Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for samfunns- og utdanningsvitenskap
Institutt for sosiologi og statsvitenskap

Stine Reitan

Kan NATO avskrekke cyberangrep?

En prosessanalyse av NATOs evne til å avskrekke cyberangrep.

Bacheloroppgave i Statsvitenskap
Veileder: Jo Jakobsen

Mai 2020

NTNU
Kunnskap for en bedre verden

Stine Reitan

Kan NATO avskrekke cyberangrep?

En prosessanalyse av NATOs evne til å avskrekke cyberangrep.

Bacheloroppgave i Statsvitenskap
Veileder: Jo Jakobsen
Mai 2020

Norges teknisk-naturvitenskapelige universitet
Fakultet for samfunns- og utdanningsvitenskap
Institutt for sosiologi og statsvitenskap

NTNU
Kunnskap for en bedre verden

Sammendrag

Denne bacheloroppgaven tar utgangspunkt i å undersøke NATOs evne til å avskrekke cyberangrep, gjennom en prosessanalyse som metodisk sett er basert på dokumentstudier. Oppgavens problemstilling er: *«Kan NATO avskrekke cyberangrep?»*. For å besvare denne er det gjennomført en empirisk analyse av toppmøteerklæringer fra 2002, frem til 2018. Litteraturgjennomgangen i oppgaven har til hensikt å syntetisere tidligere forskning på temaet, og brukes i denne oppgaven som et verktøy for å tolke funnene i analysen. Cyberangrepet på Estland i 2007 brukes for å illustrere startskuddet for alliansens utvikling i cyberspace. I tillegg er toppmøtene fra 2014, 2016 og 2018 de mest fremtredende møtene for endring i NATOs strategi for cybersikkerhet. Analysen viser at alliansen i lang tid har brukt avskrekking ved benektelse, men i 2016 gjør de et skifte til en kombinasjon av benektelse og straff. Oppgaven konkluderer med at NATOs evolusjon i cyberspace har gjort de kapable til å faktisk avskrekke cyberangrep.

Innholdsfortegnelse

1.0 Introduksjon

«Det kreves kun et tastetrykk for å slippe løs et verdensomspennende cybervirus, men det krever en verden for å stoppe det før det skaper totalt kaos» (Stoltenberg, 2019). Cybervåpen er ulikt noe annet vi har sett tidligere, i løpet av minutter kan et eneste cyberangrep påføre skader for flere milliarder på verdensøkonomien, lamme den kritiske infrastrukturen, undergrave demokratier og paralysere militære evner (Stoltenberg, 2019). Cyberspace er et felt som er drevet av usikkerhet, anonymitet og uavklarte grenser. Er det da mulig å drive effektiv avskrekking i cyberspace? Store deler av forskningen gjort på avskrekking i cyberspace argumenterer for at det er en langt større utfordring sammenlignet med tradisjonell avskrekking (Blagden, 2020, s.131 & Iasello, 2014, s.56-59). Anonymitet, som videre fører til utfordringer med attribusjon og proporsjonalitet, trekkes frem som elementer som gjør avskrekking i cyberspace svært utfordrende (Blagden, 2020, s.131 & Iasello, 2014, s.56-59). På den andre siden argumenteres det for at avskrekking i cyberspace er vanskeligere i teorien, enn hva det faktisk er i praksis (Goodman, 2010, s.129).

Denne oppgaven tar sikte på å undersøke hvorvidt det er mulig å drive avskrekking i cyberspace. For å finne ut av dette vil denne oppgaven bruke «North Atlantic Treaty Organization» (NATO) som case. NATO er på mange måter en organisasjon bygget på avskrekking, og er derfor høyst relevant og kan settes i sammenheng med cyberavskrekking som et bredere felt. Problemstillingen for denne oppgaven er dermed: *«Kan NATO avskrekke cyberangrep?»*. For å besvare denne vil jeg foreta en prosessanalyse der jeg gjennomgår NATOs evolusjon innenfor cyberforsvar i perioden 2002 frem til 2018.

Oppgaven starter med en litteraturgjennomgang, der relevant litteratur vil presenteres. Der vil konseptene attribusjon, proporsjonalitet og avskrekking gjennomgås. Denne delen inkluderer også et knippe cyberangrep som brukes for å eksemplifisere de foregående konseptene. Videre vil oppgavens metode og design gjøres rede for, der det blant annet vil utdypes ytterligere om litteraturen og empirien som er benyttet. I analysen vil empirien, i form av toppmøteerklæringer, presenteres og diskuteres opp mot konsepter presentert i litteraturgjennomgangen. Analysen i sin helhet ser på NATOs evolusjon innenfor cybersikkerhet, der hovedfokuset ligger på deres

avskrekkingsmetode. Avslutningsvis følger det en kort oppsummering og konklusjon av oppgaven.

Analysen baserer seg på å presentere og analysere det empiriske grunnlaget, som i denne oppgaven er NATOs toppmøteerklæringer fra 2002 til 2018. Litteraturen som gjennomgås i seksjon 2 vil kontinuerlig brukes som verktøy for å tolke empirien samt forklare resultatene i analysen. Cyberangrepet på Estland i 2007, i tillegg til toppmøteerklæringene fra 2014, 2016 og 2018 identifiseres som de viktigste momentene for utviklingen. Analysen viser hvordan angrepet på Estland fungerte som en katalysator for evolusjonen innenfor cybersikkerhet. Toppmøteerklæringene fra 2014, 2016 og 2018 viser hvordan NATOs avskrekkingsmetode endret seg fra eksplisitt avskrekking ved benektelse, til å bli en kombinasjon av avskrekking ved benektelse og straff. Oppgaven konkluderer på overordnet nivå med at NATO i dag benytter seg av en rekke tiltak for å best mulig avskrekke cyberangrep, og på denne måten faktisk *kan* avskrekke cyberangrep.

2.0 Litteraturgjennomgang

I denne delen av oppgaven vil det fremlegges en litteraturgjennomgang. Den er oppbygd som en omvendt pyramide, i den forstand at litteraturen blir sett fra et bredere perspektiv før den videre avgrenses og relateres til problemstillingen. I tråd med dette vil det i første omgang gjennomgås litteratur som omhandler stormakter i cyberspace, henholdsvis USA og Russland. Konsepter som proporsjonalitet, attribusjon og avskrekking er sentrale i store deler av litteraturen, og vil også gjennomgås her. Underveis vil et utvalg cyberangrep vises til, for å eksemplifisere samt vise flerfoldigheten av cyberangrep. Avslutningsvis vil litteratur mer spesifikt knyttet til NATO gjennomgås. Litteraturgjennomgangen er gjort med et formål om å oppsummere, evaluere og syntetisere forskningen.

2.1 Stormakter i cyberspace

Innenfor studiet av internasjonal politikk har stormakter en prominent plass innenfor emnet, også innenfor litteraturen som omhandler cyberspace får man et innblikk i stormakter innenfor domenet. Det er flere stater som utvikler god cyberkapasitet, men i denne oppgaven nevnes kun USA og Russland. Disse er begge gjengangere i litteraturen og er å betrakte som motpoler, USA er medlem av NATO, mens Russland regnes som den største trusselen for alliansen.

I en artikkel skrevet av Jensen, Valeriano & Maness (2019, s.212) undersøker de hvilken cyber strategi Russland bruker for å følge opp sine politiske mål, og den overordnede konklusjonen er at de benytter seg av en blanding mellom overtalelse (coercion) og spionasje. Overtalelse, eller tvang, innebærer å produsere en ønsket oppførsel eller utfall fra motstanderens side ved å tvinge den til å gjennomføre en kost-nyttevurdering, slik at motstanderen mener det er mindre kostbart å gi etter for aggressorens foretrukne forløp, enn å ikke gjøre det (Borghard & Lonergan, 2017, s.453). I artikkelen teoretiserer de først cyber strategi, før de videre gjennomgår dokumenterte cyber operasjoner gjennomført av Russland. De viktigste funnene i artikkelen er at Russland i størst grad har benyttet seg av angrep som er trakasserende og sår misnøye, fremfor angrep som er designet for å ødelegge (Jensen et al, 2019, s.229). I artikkelen nevnes flere ulike cyberangrep, som Stuxnet 2010, Estland 2007 og Georgia 2008[1], men fokuserer i hovedsak på Russlands konflikt med Ukraina, samt Russlands innblanding i valget i USA i 2016. De gjennomgående funnene i disse eksemplene er at Russlands cyberinstrumenter fokuserer mest på å forstyrre og spionere, og at de ofte brukes som supplement til kinetiske midler.

Konklusjonen er at den russiske cyberaktiviteten er bekymringsverdig, men at det så langt ikke har vært særlig sofistikerte angrep som igjen mislykkes i å overtale (Jensen et al, 2019, s.229). Avslutningsvis legges det til at «Moscow acts more like a rogue state undermining the norm against targeting critical infrastructure than it does like a responsible actor in the digital domain» (Jensen et al, 2019, s.229). I en artikkel av Kramer, Butler & Lotrionte (2016, s.3) nevnes Russland med samme intonasjon. De mener at Russland har en selvsikker cyberposisjon basert på deres vilje til å målrette kritisk infrastruktur (Kramer et al, 2016, s.3). Samtidig nevnes det også her at de i størst grad benytter seg av forstyrrende cyberangrep som har til hensikt å påvirke den offentlige debatten (Kramer et al, 2016, s.3).

I artikkelen av Kramer et. al (2016) er hensikten å legge frem et konsept for utvidet cyberavskrekking, med fokus på en potensiell konflikt som involverer NATO. Artikkelen identifiserer Russland som den største trusselen i cyberspace og ønsker å opprette «cyber framework nations» for å styrke det kollektive forsvaret (Kramer et al, 2016, s.1). Hensikten

[1] En kort forklaring av disse kommer utover i teksten.

med å etablere en slik nasjon, er for at denne skal kunne hjelpe mindre kapable stater til å etablere et effektivt system for å unngå angrep, samt få assistanse om de skulle bli angrepet (Kramer et al, 2016, s.6). Artikkelen mener USA bør være den første «cyber framework nation» (Kramer et al, 2016, s.1). Argumentene bak dette er at USA er anerkjent for å ha gode evner i cyberspace og samtidig har mulighet til å utvide sin kapasitet ytterligere (Kramer et al, 2016, s.4). I en artikkel av Libicki (2018) beskrives også USA som den mektigste cybernasjonen og at de er i en egen klasse når det kommer til deres cyberkapasitet. Artikkelen har til hensikt å vise hvordan god kapasitet innenfor cyber og trusselen om å bruke den, kan bidra til mer effektiv avskrekking og bruker USA som eksempel (Libicki, 2018, s.45). Stuxnet-angrepet pekes på som et eksempel på USA sin ekspertise på området. Selv om ingen formelt har tatt på seg ansvaret for dette angrepet er det mange som peker i retning USA, i så måte tar denne artikkelen dette som et faktum. Målet for Stuxnet-ormen var å stoppe Iran fra å fremstille sitt eget uran[2]. For å gjøre dette ble de iranske atomsentrifugene og systemene som styrte dem målrettet ved å omprogrammere og spionere på systemet (Farwell & Rohozinzki, 2011, s. 23-24). Stuxnet-angrepet regnes som et av de mest sofistikerte og ødeleggende cyberangrepene i vår tid. USAs kapasitet innenfor cyberspionasje, cybersabotasje og undergraving av cybersystemer betraktes som ikke-sammenlignbar med andre staters kapasitet (Libicki, 2018, s.45).

Skillelinjen mellom Russland og USA i cyberspace er at USA utvikler god kapasitet på området for å beskytte seg selv, mens Russland er i andre enden av spekteret og ofte går frem som aggressor. Samtlige artikler understreker at Russlands utvikling i cyberspace er bekymringsverdig, på lik linje som samtlige artikler trekker USA frem som en stat med god kapasitet og en stat å ta lærdom av for å beskytte seg selv.

2.2 Proporsjonalitet

I Henry Kissingers' bok *World Order* argumenteres det for at cyberspace er et domene som er i hurtig utvikling og som i og for seg selv ikke nødvendigvis er en trussel, men at truslene i cyberspace er udefinerte, uendelige og under et teppe av anonymitet (Kissinger, 2014, s.342). Kapittelet i boken er skrevet med hensikt om å belyse hvordan effektene av cyberspace vil påvirke verdensordenen, og gir uttrykk for at avskrekking og attribusjon i cyberspace er sentrale punkter det trengs mer kunnskap om (Kissinger, 2014, s.342-347). Det som trekkes frem som

[2] Et stoff som brukes i produksjonen av atomvåpen.

den største utfordringen i cyberspace er imidlertid proporsjonalitet når det kommer til å besvare et cyberangrep, mer spesifikt om et virtuelt angrep kan besvares kinetisk (Kissinger, 2014, s.342-347). I en artikkel av Iasello (2014) trekkes også proporsjonalitet frem som en stor utfordring i cyberspace, men her brukes internasjonal lov som Genève konvensjonen og krigens lov som rammeverk. Et motangrep i cyberspace må være proporsjonelt til det originale angrepet, det vil si at det ikke skal gjøre mer skade enn det første angrepet, dette er for å unngå en eventuell eskalering av konflikten (Iasello, 2014, s.59). Motangrepet må være kraftig, men ikke så kraftig at det åpner opp for negative reaksjoner i verdenssamfunnet, fordi en stats kredibilitet hviler på dens kapasitet til å gjennomføre det den sier uten å oppfattes tunghendt (Iasello, 2014, s.59). Det som trekkes frem som det viktigste er at en stat som handlet selvstendig, det vil si uten tilknytning til internasjonale organisasjoner, risikerer å straffes økonomisk eller diplomatisk av stater med tilknytning til den skadelidende staten (Iasello, 2014, s.59). Derfor bør hvilken type kinetisk eller ikke-kinetisk respons, hurtigheten på motangrepet, de anslåtte konsekvensene og potensielt politisk nedfall, tas med i beslutningsprosessen i forkant av et motangrep (Iasello, 2014, s.60). Hovedessensen er at et cyberangrep kan besvares med kinetiske virkemidler, så lenge det er proporsjonelt og ikke påfører mer skade enn det originale angrepet.

I en artikkel av Smeets (2018) fremmes bruken av cyberoperasjoner fremfor kinetiske på bakgrunn av at det humanitære perspektivet og fordi det kan ha stor strategisk verdi. I artikkelen skiller de mellom «counter force cyber capabilities» (CFCC) og «counter value cyber capabilities» (CVCC) for å vise hvordan offensive cyberevner kan forsterke konvensjonelle tiltak, så vel som å være en uavhengig ressurs (Smeets, 2018, s.90). CFCC omhandler å ta sikte på militær infrastruktur og er ofte knyttet til andre kinetiske virkemidler, et eksempel på dette er det Russiske angrepet mot Georgia i 2008 der kinetiske- og cybervåpen ble brukt simultant (Smeets, 2018, s.94-96 & Shakarian, 2011, s.63). CVCC tar sikte på motstanderens nasjonale styrke i form av kritisk sivil infrastruktur og er sjeldnere brukt i sammenheng med kinetiske virkemidler (Smeets, 2018, s.94-96). Et eksempel på dette er Stuxnet-ormen. Artikkelen gir videre fire forslag til bruk av offensive cyberevner, og spesifiserer forholdene der de kan gi strategisk verdi: 1; Det gir et ekstra alternativ til statsledere, 2; Kan brukes effektivt i sammenheng med annen militær kapasitet, 3; Kan brukes for å oppnå en form for psykologisk kontroll, og 4; Kan brukes effektivt uten store humanitære tap (Smeets, 2018, s.97-102). De viktigste funnene i denne artikkelen er at det er mange fordeler ved å bruke offensive

cyberoperasjoner, men det er fortsatt mye de *ikke* kan gjøre. Det er fortsatt en del problemer med anonymitet og attribusjon, men forfatteren konkluderer med at offensive cyberoperasjoner kan gi stater en strategisk fordel som ofte ikke krever menneskeliv og at det gir statsledere et ekstra alternativ i en rekke situasjoner (Smeets, 2018, s.105).

2.3 Attribusjon

Attribusjon handler om å besvare spørsmålet: hvem gjorde det? Attribusjon, eller tilskrivelse, dreier seg om å finne den som står bak et cyberangrep og tilskrive dem skyld, det kan være individer, ikke-statlige aktører og stater (Fitton, 2016, s.114). Anonymitet er en sentral karakteristikk for cyberspace, og dette gjør tilskrivning av skyld veldig utfordrende, tidkrevende og komplekst i motsetning til fysiske angrep (Fitton, 2016, s.114). Rid og Buchanan (2015) argumenterer for at "Attribution is what states makes of it". I sin artikkel ser de på attribusjon i cyberspace på flere ulike nivå, et operasjonelt-, teknisk- og strategisk nivå. Artikkelen har til hensikt å gi en forklaring på de mange utfordringene med attribusjon i cyberspace, men samtidig forsøker den å gi beslutningstakere en mulig løsning på problemet (Rid & Buchanan, 2015, s.4). De konkluderer med at attribusjon er komplisert men mulig, og det krever en rekke ulike ferdigheter; godt samarbeid og lederskap, tid, god kommunikasjon og evnen til å se begrensninger og utfordringer (Rid & Buchanan, 2015, s.4). Samtidig understreker de at hvis attribusjon gjøres dårlig, kan dette være med på å undergrave en stats troverdighet, effektivitet og potensielt dens sikkerhet (Rid & Buchanan, 2015, s.4). Kanskje viktigst av alt, poengterer de at suksessfull attribusjon kan være avhengig av den politiske viljen. Mye avhenger av hvilken grad av ressurser staten ønsker å bruke på å finne ut hvem som står bak (Rid & Buchanan, 2015, s.30).

I en artikkel av Goodman (2010) argumenterer han imidlertid for at attribusjon er vanskeligere i teorien, enn det faktisk er i praksis. At attribusjon er mer komplekst og krever mer i cyberspace enn i den fysiske verden er det en viss enighet om. Men artikkelen legger frem et alternativ som gjør at attribusjon ikke nødvendigvis trenger å være så komplisert som det er i teorien. Artikkelen tar utgangspunkt i en stat som nekter å erkjenne skyld, og som heller ikke ønsker å delta i etterforskningen for å finne den ansvarlige. Goodman (2010, s.109) mener at i slike tilfeller kan offerstaten, enten basert på gjensidige avtaler om rettshjelp, eller den iboende retten til selvforsvar, tildele ansvar for angrepet til den ikke-samarbeidende staten. På denne måten

løser man attribusjonsproblemet og man unngår kostbar etterforskning (Goodman, 2010, s.109).

Attribusjon er spesielt utfordrende i cyberspace og avhenger ofte av den politiske viljen til å finne den som står bak. Likevel ser man at det finnes løsninger gjennom samarbeid og internasjonale lover som gjør det mulig å attribuere angrep.

2.4 Avskrekking

Avskrekking oppnås når en aktør – en stat, gruppe eller individ – konkluderer med at de antatte kostnadene av et angrep overgår de antatte fordelene (Blagden, 2020, s.133). Avskrekking knyttes ofte til den kalde krigen og datidens atomavskrekking, men det er i realiteten en gammel praksis (Morgan, 2012, s.86). Hvis man ser på klassisk maktbalanse, kan man trekke tråder til gjensidig avskrekking. Under den kalde krigen ble avskrekking viktigere enn aldri før, og de ble viet mye tid og ressurser til å forstå hvordan det fungerer og hvordan det gjøres mest mulig effektivt (Morgan, 2012, s.86). Etter denne epoken har avskrekking blitt en sentral del av internasjonal politikk.

I litteraturen om avskrekking finner man flere ulike typer og egne definisjoner for de enkelte, men i denne oppgaven er fokuset på cyberavskrekking. Goodman (2010) definerer cyberavskrekking som «Hvorvidt kostnadene av cyberaggresjon overveier fordelene og om fordelene ved tilbakeholdenhet i cyberspace overveier kostnadene» (Goodman, 2010, s.107). Målet med cyberavskrekking er å redusere risikoen for cyberangrep til et akseptabelt nivå og til en akseptabel kostnad (Iasello, 2014, s.63). Til syvende og sist er de mange ulike definisjonene bygget på det samme, nemlig en kost-nytte-vurdering av hvorvidt et angrep vil være lønnsomt eller ikke. På mange måter kan tradisjonell avskrekking og avskrekking i cyberspace på overflaten se ut som å bygge på de samme prinsippene, noe de på mange måter er, men i realiteten er cyberavskrekking en langt større utfordring. Iasello (2014, s.54) påpeker for eksempel i sin artikkel at det er bare en håndfull av nasjoner som har vist seg å være kapable til å utvikle atomvåpen, mens over 140 nasjoner har, eller er i prosessen av, å utvikle cybervåpen.

Å utvikle en avskrekkingsmetode som skal være effektiv mot noen få, versus en metode som skal være effektiv mot et hundretalls, krever forståelig nok en helt annen fremgangsmåte. I

tillegg er det stor usikkerhet ved cybervåpens slagkraft, sammenlignet med kinetiske våpen, noe som poengteres i Libicki's (2018, s.51) artikkel. Med kinetiske våpen har andre land god kunnskap om hva et individuelt våpen kan gjøre, hvor sårbare de er for et slikt angrep og kan i stor grad predikere kostnadene for gjenoppreisning, fordi det vil være basert på å erstatte ødelagt materiale (Libicki, 2018, s.51). Den samme kunnskapen finnes ikke for cybervåpen. Libicki (2018, s.51) gir fire grunner til hvorfor effektene av cyberangrep er uforutsigbare: 1; Offeret for et cyberangrep vil ikke vite nøyaktig hvilke evner aggressoren har, 2; Cyberangrep har uendelig rekkevidde i motsetning til kinetiske våpen 3; aggressoren har bare en delvis innsikt i offerets forsvar, 4; Hverken aggressor eller offer vet hvor lang tid det tar å komme seg til normalen etter et angrep.

2.4.1 Avskrekking ved benektelse og Avskrekking ved straff

Å avskrekke et potensielt cyberangrep kan gjøres på to måter. Avskrekking ved benektelse oppstår når en mulig aggressor konkluderer med at et angrep vil være ineffektivt på grunn av forsvarsmekanismene som er på plass – på denne måten blir aggressor *nektet* muligheten til å oppnå sine mål (Blagden, 2020, s.133). Denne formen for avskrekking er mindre konfliktdrevet, fordi den søker å overbevise en mulig aggressor om at deres innsats ikke vil lykkes, og dermed vil det heller ikke være noe hevnspørsmål (Iasello, 2014, s.55). Baksiden med å bruke denne formen for avskrekking, er at det krever et stort engasjement fra myndighetene for å sikre deres nettverk og systemer, samtidig som det krever et fullstendig samarbeid med de private eierne av viktig infrastruktur (Iasello, 2014, s.56). Ved å jobbe på denne måten påfaller det også følgelig store kostnader.

Avskrekking ved straff, derimot, har ikke til hensikt å redusere et angreps effektivitet, men hviler på trusselen om gjengjeldelse på en skala som gjør at aggressoren vil være dårligere stilt enn hvis han ikke hadde angrepet i utgangspunktet (Blagden, 2020, s.133). Selv om det initiale angrepet var et cyberangrep, er ikke motangrepet begrenset til cyberspace, men kan utspille seg med diplomatiske midler, kinetiske motangrep eller økonomiske sanksjoner (Iasello, 2014, s.55). Denne typen avskrekking er ikke fullstendig berodd på at man kun straffes i etterkant av et angrep, det kan også innebære forebyggende angrep mot en potensiell aggressor (Iasello, 2014, s.55). Hvis man tar utgangspunkt i at USA sto bak Stuxnet-angrepet, kan man se på dette som forebyggende avskrekking ved straff mot Iran (Iasello, 2014, s.55).

Likevel understrekes det at avskrekking bare er et alternativ hvis staten, gruppen eller individet de har til hensikt å avskrekke er rasjonelle; og som sådan kan avskrekkes fordi de ikke er villige til å risikere å miste noe av større verdi (Iasello, 2014, s.64). Hvis motstanderen ikke har er rasjonelt syn på verden og hans plass i den, og heller ikke har noe å tape eller bli truet med, kan det være svært utfordrende å avskrekke ham fra et bestemt handlingsforløp (Iasello, 2014, s.64). Derfor er det ofte lettere å avskrekke stater, fremfor individer og uavhengige organisasjoner (Iasello, 2014, s.64).

2.5 North Atlantic Treaty Organization

NATO er en politisk og militær forsvarsallianse som har som mål å garantere medlemslandenes frihet og sikkerhet (NATO, u.å.). Politisk er NATO med på å fremme demokratiske verdier og gjør det mulig for medlemsland å rådføre seg og samarbeide om forsvars- og sikkerhetsrelaterte temaer for å løse problemer, bygge tillit, og i det lange løp, forhindre konflikter (NATO, u.å.). På den militære siden er NATO først og fremst forpliktet til å finne en fredelig løsning av tvister, men hvis den diplomatiske innsatsen mislykkes, har organisasjonen militærmakt til å gjennomføre krisestyringsoperasjoner i henhold til Washington-traktaten eller under FN-mandat (NATO, u.å.).

NATOs strategiske konsept fremlegger tre essensielle kjerneoppgaver for alliansen: kollektivt forsvar, krisehåndtering og sikkerhetssamarbeid (Brent, 2019). Siden 2014 har cybersikkerhet også vært en kjernesak som inngår i det kollektive forsvaret (Brent, 2019). Organisasjonen er etablert med et overordnet mål om å fremme fred og sikkerhet, og er på mange måter en organisasjon som er bygget på avskrekking. Ifølge Burton (2015, s.309) benytter NATO seg av avskrekking ved benektelse i cyberspace. Dette vil utdypes og diskuteres nærmere i analysedelen i oppgaven.

3. Metode og design

I dette delkapitlet vil metoden som er benyttet for å innhente data gjøres rede for. Videre vil utfordringer og valg tatt underveis i prosessen presenteres. I tillegg vil oppgavens kvalitet gjennomgås.

Problemstillingen for denne analysen er utformet slik: *«Kan NATO avskrekke cyberangrep?»*. NATOs evolusjon innenfor cybersikkerhet vil bli særskilt vektlagt i analysen. For å besvare problemstillingen har jeg valgt å gjennomføre en prosessanalyse som er bygget på en ren dokumentstudie. Hensikten med dette er å få en bredere forståelse av hvordan cyberangrep kan avskrekkes gjennom å bruke NATO som case. I analysedelen vil empirien, der det er mulig, i all hovedsak bestå av primære kilder, i form av toppmøteerklæringer. Ytterligere vil andre artikler og utdrag fra taler hentet fra NATOs egne sider brukes der de er relevante, i tillegg til noen sekundære kilder. Litteraturen som er gjennomgått i seksjon 2 brukes kontinuerlig som et verktøy for å tolke empirien og forklare resultatene i analysen. Hensikten er å gjennomføre en empirisk prosessanalyse basert på innsamling og tolkning av primærkilder.

3.1 Datainnsamling

I denne oppgaven har jeg valgt å generere data ved å gjøre en ren dokumentstudie. En slik studie kan gjøres på mange ulike måter og til mange ulike formål, men felles for alle er at man i hovedsak innhenter og bruker dokumenter som er produsert for andre formål enn forskning (Tjora, 2017, s.182). Ved å anvende og analysere allerede eksisterende dokumenter er det mulig å hente informasjon om hendelser og saksforhold som er skrevet ned på spesifikke tider og steder, og som er produsert med ulike formål (Tjora, 2017, s.183).

For å belyse NATOs utvikling innenfor cyberforsvar har det vært hensiktsmessig å se på NATOs egne referat fra toppmøter for å få en forståelse av arbeidet som er gjort innenfor emnet. Disse dokumentene kan tenkes å være nyttige for å besvare problemstillingen fordi de viser en tydelig bevisstgjøring, kontinuerlig fokus og utvikling innenfor håndteringen av, og avskrekkingen mot, cyberangrep. I analysen vil punktene som omhandler cybersikkerhet i toppmøteerklæringer fra 2002 frem til 2018 bli brukt. Disse er hentet direkte fra NATOs egne hjemmesider og er de politiske dokumentene på høyeste nivå som alliansen handler etter, på bakgrunn av dette er disse dokumentene uvurderlige og følgelig sikre kilder. Det vil vies mest plass til toppmøteerklæringene fra 2014, 2016 og 2018 fordi disse etter min vurdering er de mest imperative og de som inneholder de mest elementære endringene i NATO med henhold til cyberforsvar.

Cyberangrepet mot Estland i 2007 har under arbeidet med denne oppgaven vist seg å være en

viktig del av alliansens evolusjon, og brukes i denne oppgaven for å illustrere starsskuddet for alliansens utvikling. Akkurat dette angrepet er viktig for denne oppgaven fordi kjølvannet av angrepet markerer et tydelig skifte i utviklingen, og førte til at den første policyen for cyberforsvar ble utformet. Angrepet er et godt empirisk eksempel på hvordan et cyberangrep kan utspille seg, men er også det angrepet som har hatt mest innvirkning på alliansen i nyere tid. Litteratur knyttet til Estland angrepet er hentet både fra egne NATO dokumenter, i tillegg til sekundære kilder som skildrer og analyserer andre aspekter av hendelsen.

3.2 Utfordringer og kvalitet.

Cyberspace og avskrekking er store tema, og følgelig er også litteraturen innenfor emnene brede og mangfoldige. I arbeidet med oppgaven har det vært viktig for meg å få et innblikk i flere sider av cybertematikken, og få en forståelse for det store bildet, selv om min oppgave har et begrenset fokusområde. Arbeidet med oppgaven har på mange måter vært en læringsprosess, i og med at tema ble valgt på bakgrunn av en generell interesse og et ønske om å få en bredere forståelse for cyberpolitikk. Å snevre tema inn til å fokusere på NATO og deres form for avskrekking i cyberspace ble en måte å spisse tema inn på noe spesifikt, men som likevel kan ha en overføringsverdi. Ved at dette temaet ble valgt på bakgrunn av en generell interesse, og at forkunnskapene innenfor temaet var begrenset i begynnelsen av arbeidet, vil jeg si at pålideligheten i denne oppgaven er god. Pålitelighet handler om forskerens evne til å være objektiv, og ikke la egne mulig forutinntatte holdninger forme forskningen (Tjora, 2017, s.235). Underveis i arbeidet med oppgaven har jeg gradvis fått en god forståelse for tema, men jeg vil likevel argumentere for at jeg har forholdt meg objektiv og ikke forhastet noen konklusjoner.

Gyldighet handler om spørsmålet om hvorvidt de svarene man finner i egen forskning, faktisk er svar på de spørsmålene man forsøker å stille (Tjora, 2017, s.232). Resultatene i analysen er basert på min egen tolkning av det empiriske materialet og er underbygget med tidligere forskning gjennomgått i seksjon 2. Jeg mener oppgaven har god gyldighet, men at den mulig svekkes noe på bakgrunn av min uerfarenhet som forsker.

Generaliserbarhet, eller overførbarhet, er knyttet til hvorvidt forskningen har en relevans utover tilfeller som har vært utforsket (Tjora, 2017, s.231). Målet med dette er å utvikle forskning som kan gi kunnskap som kan brukes av andre, og på denne måten ha en overføringsverdi. Jeg tror

denne oppgaven kan gi økt kunnskap innenfor temaet avskrekking i cyberspace. Ved å bruke NATO som rammeverk for temaet får man satt det i en spesifikk kontekst, men jeg tror likevel at funnene i analysen kan ha en viss relevans utover mitt valgte forskningstema. Likevel bør det nevnes at min forskning er gjort over en relativt kort periode og med begrensninger i forhold til omfang. I et større forskningsprosjekt ville jeg viet mer plass til overtalelse (coercion) i cyberspace, og inkludert en grundigere gjennomgang av flere cyberangrep for å øke overføringsverdien. Funnene i analysen bør derfor behandles med forsiktighet, og betraktes som antakelser, heller enn bestemte konklusjoner.

4.0 Analyse

I denne delen av oppgaven vil empirien presenteres, og samtidig tolkes og analyseres kontinuerlig. Litteraturen som er presentert i seksjon 2 brukes underveis som verktøy for å tolke og forklare funnene i analysen. Analysen følger en kronologisk rekkefølge, og vil starte med å gjennomgå toppmøtet fra 2002 og jobbe seg frem til toppmøtet i 2018. Underveis i analysen vil det vies mer plass til cyberangrepet mot Estland i 2007, i tillegg til toppmøteerklæringene fra 2014, 2016 og 2018.

4.1 NATOs tidlige cyberevolusjon

NATO har alltid vært opptatt av å beskytte sine kommunikasjons- og informasjonssystemer, men det var ikke før i 2002 at cyberforsvar ble satt på alliansens politiske agenda under toppmøtet i Praha (NATO, 2020). Et av tiltakene som ble gjort var å etablere NATO Computer Incident Response Capability (NCIRC), som er organet som beskytter NATOs egne nettverk gjennom teknisk og lovgivende støtte for cyberforsvar døgnet rundt (NATO, 2019). Selv om cybersikkerhet ble satt på agendaen, var det kun ett punkt som omhandler cybersikkerhet, punkt 4f sier ganske enkelt «Styrke vår kapasitet til å forsvare oss mot cyberangrep», men inkluderer ingen plan for hvordan dette skal utføres (NATO, 2002). Det er tydelig en intensjon om å styrke kapasiteten, men uten en handlingsplan for hvordan dette skal gjøres blir det ingen utvikling på området.

I årene som fulgte var det heller ikke noen merkverdig utvikling på området, foruten toppmøtet i Riga 2006 der de allierte gjentok behovet for å beskytte sine informasjonssystemer (NATO, 2020 & NATO, 2006). I denne toppmøteerklæringen spesifiseres det mer tydelig at intensjonen

er å beskytte egne informasjonssystemer i NATO sentralt, hvordan allierte stater skal beskytte seg nevnes ikke. Men, heller ikke i denne erklæringen fremlegges det noen plan for hvordan de vil styrke kapasiteten. Likevel kan man skimte en påbegynnende avskrekking ved benektelse, i den forstand at NATO har som formål å beskytte seg. Selv om toppmøtet i Riga satte cyber tilbake på agendaen, er det naturlig å anta at utviklingen fortsatt ville vært sendrektig hadde det ikke vært for angrepet mot Estland som virkelig satte cybersikkerhet på dagsordenen.

4.2 Cyberangrepene i Estland 2007

I slutten av april i 2007 opplevde Estland å bli utsatt for en rekke cyberangrep over en periode på om lag 3 uker. Bakgrunnen for angrepene var at de Estlandske myndighetene i januar i 2007 annonserte at de ville flytte ett andre verdenskrig monument ut av hovedstaden Tallin (Schmidt, 2013, s.1). Monumentet ble reist i 1947 og er en statue av en soldat ikledd den røde armes uniform, og var laget for å hedre de falne soldatene under krigen (Schmidt, 2013, s.2). Etter at Estland gjenvant sin politiske suverenitet i 1991 ble det gnisninger mellom Estlands befolkning og Russland om hva statuen sto for. For Russland og flere russisk-estlandske mennesker var denne statuen et symbol på hvordan den røde arme hadde kjempet mot Tyskerne under andre verdenskrig (Schmidt, 2013, s.2). For Estlendere derimot, var dette heller et symbol for hvordan den røde arme og videre Sovjet Unionen bidro til den årelange undertrykkelsen av Estlands uavhengighet (Schmidt, 2013, s.3). Etter flere år med debatt, splittelser og appeller rundt statuen vedtok statsminister Andrus Ansip å flytte den den 26 april 2007 (Schmidt, 2013, s.3). Allerede dagen etter kom de første tegnene til et cyberangrep.

Angrepene var rettet mot en rekke ulike servere, som e-post, rutere og DNS (Domain Name System), som i all hovedsak tilhørte politiske enheter, men også Estlands to største banker, telekommunikasjonsselskaper og internett-leverandører (Joubert, 2012, s.1). Estland var allerede på denne tiden avhengige av internett for sin kritiske infrastruktur; elektroniske nettverk er integrert i funksjonen til statlige operasjoner, 97% av banktransaksjoner skjer online og Tallinns vannforsyning er avhengig av internett (Herzog, 2011, s.51). Estlands statlige operasjoner var så avhengige av internett at det er blitt referert til som et «paperless government» (Herzog, 2011, s.51). Ved å angripe både kritisk infrastruktur og politiske enheter simultant paralyserer aggressoren samtidig statens handlingsrom for å stoppe angrepene.

De fleste angrepene var såkalte «Distributed Denial of Service» (DDoS) angrep. Dette er en

metode der de som angriper etablerer millioner av «zombie» datamaskiner som overfyller nettsider langt over dens kapasitet og som videre gjør at systemet krasjer og det blir fullstendig stillstand (Joubert, 2012, s.1). Denne typen angrep er på ingen måte særlig sofistikerte angrep, men for et land som er fullstendig avhengig av internett for å fungere, og som heller ikke har et etablert cyberforsvar, blir denne typen angrep veldig forstyrrende og ødeleggende.

Naturligvis ble det antatt at Russland sto bak angrepene, men selv om det ble satt inn eksperter fra både EU og NATO for å undersøke dette, klarte de ikke å finne tilstrekkelig bevis for å attribuere angrepet til Russland (Herzog, 2011, s.53). I tillegg nektet Russland for å stå bak. Dette er et klassisk eksempel på attribusjonsproblemet, der ingen vil ta på seg skyld og man heller ikke klarer å bevise hvem som står bak. Hvis man regner med at Russland sto bak, uavhengig av om det var autonome- eller statlige aktører, var et cyberangrep muligens den smarteste måten å angripe Estland på. Som medlem av NATO er Estland underlagt Washington traktaten, der artikkel 5 konstaterer at "et væpnet angrep mot en, er et angrep på oss alle" (NATO, 1949). Hadde Russland valgt et kinetisk angrep ville artikkel 5 tredd i kraft, men siden cyberangrep på denne tiden ikke ble regnet som et væpnet angrep, og det heller ikke fantes noen handlingsplan for å håndtere slike angrep, ble dette umulig. Et cyberangrep ble Russlands måte å angripe på uten å risikere noen store tap eller kostnader selv. Angrepet mot Estland ble på mange måter en oppvekker for alliansen, der det ble åpenbart at det var behov for en tydelig handlingsplan for håndteringen av cyberangrep, i tillegg til å etablere et fungerende forsvar mot det.

I kjølvannet av angrepet på Estland ble NATO og de allierte enige om at det trengtes hurtig utvikling på området, og resultatet av dette ble at NATO godkjente sin første policy om cyberforsvar i januar 2008 (NATO, 2020). Den nye policyen understreket at NATO og allierte må beskytte sine informasjonssystemer i samsvar med deres ansvarsområder; dele beste praksis; og hjelpe allierte på forespørsel for å motvirke cyberangrep (NATO, 2008A). I tillegg etablerte de "Cooperative Cyber Defence Centre of Excellence" i Estland, et senter for å drive forskning på, og opplæring om, cyberkrigføring (NATO, 2008B). Denne policyen omhandler kun å beskytte seg *mot* et angrep, og er derfor å betrakte som et av de første skrittene for alliansen i å etablere en fungerende avskrekking ved benektelse.

4.3 Evolusjonen etter Estland

Etter angrepet mot Estland i 2007 var cybersikkerhet høyt oppe på agendaen hos NATO, men et nytt russisk angrep, denne gangen mot Georgia, gjorde alliansen oppmerksom på enda et aspekt av cybersikkerhet. I løpet av sommeren 2008 ble Georgia invadert av Russland, men i tillegg til den konvensjonelle formen for krigføring, ble det også brukt cybervåpen, noe som gjorde dette til en hybridkrig (NATO, 2020). Denne nye måten å bruke cybervåpen på ble da enda et aspekt å ta i betraktning i det videre arbeidet med å etablere et fungerende cyberforsvar.

Under toppmøtet i Lisboa i 2010 konstaterer de først at cybertrusselen blir stadig større og blir mer sofistikert, og at det trengs flere virkemidler for å sikre NATOs kritiske systemer (NATO, 2010). Under toppmøtet ble et nytt strategisk konsept vedtatt, der «North Atlantic Council» ble bedt om å utvikle en grundig cyberforsvarpolicy, i tillegg til å utarbeide en handlingsplan for gjennomføringen av den innen juni 2011 (NATO, 2010). Denne policyen inkluderte flere viktige mål: NCIRC skal ha full operativ kapasitet innen 2012 for å ha sentralisert cyberbeskyttelse for alle NATO-organer; utvikle cyber «Rapid Reaction Teams» (RRTs) som umiddelbart kan rykke ut hvis en alliert blir angrepet; utvidet samarbeid mellom allierte stater, men også til organisasjoner som FN og EU (NATO, 2010). Denne policyen ble etablert etter planen og ble i 2011 den andre policyen på cyberforsvar i NATO (NATO, 2020).

I motsetning til det tidlige arbeidet med cyberforsvar, har denne policyen en mye mer spesifikk plan for hvordan de vil beskytte seg mot cyberangrep. Selv om det største fokuset fortsatt omhandler å beskytte NATO sentralt, er det her for første gang et tiltak som omhandler beskyttelse for de allierte statene, nemlig RRTs. Også her ser man en tydelig avskrekking ved benektelse strategi. Toppmøteerklæringen fra Chicago 2012 bekreftet NATO å fortsatt forplikte seg til policyen som ble etablert i 2011 (NATO, 2012).

4.4 «Wales Summit Declaration 2014»

Under toppmøtet i Wales i 2014 gjorde NATO flere store endringer i politikken rundt cybersikkerhet, og for første gang er det to punkter som omhandler cybersikkerhet, nummer 72 og 73. Punkt 72 begynner med å understreke den økende cybertrusselen, og for å håndtere denne er det etablert en «Enhanced Cyber Defence Policy». Policyen legger til grunn at NATOs hovedansvar er å forsvare egne nettverk, og at enhver alliert har et ansvar for å utvikle relevant kapasitet for å beskytte egne nettverk (NATO, 2014). Likevel skal enhver forespørsel om

bistand behandles i tråd med solidaritet ovenfor de allierte (NATO, 2014). I tillegg bekrefter policyen prinsippene om udeleligheten av alliert sikkerhet for å forhindre, oppdage, motstå, gjenopprette og forsvare seg mot cyberangrep (NATO, 2014). Disse prinsippene kan knyttes tett til avskrekking ved benektelse, fordi det kun refereres til måter å beskytte seg på, og nevner ingenting om mulige motangrep.

Videre nevnes det at gode bi- og multilaterale samarbeid er viktig for å styrke motstandsdyktigheten, i tillegg til å utvide handlingsrommet når det kommer til å attribuere et angrep (NATO, 2014). Organisasjoner som EU og FN trekkes frem som viktige samarbeidspartnere, i tillegg til den private sektoren for å få tilgang til ny teknologi og elementær kompetanse (NATO, 2014). Videre poengteres det også at de vil øke nivået på utdanning, trening og øvelser for å styrke kapasiteten ytterligere (NATO, 2014).

Det er spesielt to endringer som har størst innvirkning på utviklingen av cybersikkerheten. For det første, NATO bekrefter at cybersikkerhet er en del av NATOs kjerneoppgaver når det kommer til kollektivt forsvar (NATO, 2014). Bakgrunnen for dette er at cyberangrep kan være like skadelige for moderne samfunn som konvensjonelle angrep, noe som kan settes i sammenheng med effektene av cyberangrepet mot Estland.

For det andre, anerkjenner NATO at internasjonal lov gjelder i cyberspace (NATO, 2014). Denne typen lov setter klare grenser når det kommer til proporsjonalitet og ikke-eskalering, men i og med at alliansen ikke nevner noe om motangrep i denne erklæringen, er dette punktet ikke veldig relevant. Men, det åpner dører spesielt når det kommer til attribusjon. Det gir muligheten til å attribuere et angrep basert på den iboende retten til selvforsvar. I tillegg til utvidede bi- og multilaterale samarbeid øker de muligheten sin til å suksessfullt attribuere et potensielt angrep, noe som igjen vil fungere avskrekkende. Jo bedre alliansen blir på attribusjon, jo mer avskrekkende vil det fungere fordi en aggressor mulig regner nytten lavere enn kostnaden. Selv om alliansen ikke har noen mulighet til å gjøre et motangrep mot aggressoren, kan det likevel få konsekvenser for senere samarbeid. Toppmøteerklæringen i 2014 tar et stort skritt videre i å utvikle bedre politikk på cybersikkerhet, men forblir innenfor avskrekking ved benektelse enn så lenge.

4.5 «Warsaw Summit Communiqué 2016»

Under toppmøtet i Warszawa understreker de at cyberangrep er en økende trussel, og at cybersikkerhet forblir en del av alliansens kjerneoppgaver. I tillegg forplikter de seg til å fortsette videreutviklingen og implementeringen av «Enhanced Cyber Defence Policy» (NATO, 2016A). En videreføring av tiltakene fra 2014 var å forvente, men det er likevel to punkter fra Warszawa som virkelig endrer alliansens cybersikkerhet.

For det første, skapte de en «Cyber Defence Pledge». Dette løftet innebærer blant annet at de allierte statsoverhodene forplikter seg til å være best mulig forberedt på alle utfordringer de vil møte i cyberspace (NATO, 2016B). I tillegg må hver alliert ta ansvar for å forbedre sin egen motstandskraft, beskytte egne nettverk, og øke evnen til å besvare et hvert cyberangrep (NATO, 2016B). I tillegg inkluderer den et løfte om å fortsette å ha gode bi- og multilaterale samarbeid, for å få tilgang til ny kunnskap og teknologi, men også for å øke utdanningskapasiteten innenfor cybersikkerhet (NATO, 2016A). Det er tydelig at dette løftet på mange måter inneholder mye av de samme lovnadene som ble uttrykt i 2014, men den store endringen her er at det er transformert til et nedskrevet løfte. NATO sentralt, samt hver enkelt alliert, har gjennom dette løftet forpliktet seg til å gjøre alt de kan for å heve sin forsvarsevne i cyberspace. I tillegg vil alliertes progresjon innenfor cybersikkerhet blir gjennomgått under hvert toppmøte, for å forsikre seg om at alle holder sin forpliktelse til «Cyber Defence Pledge» (NATO, 2016B). Dette løftet er skapt av alliansens øverste ledere, og kan regnes som et av de mest innflytelsesrike dokumentene som er skapt for å håndtere den økte cybertrusselen.

For det andre, ble cyberspace anerkjent som et domene der NATO må forsvare seg og operere like effektivt som de gjør til sjøs, i luften og på land (NATO, 2016A). Bakgrunnen for dette er å øke alliansens evne til å beskytte seg, samt gjennomføre operasjoner på tvers av disse domenene (NATO, 2016A). Ved å likestille cyberspace med de tre andre domenene, vil de kunne opprettholde handlings- og beslutningsfriheten under alle omstendigheter (NATO, 2016A). Å anerkjenne cyberspace som et domene, vil gjøre at et angrep her vil kunne føre til de samme konsekvensene som et tradisjonelt angrep innenfor noen av de andre domenene. Denne likestillingen åpner nemlig muligheten til å gjøre motangrep, noe som radikalt endrer alliansens tidligere metode for avskrekking som utelukkende har vært benektelse. Endringen gjør at alliansen nå fører en kombinasjon av benektelse og straff, noe som vil styrke deres generelle avskrekking. Den aller mest revolusjonerende endringen denne likestillingen fører til,

er likevel de alliertes mulighet til å be om en påberopelse av artikkel 5 i Washington traktaten. Det finnes ingen offisiell grense for når en påberopelse av artikkel 5 er garantert, men at muligheten finnes, vil også bidra til å øke alliansens generelle avskrekking.

Likestillingen av domenene åpner også opp for å besvare cyberangrep med kinetiske midler, som for mange potensielle aggressorer vil gjøre den mulige gevinsten av et angrep for liten med tanke på de mulige tapene det kan føre til. Alliansen opprettholder sitt defensive mandat og sin intensjon om å følge prinsipper om tilbakeholdenhet, i tillegg til å jobbe for internasjonal fred, sikkerhet og stabilitet – også i cyberspace (NATO, 2016A & NATO, 2020). Dette understreker alliansens mål om å hovedsakelig drive avskrekking ved benektelse, men at et hvert angrep vil motsvares innenfor rammene av proporsjonalitet.

4.6 «Brussels Summit Declaration 2018»

I denne toppmøteerklæringen er cybertiltakene nevnt allerede i punkt 20, i motsetning til punkt 70 i de foregående erklæringene. I tillegg nevnes cyber innenfor er rekke andre problemstillinger, noe som kan tolkes som at cyberforsvar stadig blir en viktigere del av det kollektive forsvaret. Punkt 20 starter med å understreke at cybertrusselen stadig øker, blir mer kompleks og mer ødeleggende (NATO, 2018). Videre bekrefter de igjen at cybersikkerhet fortsatt er en kjernesak for det kollektive forsvaret, samt at de vil fortsette arbeidet med å implementere cyberspace som eget domene (NATO, 2018). De ønsker også et utvidet fokus på «Cyber Defence Pledge» for å ytterligere styrke cyberforsvaret, både for NATO sentralt, men også for individuelle allierte (NATO, 2018). Samtidig bekrefter de igjen at de vil følge internasjonalt lovverk i cyberspace, i tillegg til å videreutvikle bi- og multilaterale samarbeid for å holde tritt med teknologi og akademia (NATO, 2018).

Det mest merkverdige punktet i denne erklæringen er derimot at NATO for første gang beslutter at de vil benytte seg av hele spekteret av cyberevner, i tillegg til å «integrate sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions, in the framework of strong political oversight» (NATO, 2018). Alliansen understreker at de fortsatt forholder seg til sitt defensive mandat, men dette er likevel en endring som åpner for en mer offensiv tilnærming til cybersikkerhet.

Et annet viktig moment fra denne erklæringen er lovnaden om å jobbe sammen for å utvikle tiltak som gjør at man kan påføre en eventuell aggressor skade eller kostnader (NATO, 2018). I tillegg nevner de at individuelle allierte selv kan vurdere hvorvidt de ønsker å tilskrive og svare på eventuelle cyberangrep og at attribusjon er et suverent nasjonalt privilegium (NATO, 2018). Å åpne opp for at allierte selv kan vurdere attribusjon og motangrep er med på å styrke individuelle alliertes suverenitet, og er en tillitserklæring fra NATOs side. Det gir den enkelte alliert muligheten til å beskytte sin suverenitet, mens de også har alliansen i ryggen. Likevel bør attribusjon gjøres med forsiktighet, og motangrep gjøres proporsjonelt. Gjennomfører man et motangrep mot en stat som ikke sto bak et angrep, vil man selv bli aggressor, og er åpen for angrep tilbake.

Samlet sett peker dette erklæringen i retning av en mer offensiv strategi, der de åpner opp for å bruke hele spekteret av cybermidler i tillegg til at de vil utvikle tiltak for å straffe en aggressor. NATO som organisasjon har er løfte om å jobbe for fred og stabilitet, men de har også et løfte om å sikre de alliertes sikkerhet. Dette skiftet mot en mer offensiv tilnærming vil fungere avskrekkende i aller høyeste grad. Ved å ikke bare fokusere på å beskytte seg selv, men også demonstrere hvilke offensive kapasiteter de har, vil alliansen utad se mektigere ut, som igjen har en avskrekkende effekt. Samtidig vil det å åpne opp for en mer offensiv tilnærming til avskrekking gjøre det mulig å jobbe mer forebyggende. Et godt eksempel på dette er som nevnt Stuxnet, der Iran ble straffet i forkant av en handling. I tillegg er cybervåpen som nevnt en human form for krigføring, noe som passer under alliansens fredelige mandat. Denne erklæringen viser et permanent skifte fra avskrekking ved benektelse til en kombinasjon av benektelse og straff. Det var allerede tendenser til dette i erklæringen fra 2016, men de nye offensive punktene i denne erklæringen bekrefter dette ytterligere. Å føre en kombinasjon der man i aller høyeste grad forsøker å nekte en aggressor muligheten til å angripe, men samtidig har muligheten til å gjøre et motangrep hvis det skulle skje, er nok den mest effektive måten å drive avskrekking på.

5.0 Oppsummering og konklusjon

Hensikten med denne oppgaven har vært å besvare problemstillingen: *«Kan NATO avskrekke cyberangrep?»*. For å besvare denne er det gjennomført en prosessanalyse av NATOs evolusjon

innenfor cybersikkerhet, og funnene er satt i sammenheng med litteratur innenfor avskrekking i cyberspace. Analysen har tatt for seg toppmøteerklæringer fra 2002 frem til 2018 i kronologisk rekkefølge.

Analysen viser at i begynnelsen av NATOs evolusjon har de utelukkende en avskrekking ved benektelse, ved at fokuset kun omhandler å beskytte seg selv. De tidlige årene av alliansens evolusjon viser også kun en intensjon om å styrke sin kapasitet, uten noen form for handlingsplan på hvordan. Det er ikke før cyberangrepene mot Estland i 2007 at det ble utviklet en plan for hvordan de ønsket å utvikle sin forsvarskapasitet i cyberspace. Disse angrepene markerer startskuddet for alliansens utvikling, og som viser en tydelig plan for å beskytte seg mot cyberangrep, med andre ord; avskrekking ved benektelse. I 2014 inkluderes cybersikkerhet i alliansens kjerneoppgave for kollektivt forsvar, i tillegg til at internasjonalt lovverk anerkjennes i cyberspace. Dette åpner flere dører når det kommer til attribusjon, men avskrekkingsmetoden er fortsatt utelukkende benektelse. Det er ikke før i 2016 at strategien går over til å bli en kombinasjon av benektelse og straff. Bakgrunnen for dette er at cyberspace anerkjennes som et domene i likhet med sjø, luft og land. Dette åpner for å gjennomføre motangrep og om nødvendig påberope artikkel 5 i Washington traktaten. Denne endringen styrker den generelle avskrekkingen betraktelig, og gjør et cyberangrep like kostbart som et konvensjonelt angrep. I 2018 styrker de den kombinerte avskrekkingsmetoden ytterligere ved å åpne opp for en mer offensiv strategi. Dette gir NATO og de allierte muligheten til å vise sin cyberkapasitet, som igjen fungerer avskrekkende på aggressorer.

Samlet sett viser analysen hvordan NATO har gått fra å benytte seg eksplisitt av avskrekking ved benektelse, til å gå over til å føre en kombinasjon av benektelse og straff. Alliansen har utviklet seg i takt med trusselbildet, og har utført nødvendige tiltak for å sikre de allierte og NATO sentralt. På bakgrunn av funn i analysen og et fravær av signifikante angrep mot alliansen i senere tid, vil jeg konkludere med at NATO faktisk *kan* avskrekke cyberangrep. Denne konklusjonen trekkes med forbehold om at aktørene alliansen har til hensikt å avskrekke er rasjonelle aktører. Det vil imidlertid bli spennende å se hva fremtiden bringer av tiltak og angrep, og om NATO vil kunne fortsette å holde tritt med potensielle aggressorer.

Litteraturliste

Blagden, D. (2020). Deterring Cyber Coercion: The Exaggerated Problem of Attribution. *Survival*, *62*(1), 131-148. DOI: 10.1080/00396338.2020.1715072

Borghard, E & Lonergan, S.W. (2017). The Logic of Coercion in Cyberspace. *Security Studies*, *26*(3), 452-481, DOI: 10.1080/09636412.2017.1306396

Brent, L. (2019). NATO's role in cyberspace. *NATO Review*. Hentet fra: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

Burton, J. (2015). NATO's cyber defence: strategic challenges and institutional adaptation. *Defence Studies*, *15*(4), 297-319, DOI: 10.1080/14702436.2015.1108108

Farwell, J.P & Rohozinski,R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23-40, DOI: 10.1080/00396338.2011.555586

Fitton, O. (2016). Cyber Operations and Gray Zones: Challenges for NATO. *Connections: The Quarterly Journal. 15*(2), 109-119, DOI: http://dx.doi.org/10.11610/Connections.15.2.08

Goodman, W. (2010). Cyber Deterrence: Tougher in Theory than in Practice? *Strategic Studies Quarterly*, *4*(3), 102-135. Hentet fra: www.jstor.org/stable/26269789

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, *4*(2), 49-60. DOI: http://dx.doi.org/10.5038/1944-0472.4.2.3

Iasiello, E. (2014). Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security*, *7*(1), 54-67. DOI: http://dx.doi.org/10.5038/1944-0472.7.1.5

Jensen, B, Valeriano, B & Maness, R. (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies, 42*(2), 212-234. DOI: 10.1080/01402390.2018.1559152

Joubert, V. (2012). Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?. NATO Defense College, *Research Division*. Hentet fra: https://www.files.ethz.ch/isn/143191/rp_76.pdf

Kissinger, H. (2014). *World Order*. New York: Penguin Press.

Kramer, F, Butler, R & Lotrionte C. (2016). Cyber, Extended Deterrence, and NATO. *Atlantic Council*, 1-12. Hentet fra: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf

Libicki, M. (2018). Expectations of Cyber Deterrence. *Strategic Studies Quarterly*, *12*(4), 44-57. Hentet fra: www.jstor.org/stable/26533614

Morgan, P.M. (2012). The State of Deterrence in International Politics Today. *Contemporary Security Policy*, *33*(1), 85-107, DOI: 10.1080/13523260.2012.659589

NATO. (1949, 4. April). The North Atlantic Treaty. Hentet fra: https://www.nato.int/cps/en/natolive/official_texts_17120.htm

NATO. (2002, 21. November). Prague Summit Declaration. Hentet fra: https://www.nato.int/cps/en/natohq/official_texts_19552.htm?

NATO. (2006, 29. November). Riga Summit Declaration. Hentet fra: https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en

NATO. (2008A, 3. April). Bucharest Summit Declaration. Hentet fra: https://www.nato.int/cps/en/natolive/official_texts_8443.htm

NATO. (2008B, 14. Mai). NATO opens new centre of excellence on cyber defence. Hentet fra: https://www.nato.int/docu/update/2008/05-may/e0514a.html

NATO. (2010, 20. November). Lisbon Summit Declaration. Hentet fra:

https://www.nato.int/cps/en/natolive/official_texts_68828.htm

NATO. (2012, 20. Mai). Chicago Summit Declaration. Hentet fra: https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en

NATO. (2014, 5. September). Wales Summit Declaration. Hentet fra: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO. (2016A, 9. Juli). Warsaw Summit Communiqué. Hentet fra: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO. (2016B, 8. Juli). Cyber Defence Pledge. Hentet fra: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO. (2018, 30. August). Brussels Summit Declaration. Hentet fra: https://www.nato.int/cps/en/natohq/official_texts_156624.htm

NATO. (2019, 19. Februar). NATO Cyber Defence. Hentet fra: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf

NATO. (2020, 17. Mars). Cyber Defence. Hentet fra: https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO. (u.å). What is NATO. Hentet fra: https://www.nato.int/nato-welcome/index.html

Rid, T & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*(1-2), 4-37, DOI: 10.1080/01402390.2014.977382

Schmidt, A. (2013). The Estonian Cyberattacks. I: Healey, J (red.). *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*. Arlington: Cyber Conflict Studies Association.

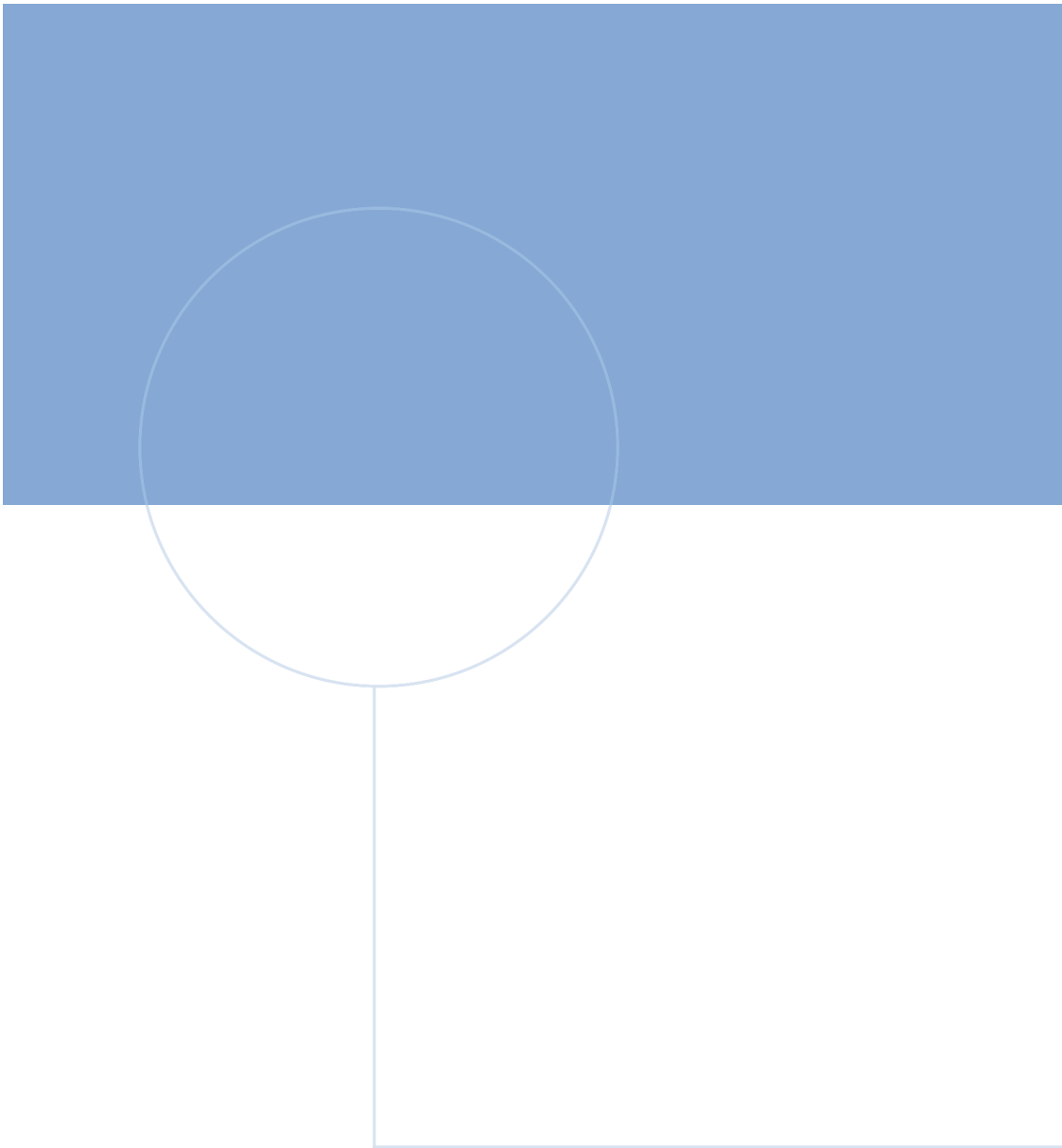
Shakarian, P. (2011). The 2008 Russian Cyber Campaign Against Georgia. Hentet fra:

https://www.academia.edu/1110559/The_2008_Russian_Cyber_Campaign_Against_Georgia

Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly*, *12*(3), 90-113. Hentet fra: www.jstor.org/stable/26481911

Stoltenberg, J. (2019). NATO will defend itself. *Prospect*. Hentet fra: https://www.prospectmagazine.co.uk/world/nato-will-defend-itself-summit-jens-stoltenberg-cyber-security

Tjora, A. (2017). *Kvalitative forskningsmetoder i praksis* (3.utg.). Oslo: Gyldendal Norsk Forlag AS



NTNU

Kunnskap for en bedre verden