Eksamen i Modul VII

Bacheloroppgave

«NATOs tilnærming til cyberdomenet i perioden 1999-2019»

av

Kadetter Marius Talgø og Matias Valenzuela

Godkjent for offentlig publisering

Kull 68 **Luftkrigsskolen** **2020**

Publiseringsavtale

En avtale om elektronisk publisering av bachelor/prosjektoppgave

Kadetten(ene) har opphavsrett til oppgaven, inkludert rettighetene til å publisere den.

Alle oppgaver som oppfyller kravene til publisering vil bli registrert og publisert i Bibsys Brage når kadetten(ene) har godkjent publisering.

Oppgaver som er graderte eller begrenset av en inngått avtale vil ikke bli publisert.

Jeg(Vi) gir herved Luftkrigsskolen rett til å gjøre denne oppgaven tilgjengelig elektronisk, gratis og uten kostnader	[X] Ja	[ ] Nei
Finnes det en avtale om forsinket eller kun intern publisering? (Utfyllende opplysninger må fylles ut) Hvis ja: kan oppgaven publiseres elektronisk når embargoperioden utløper?	[ ] Ja [ ] Ja	[X] Nei [ ] Nei

Plagiaterklæring

Jeg (Vi) erklærer herved at oppgaven er mitt eget arbeid og med bruk av riktig kildehenvisning.

Jeg (Vi) har ikke nyttet annen hjelp enn det som er beskrevet i oppgaven.

Jeg (Vi) er klar over at brudd på dette vil føre til avvisning av oppgaven.

Dato: 15 – 01- 2020

Innhold

1 Innledning

1.1 Bakgrunn

Under operasjon «Allied Force» i 1999 ble NATO et mål for cyberangrep. Angrepene bestod av denial-of-serviceangrep[1] (DOS), metning av e-postservere, samt 'defacement'[2] av nettsidene til Supreme Headquarters Allied Powers Europe (SHAPE). Angrepene ble gjennomført av hacktivister fra Serbia og angivelig Russland, og ble gjennomført som en protest mot bombingen i Kosovo (Verton, 1999; Messmer, 1999). 20 år senere stod NATOs generalsekretær, Jens Stoltenberg, på talerstolen under «the Cyber Defence Pledge Conference» i London og uttalte følgende:

> Cyber-attacks can be as damaging as conventional attacks. A single attack can inflict billions of dollars' worth of damage to our economies, bring global companies to a standstill, paralyse our critical infrastructure, undermine our democracies and have a crippling impact on military capabilities. (NATO, 2019)

Stoltenberg sa videre at det er enighet i NATO om at artikkel 5 kan utløses som følge av et cyberangrep. Et slikt angrep på et medlemsland kan dermed regnes som et angrep mot alle og kan besvares med militære virkemidler (NATO, 2019). Dette vitner om at cybertrusler har utviklet seg mye de siste 20 årene.

Hovedårsaken til at denne utviklingen har funnet sted er digitaliseringen verden har gjennomgått. Internett har bredd seg utover verden og blitt mer og mer tilgjengelig. Nasjoner, store som små, har utviklet sin infrastruktur for å passe inn i en digitalisert verden. Dette har gjort at banker, bedrifter og statlige tjenester har koblet seg på internett for å effektivisere sin virksomhet. Flere og flere mennesker får dermed tilgang til internett. I år 2000 var det omtrent 392,000,000 brukere av internett, mens det i 2019 var omtrent 4,536,000,000 brukere (Miniwatts Marketing Group, 2019). Den digitale populasjonen har dermed økt betraktelig.

På samme tid som den digitale populasjonen har økt har også den digitale sikkerhetstrusselen økt. Teknologien for å gjennomføre cyberangrep er, og har i lang tid vært, lett tilgjengelig. Verktøyet man trenger er en datamaskin med tilgang til internett, og ferdighetene kan anskaffes på gutterommet. Bare i Norge er det flere eksempler på ungdommer som har hacket seg inn i mailservere, finansinstitusjoner og kommuner (Karseth, Berge, & Johansen, 2019;

[1] DOS, herunder også DDOS (Distributed Denial of Service) er betegnelsen på aktivitet som har til hensikt å nekte brukere tilgang på en datasystem og tjenestene systemet administrerer.
[2] Defacement er et begrep som brukes på cyberangrep hvor man fjerner innhold fra nettsteder og gjerne erstatter dette med bilder eller tekst for å fremme egne synspunkt og politisk ståsted.

Sundvor, 2015; Grønning, 2011). Med dette i bakhodet kan man tenke seg til hva en statlig militær organisasjon kan oppnå med tilgang på avansert utstyr og materiell, et stort budsjett og organisert utdanning og trening.

I nyere tid har også begrepet «tingenes internett» dukket opp. Tingenes internett er opprinnelig et engelsk begrep, «Internet of Things», og betegner hverdagslige gjenstander som kobles til internett. Dette kan være gjenstander som printere, kjøleskap og termostater. Hensikten med disse er å gjøre hverdagen enklere ved å gi tilgang til disse gjennom andre enheter som datamaskiner eller mobile gjenstander. Slike enheter er som regel utviklet med fokus på forbrukervennlighet og profitt fremfor sikkerhet. De kan dermed utgjøre en sikkerhetsrisiko om de kobles til et ellers sikkert nett. Dette kom spesielt frem under en episode hvor stortinget så seg nødt til å stenge av ni printere etter mistanke om at en russisk etterretningsagent skal ha prøvd å få tilgang til stortingets lukkede nett gjennom disse (Wernersen & Asvall, 2018). Slike enheter kan man også finne andre steder, for eksempel i militære organisasjoner eller i lukkede nettverk tilhørende kritisk infrastruktur som strømnettet eller vannverket.

Trusselen digitaliseringen har medført bidrar dermed til at digital sikkerhet har blitt et militært anliggende. Militære organisasjoner som har til hensikt å forsvare nasjonen, må også kunne forsvare den mot omfattende cyberangrep som i verste fall kan stanse strømnettet og vannforsyning til sivile borgere. I tillegg er militæret avhengig av å forsvare sine egne systemer. Ved å bruke lukkede nett til å dele informasjon oppnår man store fordeler, som evnen til å dele informasjon til mange enheter over lange distanser på veldig kort tid. Dette kan gi store operasjonelle fordeler som gjør at man kan danne et felles situasjonsbilde på tvers av avdelinger, forsvarsgrener og nasjoner. For beslutningstakere betyr dette at ressursene blir mer tilgjengelige og enklere å utnytte. På samme tid som det gir store fordeler blir det også sårbart. På lik linje med resten av det digitaliserte samfunnet blir det lettere å finne inngangsveier for å ramme nettverk og systemer dess større nettverket er og dess flere tilkoblete enheter man har.

Gitt utviklingen og implementeringen av digitale enheter i det offentlige og ved militære institusjoner, samt utviklingen innen cyberkrigføring og cybersikkerhet de siste 20 årene, er det ingen overraskelse at NATOs ledere er enige om at et cyberangrep kan være av så alvorlig art at det vil kunne utløse artikkel 5 (Jens Stoltenberg). Det må dermed ha skjedd en tilsvarende utvikling i hvordan NATO forstår cyberangrep og alliansens bevissthet rundt dem.

1.2 Avgrensning og problemstilling

Denne oppgaven vil besvare problemstillingen:

Hvordan har NATOs tilnærming til cyberforsvar endret seg i takt med utviklingen av cybertrusselen i perioden 1999-2019?

Oppgaven vil først beskrive hvordan cybertrusselen har utviklet seg de siste 20 årene ved å greie ut om noen eksemplifiserende hendelser som har funnet sted i perioden. Den vil deretter ta utgangspunkt i deklarasjoner og uttalelser fra alliansens toppmøter for å gjøre rede for hvilke endringer som har funnet sted i NATOs tilnærming til cyberforsvar. Videre vil oppgaven drøfte hvordan utviklingen av cybertrusselen kan ha påvirket NATOs forståelse av denne for deretter å oppsummere og konkludere problemstillingen.

Hensikten med denne oppgaven er å belyse om, og i så fall hvordan, utviklingen av trusselen har påvirket NATOs tilnærming til cyberforsvar. Dette kan gi innsikt til hvordan NATO som organisasjon tilpasser seg nye trusler. I tillegg vil oppgaven bidra til å gi forståelse for forholdet mellom å oppfatte en trussel og å forstå den. Dette skillet vil bli synliggjort da oppgaven behandler informasjonen i kronologisk rekkefølge, noe som gir mulighet til å sammenligne beslutninger som blir tatt i alliansen opp mot den samtidige utviklingen av trusselen. På den måten kan man se hvordan tiltakene sammenfaller med oppfatningen av trusselen.

Denne oppgaven vil ta utgangspunkt i NATOs offisielle kilder, primært deklarasjoner og uttalelser fra toppmøter. I tillegg vil oppgaven forholde seg til cyberforsvar, som inkluderer forsvar mot både militære cyberangrep og cyberkriminalitet. Det poengteres at det er vanskelig å skille mellom cyberkriminalitet og et militært cyberangrep da slike hendelser i utgangspunktet kan fremstå helt like. Forskjellen ligger i hvem som står bak. Er det en statlig aktør kan det defineres som et militært cyberangrep og er det en sivil person eller gruppe kan det defineres som cyberkriminalitet. Utfordringen ligger i å identifisere dette, da det har vist seg vanskelig å spore cyberangrep. Et militært cyberangrep ført frem av en statlig aktør kan dermed forveksles med en kriminell handling utført av en person eller en gruppe, og vice versa. Denne oppgaven vil derfor fokusere på hvordan en militær organisasjon (her NATO) forholder seg til trusler og angrep i det digitale rom. Dette utelukker ikke utførelsen av cyberkriminalitet for å oppnå militære mål.

1.3 Begreper

Cyber er et gjennomgående begrep i denne oppgaven, og kan defineres som elektroniske kommunikasjonsnettverk, herunder også internett. Begrepet blir som regel brukt i kombinasjon med andre begreper for å sette disse i kontekst med nettopp elektroniske kommunikasjonsnettverk. NATO har egne definisjoner på noen av disse. For å unngå å endre meningsinnholdet vil definisjonene bli gjengitt på originalspråket. De følgende definisjonene er hentet fra «The Official NATO Terminology Database» (u.d).

- Cyberspace: "The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data."
- Cybersikkerhet (cyber security): "The application of security measures for the protection of communication, information and other electronic systems, as well as the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation."
- Cyberforsvar (cyber defence): "The means to achieve and execute defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems."

Det er verdt å merke seg at disse begrepene kan ha endret betydning fra de først ble brukt til i dag[3]. Ettersom kildegrunnlaget tar for seg toppmøter fra 1999 til 2019 kan for eksempel begrepet cyber tidlig i perioden ha hatt en annen betydning enn hva det hadde i 2019. Uavhengig av dette vil begrepene i oppgaven behandles med definisjonen gitt i dette kapittelet.

1.4 Disposisjon

Oppgaven vil først gjøre rede for arbeidsmetode og kildegrunnlag, samt en vurdering av disse. Deretter vil oppgaven ta for seg kildene, oppsummere utviklingen av cybertrusselen og relevante beslutninger, uttalelser og vedtekter i NATO fra de siste 20 årene. Videre vil oppgaven drøfte utviklingen av trusselen opp mot endringene i NATO for å identifisere om og

[3] Det bemerkes at NATOs begrepsdatabase ikke daterer de ulike definisjonene, og at det dermed ikke lar seg gjøre å spore eventuelle endringer i disse.

hvordan NATOs tilnærming til cyberforsvar har endret seg i takt med utviklingen av trusselen. Til slutt vil oppgaven oppsummere eventuelle funn for deretter å konkludere.

2.0 Metode

2.1 Arbeidsmetode

For å besvare problemstillingen er det brukt et utvalg av dokumenter som vi finner relevante for NATOs uttalte tilnærming til cyber. Deretter beskrives enkelte cyberhendelser – angrep, sabotasje eller liknende – som har preget utviklingen i bruken av digitale måter å påvirke en aktør på. NATOs tilnærming og de utvalgte hendelsene er hentet begge hentet fra samme 20-års periode, og disse blir analysert for å se nærmere på hvorvidt det er en sammenheng mellom de to elementene.

Ettersom en sentral del av oppgaven er å se nærmere på eventuelle endringer i alliansens tilnærming til cyberforsvar over tid, er det hensiktsmessig å se på beslutninger tatt på et politisk nivå. Kildegrunnlaget omfatter derfor dokumenter som er publisert av NATO i forbindelse med toppmøter i North Atlantic Council (NAC). Disse dokumentene er det igjen foretatt en kvalitativ innholdsanalyse av, i den hensikt å identifisere innholdet som er relevant for oppgaven. Dette innholdet har blitt sammenfattet i kronologisk rekkefølge for å tegne et bilde av NATOs utvikling innen cyberforsvar over tid. Dette har gitt muligheten til å se nærmere på, og sammenligne uttalelsene som har kommet med ujevne mellomrom i perioden 1999-2019. Metoden er derfor hensiktsmessig for å analysere eventuelle sammenhenger og endringer i uttalelsene.

Det er foretatt et utvalg av sikkerhetstruende hendelser i form av cyberangrep. Dette utvalget har basert seg på hendelser som tilsynelatende involverer statlige aktører, hvorpå hensikten med angrepene har vært politisk innblanding, subversjon, eller å svekke eller degradere militær evne. Disse hendelsene er så blitt sammenfattet i kronologisk rekkefølge for å skape et bilde av hvordan cybertrusselen har utviklet seg over tid. Hendelsene sees deretter i sammenheng med endringene i NATOs tilnærming til cyberforsvar for å se hvordan utviklingen av trusselen har påvirket NATOs utvikling. På den måten blir det mulig å peke på hvordan NATOs oppfatning av cybertrusselen kan ha endret seg over tid og hvorvidt denne endringen kan ha sammenheng med hendelsene som blir beskrevet.

Den analytiske metoden som er anvendt styrker oppgaven på flere punkter. Blant annet vil anvendelsen av offentlige dokumenter fra NAC gi oppgaven et riktig bilde av hvordan alliansen uttalt forholder seg til cyber, da dette er uttalelser som kommer fra primærkilden. I

tillegg bidrar metoden til å gi god oversikt over hvordan faktorene som blir diskutert har endret seg over tid. En svakhet med metoden er utvalget som er gjort av hendelser. Dette er et subjektivt utvalg og vil kunne svekke objektiviteten da disse er valgt på skjønn. I tillegg er det begrenset med hendelser som er brukt til å beskrive utviklingen av cybertrusselen, noe som kan gi et snevrere syn på hvordan denne har utviklet seg. De hendelsene som er benyttet i oppgaven vurderes som å være tilstrekkelig beskrivende for hovedtrekkene i utviklingen til cybertruslene. Hendelsene er også spredt i tid i den hensikt å dekke opp hele den aktuelle perioden.

2.2 Datagrunnlag og kilder

Datagrunnlaget for denne oppgaven er omfattende og variert. Den består både av offisielle uttalelser og vedtekter på øverste nivå i NATO, og omfatter deklarasjoner og andre vedtekter besluttet under alliansens toppmøter. I tillegg nyttes en rekke bøker og nyhetsartikler som sekundærkilder for de historiske hendelsene omtalt i oppgaven. Bakgrunnen for kildene beskrives videre i dette avsnittet.

2.2.1 North Atlantic Council og NATO Summit

North Atlantic Council er NATOs øverste organ og møtes regelmessig på ulike nivå. Uavhengig av hvilket nivå NAC møtes på foreligger det beslutningsmyndighet basert på konsensus i de sakene som diskuteres. Det laveste nivået representeres av permanente representanter fra hvert medlemsland, også kjent som NATO-ambassadører. Disse møtes ukentlig. På et høyere nivå representeres medlemslandene av sine forsvarsministre og utenriksministre. Disse møtes henholdsvis to til tre ganger per år. På det høyeste nivået møtes stats- eller regjeringssjefer eller deres stedfortredere. Disse møtene er alliansens toppmøter - kjent som *summits*. Disse møtene utgjør det høyeste nivået av NAC og avholdes med ujevne mellomrom. Slike møter arrangeres for eksempel i etterkant av viktige geopolitiske hendelser eller når den videre utviklingen av alliansen skal bestemmes. Møtene har til hensikt å drøfte og introdusere ny alliansepolitikk, vurdere innlemming av nye medlemmer, iverksette større endringer og/eller forsterke partnerskap og samarbeid mellom medlemsland. Alle møter i NAC styres av generalsekretæren eller visegeneralsekretæren i hans sted (NATO, 2018).

2.2.2 Deklarasjoner og vedtekter

De offisielle uttalelsene i etterkant av toppmøtene kommer i form av dokumenter som oppsummerer beslutninger som er tatt i de saker som har vært oppe til diskusjon. Ved enkelte møter i NAC der det er enighet om særskilte vedtak, vil disse også publiseres i etterkant av

møtene. Et sentralt eksempel på dette er *Cyber Defence Pledge* - et løfte om å opprettholde fokus på trusler i cyberdomenet vedtatt under toppmøtet i Warszawa i 2016 (NATO, 2016).

2.2.3 Sekundærkilder til cyberhendelser

Kildegrunnlaget for de historiske hendelsene som benyttes er variert. Det omfatter bøker, nyhetsartikler, analyser, rapporter og innlegg i tidsskrift. Felles for kildene er at de langt på vei er deskriptive, noe som bidrar til å sikre objektivitet og en korrekt fremstilling av hendelsene. Det gjøres oppmerksom på at kildene har opphav i NATO eller i NATO-allierte land.

2.3 Valg av datagrunnlag

Ettersom en organisasjon av NATOs størrelse publiserer et stort antall offisielle dokumenter ville det vært et omfattende arbeid å gjennomgå alle disse. Beslutningen på å fokusere på kilder med opphav i toppmøtene er derfor tatt for å holde mengden kilder håndterlig, samtidig som de vil dekke de viktigste uttalte endringene i alliansen. Det erkjennes at dette er en svakhet med oppgaven da et bredere utvalg av kilder kunne gitt et mer nyansert syn på problemstillingen, samt bidratt til å forklare gangen i erkjennelsesprosessen mot et vedtak. På tross av dette er det grunnlag for å si at de få, men høyst pålitelige kildene som benyttes vil gi et bilde av hva alliansens uttalte policy er. Dette fordi kildene er offisielle uttalelser der NATO samlet presenterer sitt syn og ståsted. En annen faktor som må understrekes er at datagrunnlaget ikke nødvendigvis speiler hvilke endringer som eventuelt er gjort i alliansens doktriner eller strategier, men snarere en uttalt holdning til problematikken rundt cyber. Når det gjelder kildegrunnlaget for cyberhendelsene er disse valgt på bakgrunn av tilgjengelighet og variasjon, det vil si at de har vært språklig tilgjengelige og de er i stor grad uavhengige av hverandre for å sikre objektivitet.

En annen faktor som påvirker kildegrunnlaget er valget om å ha en ugradert oppgave, noe som naturligvis medfører noen begrensninger i hvilke kilder som kan benyttes. Ettersom oppgavens fokus er NATOs *offisielle* tilnærming til cyberforsvar, er det dog ikke nødvendigvis behov for å vurdere innholdet i eventuelle graderte dokumenter.

2.4 Kildekritikk

Kildegrunnlaget til oppgaven består i hovedsak av primærkilder i form av offisielle uttalelser og deklarasjoner fra NATO-toppmøter, samt andre offisielle uttalelser. I tillegg vil det som tidligere nevnt være bruk av sekundærkilder for å kontekstualisere dokumentene og skape

forståelse for vedtakene og beslutningene som er blitt gjort. Kildegrunnlaget anses som tilgjengelig og relevant for oppgaveformuleringen. Offisielle uttalelser og deklarasjoner publiseres fortløpende etter toppmøter og disse er styrende for NATOs policyer.

2.4.1 Offisielle uttalelser og dokumenter

Hva gjelder autentisitet og troverdighet anses de offisielle uttalelsene og dokumentene fra NATO som tilfredsstillende da kildene representerer det høyest nivået i NAC og/eller publiseres for allmennheten gjennom alliansens nettsteder. Dette gjør seg også gjeldende for kildenes representativitet. Ettersom oppgaven undersøker utviklingen i NATOs tilnærming til cyberforsvar vurderes NAC til å være det mest representative organet for beslutningstaking og styring av NATO som organisasjon.

Tekstene som er benyttet er ment til å kommunisere beslutninger tatt i NAC videre ned i organisasjonen. I tillegg er de et virkemiddel for å kommunisere til stater utenfor organisasjonen hvordan NATO stiller seg til sikkerhetspolitiske spørsmål. Det er her viktig å ha i mente at de uttalelsene og de krav som blir stilt til medlemslandene ikke nødvendigvis samsvarer med de faktiske handlingene. Hvorvidt hvert enkelt medlemsland etterfølger beslutninger og vedtak som blir fattet av NAC er vanskelig å svare på. Dette kan eksemplifiseres med 2-prosent-målet, hvor hvert medlemsland skal bruke minst 2 prosent av sitt BNP på forsvar. Dette er det enighet om i alliansen, men det etterfølges av svært få.

Oppsummert ansees disse kildene som relevante og nødvendige for å besvare problemstillingen. Dokumentene vil bidra til å gi svar på hvordan NATOs tilnærming har endret over tid. Det de derimot ikke vil gi svar på er det som skjer ‘bak lukkede dører’, det vil for eksempel si de prosessene som har ledet fram til utgivelsen av kildene. På tross av dette ansees de som tilstrekkelige for å besvare problemstillingen da fokuset for oppgaven er NATOs tilnærming til cyberutfordringer uttrykt gjennom nettopp offisielle uttalelser og vedtekter.

2.4.2 Historiske hendelser i perioden

Når det gjelder kildegrunnlaget forøvrig, det vil si alle ikke-offisielle kilder fra NATO, er disse primært nyhetskilder, artikler publisert i tidsskrift eller bøker om emnet. En ekstra kvalitetssikring er at de ulike historiske hendelsenes beskrivelse er basert på flere uavhengige kilder. Det er gjort en vurdering av dette kildegrunnlaget og ettersom hendelsene er forsøkt beskrevet deskriptivt ansees de som troverdige da det ikke er oppdaget noen vesentlige

uoverensstemmelser[4] i fakta blant kildene som er benyttet. Hendelsene søker å gi en kontekstualisering og aktualisering av utfordringer i cyberspace knyttet til sin periode. Ved å benytte ulike objektive kilder vil det bidra til at hendelsene beskrives så korrekt som mulig. En svakhet med kildegrunnlaget er at det primært har opphav i land og organisasjoner fra Vest-Europa og Nord-Amerika som kan gjøre at de ansees som subjektive, all den tid Russland nevnes som en sentral aktør bak flere cyberhendelser. På bakgrunn av dette er det forsøkt å gjøre kildegrunnlaget så bredt som mulig slik at man sikrer en nøytral fremstilling av hendelsene. Med bakgrunn i deres uavhengighet av hverandre og deskriptive natur, er kildene som blir benyttet vurdert av forfatterne til å være tilstrekkelige for å oppnå dette.

3.0 Empiri

Empirien er her delt i to underkategorier, hvor det først redegjøres for sentrale hendelser som har preget cybersikkerhet i perioden 1999-2019. Deretter presenteres sammendrag av relevant informasjon fra deklarasjonene som er publisert i etterkant av NATO-toppmøtene.

3.1 Sentrale episoder og hendelser

3.1.1 Kosovo

På samme måte som krigen i Vietnam ble kjent som den første TV-krigen, ble krigen i Kosovo kjent som den første internettkrigen (Lynch, 1999). Både organisasjoner og enkeltindivider brukte internett til å publisere informasjon om krigen og å proklamere sin støtte til en av sidene. Dette gjorde også NATO gjennom sin offisielle informasjonsnettside. Konflikten og dens gang ble dermed tilgjengelig på internettbaserte medier.

Under operasjon «Allied Force» led NATOs internettstruktur av en serie med angrep. Metodene som ble brukt var DOS-angrep, metning av e-postservere og 'defacement' av forskjellige nettsteder, inkludert det offisielle informasjonsnettstedet til NATO. Dette var ifølge John Pike, en etterretningsanalytiker hos «Federation of American Scientists»[5], et skoleeksempel på en kostnadseffektiv måte å svekke informasjonen fra NATO til omverden på (Verton, 1999). Angrepene ble i stor grad gjennomført av den serbiske hacktivistgruppen «the Black Hand» og den russiske hacktivistgruppen «the Russian Hacker Brigade». I starten av konflikten ble NATO og de allierte landene angrepet omtrent en gang i uken, noe som

[4]Den eneste ulikheten som forfatterne har oppdaget gjelder antall personer rammet av cyberangrepet som beskrevet i kapittel 3.1.4. Antallet varierer mellom 200,000 og 225,000, begge kildene benytter i dette tilfellet et omtrentlig antall, og denne uoverensstemmelsen ansees derfor som irrelevant for denne oppgaven.
[5] FAS er en uavhengig organisasjon som forsker på internasjonal sikkerhet (Federation of American Scientists, 2020).

skulle øke utover konflikten. Mot slutten var det omtrent 18 slike angrep i uken (Healey, 2011)

Gruppenes uttalte mål var å forstyrre NATOs militære operasjoner. Hacktivistgruppen hevdet de kunne ta seg inn i NATOs viktigste datasystemer og slette dataen på disse. Gruppen selv hevder de klarte å gjennomføre et slikt angrep på en av datamaskinene tilhørende U.S Navy. Datamaskinen ble koblet av nettet like etter denne hendelsen. I tillegg til dette ble det registrert cyberangrep fra Kina etter feilbombingen av den kinesiske ambassaden i Beograd (Healey, 2011).

Hacktivistene forsøkte også å hindre NATO tilgang til egne nettsteder med DOS-angrep. Ansvarshavende for NATOs nettsteder under konflikten uttalte at de hadde omtrent 100 servere og at de fryktet at alle NATOs nettsteder var blitt angrepet. Underveis i konflikten så de seg nødt til å bytte alle serverne til raskere servere med høyere båndbredde for å takle all trafikken (Messmer, 1999).

3.1.2 Tallin 2007

Tidlig i 2007 besluttet estiske myndigheter å flytte et monument som siden 1947 hadde stått i Tallin som en minnebauta for sovjetiske soldater under den andre verdenskrig. Monumentet har lenge vært et viktig symbol både for estlendere og russere bosatt i landet, men med et noe ulikt budskap for de to gruppene. For den russiske minoriteten er monumentet et symbol på frigjørelsen og slutten på den store fedrelandskrigen[6], for estlendere har det derimot stått til minne om at de er en undertrykket lillebror i naboskapet med Russland. Monumentets symbolske historie har bidratt til at det har blitt stående i en dragkamp mellom pro-russiske grupperinger og estiske nasjonalister. Da flyttingen – som også innebar å grave opp levninger etter sovjetiske soldater på stedet – skulle starte i april 2007, ble det møtt med store protester som utartet til opprør i flere deler av Tallinn. Da politiet om morgenen dagen etter hadde fått kontroll på demonstrantene kunne man få inntrykk av at den umiddelbare uroen var over. Det viste seg fort at protestene ikke var stilnet, men at de nå var flyttet til ett annet domene – internett (Ottis, 2007, ss. 1-3).

[6] Fedrelandskrigen er et begrep russere gjerne bruker om slagene som stod på Østfronten og i Sovjetunionen under den andre verdenskrig (Enstad, 2019)

Estland var allerede i 2007 et svært digitalisert samfunn. Som følge av dette foregikk omlag 98% av bankutvekslinger i landet digitalt og nær sagt alle hadde tilgang på høyhastighetsinternett. Om morgenen dagen etter de store opptøyene i Tallinn begynte nettverk og servere i landet plutselig å bli overbelastet av datainformasjon på grunn av såkalte DOS dels rettet mot bankvirksomhet, og dels mot private datamaskiner, telefoner og kredittkort. Blant annet ble all datakommunikasjon til landets to største banker lammet i en kortere periode, og de påfølgende ringvirkningene varte i flere dager. Angrepene var både direkte rettet mot utvalgte nettverk, men ble også gjennomført som DDOS, der flere enheter (f.eks. datamaskiner eller smarttelefoner) knyttes sammen i det som kalles et 'botnet' for å overbelaste, eller 'mette' et utpekt nettverk. Disse metodene var ikke ukjente på dette tidspunktet, men omfanget av angrepene var nytt. Offentlige og private tjenester så vel som kommunikasjonssystemer og media opplevde regelmessige forstyrrelser og overbelastning i totalt 22 dager. Angrepene foregikk i mer eller mindre koordinerte bølger, og opphavet ble i de fleste tilfellene sporet til å ha opphav utenfor landets grenser. Ulike nettsteder og fora florerte med detaljerte instrukser på russisk og estisk om hvordan man kan gjennomføre DOS-angrep og hvilke nettverk som ble utpekt som mål. På tross av sterke indisier på at angrepene hadde opphav i Russland har landet nektet for å ha stått bak, og det er heller ikke bevist hvem som er skyldig[7] (Geers, 2008, s. 8; Kaplan, 2016, ss. 162-164; Ottis, 2007).

3.1.3 Georgia

I august 2008 startet den Russisk-Georgiske krigen. Etter uker med diskusjon om fremtiden til det Sør-Osseatiske området iverksatte georgiske styrker et angrep mot byen Tskhinvali som et motsvar til påståtte provokasjoner fra Russland. Dette førte til en intensiv russisk offensiv mot Georgia. I tillegg til konvensjonelle militære styrker, ble det gjennomført et angivelig russisk koordinert cyberangrep mot georgiske nettsteder. Nettstedene var relatert til finans, kommunikasjon og regjeringen. Dette er trolig den første gangen et slikt cyberangrep finner sted i en militær operasjon hvor det er synkronisert med luft-, sjø-, og landoperasjoner (Hollis, 2011).

Cyberangrepene, fremført som både DDOS og 'defacement', førte til at kritiske nettsteder for kommunikasjon både innad i Georgia og ut av landet ble utilgjengelige (Markoff, 2008). Dette hindret nyhetskanaler og regjeringen i å informere og instruere befolkningen i Georgia

[7] To personer ble fengslet og/eller bøtelagt i forbindelse med angrepene. En estisk statsborger ble arrestert da man sporet aktivitet tilbake til hans datamaskin, mens en russisk aktivist ble bøtelagt i Russland som følge av sporing. Utover dette har det ikke lyktes Estland eller andre å bevise hvem som stod bak organiseringen av angrepene foruten indiser om at de har hatt sitt opphav i Russland (Ottis, 2007, ss. 3-4; Kaplan, 2016, s. 163).

mens de var under angrep, samtidig som Georgia ble hindret i å informere omverden om hva som pågikk. Effekten av dette blir tydeligere om man ser det i sammenheng med de andre operasjonene i de øvrige domenene. Russiske bakkestyrker kunne for eksempel gå uhindret frem uten å bli utfordret av vesten, blant annet fordi informasjonen om dette ikke kunne overleveres fra den Georgiske regjeringen. Cyberangrepene, som angivelige ble fremført av Russland, førte dermed til overlegenhet i informasjonsdomenet, som videre ledet til at russiske styrker kunne fremføre operasjonene sine i de andre domene nærmest uhindret (Hollis, 2011).

3.1.3 Stuxnet

I 2006 installerte iranske forskere gass-sentrifuger for å anrike uran til bruk i kjernereaktoren i Natanz. De samme sentrifugene brukes til produksjon av kjernevåpen. Dette ble oppfattet som truende for USA, da et atom-væpnet Iran ble vurdert som en eksistensiell trussel. USA bestemte seg dermed for å gjøre noe med reaktoren (Kaplan, 2016, ss. 203-211).

Reaktoren i Natanz, som de fleste reaktorer, ble fjernstyrt av en datamaskin. Det var dermed aktuelt å påvirke reaktoren gjennom cyberspace. National Security Agency[8] (NSA) i USA gikk tidlig inn i nettverket til reaktoren for å finne svakheter. Ved å gjøre dette fant de ut at Siemens, et stort tysk selskap innen elektronikk, hadde lagd sentrifugene. De kunne dermed anskaffe det samme systemet. På denne tiden visste NSA at de gjennom et cyberangrep kunne påvirke og manipulere maskinvaren til reaktoren. Innledningsvis rettet de angrepet mot såkalte avbruddsfrie strømforsyninger, som var installert for å sikre jevn spenning til sentrifugene for å unngå skade på disse. I angrepet økte de spenningen som førte til at 50 av sentrifugene eksploderte. Iranerne mistenkte at dette var sabotasje fra Tyrkia som hadde solgt dem strømforsyningene. Mens sentrifugene og strømforsyningene ble byttet ut forberedte NSA, sammen med Central Intelligence Agency[9] (CIA) og Unit 8200[10] et annet angrep (Kaplan, 2016, ss. 203-211).

I forberedelsesfasen satt de sammen sentrifugene og styringssystemet de hadde anskaffet fra Siemens i en av våpenlabene hos Department of Energy i USA. Her simulerte de angrepet de tenkte å gjennomføre og fikk sentrifugene til å rotere fem ganger raskere enn vanlig. Sentrifugene ble ødelagt og testen ble sett på som vellykket. Det neste steget var dermed å få

[8] NSA er en etterretningsvirksomhet i USA som har hovedansvar for blant annet cybersikkerhet (Næss & Notaker, 2015)
[9] CIA er en etterretningsvirksomhet i USA som har ansvar for etterretning utenfor USA. En av hovedoppgavene er dekkoperasjoner (Notaker, 2019)
[10] Unit 8200 er en israelsk etterretningsenhet med hovedansvar for cybersikkerhet (Reed, 2015)

overført ormen til styringsenheten til reaktoren. Ettersom iranerne var klar over sårbarheter med digitale kontrollsystemer hadde de puttet systemet på et lukket nettverk skjermet fra internett. NSA brukte derfor kontaktene i Unit 8200 som igjen brukte agenter fra Mossad, en israelsk etterretningsenhet, til å overføre viruset med en USB-disk (Kaplan, 2016, ss. 203-211).

Systemet ville vanligvis varslet når det var noe galt med sentrifugene, men viruset var designet til å ta kontroll over dette og sende et falskt signal som sa at alt fungerte som det skulle. NSA gikk inn i operasjonen med en tanke om at de skulle gjøre lite skade slik at de ansatte ved reaktoren ikke skulle mistenke sabotasje. Tanken var at det skulle fremstå som enkle systemsvikter grunnet menneskelige feil eller dårlig design. I første omgang påvirket de ventilene som kontrollerte hvor mye urangass som strømmet inn i sentrifugene slik at de ble skadet. I andre omgang endret de inngangsvinkel og påvirket frekvensstyringsenhetene som styrte rotasjonshastighetene på sentrifugene. Innen starten av 2010 hadde de klart å ødelegge 2000 av 8700 sentrifuger. Amerikanske etterretning estimerte at Irans atomprogram var satt tilbake to til tre år (Kaplan, 2016, ss. 203-211).

Operasjonen fikk problemer i 2010 da viruset ble oppdaget. Det var ikke Iran som hadde oppdaget viruset, men flere sikkerhetsfirmaer innen programvare oppdaget et virus som dukket opp rundt om i verden. Viruset var designet til å angripe den spesifikke programvaren utviklet av Siemens, og ville ikke gjøre skade på andre systemer. Likevel hadde viruset spredd seg gjennom internett (Zetter, 2014). En tysk sikkerhetsforsker klarte etterhvert å spore viruset og avsløre dets hensikt. Dette resulterte i at iranerne fant ut at det var et virus som gjorde skadet på sentrifugene, og gjorde mottiltak og koblet Siemenskontrolleren av reaktoren. Viruset klarte likevel å gjøre skade, og NSA økte intensiteten på operasjonen da de allerede var kompromittert. Dette resulterte i at ytterligere 1000 sentrifuger ble ødelagt før operasjonen ble stanset (Kaplan, 2016, ss. 203-211).

3.1.4 Kraftnett i Ukraina 2015

Lille julaften 2015 opplevde over 200,000 ukrainere strømbrudd som følge av et omfattende cyberangrep på deler av det regionale strøm-distribusjonsnettet. Angriperne siktet seg inn på kontrollstasjoner som distribuerer strøm til forbrukerne. Utvalgte slike kontrollstasjoner tilhørende minst tre ulike kraftselskaper ble hacket og skrudd av, som da resulterte i strømbrudd hos forbrukerne (Donghui Park, 2017). Ukrainske myndigheter var blant de som tidlig pekte ut russiske sikkerhetstjenester til å være opphavet for angrepet (Lee, Assante, &

Conway, 2016, s. iv), men dette er ikke blitt bevist. På tross av at angrepet ikke kan akkrediteres, blir dette beskrevet som et sofistikert og omfattende angrep man ikke tidligere har sett mot sivil infrastruktur i kraftsektoren. Amerikanske myndigheter og sivile aktører bistod Ukraina i undersøkelsen av angrepene, blant annet for å analysere hvordan de var gjennomført og hvordan man bedre kan sikre seg mot liknende angrep i fremtiden. Det amerikanske departementet med ansvar for nasjonens sikkerhet – *Department of Homeland Security* (DHS) – beskrev angrepene slik:

> After gaining a foothold in the victim networks, attackers acquired legitimate credentials and leveraged valid remote access pathways to conduct their attack. The physical impact events of the cyber-attacks launched within 30 minutes of each other, impacting multiple central and regional facilities. Over 50 regional substations experienced malicious remote operation of their breakers conducted by multiple external humans. This was done using either existing remote administration tools at the operating system level or remote [industrial control system] client software via virtual private network (VPN) connections. (Homeland Security, 2016)

I grove trekk skaffet angriperne seg digital innpass og tilstedeværelse i kraftselskapenes nettverk for så å overta og fjernstyre enkelte deler av kontrollsystemet til distribusjonsnettet.

3.1.5 Sammendrag av hendelsene 1999-2015

Utviklingen av cybertrusselen fra 1999 til i dag har vært stor. I begynnelsen var cyberangrep enkle ukoordinerte aksjoner bestående av DDoS, DoS og 'defacement'. Dette kunne føre til at enkelte nettsteder og servere ble utilgjengelig i en kortere tidsperiode og dermed hindre effektiv kommunikasjon. Midlene for å gjennomføre slike angrep har ikke endret seg stort, men måten de har blitt anvendt på har utviklet seg mye. Fra enke ukoordinerte angrep har dette utviklet seg til koordinerte angrep mot finans-, kommunikasjons-, og militære institusjoner. De samme midlene som ble brukt til å hindre kommunikasjon hos enkelte organisasjoner eller enheter i kortere perioder har dermed kunne blitt brukt til å hemme hele nasjoner. På den måten har cyberangrep blitt fremført som en måte å tvinge frem politikk. Når man setter dette sammen med andre militære operasjoner i andre domener har cyberangrepene fått enda større effekt. Kommunikasjon både internt til egen befolkning og ut av nasjonen har vist seg å være kritisk i en krigssituasjon hvor man er avhengig av å instruere, informere og kommunisere. Dette bidrar dermed til at den angripende nasjonen får et stort overtak i informasjonsdomenet, noe som kan fungere som en styrkemultiplikator.

Midlene man har brukt til cyberangrep har også sett en utvikling. Fra enkle DoS og DDoS-angrep har man klart å utvikle spesifikke cybervåpen som kan angripe dedikerte mål. Dette

kan være alt fra komponenter i strømnettet til andre enheter kritisk for infrastruktur. På den måten gir cyberangrep muligheter til å skade og eventuelt ødelegge slike komponenter. Dette kan gjøre cyber til et svært potent våpen som kan ta ut kritisk infrastruktur. Vannverk og kraftverk blant andre kan være potensielle mål som medfører stor skade. Om man i tillegg til dette gjennomfører DDoS-operasjoner for å ta ut for eksempel kommunikasjonsservere og synkroniserer dette med en konvensjonell militær offensiv vil cyber som våpen kunne ha stor påvirkning på slagmarken. Det er viktig å presisere at hvilke kapasiteter og hvor sofistikerte systemer en aktør har, vil måle seg mot de sikkerhetstiltak som er implementert for slik infrastruktur, og dermed bestemme hvilke aktører som faktisk evner å gjennomføre slike angrep.

Cybertrusselen har på mange måter utviklet seg med digitaliseringen av verden. Ettersom flere og flere enheter og komponenter har blitt koblet på nett for å effektivisere kommunikasjon og styring mellom de, har den totale sårbarheten økt. I tillegg er det verdt å påpeke at cyber som våpen har noen særegenheter som skiller det fra andre konvensjonelle våpen. Attribusjon virker å være en av disse. Som det kommer frem i flere av eksemplene som er brukt, er det vanskelig å bevise hvem utøveren av disse aksjonene er. I tillegg kan slike angrep gå rett på dypet uten å ta hensyn til motstanderens frontlinjer og styrker. På den måten får man muligheten til å føre en virtuell krig i cyberdomenet som påvirkes lite av den øvrige krigføringen, men som har potensiale til å påvirke den.

3.2 NATOs toppmøter

I dette kapittelet vil relevante uttalelser fra NATOs toppmøter med eventuelle tilhørende dokumenter fra 1999 til 2019 gjengis. Begrepene toppmøte og 'summit' blir begge benyttet.

3.2.1 Washington 1999

Deklarasjonen fra dette toppmøtet nevner ingenting spesifikt om cybersikkerhet. I punkt 5 i deklarasjonen ser man at alliansen, som en del av tilpasningen til nye sikkerhetsutfordringer, har oppdatert sitt strategiske konsept. Strategic Concept av 1999 ble godkjent under dette toppmøtet (NATO, 1999a). Dette dokumentet tar for seg sikkerhetstrusler innen informasjonssystemer spesifikt under overskriften "Security challenges and risks" punkt 3. Her påpekes det at "... state and non-state adversaries may try to exploit the Alliance's growing reliance on information systems through information operations designed to disrupt such systems." (NATO, 1999b).

3.2.2 Praha 2002

I deklarasjonen fra toppmøtet i Praha 2002 heter det at NATO skal transformeres blant annet med nye kapabiliteter for å tilpasse seg nye trusler og sikkerhetsutfordringer i det 21. århundret. Under punkt 4 i deklarasjonen kommer det frem at alliansen skal beskytte sine populasjoner, militære styrker og sitt territorium mot ethvert væpnet angrep, og her nevnes cyberforsvar som et eget punkt blant flere tiltak:

> We [NATO] are determined to deter, disrupt, defend and protect against any attacks on us, in accordance with the Washington Treaty and the Charter of the United Nations. ... We have therefore decided to: … Strengthen our capabilities to defend against cyber attacks. (NATO, 2002)

Alliansen besluttet med andre ord at de blant annet skulle styrke sine kapabiliteter til å forsvare seg mot cyberangrep (NATO, 2002).

3.2.3 Riga 2006

Under toppmøtet i Riga godkjente topplederne i NATO, under punkt 24 i deklarasjonen, et sett med initiativer for å være bedre rustet for moderne trusler (NATO, 2006). Et av initiativene som ble godkjent omhandlet nettverkssikkerhet. I dette underpunktet står det: "work to develop a NATO Network Enabled Capability to share information, data and intelligence reliably, securely and without delay in Alliance operations, while improving protection of our key information systems against cyber attack" (NATO, 2006). Alliansen understreker dermed viktigheten av sin nettverkskapasitet og dens sårbarhet med tanke på cyberangrep.

I tillegg ba NATO «the Council of Permanent Session» om å konsultere de mest umiddelbare risikoene innen energisikkerhet under punkt 45 (NATO, 2006). Dette hadde bakgrunn i hvordan forstyrrelse av ressursflyten kan true alliansens sikkerhet som ble understreket i NATOs «Strategic Concept» (1999b). Hensikten med dette var å identifisere og definere områder hvor NATO kan bidra med ivaretakelsen av sikkerhetsinteresser med bakgrunn i energitilgang

3.2.4 Bucharest Summit 2008

Ved toppmøtet i Bucuresti i 2008 var cyberdomenet både implisitt og direkte nevnt, noe som kommer frem i flere av punktene i deklarasjonen. En viktig setning i deklarasjonens punkt 44 lyder: "We will also ensure that we have the right kind of capabilities to meet the evolving

security challenges of the 21st century, and to do so, we will transform, adapt and reform as necessary." (NATO, 2008). Dette er en anerkjennelse og understreking av at alliansen har fokus på å møte nye trusler som er relevante for det 21. århundret. Videre understrekes viktigheten av å styrke egen informasjonsbehandling gjennom en forbedring av nettverkskapabiliteter, nok et implisitt punkt som omfatter cyber.

Videre i deklarasjonen ser vi under punkt 45 at truslene om cyberangrep er i fokus. Det refereres her direkte til den nylig vedtatte (januar 2008) 'Policy on Cyber Defence', og innholdet i denne. Dette var alliansens første vedtak om en felles cyberforsvars-policy og presiserte følgende:

> Our Policy on Cyber Defence emphasises the need for NATO and nations to protect key information systems (...) and provide a capability to assist Allied nations, upon request, to counter a cyber attack. We look forward to continuing the development of NATO's cyber defence capabilities and strengthening the linkages between NATO and national authorities. (NATO, 2008)

Deklarasjonen understreker altså etableringen av en cyberpolicy og viktigheten av å videreutvikle denne, herunder en utvikling av kapabiliteter innen cyberforsvar.

3.2.5 Strasbourg / Kehl Summit 2009

Deklarasjonen fra 2009 omfatter flere punkter som eksplisitt angår cyber. For eksempel understrekes det i punkt 49 at NATO skal styrke kommunikasjons- og informasjonssystemer som er av kritisk betydning mot cyberangrep (NATO, 2009). I tråd med Strategic Concept av 1999 (1999b), legges alliansens økende avhengighet av slike systemer til grunn:

> We remain committed to strengthening communication and information systems that are of critical importance to the Alliance against cyber attacks, as state and non-state actors may try to exploit the Alliance's and Allies' growing reliance on these systems. … We will accelerate our cyber defence capabilities in order to achieve full readiness. Cyber defence is being made an integral part of NATO exercises. (NATO, 2009)

Som følge av dette fokuset, opprettet NATO Cyber Defence Management Authority[11] (CDMA). De styrket den allerede eksisterende Computer Incident Response Capability[12] (NCIRC), samt aktiverte Cooperative Cyber Defence Centre of Excellence[13] (CCDCOE) i Estland.

I arbeidet med å styrke NATOs cyberkapabiliteter påpekes det at cyberforsvar skal bli integrert del av øvelser. I tillegg påpekes det at NATO arbeider med å styrke arbeidet med beskyttelse mot cyberangrep sammen med sine partnerland. I den forbindelse er det utarbeidet et rammeverk for samarbeid om cyberforsvar med disse.

3.2.6 Lisboa 2010

Etter toppmøtet i 2010 så man i deklarasjonen en utstrakt bruk av cyber-begrepet og fokus på å beskytte alliansen mot cyberangrep. I tillegg til presiseringer om fortsatt fokus på 'nye' trusler – som omfatter cyberangrep – ser man at hele punkt 40 i deklarasjonen omtaler cyberdomenet:

> Cyber threats are rapidly increasing and evolving in sophistication. ... [W]e will take into account the cyber dimension of modern conflicts in NATO's doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber attack against systems of critical importance to the Alliance. We will strive in particular to accelerate NATO Computer Incident Response Capability (NCIRC) to Full Operational Capability (FOC) by 2012 and the bringing of all NATO bodies under centralised cyber protection. We will use NATO's defence planning processes in order to promote the development of Allies' cyber defence capabilities, to assist individual Allies upon request, and to optimise information sharing, collaboration and

[11] CDMA ble opprettet som en del av NATOs cyberforsvarspolicy. CDMA er en myndighet i NATO som har ansvar for å sette i gang og koordinere øyeblikkelig og effektiv cyberforsvarstiltak der det er aktuelt. Myndigheten fungerer som en sentral kommando for tekniske-, politiske- og informasjonsdelingstiltak for alliansens medlemmer, samt å dirigere og styre eksisterende NATO-nettverksenheter (Myrli, 2009).
[12] NCIRC er en utøvende avdeling som skal kunne løse oppgaver som å detektere og forhindre virusinfeksjoner og inntrenging i NATOs nettverk. I tillegg skal de ivareta kryptografiske enheter for internett, gi teknisk støtte til hendelser i datasikkerhet, samt policy- og etterforskingstjenester (Myrli, 2009)
[13] CCDCOE er et forskningssenter akkreditert av NATO som en fullverdig militær organisasjon. Senteret gjennomfører årlige konferanser med fokus på lovlige og teknologiske aspekter ved cyberdomenet og forsker på cyberkonflikt. I tillegg har CCDCOE, siden 2010, årlig organisert den internasjonale øvelsen 'Locked Shields' som er den største og mest komplekse cyberforsvarsøvelsen i verden. Denne øvelsen bidrar til trening innen cyberforsvar av vanlige IT-systemer, militære systemer og kritisk infrastruktur, så vel som strategisk beslutningstaking, rettslige problemstillinger og media (Cooperative Cyber Defence Center of Excellence, u.d.).

> interoperability. To address the security risks emanating from cyberspace, we will work closely with other actors, such as the UN and the EU, as agreed. (NATO, 2010)

Her ser man tydelig at cybertrusler er i fokus og at alliansen vedtar å fremskynde opprettelsen av NATO Computer Incident Response Capability for å møte fremtidige angrep. I tillegg understrekes det at NATO skal samarbeide tett med andre organisasjoner for å møte utfordringer knyttet til cybersikkerhet. Det er verdt å legge merke til at NCIRC også har vært nevnt i tidligere deklarasjoner, men altså ikke FOC på dette tidspunktet.

3.2.7 Chicago 2012

I deklarasjonen etter Chicago-toppmøtet. NATO påpeker den stadig økende tendensen av cyberangrep og at disse blir mer og mer sofistikerte og komplekse. Videre nevnes det at vedtakene som ble gjort i Lisboa er nå på vei til å bli implementert; herunder et Cyber Defence Concept, en Cyber Defence Policy og en Cyber Defence Action Plan. I tillegg står det at NCIRC er godt på vei til å inneha Full Operational Capability (FOC), og vil ha dette innen utgangen av 2012 (NATO, 2012). Det arbeides også med reform, hvor målet er at alle NATO-enheter skal være under en sentralisert cyberbeskyttelse. I forlengelsen av dette skal det integreres tiltak innen cyberforsvar i alliansens strukturer og prosedyrer, som fremhevet i punkt 49 av deklarasjonen:

> We will further integrate cyber defence measures into Alliance structures and procedures and, as individual nations, we remain committed to identifying and delivering national cyber defence capabilities that strengthen Alliance collaboration and interoperability, including through NATO defence planning processes. We will develop further our ability to prevent, detect, defend against, and recover from cyber attacks. (NATO, 2012)

For å adressere sikkerhetstrusler innen cyber har NATO forpliktet seg til å samarbeide med relevante partnerland på en case-til-case basis, samt å samarbeide med internasjonale organisasjoner som EU, Europarådet, FN og Organisasjon for sikkerhet og samarbeid i Europa. I tillegg vil NATO ta full utnyttelse av ekspertisen tilbudt av CCDCOE (NATO, 2012)

3.2.8 Wales 2014

Under toppmøtet i Wales ble «Enhanced Cyber Defence Policy» vedtatt (NATO, 2014). I denne blir cyberforsvar anerkjent som en av NATOs kjerneoppgaver innen kollektivt forsvar. Bakgrunnen for dette er anerkjennelsen av at et cyberangrep mot et moderne samfunn kan ha like ødeleggende effekt som et konvensjonelt angrep, som nevnt i deklarasjonens punkt 72:

> As the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, we have endorsed an Enhanced Cyber Defence Policy (ECDP). … It [ECDP] recalls that the fundamental cyber defence responsibility of NATO is to defend its own networks … emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks. Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. (NATO, 2014)

Det understrekes i tillegg at beslutningen om hvorvidt et cyberangrep vil utløse artikkel 5 vil tas av NAC fra sak til sak. Dette er et viktig punkt som viser en anerkjennelse av at cyberangrep potensielt vil kunne utløse en artikkel 5 situasjon. Som uttrykt over, påpekes det at fundamentet i NATOs ansvarsområde innen cyberforsvar er å beskytte sine egne nettverk. Den nye policyen anerkjenner også at krigens folkerett og FN-pakten gjør seg gyldig i cyberspace (NATO, 2014).

Videre nevnes det at alliansen vil fortsette å integrere cyberforsvar i NATO-operasjoner samt operasjonell- og beredskapsplanlegging, og forsterke informasjonsdeling og situasjonsforståelse blant de allierte (NATO, 2014). De vil også intensivere samarbeid med industrien gjennom «NATO Industry Cyber Partnership» i den hensikt å styrke sine cyberkapabiliteter, noe som kommer frem av punkt 73.

3.2.9 Warszawa 2016

Deklarasjonen fra 2016 er et omfattende dokument som beskriver flere viktige punkter som har betydning for alliansen. Den vitner om et stort fokus på energisikkerhet, cybersikkerhet og hybride trusler. I tillegg nevnes flere aktører eksplisitt i ulike sammenhenger.

Et viktig punkt å trekke frem er at Russland pekes på som en aktør som truer stabiliteten i det Euro-Atlantiske området. Følgende beskrives under punkt 9 og 10 av uttalelsene: "Russia's recent activities and policies have reduced stability and security, increased unpredictability, and changed the security environment ..." (NATO, 2016).

> Russia's destabilising actions and policies include: the ongoing illegal and illegitimate annexation of Crimea, which we do not and will not recognise and which we call on Russia to reverse; the violation of sovereign borders by force; the deliberate destabilisation of eastern Ukraine; large-scale snap exercises contrary to the spirit of the Vienna Document, and provocative military activities near NATO borders, including in the Baltic and Black Sea regions and the Eastern Mediterranean; its irresponsible and aggressive nuclear rhetoric, military concept and underlying posture; and its repeated violations of NATO Allied airspace. (NATO, 2016)

Det presiseres tydelig at Russlands handlinger i Ukraina er en viktig del av at de blir utpekt som en destabiliserende faktor. For NATO trekkes Ukraina fram under flere punkter som en viktig partner[14] og understreker i punkt 66 følgende: «We will also support Ukraine's efforts to strengthen its resilience against hybrid threats, including through intensifying activities under the NATO-Ukraine Platform on Countering Hybrid Warfare» (NATO, 2016).

Den plattformen som nevnes her er en del av det nettverket *The European Centre of Excellence for Countering Hybrid Threats*[15] (Hybrid CoE).

Cyberdomenet blir også eksplisitt nevnt i deklarasjonen. Etter å ha anerkjent cyberforsvar som en av kjerneoppgavene i kollektivt forsvar i 2014, ble cyberspace etter toppmøtet i Warszawa anerkjent som et eget domene, på lik linje med sjø, land og luft:

> Cyber attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. We agreed in Wales that cyber defence is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of

[14] Ukraina har siden 1994 vært et medlem av NATOs Partnership for Peace-program.
[15] Hybrid CoE beskriver hybride trusler som for eksempel destabilisering gjennom påvirkning av befolkning, informasjonssystemer eller teknologiske svakheter hos en fiende. I tillegg karakteriseres hybride trusler med at de kan skape forvirring rundt attribusjon og at de har til hensikt å påvirke beslutninger hos fienden (The European Centre of Excellence for Countering Hybrid Threats, 2020). En inngangsport for å påvirke disse områdene kan være gjennom informasjonsnettverk, og danner med det en link mellom operasjoner i cyberspace og hybridoperasjoner.

> operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. (NATO, 2016)

Sitatet er hentet fra deklarasjonens punkt 70, og understreker nok en gang viktigheten av cyberforsvar. Tiltakene som nevnt over ble gjort for blant annet å støtte opp under NATOs avskrekking og forsvar. Videre står det at NATO vil fortsette å følge prinsippene om tilbakeholdenhet og støtte internasjonal fred, sikkerhet og stabilitet i cyberspace (NATO, 2016). I tillegg ble NATOs «Cyber Defence Pledge» vedtatt, hvor medlemslandene har forpliktet seg til å forbedre sine forsvar hva gjelder nasjonale nettverk og infrastruktur. I dette ligger det at landene skal forsterke sin motstandsdyktighet og sin evne til å respondere raskt og effektivt mot cyberangrep, noe som også inkluderer i en hybrid kontekst. Det påpekes også at det primæransvaret for å respondere på hybride trusler eller angrep ligger hos den angrepne nasjonen. NATO er forberedt på å assistere en alliert i alle steg i en slik konflikt.

3.2.10 Brussel 2018

NATO bekreftet i deklarasjonen fra 2018 at cyberangrep er en vedvarende og uforutsigbar trussel (NATO, 2018). Det nevnes at alliansen står ovenfor cybertrusler i form av både feilaktig informasjon – det vi kanskje kjenner best som *fake news* – og andre destabiliserende angrep. Deklarasjonen peker direkte på Russland som en utøver av slike angrep og at det i seg selv er en faktor som må tas høyde for. Særlig punkt 20 og 29 i deklarasjonen omhandler hvordan alliansen ser på slike trusler, samt enkelte tiltak som blir gjort for å møte disse:

> Cyber threats to the security of the Alliance are becoming more frequent, complex, destructive, and coercive. NATO will continue to adapt to the evolving cyber threat landscape, which is affected by both state and non-state actors, including statesponsored. Cyber defence is part of NATO's core task of collective defence. We must be able to operate as effectively in cyberspace as we do in the air, on land, and at sea to strengthen and support the Alliance's overall deterrence and defence posture. We therefore continue to implement cyberspace as a domain of operations. (NATO, 2018)

> We have also taken far-reaching decisions to adapt and strengthen the NATO Command Structure, the military backbone of the Alliance. It will enable our Supreme Commanders to command and control forces to deal with any military challenge or security threat at any time ... .We will establish a Cyberspace Operations Centre in

> Belgium to provide situational awareness and coordination of NATO operational activity within cyberspace. (NATO, 2018)

Det understrekes at cyberforsvar er en av kjerneoppgavene til alliansen og at NATO skal være i stand til å operere like effektivt i cyberspace som i de øvrige domenene luft, land og sjø. Av konkrete tiltak vedtas det å opprette et operasjonssenter for cyberoperasjoner som skal inngå i NATOs eksisterende kommandostruktur (NATO, 2018).

3.2.11 London 2019

Deklarasjonen fra toppmøtet i London i desember 2019 understreker at cybertrusler er et av flere fokusområder for alliansen. Kommunikeet er relativt kort sammenliknet med de som tidligere er presentert i denne oppgaven, men uttrykker likevel ganske konkrete forhold som alliansen må håndtere i dag og i fremtiden. I likhet med øvrige deklarasjoner nevnes det en rekke trusler som NATO står ovenfor, og Russland og Kina er aktører som representerer utfordringer og til dels truende atferd for politisk sikkerhet i NATOs nærområder. Punkt tre nevner cyber som en konkret trussel, og i punkt seks kan man lese:

> NATO and Allies, within their respective authority, are committed to ensuring the security of our communications, including 5G, recognising the need to rely on secure and resilient systems. … We are increasing our tools to respond to cyber attacks, and strengthening our ability to prepare for, deter, and defend against hybrid tactics that seek to undermine our security and societies. (NATO, 2019)

Det uttrykkes en anerkjennelse av trusler i form av både cyber og kommunikasjonssikkerhet, samtidig som det understrekes alliansen skal jobbe for å håndtere slike trusler. Et annet viktig punkt i deklarasjonen er at verdensrommet (space) anerkjennes som et operasjonsdomene (NATO, 2019)

3.2.12 Utviklingstrekk i NATOs cyberforsvar 1999-2019

Over en 20-års periode har det skjedd en gradvis økning i omtalen av cyberbegrepet gjennom uttalelsene i etterkant av NATOs toppmøter. Alliansens har også tatt faktiske grep når det gjelder fokuset på cyberdomenet i denne perioden. Ytterpunktene i denne utviklingen kan illustreres ved uttalelser i hhv. 2002 og 2016. Etter toppmøtet i Praha på starten av 2000-tallet anerkjennes behovet for å bedre alliansens kapabiliteter for forsvar mot cybertrusler – en vag, men likevel eksplisitt anerkjennelse av at cyberangrep er en potensiell trussel. Om man ser til 2016 kan man lese at cyber anerkjennes som et eget operasjonsdomene som alliansen skal vie

like mye oppmerksomhet til som de tradisjonelle land-, sjø- og luftdomenene. På 14 år gikk med andre ord alliansen fra å anerkjenne at cyberangrep kan være en trussel, til å etablere cyberdomenet som et operasjonsområde på høyde med de konvensjonelle arenaene for krigføring.

Det er ikke bare trusselen knyttet til cyberangrep som har fanget NATOs oppmerksomhet i den aktuelle perioden. Det har også vært en endring i hvem man anser som aktører bak potensielle angrep. I uttalelsen etter toppmøtet i 1999 beskrives Russland og Ukraina begge i samme ordelag som 'allierte' og 'partnere' og det understrekes at man har felles mål og visjoner for sikkerhet og stabilitet i Europa. Som en sterk kontrast til denne uttalelsen kan vi se på deklarasjonene fra Warszawa og Brussel fra hhv. 2016 og 2018.

4.0 Drøfting/Analyse

4.1 NATOs tilnærming til cybertrusselen i 1999 - 2006

I 1999 under krigen i Kosovo, kjent som den første internettkrigen, ble det gjennomført cyberangrep mot NATO i en krigssituasjon. I kjølvannet av denne konflikten så man en gradvis identifisering av utfordringer rundt informasjonssikkerhet og det som vi i dag ville kalt cybersikkerhet. Angrepene hadde som mål å forstyrre NATOs pågående militære operasjoner og ble tilsynelatende gjennomført av hacktivister. De rammet NATOs offisielle informasjonsnettsted, NATOs e-postservere og en datamaskin tilhørende U.S Navy. Å ramme NATOs offisielle nettsteder viste seg å være en kostnadseffektiv måte å svekke alliansens evne til å informere omverden om konflikten og dens gang. Dette førte til at de som ville informere seg om krigens gang måtte ty til andre informasjonskilder. For pro-serbiske aktivister var dette en seier, da de var svært aktive i informasjonsdelingen på denne tiden. I tillegg ble det registrert cyberangrep som kom fra Kina etter feilbombingen av den kinesiske ambassaden i Beograd.

Like etter hendelsene i Kosovo, ble NATOs toppmøte i Washington gjennomført. I deklarasjonen fra toppmøtet nevnes verken cyber eller andre begreper med samme betydning, og vi kan dermed ikke se at cyberangrepene gjenspeiles i alliansens uttalelser. Det er dermed vanskelig å se en sammenheng mellom hendelsene i Kosovo og veien videre for NATO ut fra denne deklarasjonen alene. Om man derimot ser til «The Alliance's Strategic Concept» av 1999 som ble vedtatt på det nevnte møtet, kan man trekke noen paralleller til hendelsene i Kosovo. Dokumentet identifiserer blant annet sentrale egenskaper i sikkerhetsmiljøet og gir veiledning til videre bruk av NATOs militære styrker. Et av punktene tar opp

sikkerhetsproblematikken med den stadig økende avhengigheten av informasjonssystemer. "... state and non-state adversaries may try to exploit the Alliance's growing reliance on information systems through information operations designed to disrupt such systems." (NATO, 1999b). Dette strategiske konseptet vitner om at cybersikkerhet i form av beskyttelse av informasjonssystemer kan være en viktig oppgave for alliansen. Hendelsene i Kosovo beviste langt på vei at denne oppgaven var helt reell. Hvorvidt dette punktet fra Strategic Concept allerede var nedfelt i teksten før hendelsene i Kosovo fant sted, eller om det havnet der som følge av cyberangrepene i Kosovo, kan ikke konkluderes med. Det er likevel en observasjon at dette innholdet i «Strategic Concept» av 1999 vedtas samme år som alliansen har blitt utsatt for hacking av sine informasjonssystemer.

I årene etter Kosovokrigen så man et økt fokus på cyberangrep som en trussel. I deklarasjonen fra toppmøtet i Praha i 2002 står det at NATO skal transformeres med nye kapabiliteter for å tilpasse seg nye trusler og sikkerhetsutfordringer i det 21. århundret, noe som inkluderer kapabiliteter innen cybersikkerhet. Dette kommer frem i punkt 4 i deklarasjonen hvor det står at NATO skal beskytte seg og sine mot ethvert væpnet angrep og som følge av dette besluttet de å styrke sin evne til forsvare seg mot cyberangrep. Her ser man altså at det i løpet av tre år først oppleves cyberangrep, deretter fastslår alliansen at slike angrep må man ruste seg bedre mot i fremtiden. Uttalelsene fra 2002 vitner da om at NATO kan ha lært av angrepene i Kosovo. Dette nevnes dog ikke eksplisitt som en årsak til det økte fokuset på å forsvare seg mot cyberangrep. Sett opp imot det strategiske konseptet fra 1999 og angrepene i Kosovo, hvor trusselen var identifisert, fattes det i 2002 vedtak om å styrke alliansens kapasitet til å forsvare seg mot cyberangrep. Utviklingen fra de erfarte hendelsene i 1999 og frem til uttalelsene i 2002 kan sees på som at trusselen som var oppfattet og ble erfart, begynte å bli mer forstått.

Under toppmøtet i Riga 2006 ser man en økende forståelse for cybertrusselen. I deklarasjonen nevnes det et sett med initiativer som skal gjøre NATO mer forberedt på moderne trusler. Et av disse initiativene omhandler nettverkssikkerhet og fastslår at NATO skal utvikle en «NATO Network Enabled Capability» for å dele informasjon, data og etterretning på en trygg og sikker måte under operasjoner. Samtidig skal den styrke beskyttelsen av informasjonssystemene mot cyberangrep. I motsetning til toppmøtet i 2002 er retorikken og formuleringen i deklarasjonen mye mer spisset om hva en cybertrussel kan være og hva tiltaket skal innebære. Tiltaket virker å være tilpasset hendelsene i Kosovo, hvor man opplevde angrep mot e-postservere som påvirker informasjonsflyt og angrep mot dataservere

som forsinker informasjonsflyt og operasjoners gang. Man ser her at trusselen man oppfattet og erfarte i 1999 er blitt satt ord på, noe som tyder på at NATO i større grad forstår trusselen et cyberangrep kan medføre. Det må likevel påpekes at det er vanskelig å si noe om kausalitet i dette tilfellet, da trusselen mot informasjonssystemer ble påpekt i «The Alliances Strategic Concept» av 1999. Hvorvidt punktet som omfatter sårbarheten og avhengigheten av informasjonssystemer står i konseptet som følge av at trusselen allerede var identifisert, eller om det havnet der som følge av erfaringene i Kosovo er kan ikke konkluderes. Likevel virker det å være klart at hendelsene i Kosovo har bidratt til å øke forståelsen for trusselen og dermed gjort det lettere for NATO å fatte konkrete tiltak.

I perioden fra 1999 og til tidlig på 2000-tallet så gikk NATO på få år fra å identifisere en trussel i form av cyberangrepene i Kosovo, til å fatte uttalte tiltak for å møte slike trusler. Alliansens toppmøter fra hhv. 1999, 2002 og 2006 vitner om dette. Fra å generalisere under toppmøtet i Praha, hvor NATO beslutter å ruste seg bedre mot cyberangrep, fattes det på toppmøtet i Riga konkrete tiltak om hvilken enhet som skal opprettes og hva denne skal ha som ansvarsområdet. Om man sammenligner tiltaket som blir vedtatt i Riga opp imot angrepene i Kosovo. Det ser dermed ut som at erfaringene fra Kosovo har utviklet og formalisert seg til et konkret tiltak, noe som tyder på at hendelsene har hatt direkte påvirkning på utviklingen av NATOs forståelse for cybertrusler.

4.2 NATOs tilnærming til cybertrusselen 2007 - 2014

I dette kapittelet vil vi se på hendelsene i Tallinn, Georgia og Stuxnet for å se hvordan disse har påvirket NATOs utvikling av forståelse for cybertrusselen.

Cyberangrepene mot Estland i 2007 og Georgia i 2008 viste ytterligere potensialet til cybervåpen. Førstnevnte som et enkeltstående angrep på en stat, og sistnevnte som del av en større militær operasjon. På denne tiden hadde NATO begynt å etablere tiltak for å kunne motstå cyberangrep, men disse tok utgangspunkt i å forsvare NATOs egne nettverk. Dette forstås som at alliansen var forberedt på cyberangrep mot egen militær organisasjon slik de opplevde i Kosovo, og at de dermed ikke tok høyde for å operere utenfor egne nettverk. Det kan dermed tenkes at de ovennevnte cyberangrepene virket overraskende på NATO da organisasjonen ikke var forberedt på cyberangrep i slik størrelsesorden. Aktørene under angrepene i Kosovo ble antatt utført av ikke-statlige aktører som sympatiserte med Serbia, mens det er sterke indisier på at en statlig aktør står bak de nye angrepene. NATO fremstod dermed som en organisasjon som i liten grad kunne gjennomføre og lede cyberforsvarsoperasjoner på denne tiden. Dette kan eksemplifiseres med angrepet på Estland,

hvor staten ble stående uten alliert hjelp i angrepets varighet på 22 dager. Dette tidsperspektivet hadde trolig gitt rom for å intervenere og gi bistand. En av egenskapene til cyber er at angrep og forsvar utøves i sanntid, noe som tillater kort reaksjonstid. I tillegg kan cyberforsvar utøves uten å flytte og mobilisere enheter i samme grad som man må i andre våpenarter. Det er dermed rimelig å anta at NATO hverken hadde kapabiliteter eller systemer for å kunne støtte sine medlemsland, da fokuset dens var på egne nettverk og beskyttelse av disse.

Om man ser til toppmøtet i 2008, som fant sted før hendelsene i Georgia, ser man at alliansen innlemmet en «Policy on Cyber Defence» januar samme år. I deklarasjonen fra toppmøtet understrekes viktigheten av dens innhold. Blant annet at NATO og dets medlemmer har behov for kapabiliteter som muliggjør bistand til medlemsland som står ovenfor et cyberangrep. Om man relaterer dette mot hendelsene i Estland er det mulig å se en klar linje mellom NATOs endringer og utviklingen av trusselen. NATO har inntil denne tiden hatt fokus på beskyttelse av egne nettverk, men etter angrepene i Estland og Georgia virker det som at organisasjonen innser at statlige aktører både kan og vil gjennomføre komplekse cyberangrep. Da også mot andre mål enn alliansens egne nettverk, slik som viktig sivil infrastruktur. Det virker dermed som at NATOs oppfatning av cybertrusselen har endret seg mye fra 2006 til 2008. Fra å fokusere på egne nettverk, har NATO innsett at de ikke bare må kunne forsvare seg selv, men også sivil infrastruktur som er vital for både stat og forsvar.

Angrepet mot Estland fremstår som en oppvåkning for NATO, som får ytterligere drivkraft av hendelsene i Georgia. I perioden etter dette fattes det en rekke tiltak. Blant annet ser man i 2009 i deklarasjonen fra toppmøtet i Strasbourg og Kehl at NATO vil integrere cyberforsvar som en del av sine øvelser. På den måten vil alliansen kunne øve cyberforsvarskapabiliteter på lik linje som i land-, sjø-, og luftdomenet. Dette kan relateres til angrepet i Georgia, hvor cyberkapasiteter ble brukt koordinert og synkronisert med andre operasjoner. Resultatet av dette var overlegenhet i informasjonsdomenet. Ved å hindre effektiv kommunikasjon fra regjeringen og mediehus skapte angriperen forvirring og uforutsigbarhet for sin motstander. Ser man dette i lys av NATOs vedtak om å innlemme cyberforsvar i sine øvelser, kan det virke som at NATO begynner å forstå at cyberspace bør integreres som en del av kollektivt forsvar. I Georgia var russiske cyberangrep integrert i resten av operasjonene, sammen med luft-, og landoperasjoner. Det fremstår dermed som NATO forstår at de er nødt til å trene på forsvar i cyberspace, på lik linje som de andre domenene for å kunne motstå en fremtidig trussel som en allianse. Videre oppretter NATO to nye enheter, samt styrker den eksisterende

NCIRC som skal beskytte alliansens egne nettverk. De to nye enhetene er CDMA og CCDCOE. CDMA skal fungere som en sentral kommando for blant annet informasjonsdelingstiltak, og har ansvar for å sette i gang og koordinere øyeblikkelige og effektive cyberforsvarstiltak der det er aktuelt. CCDCOE skal fungere som et forskingssenter på cyberoperasjoner, og ble opprettet i Tallin i Estland. I tillegg til å drive forskning arrangerer de årlige cyberøvelser og konferanser som skal tilføre kunnskaper og erfaringer til NATO. Gjennom disse tiltakene ser man at NATO har tatt lærdom av Estland og Georgia. Ved å tilføre disse kapasitetene ser man at alliansen forbereder seg på videre utvikling og legger til rette for å innlemme cyberforsvar som en del av det kollektive forsvaret.

I deklarasjonen fra toppmøtet i Lisboa 2010 ser man at fokuset på cyber har økt betraktelig. Begrepet blir brukt i 40 av punktene. 2010 er også året hvor Stuxnet blir kompromittert og kjent for allmenheten. Deklarasjonen omtaler cybertrusler som stadig mer avanserte og økende i omfang. Denne erkjennelsen stemmer godt over ens med utviklingen cyber har hatt som trussel. Fra å være enkle angrep fra antatte ikke-statlige aktører, har trusselen blitt mer sammensatt. På denne tiden har det blitt gjennomført avanserte cyberoperasjoner av antatte statlige aktører. Dette ser man både i eksempelet fra Georgia, og eksempelet om Stuxnet. Stuxnet skiller seg fra de andre angrepene. Angrepene i Estland og Georgia bestod stort sett av DoS og DDoS, mens operasjonen mot det iranske atomprogrammet ble gjennomført med et sammensatt cybervåpen designet spesielt for å ramme et spesifikt datanettverk. En av aktørene bak Stuxnet var NATO-medlemmet USA, men operasjonen ble utført utenom alliansen. Det er vanskelig å si noe om kunnskapene NATO hadde om denne operasjonen i tiden den pågikk. Uavhengig av dette synliggjør hendelsen at statlige aktører har etablert seg i cyberdomenet med svært avanserte kapabiliteter. Videre i deklarasjonen informerer NATO om at de skal implementere cyber som dimensjon i sine doktriner. Dette for å utbedre organisasjonens kapabiliteter til å beskytte systemer som er kritisk viktige. Dette har potensiale til å styrke NATOs cyberforsvar i helhet, da en doktrinær tilnærming vil bidra til å skape bedre felles forståelse og enhetlige løsninger på problemer cyberangrep kan medføre. I tillegg kommer det frem at NATO skal utarbeide en mer dyptgående cyberpolicy enn den som allerede eksisterer, samtidig som alliansen skal arbeide tettere med sivile organisasjoner som EU og FN. Dette kan sees i lys av cyberoperasjoners natur, som sjelden kan isoleres som militære problemer. Cyberangrep tenderer å være rettet mot sivil infrastruktur, som påvirker sivile så vel som militære. Disse tiltakene ser ut til å forme alliansen i den retningen den må

for å senere kunne innlemme cyberforsvar som en del av det kollektive forsvaret, samtidig som de søker å øke forsvarsevnen i det sivile.

De neste årene vedtas en rekke endringer i NATOs cyberforsvar. I deklarasjonen fra toppmøtet i Chicago 2012 ser man at det blir vedtatt planer for å implementere den nye cyberforsvarspolicyen, «Enhanced Cyber Defence Policy» (ECDP). Denne policyen blir vedtatt under toppmøtet i Wales 2014. Med denne blir cyberforsvar anerkjent som en av NATOs kjerneoppgaver innen kollektivt forsvar. I tillegg anerkjenner de krigens folkerett og FN-traktatene til å være gjeldende i cyberspace. Dette kan ansees som en forlengelse av vedtakene gjort fra 2008 og utover, da man ser at hvordan cybertrusselen har utviklet seg. Fra å være et enkelt middel for å nekte eller forsinke nettverk, har det utviklet seg til å bli et våpen man kan utnytte for å påvirke andre staters politikk og et våpen som kan brukes implementert med andre forsvarsgrener i krig. Det virker dermed som at NATO sin forståelse for cybertrusselen har økt betraktelig, da de nå anser cyberforsvar som en kjerneoppgave i det kollektive forsvaret. Dette betyr blant annet at et cyberangrep vil kunne utløse NATOs artikkel 5, hvor et angrep på en alliert er å anse som et angrep på alle. På denne måten gir NATO seg selv muligheten til å kunne intervenere når en alliert stat blir angrepet i cyberspace. I tillegg ligger det en ansvarsgjøring i dette. Ettersom cyberforsvar blir en del av det kollektive forsvaret blir medlemslandene pålagt å inneha et eget nasjonalt cyberforsvar. Dette blir understreket i deklarasjonen fra Wales da den siterer EDCP som sier at NATOs hovedansvar er å beskytte egne nettverk, og at allierte må ha egne kapasiteter for beskyttelse av nasjonale nettverk. NATO har de siste årene etablert verktøy for å koordinere og lede cyberforsvar i regi av alliansen, samtidig som de har pålagt medlemmene et ansvar i å inneha kapasitetene som trengs.

4.3 NATOs tilnærming til cybertrusselen i 2015 - 2019

Utviklingen i cyberdomenet frem til i dag har vært formidabel på mange måter, og særlig i 2016 nådde NATO en viktig milepæl. Under toppmøtet i Warszawa vedtok alliansen at cyber skulle ansees som et operasjonelt domene, på lik linje med sjø, luft og land. Det ble ikke nevnt noen eksplisitt årsak til at de på dette tidspunktet 'opphøyet' cyber til et eget domene, men samtidig ble det ansett at trusler mot internasjonal fred, sikkerhet og stabilitet også skulle ivaretas i 'cyberspace'. Flere situasjoner har i de senere år vært truende for nettopp internasjonal sikkerhet i Europa, og særlig konflikten i Ukraina er et eksempel på dette.

Som nevnt i kapittel 3.1.4 opplevde Ukraina i førjulen 2015 for første gang at cyberangrep ble brukt mot sivil infrastruktur i et stort omfang. Ved å bryte seg inn i, og overstyre

distribusjonsnettet for strømforsyning til befolkningen viste hackere at de var i stand til å påvirke over 200,000 mennesker ved bruk av ukonvensjonelle digitale angrep. Disse angrepene var ikke noe som påvirket en NATO-alliert direkte, og man har heller ikke kunnet attribuere dem til noen bestemt aktør. Likevel er det grunn til å drøfte hvorvidt hendelsene kan ha påvirket alliansens syn på cyberforsvar, blant annet fordi Ukraina ligger sentralt i Europa, et naturlig fokusområde for alliansen, og fordi de er en partnernasjon i PfP-programmet.

I den sammenheng er det naturlig å se på hendelsene i Ukraina, som på mange måter bryter med nettopp prinsippene om fred, stabilitet og sikkerhet. Et så omfattende og i stor grad isolert angrep på sivil infrastruktur kan ha tydeliggjort behovet for å kunne møte trusler i dette domenet alene, og ikke 'bare' som en del av andre militære operasjoner. Deklarasjonen fra toppmøtet adresserer også den forverrede sikkerhetspolitiske situasjonen i Ukraina generelt, etter Russlands annektering av Krim-halvøya i 2014. Det understrekes at samarbeidet mellom NATO og Ukraina er viktig for stabilitet i det Euro-Atlantiske området og at Russlands militære tilstedeværelse og destabiliserende atferd i Ukraina er en sentral utfordring. Det er altså helt klart at hendelsene i Ukraina i perioden før toppmøtet i 2016 har påvirket alliansens uttalelser, selv om de ikke eksplisitt nevner cyberangrepene i 2015. Samtidig har det blitt mer enn antydet at det er russisk sikkerhetstjeneste som står bak cyberangrepene, men det skal igjen understrekes at dette ikke er bevist og at angrepene ikke nevnes som en konkret årsak til etableringen av cyber som eget domene. Likevel var de en sentral del av den destabiliseringen i NATOs nærområde som nevnes som en årsak til det økte fokuset på cyber, og kan derfor tenkes å ha påvirket alliansens uttalelser og policy. Det at cyberangrep viste seg å kunne påvirke over 200,000 mennesker er altså å anse som en faktor som kan ha bidratt til å opphøye statusen til cyberdomenet.

I deklarasjonen fra Brussel i 2018 videreføres fokuset på at Russland er en uforutsigbar aktør i Europa. Her nevnes de eksplisitt som en sentral utøver av for eksempel cyberangrep som har til hensikt å virke destabiliserende. Nok en gang understrekes det at cyber er et eget domene, og i tillegg vedtas det å etablere et 'Cyber Operations Centre' i Belgia. Det fremkommer ingen begrunnelse for at Russland nevnes, men samtidig antydes det at de er en aktør som er kjent for å bedrive undergravende virksomhet gjennom cyberangrep og påvirkningskampanjer. Hendelsene i Ukraina kan sies å være en handling som Russland potensielt kan utføre, altså i tråd med NATOs aktørvurdering av Russland. Igjen er dette en

implisitt slutning av at de nevnes som en mulig aktør på dette feltet og at de er anklaget for å stå bak Ukraina-angrepet.

En kan trekke paralleller mellom det angivelige russiske cyberangrepet på distribusjonsnettet i Ukraina og fokuset på Russland som destabiliserende aktør i NATOs uttalelser i 2016. Det er ingen eksplisitt uttalelse om at angrepet direkte er en årsak til at man etter toppmøtet i Warszawa anerkjenner cyber som eget domene. Samtidig har flere har utpekt Russland til å være ansvarlig for angrepene kort tid etter at de skjedde, og omstendighetene (Russlands tilstedeværelse i Ukraina og annekteringen av Krim) kan sies å tale for dette og at det derfor kan ha vært en medvirkende årsak til at fokuset på cyberdomenet er såpass tilstede i deklarasjonen.

5.0 Oppsummering og konklusjon

Denne oppgaven skal besvare problemstillingen: «Hvordan har NATOs tilnærming til cyberforsvar endret seg i takt med utviklingen av cybertrusselen i perioden 1999-2019?». For å gjøre det har den sett på hvordan cybertrusselen har utviklet seg i det samme tidsrommet og satt dette opp mot uttalelser og beslutninger gjort på toppmøtene til NATO.

Cybertrusselen har i denne perioden utviklet seg fra å være relativt enkel ved å mette datatrafikken i forskjellige nettverk til å bli en mer avansert trussel som kan angripe og ta kontroll over viktig infrastruktur. Mengden angrep har økt mye i perioden, noe som skyldes digitaliseringen verden har stått ovenfor. Antall mennesker, organisasjoner og stater som har koblet seg på nett har økt betraktelig, noe som har skapt mange mulige angrepspunkter og dermed økt sårbarheten. Dette har muliggjort større angrep som for eksempel de i Estland og Georgia. I tillegg har staters digitalisering av sivile infrastruktur medført en sårbarhet. Selv om slikt ofte legges til lukkede nettverk, ser man i eksempelet om Stuxnet at det ikke er noen garanti for at det er sikkert. Man ser også at aktørene har endret seg over tid. Til å begynne med virker cyberangrep å ha vært et middel anvendt av aktivister og små grupperinger mot blant annet militære nettverk for å proklamere sitt politiske ståsted. I senere tid har cyberangrep i større og større grad blitt anvendt av statlige ressurssterke aktører, og da gjerne mot sivil infrastruktur som også anvendes av militære. I noen tilfeller har dette også blitt gjort parallelt og koordinert med andre militære operasjoner for å oppnå militære mål.

NATO har på kort tid gjennomført store endringer i organisasjonen for å kunne møte slike trusler. I 1999 forelå det en erkjennelse av at den økende avhengigheten av informasjonssystemer medfører en risiko. I løpet av de neste 20 årene har NATO anerkjent

cyber som et eget krigføringsdomene, integrert cyber i øving og trening, samt opprettet en egen felleskommando for cyberoperasjoner. Selv om det har skjedd store endringer på kort tid, virker NATO likevel å ha utviklet seg tregt i forhold til utviklingen av cybertrusselen. Det ser ut som at NATOs cyberforsvar i 2007 var organisert for og forberedt på lignende angrep alliansen opplevde i 1999. Det ser dermed ut som at angrepene i Estland og på Georgia blir en oppvåkning for alliansen. I disse angrepene er det sterke indisier på at en statlig aktør står bak, og cyberdomenet blir anvendt til å påvirke politikk og å få et overtak i informasjonsdomenet i militære operasjoner. De kommende årene gjør NATO endringer som medfører at medlemslandene skal kunne bistå hverandre, samt at NATO skal kunne lede koalisjonsoperasjoner i cyberspace fra en egen kommando. I tillegg innlemmes cyberforsvar som en del av ansvaret i det kollektive forsvaret, samt at cyber etableres som et eget krigsdomene.

Det kan virke som at NATO har hatt en reaktiv utvikling på sin tilnærming til cyberforsvar. Fra 1999 til 2007 fremstår det som at alliansen har oppfattet og erkjent at cybertrusselen eksisterer. Tiltakene som blir fattet er få, og dreier seg i hovedsak om NATOs egne nettverk. Angrepene i Estland virker dermed å være en oppvåkning for NATO. Disse angrepene treffer en hel stat for å påvirke dens politikk, noe som ser ut til å være en påvirkende faktor for den videre utviklingen av NATOs forhold til cyberforsvar. Etter denne hendelsen foretas det en rekke organisatoriske tiltak i alliansen. Blant annet ble CCDCOE og CDMA opprettet. De kommende årene skjer det flere angrep, eksemplifisert med Georgia og Ukraina, hvor det mistenkes at Russland står bak. I angrepet på Georgia og Ukraina gjennomføres det cyberoperasjoner koordinert med operasjoner i andre domener. Det er først etter angrepene i Ukraina at NATO virkelig tar grep og gjør de største endringene. Selv om utviklingen NATO har hatt innen cyberforsvar har vært eksponentiell og i seg selv gått veldig fort, har den sett opp mot utviklingen av trusselen vært et steg bak. Dette vil nok være naturlig for en organisasjon av den størrelsen blant annet grunnet byråkratiske og tidkrevende prosesser. Likevel ser man at alliansen har fattet store og viktige vedtak og beslutninger på relativt kort tid. På den måten fremstår det som at organisasjonen har hatt en forholdsvis effektiv tilpasning. Denne oppgavens problemstilling kan dermed besvares med at NATOs tilnærming til cyberforsvar til dels har holdt følge med trusselen, men da på en reaktiv måte ettersom beslutninger og vedtak i stor grad har kommet i etterkant av definerende hendelser for cybertrusselen.

Referanser

Cooperative Cyber Defence Center of Excellence. (u.d.). *About us*. Hentet August 14, 2019 fra CCDCOE: https://ccdcoe.org/about-us/

Donghui Park, J. S. (2017, Oktober 11). *The Henry M. Jackson School of International Studies*. Hentet fra Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

Enstad, J. D. (2019, April 11). *Østfronten.* Hentet Januar 7, 2020 fra Store Norske Leksikon: https://snl.no/%C3%98stfronten

Geers, K. (2008). *Cyberspace and the Changing Nature og Warfare.* Tallinn: Cooperative Cyber Defence CEntre of Excellence.

Grønning, T. B. (2011, August 10). *«Fredrik» (17) jaktes av NATO, CIA og FBI*. Hentet Oktober 1, 2019 fra Dagbladet: https://www.dagbladet.no/nyheter/fredrik-17-jaktes-av-nato-cia-og-fbi/63577643

Healey, J. (2011, September 11). *Cyber Attacks Against NATO, Then and Now*. Hentet Desember 10, 2019 fra Atlantic Council: https://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-attacks-against-nato-then-and-now/

Hollis, D. (2011, Januar 6). *Cyberwar Case Study: Georgia 2008.* Hentet Desember 12, 2019 fra Small Wars Journal: https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Homeland Security. (2016, Mars 7). *Report: Ukrainian Critical Infrastructure Cyber Attack.* Hentet Desember 9, 2019 fra Public Intelligence: https://publicintelligence.net/nccic-ukrainian-power-attack/

Kaplan, F. (2016). *Dark Territory* . New York: Simon & Schuster Paperbacks.

Karseth, A., Berge, T., & Johansen, E. N. (2019, Mai 9). *13-åringen hacket Bergen kommune – nå får skoleeleven tilbud om jobb i bank*. Hentet Oktober 1, 2019 fra NRK: https://www.nrk.no/hordaland/13-aringen-hacket-bergen-kommune-_-na-far-skoleeleven-tilbud-om-jobb-i-bank-1.14542966

Lynch, A. (1999, April 15). *Kosovo Being Called First Internet War*. Hentet Desember 10, 2019 fra SFGate: https://www.sfgate.com/news/article/Kosovo-Being-Called-First-Internet-War-Web-2936299.php

Markoff, J. (2008, August 12). *The New York Times.* Hentet fra Before the Gunfire, Cyberattacks: https://www.nytimes.com/2008/08/13/technology/13cyber.html

Messmer, E. (1999, April 6). *Serb supporters sock it to NATO, U.S. Web sites*. Hentet August 21, 2019 fra CNN: http://edition.cnn.com/TECH/computing/9904/06/serbnato.idg/index.html

Miniwatts Marketing Group. (2019, Juni 30). *Internet Usage Statistics*. Hentet Oktober 1, 2019 fra Internet World Stats: https://www.internetworldstats.com/stats.htm

Myrli, S. (2009, November 24). *CYBERDEFENCE - MYRLI REPORT*. Hentet Oktober 15, 2019 fra NATO Parliamentary Assembly: https://nato-pa.int/document/2009-173-dscfc-09-e-bis-cyberdefence-myrli-report

NATO. (1999a, April 23). *The Washington Declaration.* Hentet Oktober 12, 2019 fra NATO Summit: https://www.nato.int/docu/pr/1999/p99-063e.htm

NATO. (1999b, April 24). *The Alliance's Strategic Concept.* Hentet Oktober 12, 2019 fra North Atlantic Treaty Organization: https://www.nato.int/cps/en/natolive/official_texts_27433.htm

NATO. (2002, November 21). *Prague Summit Declaration.* Hentet Oktober 12, 2019 fra North Atlantic Treaty: https://www.nato.int/cps/en/natohq/official_texts_19552.htm?

NATO. (2006, November 29). *Riga Summit Declaration*. Hentet Oktober 15, 2019 fra North Atlantic Treaty Organization: https://www.nato.int/cps/in/natohq/official_texts_37920.htm

NATO. (2008, April 3). *Bucharest Summit Declaration.* Hentet Oktober 20, 2019 fra North Atlantic Treaty Organization: https://www.nato.int/cps/en/natolive/official_texts_8443.htm

NATO. (2009, April 4). *Strasbourg / Kehl Summit Declaration.* Hentet Oktober 20, 2019 fra North Atlantic Treaty Organization: Strasbourg / Kehl Summit Declaration

NATO. (2010, November 20). *Lisbon Summit Declaration.* Hentet Oktober 20, 2019 fra North Atlantic Treaty Organization: https://www.nato.int/cps/em/natohq/official_texts_68828.htm

NATO. (2012, Mai 20). *Chicago Summit Declaration*. Hentet Oktober 16, 2019 fra North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en

NATO. (2014, September 5). *Wales Summit Declaration.* Hentet Oktober 20, 2019 fra North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO. (2016, Julie 8). *Cyber Defence Pledge*. Hentet Oktober 14, 2019 fra North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO. (2016, Juli 9). *Warsaw Summit Communiqué.* Hentet Oktober 21, 2019 fra North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO. (2017, Oktober 10). *North Atlantic Council*. Hentet Oktober 14, 2019 fra North Atlantic Treaty Organization: https://www.nato.int/cps/ic/natohq/topics_49763.htm

NATO. (2018, Juli 11). *Brussels Summit Declaration.* Hentet Oktober 22, 2019 fra North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=en

NATO. (2018, Juli 19). *Summit meetings*. Hentet Oktober 14, 2019 fra North Atlantic Treaty Organization: https://www.nato.int/cps/en/natolive/topics_50115.htm

NATO. (2018, Juli 19). *Summit Meetings.* Hentet Januar 7, 2020 fra North Atlantic Treaty Organization: https://www.nato.int/cps/en/natolive/topics_50115.htm

NATO. (2019, Mai 23). *by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London*. Hentet Oktober 12, 2019 fra North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/opinions_166039.htm

NATO. (2019, Desember 4). *London Declaration*. Hentet Desember 10, 2019 fra North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/official_texts_171584.htm

NATO. (u.d.). *NATO Term: The Official NATO Terminology Database*. Hentet November 6, 2019 fra NATO Standardization Office: https://nso.nato.int/natoterm/Web.mvc

Notaker, H. (2019, August 1). *CIA.* Hentet Januar 1, 2020 fra Store Norske Leksikon: https://snl.no/CIA

Næss, M., & Notaker, H. (2015, Januar 31). *National Security Agency.* Hentet Januar 7, 2020 fra Store Norske Leksikon: https://snl.no/National_Security_Agency

Ottis, R. (2007). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Tallinn: Cooperative Cyber Defence Centre of Excellence .

Reed, J. (2015, Juli 10). *Unit 8200: Israels Cyber Spy Agency.* Hentet Januar 7, 2020 fra Financial Times: https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c

Sundvor, O. (2015, Februar 26). *Slik hacket 17-åringen regjeringen og finans-Norge*. Hentet Oktober 1, 2019 fra Bergens Avisen: https://www.ba.no/kriminalitet-og-rettsvesen/slik-hacket-17-aringen-regjeringen-og-finans-norge/s/5-8-28600

Verton, D. (1999, April 4). *Serbs launch cyberattack on NATO*. Hentet August 21, 2019 fra FCW: https://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx

Wernersen, C., & Asvall, H. (2018, September 24). *NRK*. Hentet Oktober 2, 2019 fra Eksperter jakter på avlyttingsutstyr på Stortinget: https://www.nrk.no/norge/eksperter-jakter-pa-avlyttingsutstyr-pa-stortinget-1.14220734