonomi.

De åtte russiske casene av cybersabotasje har primært blitt gjennomført i den russiske interessesfæren, med unntak av angrepet mot Tv5Monde. De har hatt målsettinger som enten kan tolkes som straff for politiske beslutninger belyst i casene Estland og Litauen, legge press på politisk ledelse (Kirgisistan), understøttet en konvensjonell invasjon (Georgia) eller vært del av en overordnet kampanje om å destabilisere en stat (Ukraina). Cybersabotasjen mot Tv5Monde virker fortsatt som en avvikende observasjon da den geopolitiske konteksten er ukjent. Resultatet av de åtte casene har primært vært alvorlige økonomiske og sosiale konsekvenser, selv om NotPetya-viruset potensielt kunne ha rammet virksomheter som sykehus og ført til fare for liv og helse.

Til tross for den relative alvorligheten i de åtte casene så har russisk cybersabotasje som rene krigshandlinger enda ikke skjedd. De åtte casene støtter Thomas Rids syn på cybersabotasje som aktive tiltak i den russiske interessesfæren og representerer derfor ikke noe nytt og revolusjonerende. På den andre siden viser gjennomgangen av casene at cybersabotasje blir stadig mer sofistikert, målrettet og har hittil blitt brukt primært mot sivile mål. Sett sammen med hvor lite utvikling det har vært på det internasjonale arbeidet med å regulere bruk av cybervirkemidler gjennom lover, normer og avtaler så skaper det en internasjonal uforutsigbarhet om hvor grensene går for bruk av cybersabotasje.

Det knyttes stor usikkerhet rundt terskelen for hvor alvorlig et slik angrep må være før det blir oppfattet som krigslignende handlinger som rettferdiggjør militær gjengjeldelse. Eventuelle beslutninger om gjengjeldelse hviler på mer enn om det er proporsjonalt å gjengjelde med tradisjonelle militære maktmidler. Det maktpolitiske forholdet vil være styrende for viljen til å eventuelt gjengjelde. Russland annekterte Krim og startet et opprør i øst-Ukraina uten at det fikk militære konsekvenser for Russland. En fremtidig militær gjengjeldelse på bakgrunn av en cyberoperasjon vil sannsynligvis skje der det er en asymmetri i maktforholdet. For eksempel er det mer sannsynlig at Russland vil gjengjelde militært mot estiske cyberoperasjoner enn at Estland gjengjelder militært mot russiske cyberoperasjoner. For å oppsummere så viser de eksisterende casene av russisk cybersabotasje at det er konsekvent med russisk sikkerhetsstrategi og sammenlignbart med andre russiske maktmidler i deres nærområde. Det kan derfor mindre defineres som krigføring basert på Clausewitz definisjon av krig og mer som aktive tiltak som spionasje, sabotasje og påvirkning som Russland og andre stormakter har drevet med lenge før internett ble oppfunnet. Neste kapittel skal derimot redegjøre for de teoretiske funnene knyttet til cyberoperasjoner og krigføring. Det finnes flere måter å definere krig på, og det påvirker også hva slags perspektiv man har på cybersabotasje.

8.6. Tolkning av casene i et teoretisk rammeverk

Problemstillingen var i hvilken grad 12 år med russisk cybersabotasje er en forsmak på fremtidens cyberkrigføring. De teoretiske funnene i oppgaven viser hvordan svaret på problemstillingen avhenger av 1) om man definerer krig som en voldelig, instrumentell handling for å oppnå politiske målsettinger eller 2) at man skaper forhold som bryter ned militærets, styresmaktenes eller folkets vilje til å gjøre motstand og dermed oppgir sine politiske målsettinger. En av konklusjonene er at Russland har forskjøvet hele konseptet krig og dermed endret premissene for hvordan man kan påføre motstanderen sin vilje. Clausewitz og kriteriet om voldsbruk i krig er derfor et lite hensiktsmessig rammeverk for å alene forstå cyberkrig, både på bakgrunn av hvordan konflikter utkjempes idag og ikke minst at NATO har sagt at et cyberangrep kan utløse artikkel fem. Hvis man uansett legger en slik definisjon av krig til grunn så har skadevare med potensiale for å skape død og ødeleggelse allerede blitt utviklet og funnet i sivil infrastruktur (Triton-skadevaren som er nevnt tidligere) og viser dermed at cybersabotasje som ‘åpningsskudd’ til fremtidens krig er mer enn bare et teoretisk

mulighetsrom. Dette er spesielt gjeldende da internasjonale lovverk, avtaler og normsetting rundt cyberoperasjoner er lite utviklet og stormakter som Russland, USA og Kina står svært langt fra hverandre på disse temaene.

De åtte casene viser heller at russisk cybersabotasje forstås bedre som et av flere maktmidler Russland har i verktøykassa si. Gitt uforutsigbarheten og mangel på normer for bruk av cybersabotasje så er det et maktmiddel med mye potensiale da man kan destabilisere et samfunn ved å holde konfliktnivået på en intensitet lav nok til at det er vanskelig å gjengjelde. Ukraina er et godt eksempel som viser hvordan cybersabotasje blir brukt som et av flere maktmidler for å destabilisere sivile sektorer og skape misnøye blant befolkningen. Samtidig har de en frihet til å gjennomføre testing av skadevare som kan bli brukt i konflikter med høyere intensitetsnivå. For å oppsummere viser empirien frem til idag at cybersabotasje er brukt alene eller sammen med andre maktmidler for russiske politiske formål og på et intensitetsnivå som gjør det vanskelig å gjengjelde for andre stater. Det er derimot funnet skadevare som kan ha svært ødeleggende effekter på et lands sivile infrastruktur og produksjonsmidler og vil ha svært alvorlige konsekvenser for både liv og helse, men også økonomisk og politisk handlingsrom. Parallellene til Douhets visjoner om luftmakt er slående og empirien viser at cybersabotasje som et strategisk våpen på linje med atombomben er fraværende, men heller at det kan ha en betydelig påvirkning på måten krig gjennomføres på, men fungerer best synkronisert med andre virkemidler.

9. Konklusjon

Oppgavens problemstilling spør om i hvilken grad 12 år med russisk cybersabotasje er en forsmak på fremtidens cyberkrigføring. Analysen av de åtte casene med russisk cybersabotasje viser hvordan fenomenet har gjennomgått en evolusjon de siste 12 årene. De første årene brukte Russland cybersabotasje som et virkemiddel eller avstraffelse i kanonbåtdiplomati. De siste 5 årene viser casene at russisk cybersabotasje har blitt mer avansert, målrettet og har hatt større konsekvenser enn tidligere. De har allikevel primært vært i tråd med russisk nasjonal sikkerhetsstrategi. Syv av åtte caser med russisk cybersabotasje har vært rettet mot stater som anses av Russland som ‘near abroad’ , tidligere sovjetstater hvor Russland uttaler at de har en spesiell interesse.

Om disse casene er en forsmak på fremtidens cyberkrigføring kommer også an på hvordan krig defineres. Her viser de teoretiske funnene at det finnes minst to perspektiver for hvordan krig forstås. Thomas Rid hevder at vi aldri vil se cyberkrig. Han legger til grunn Clausewitz definisjon av krig som en voldelig, instrumentell handling for å oppnå politiske målsettinger. Et slikt angrep hadde man frem til 2013 fortsatt ikke sett.

Oppgaven argumenterer for at en såpass snever definisjon på krig, og spesielt nødvendigheten av voldsbruk blir analytisk begrensende for å drøfte cyberkrigføring. For det første viser oppgaven at cybersabotasje som kan forårsake død og ødeleggelse er mer enn bare et teoretisk mulighetsrom da slik destruktiv skadevare allerede er funnet i sivile systemer (Se Triton-skadevaren). For det andre har NATO stadfestet at et cyberangrep kan utløse artikkel fem. Russisk cybersabotasje kan fungere som et åpningsskudd for fremtidens krig, men sannsynligvis ikke en krig som vil begrense seg til bare i cyberdomenet. Cyberoperasjoners paralleller til luftmakt på begynnelsen av 1920-tallet er tydelige. Det er lite som tyder på at cybersabotasje er et strategisk våpen som reduserer viktigheten av andre våpengrener, men det er mer som tyder på at cyberoperasjoner vil bli svært viktig i fremtidens krigføring, men i samhandling med de tradisjonelle våpengrenene.

Oppgaven viser også hvordan Clausewita også definerer krig som det å skape forhold som bryter ned militærets, styresmaktenes eller folkets vilje til å gjøre motstand og dermed oppgir sine politiske målsettinger. Et slik begrep er mer gjenkjennelig i hvordan konflikter har utspilt seg etter andre verdenskrig og introduksjonen av atombomben hvor risikovilligheten for total krig er mindre, befolkningens appetitt for død og ødeleggelse er lavere og stater benytter seg heller av begrensede militære og ikke-militære maktmidler for å få gjennom sin målsetting. Dette er i tråd med hvordan Russland har en pågående destabiliseringskampanje mot Ukraina hvor Russland bruker en kombinasjon av cybersabotasje, støtte til opprørere og økonomiske pressmidler for å holde landet ustabilt.

Svaret på problemstillingen er at russisk cybersabotasje frem til nå gir en pekepinn på hvordan makt i cyberdomenet vil bli utført i en fremtidig tilspisset konflikt mellom to

likeverdige parter. Mangel på internasjonale normer og avtaler gir få begrensninger på bruk av cybersabotasje. På den andre siden så vil usikkerheten rundt eskalering og proporsjonalitet rundt bruk av konvensjonelle militære maktmidler for å svare på et cyberangrep enn så lenge gi insentiv til å gjengjelde cybersabotasje med cyberoperasjoner. Ved holde aktiviteten på et laviftensitetsnivå evner Russland å destabilisere og skape frykt, men under en terskel som gjør at NATO svarer militært. Den russiske cybersabotasjen vi har sett, spesielt siste fem årene er derfor en pekepinn over hvordan fremtidens cyberkrig kan se ut.

10. Litteraturliste

Alexander, Dean C (2014): "Cyber Threats Against the North Atlantic Treaty Organization (NATO) and Selected Responses". İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi, 1 (2): 1-36.

Alperovitch, Dmitri (2016): *Bears in the Midst: Intrusion into the Democratic National Committee*. www.crowdstrike.com: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. [20.04.2019 2019].

Andersen, Svein S. (2013): Casestudier : forskningsstrategi, generalisering og forklaring. Bergen: Fagbokforl.

ANSSI (2017): *Conférence de clôture : Retour technique de l'incident de TV5Monde*. I communications, Symposium sur la sécurité des technologies de l'information et des (red.) https://www.sstic.org/2017/presentation/2017_cloture/.

Bing, Chris (2017): *Research claims CCLeaner attack carried out by Chinese-linked group*. www.cyberscoop.com: Cyberscoop, https://www.cyberscoop.com/ccleaner-attack-china-intezer-labs-piriform-apt17/. [29.03 2018].

Bond, David (2018): *GRU took 'complete control' of UK-based TV station in 2015*. www.ft.com: Financial Times, https://www.ft.com/content/c35aaea2-c8b5-11e8-ba8f-ee390057b8c9. [09.10 2018].

Bradbury, Danny (2009): *The fog of cyberwar*. www.theguardian.com: https://www.theguardian.com/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access. [30.04 2018].

Bright, Arthur (2007): *Estonia accuses Russia of 'cyberattack'*. www.csmonitor.com: Christian Science Monitor, https://www.csmonitor.com/2007/0517/p99s01-duts.html. [10.04 2018].

Bruusgaard, Kristin Ven (2014): "Crimea and Russia's strategic overhaul". Parameters, 44 (3): 81.

Buchanan, Ben (2017): *The Legend of Sophistication in Cyber Operations*. https://www.warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/legend_sophistication_-_web.pdf. [13.04 2018].

CCDCOE (2017): *Cyber Definitions*. https://ccdcoe.org/: NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/cyber-definitions.html. [30.04.17 2017].

Cherepanov, Anton (2017): *TeleBots are back: Supply-chain attacks against Ukraine*. ESET, https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/. [01.02 2018].

CIA (2014): *CIA World Factbook*. www.cia.gov: Central Intelligence Agency, https://www.cia.gov/library/publications/the-world-factbook/. [03.04 2018].

CIA (2016): *Lithuania*. The World Factbook: Central Intelligence Agency, https://www.cia.gov/library/publications/the-world-factbook/geos/lh.html. [24.05 2017].

CIA (2017): *Estonia*. The World Factbook: Central Intelligence Agency, https://www.cia.gov/library/publications/the-world-factbook/geos/en.html. [01.05 2017].

Clarke, Richard A. og Robert K. Knake (2012): Cyber war : the next threat to national security and what to do about it. New York: Ecco.

Clausewitz, C (1982): On War, first published 1832, translated by Colonel JJ Graham 1908, edited and abridged by A. Rapoport, reissued 1982. Penguin Books, New York.

Coffey, Luke og Daniel Kochis (2016): *Russia's Invasion of Ukraine: The US Needs a Strategy*. The Heritage Foundation, https://www.heritage.org/europe/report/russias-invasion-ukraine-the-us-needs-strategy. [03.02 2018].

Cole, Matthew, Richard Esposito, Sam Biddle og Ryan Grim (2017): *Top-Secret NSA Report Details Russian Hacking Effort Days before 2016 Election*. The Intercept, https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/. [01.06 2018].

Collins, Kathleen (2011): "Kyrgyzstan's latest revolution". Journal of Democracy, 22 (3): 150-164.

Corera, Gordon (2016): *How France's TV5 was almost destroyed by 'Russian hackers'*. http://www.bbc.com/news/technology-37590375: BBC, [04.03 2017].

Creswell, J.W. (1998): Qualitative inquiry and research design : choosing among five traditions. Thousand Oaks, Calif: Sage.

Crowdstrike (2016): *Use of Fancy Bear Android Malware in tracking of Ukrainian Field Artillery Units*. www.crowdstrike.com: Crowdstrike, https://www.crowdstrike.com/resources/reports/idc-vendor-profile-crowdstrike-2/. [06.04 2016].

D'incau, Stefan Soesanto and Fosca (2017): *The UN GGE is dead: Time to fall forward*. http://www.ecfr.eu: European Council on Foreign Relations.

Dahlum, Sirianne (2018): *Validitet*. https://snl.no: Store norske leksikon, https://snl.no/validitet. [18.02 2019].

Davis, Joshua (2007): "Hackers take down the most wired country in europe". Wired Magazine, 15 (9): 15-09.

Denzin, Norman K. (2012): "Triangulation 2.0". Journal of Mixed Methods Research, 6 (2): 80-88.

Diesen, Sverre (2018): Lavintensivt hybridangrep på Norge i en fremtidig konflikt. Kjeller: Forsvarets forskningsinstitutt FFI.

Douhet, Giulio, Joseph P. Harahan, Richard H. Kohn og Dino Ferrari (2014): *The Command of the Air.* Tuscaloosa: Tuscaloosa: University of Alabama Press.

Dragos (2017): *TRISIS Malware*. https://dragos.com/: Dragos INC, https://dragos.com/blog/trisis/. [03.04 2019].

DSB (2014): *Nasjonalt risikobilde 2014*. www.dsb.no: Direktoratet for samfunnssikkerhet og beredskap.

Economist (2005): *A tulip revolution*. Economist, https://www.economist.com/node/3785139. [10.12 2016].

Economist (2008): *Marching off to cyberwar*. The Economist, http://www.economist.com/node/12673385. [01.05 2017].

Etterretningstjenesten (2018): *FOKUS 2018 - Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.* https://forsvaret.no: Forsvaret. Hentet 30.04.2018, fra https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus2018_bokmaal_oppslag_godkjent.pdf.

Etterretningstjenesten (2019): *FOKUS 2019 - Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.* www.forsvaret.no: Etterretningstjenesten. Hentet 14.02.2019, fra https://forsvaret.no/fakta_/ForsvaretDocuments/fokus2019_web.pdf.

F-Secure (2015): *THE DUKES 7 years of Russian cyberespionage*. https://labsblog.f-secure.com/: F-Secure, https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf. [29.05 2019].

Facon, Isabelle (2017): Russia's national security strategy and military doctrine and their implications for the EU in-depth analysis. Luxembourg: European Parliament, Directorate-General for External Policies, Policy Department.

FireEye (2014): *APT 28: A Window into Russia's Cyber Espionage Operations?* https://www2.fireeye.com: Fireeye, https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf. [03.03 2018].

FireEye (2015): *HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group*. https://www.fireeye.com: FireEye, https://www.fireeye.com/blog/threat-research/2015/07/hammertoss_stealthy.html. [04.05 2017].

FireEye (2016): *Cyber attacks on the Ukranian grid: What you should know*. https://www.fireeye.com: FireEye, https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf. [12.11 2017].

FireEye (2017): *APT28: At the center of the storm*. https://www.fireeye.com: FireEye, https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html. [03.04 2018].

FireEye (2018): *TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers*. I www.FireEye.com (red.) *Threat Research Blog.* https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html: FireEye.

Fitton, Oliver James (2016): Cyber Operations and Gray Zones: Challenges for NATO. Connections. Lancaster University.

Flick, Uwe (2007): Managing Quality in Qualitative Research. London, UK: SAGE Publications, Ltd.

Franke, Ulrik (2015): *War by non-military means*. Understanding Russian Information Warfare, https://www.foi.se/rest-api/report/FOI-R--4065--SE:

Frenkel, Sheera (2015): *Experts Say Russians May Have Posed As ISIS To Hack French TV Channel*. www.buzzfeed.com: Buzzfeed, https://www.buzzfeed.com/sheerafrenkel/experts-say-russians-may-have-posed-as-isis-to-hack-french-t?utm_term=.grJzv2Xv1#.wlpRLeoLz. [14.11 2016].

Friis, Karsten, Lilly Pijnenburg Muller og Lars Gjesvik (2018): Cyber-weapons in International Politics : Possible sabotage against the Norwegian petroleum sector. NUPI, http://hdl.handle.net/11250/2486814: NUPI.

Galeotti, Mark (2016): "Putin's hydra: inside Russia's intelligence services". European Council on Foreign Relations Policy Brief.

Galeotti, Mark (2017): *STOLYPIN: Russia has no grand plans, but lots of 'adhocrats'*. http://www.intellinews.com/: intellinews, http://www.intellinews.com/stolypin-russia-has-no-grand-plans-but-lots-of-adhocrats-114014/. [05.04 2018].

Gambino, Lauren, Sabrina Siddiqui og Shaun Walker (2016): *Obama expels 35 Russian diplomats in retaliation for US election hacking*. www.theguardian.com: The Guardian,

https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack. [12.11 2017].

Geary, Sarah (2017): *Cyber Proxies: A Central Tenet of Russia's Hybrid Warfare*. www.thecipherbrief.com: The Cipher Brief, https://www.thecipherbrief.com/article/tech/cyber-proxies-central-tenet-russias-hybrid-warfare-1092?utm_content=buffer85ae7&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer. [01.09 2018].

Gerring, John (2007): Case study research : principles and practices. Cambridge: Cambridge University Press.

Gibson, William (1995): "*Neuromancer. 1984*". *New York: Ace*.

Giles, Keir og Kenneth Geers (2015): "Russia and Its Neighbours: Old Attitudes, New Capabilities". Cyber War in Perspective: Russian Aggression against Ukraine: 19-28.

Giles, Keir og Andrew Monaghan (2014): *Legality in Cyberspace: An Adversary View*. Army War College Carlisle Barracks PA Strategic Studies Institute.

Godwin III, James B, A Kulpim, Karl Frederick Rauscher og Valery Yaschenko (2014): *Critical terminology foundations 2*. Russia-US Bilateral on Cybersecurity. Policy Report,

Goodin, Dan (2017): *NSA-leaking Shadow Brokers just dumped its most damaging release yet*. Arstechnica.com: https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/. [23.01 2018].

Graff, Garret M. (2017): *Inside the hunt for russia's most notorious hacker*. https://www.wired.com: Wired Magazine, https://www.wired.com/2017/03/russian-hacker-spy-botnet/. [05.04 2017].

Gray, Colin S (2013): Making Strategic Sense of Cyber Power: Why The Sky is Not Falling. Lulu.

Greenberg, Andy (2018): *The Untold Story of NotPetya, The Most Devastating Cyberattack in History*. Wired: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. [15.10 2018].

Grønmo, Sigmund (2016): Samfunnsvitenskapelige metoder. Bergen: Fagbokforl.

Guerrero-Saade, Juan Andres, Costin Raiu, Daniel Moore og Thomas Rid (2017): *Penquin's Moonlit Maze*. securelist.com: https://kas.pr/4P8E. [06.06 2018].

Guterrres, António (2018): Cold War 'Back with a Vengeance' amid Multiple Entrenched Divides in Middle East, Secretary-General Tells Security Council, Urging Efforts to Avert Further Chaos. https://www.un.org/press/en/2018/sgsm18986.doc.htm: www.UN.org.

Harašta, Jakub og Jakub Míšek (2016): "Cyber War in Perspective: Russian Aggression against Ukraine". Vojenské rozhledy, 25 (2): 151-153.

Harding, Luke (2016): *What are the Panama Papers? A guide to history's biggest data leak*. https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers. [05.07 2017].

Heickerö, Roland (2010): "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations". Swedish Defence Research Agency (FOI).

Hornak, Leo (2016): *The Russian hackers going after Clinton also tried to destroy a French TV network*. PRI: https://www.pri.org/stories/2016-10-12/russian-hackers-going-after-clinton-also-tried-destroy-french-tv-network. [13.02 2019].

Hutchins, Eric M, Michael J Cloppert og Rohan M Amin (2011): "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains". Leading Issues in Information Warfare & Security Research, 1: 80.

Ilves, Tomas Hendrick (2014): *Rebooting Trust? Freedom vs Security in Cyberspace*. https://vp2006-2016.president.ee/en/official-duties/speeches/9796-qrebooting-trust-freedom-vs-security-in-cyberspaceq/: Office of President Estonia, Munich, 31.01.2014

Ivanov, Anton og Orkhan Mamedov (2017): *ExPetr/Petya/NotPetya is a Wiper, Not Ransomware*. https://securelist.com: Kaspersky Labs, https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/. [24.04 2018].

Jewkes, Stephen; Vukmanovic, Oleg (2017): *Suspected Russia-backed hackers target Baltic energy networks*. Reuters.com: http://uk.reuters.com/article/uk-baltics-cyber-insight-idUKKBN1871W9. [04.04 2018].

Krebs, Brian (2008): "Report: Russian hacker forums fueled Georgia cyber attacks". The Washington Post, 16.

Labs, NioGuard Security (2017): *Targeted attack against the Ukrainian military*. https://nioguard.blogspot.no/: Nioguard Security Labs, https://nioguard.blogspot.no/2017/05/targeted-attack-against-ukrainian.html. [13.05.17 2017].

Levy, Jack S. (2008): Case Studies: Types, Designs, and Logics of Inference.

Lindsay, Jon R. (2013): "Stuxnet and the Limits of Cyber Warfare". Security Studies, 22 (3): 365-404.

Lysne, Olav (2015): Digital sårbarhet - sikkert samfunn : beskytte enkeltmennesker og samfunn i en digitalisert verden. Norges offentlige utredninger, 978-82-583-1249-6. Oslo: Justis- og beredskapsdepartementet.

Manky, Derek (2013): "Cybercrime as a service: a very modern business". Computer Fraud & Security, 2013 (6): 9-13.

Manual, Tallinn (2013): Tallinn Manual on the international law applicable to cyber warfare 2013. Cambridge University Press, Cambridge.

Markoff, John (2008): "Before the gunfire, cyberattacks". New York Times, 12: 27-28.

Marsh, Sarah (2018): *US joins UK in blaming Russia for NotPetya cyber-attack*. www.theguardian.com: The Guardian, https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine. [25.01 2019].

Maurer, Tim og Scott Janz (2014): "The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context". The International Relations and Security Network, 17.

McClintock, Bruce H. og Andrew Radin (2017): *Russia in Action, Short of War*. Rand Corporation: https://www.rand.org/blog/2017/05/russia-in-action-short-of-war.html. [10.05.17 2017].

Minárik, Henry Rõigas and Tomáš (2015): UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law. I CCDCOE (red.) INCYDER. https://ccdcoe.org: NATO Cooperative Cyber Defence Centre of Excellence.

Mitchell, Paul T. (2013): "Cyberspace and the State: Toward a Strategy for Cyber-Power by David J. Betz and Tim Stevens". Journal of Strategic Studies, 36 (5): 753-755.

Murphy, Francois og James Mackenzie (2008): *France won't back Ukraine and Georgia NATO bids*. www.reuters.com: https://www.reuters.com/article/us-nato-france-ukraine/france-wont-back-ukraine-and-georgia-nato-bids-idUSL01151170200804012feedType=RSS&feedName=worldNews. [06.09 2018].

Muzalevsky, Roman (2010): "Shifting Regional Dynamics Force Russia to Suspend Promised Loan to Kyrgyzstan". Eurasia Daily Monitor, 7 (50).

NATO (2016): *Warsaw Summit Communiqué.* www.nato.int: NATO. Hentet 20.08.2017, fra http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

NCCIS (2016): *GRIZZLY STEPPE – Russian Malicious Cyber Activity.* https://www.us-cert.gov: Department of Homeland Security. Hentet 14.10-16, fra https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

NCCIS (2017): *Enhanced Analysis of GRIZZLY STEPPE Activity.* https://www.us-cert.gov/: Department Of Homeland Security (DHS) and the Office of the Director of National Intelligence (DNI), fra https://www.us-cert.gov/ncas/current-activity/2017/02/10/Enhanced-Analysis-GRIZZLY-STEPPE.

Neustar (2015): *April 2015 NEUSTAR DDOS ATTACKS & PROTECTION REPORT: NORTH AMERICA*. https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/2015-us-ddos-report.pdf: NEUSTAR.

Nye, Jr Joseph S. (2010): "Cyber Power". Harvard University Belfer Center Science & International Affairs.

Patton, Michael Quinn %J Health services research (1999): "Enhancing the quality and credibility of qualitative analysis". 34 (5 Pt 2): 1189.

Perrin, Chad (2008): *The CIA triad*. http://www.techrepublic.com/blog/security/the-cia-triad/488. [20.03 2017].

Persen, Kjell, et al. (2017): PST bekrefter: Russiske hackere har angrepet Forsvaret, UD, Ap, Statens strålevern og PST. http://www.tv2.no: TV2, http://www.tv2.no/a/8903847/. [20.03 2017].

Reichborn-Kjennerud, Erik og Patrick Cullen (2016): "What is Hybrid Warfare?". Norwegian Institute of International Affairs Policy Brief, 1: 2016.

Repstad, Pål (2007): Mellom nærhet og distanse : kvalitative metoder i samfunnsfag. Oslo: Universitetsforlaget.

Rid, T. og B. Buchanan (2015): "*Attributing Cyber Attacks*". *J. Strateg. Stud.,* 38 (1-2): 4-37.

Rid, Thomas (2013): *Cyber war will not take place.* Oxford University Press, USA.

Rid, Thomas (2016): Rise of the Machines: A Cybernetic History. WW Norton & Company.

Sanger, David; Broad William (2017): *Hand of U.S. Leaves North Korea's Missile Program Shaken*. https://www.nytimes.com: The New York Times, https://www.nytimes.com/2017/04/18/world/asia/north-korea-missile-program-sabotage.html. [01.06 2017].

SANS (2016): *Analysis of the Cyber Attack on the Ukrainian Power Grid*. https://ics.sans.org: SANS ICS, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf. [24.08 2016].

Schwartz, Mathew J. (2017): *French Officials Detail 'Fancy Bear' Hack of TV5Monde*. https://www.bankinfosecurity.com/french-officials-detail-fancy-bear-hack-tv5monde-a-9983: https://www.bankinfosecurity.com/, https://www.bankinfosecurity.com/french-officials-detail-fancy-bear-hack-tv5monde-a-9983. [13.02 2019].

Seawright, Jason og John Gerring (2008): "Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options". Political Research Quarterly, 61 (2): 294-308.

Sershen, Daniel (2006): *Kyrgyzstan: Base Shooting Sours US-Kyrgyz Relations*. Eurasianet.org: https://eurasianet.org/kyrgyzstan-base-shooting-sours-us-kyrgyz-relations. [24.04 2017].

Sigholm, Johan (2013): "Non-state actors in cyberspace operations". Journal of Military Studies, 4 (1): 1-37.

SOU (2015:23): *Informations- och cybersäkerhet i Sverige.* Stockholm: Elanders Sverige AB, fra http://www.regeringen.se/contentassets/8ae8ef6d5d3f45058c981cbab4e297de/informations--och-cybersakerhet-i-sverige.-strategi-och-atgarder-for-saker-information-i-staten-sou-201523.

Stavros, Constantino og Kate Westberg (2009): "Using triangulation and multiple case studies to advance relationship marketing theory". Qualitative Market Research: An International Journal, 12 (3): 307-320.

Stoltenberg, Jens (2015): Keynote Speech by NATO Secretary General Jens Stoltenberg at the Opening of the NATO Transformation Seminar. www.nato.int: NATO, https://www.nato.int/cps/en/natohq/opinions_118435.htm. [30.05 2019].

Stone, Richard (2013): "*A call to cyber arms*". *Science,* 339 (6123): 1026-1027.

Tikk, Eneken og Mika Kerttunen (2018): "International Cybersecurity: Orchestral Manoeuvres in the Dark". NUPI's Centre for Cybersecurity Studies, (NUPI Policy Brief; 2018-11).

Välisluureamet (2019): *International Security and Estonia 2019*. https://www.valisluureamet.ee: Välisluureamet, https://www.valisluureamet.ee/pdf/raport-2019-ENG-web.pdf. [30.05 2019].

Vesilind, Priit, James Tusty og Maureen Tusty (2008): *The Singing Revolution: How Culture Saved a Nation.* Varrak.

Wakefield, Jane (2017): *Tax software blamed for cyber-attack spread*. www.bbc.co.uk: BBC, http://www.bbc.com/news/technology-40428967. [24.04 2018].

Waltzman, Rand (2017): *The Weaponization of Information*. *Senate Armed Services Committee.* https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf.

Williams, Brad D. (2017): *Hackers' methods feel familiar in Ukraine power grid cyberattack*. http://fifthdomain.com/: Fifth Domain Cyber, http://fifthdomain.com/2017/01/29/how-a-power-grid-got-hacked/. [03.03.17 2017].

Wilson III, Ernest J (2008): "Hard power, soft power, smart power". The Annals of the American Academy of Political and Social Science, 616 (1): 110-124.

Wilson, Kara (2015): *In Case You Missed it: The FireEye Top Five Stories of the Week*. https://www.fireeye.com: FireEye, https://www.fireeye.com/blog/executive-perspective/2015/06/in_case_you_missedi0.html. [01.02.17 2017].

Winterfeld, Steve og Jason Andress (2012): The Basics of Cyber Warfare : Understanding the Fundamentals of Cyber Warfare in Theory and Practice. Rockland: Rockland, MA: Elsevier Science & Technology Books.

Yin, Robert K (2013): *Case study research: Design and methods.* Los Angeles, California: Sage publications.

Zetter, Kim (2011): "How digital detectives deciphered Stuxnet, the most menacing malware in history". Wired Magazine, 11: 1-8.