Bacheloroppgave

ADM650 Jus og administrasjon

Cyberkrigføring - den nye slagmarken?

Cyberwarfare - the new battlefield?

Eirin Kjerstad Bøe og Vivetha Umakaran

Totalt antall sider inkludert forsiden: 26

Molde, 22.05.2017

Høgskolen i Molde
Vitenskapelig høgskole i logistikk

Obligatorisk egenerklæring/gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

Du/dere fyller ut erklæringen ved å klikke i ruten til høyre for den enkelte del 1-6:		
1.	**Jeg/vi erklærer herved at min/vår besvarelse er mitt/vårt eget arbeid, og at jeg/vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen.**	☒
2.	**Jeg/vi erklærer videre at denne besvarelsen:** • ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands. • ikke refererer til andres arbeid uten at det er oppgitt. • ikke refererer til eget tidligere arbeid uten at det er oppgitt. • har alle referansene oppgitt i litteraturlisten. • ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse.	☒
3.	**Jeg/vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§14 og 15.**	☒
4.	**Jeg/vi er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert i Ephorus, se Retningslinjer for elektronisk innlevering og publisering av studiepoenggivende studentoppgaver**	☒
5.	**Jeg/vi er kjent med at høgskolen vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk**	☒
6.	**Jeg/vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider**	☒

Publiseringsavtale

Studiepoeng: 15

Veileder: Frank Robert Lien

Fullmakt til elektronisk publisering av oppgaven

Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).
Alle oppgaver som fyller kriteriene vil bli registrert og publisert i Brage HiM med forfatter(ne)s godkjennelse.
Oppgaver som er unntatt offentlighet eller båndlagt vil ikke bli publisert.

Jeg/vi gir herved Høgskolen i Molde en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering: ☒**ja** ☐**nei**

Er oppgaven båndlagt (konfidensiell)? ☐**ja** ☒**nei**
(Båndleggingsavtale må fylles ut)
- Hvis ja:
Kan oppgaven publiseres når båndleggingsperioden er over? ☐**ja** ☐**nei**

Er oppgaven unntatt offentlighet? ☐**ja** ☒**nei**
(inneholder taushetsbelagt informasjon. Jfr. Offl. §13/Fvl. §13)

Dato: 22.05.2017

Forord

Denne bacheloroppgaven er den avsluttende delen av vår utdannelse på Høgskolen i Molde, Bachelor i jus og administrasjon 2014-2017. Vi har gått i dybden av et tema vi hadde begrenset kunnskap fra før av, noe som både har vært utfordrende, og like spennende som lærerikt.

Da tiden var kommet for å velge tema og problemstilling for bacheloroppgaven, bestemte vi oss for å skrive om hacking og cyberangrep, og ta utgangspunktet i ulike hendelser mellom stater. Dette er store saker som har fått masse mediedekning og fått statene til å reagere med å opprette cyberavdelinger og har satt cyberangrep i fokus. På leting etter vårt tema hadde vi idemyldring med hverandre og bekjente. Vi så på dokumentarfilmen *«Zero Days»*, som handler om Stuxnet-ormen, et virusprogram utviklet i USA som ble brukt i å angripe et atomkraftverk i Iran. Da vi innså hvor omfattende og intrikat problemstillingene rundt cyberkrigføring var bestemte vi oss for å gå i dybden. Pensumbøker, og andre relevante bøker om cyberdomene, cyberkrig og hacking har vært viktig for å se tilbake på historien. Samtidig som vi brukte mye sosiale medier til å lese igjennom angrep og hacking som har fått en del oppmerksomhet, innså vi at offentlige myndigheter som Forsvaret, Regjeringen og andre ulike forskningsinstitutt har et økt fokus på cyberdomenet og den nye krigføringen. Vi syntes at dette virket både gøy og spennende. Selv om vi hadde lite kunnskap om emnet fra før av, forsto vi raskt at dette er noe som er verdt å skrive om, grunnet at det er en del som ikke vet at dette må tas på alvor. Det er i de siste årene det er blitt økt forsking på dette emnet, og flere skriver rapporter om cyberkrigføring i lyset av forsvarets operative evne. I starten var det utfordrende siden vi hadde altfor mye informasjon om emnet, som gjorde det meget vanskelig å begrense oss til temaet. Men etter å ha funnet vår vinkling på teamet fungerte dette heller som en motiverende faktor. Vi satt med en følelsen av å gjøre noe ikke mange av oss hadde gjort før. Dette fikk oss meget motivert til å stå på med oppgaven. Vi håper derfor at vår oppgave vil bidra med ny og innsiktsfull informasjon, til videre forskning eller oppgaver.

Sammendrag

Vi lever i en mer teknologisk og globalisert verden. Med den politiske globaliseringen økes frakoplingen der tid og rom ikke spiller like stor rolle og der nasjonalstatenes grenser viskes ut. I det internasjonale samfunnet opplever statene større sårbarhet i møte med den teknologiske utviklingen. Cyberkrigføring og hacking har i de siste årene vært et problem for mange stater. E-tjenesten og forsvaret har satt det i fokus under årsrapporten for 2017. Det har vært en øking av cyberangrep og hacking mellom stater i de siste ti årene. Georgia, Estland, USA, Iran og Russland er noen av aktørene som har vært involvert i disse. FN-pakten står som rettskilden som skal regulere interaksjon mellom stater og det er denne som skal anvendes i saker som omhandler cyberangrep og hacking mellom stater.

Formålet med denne Bacheloroppgaven er å belyse hvordan cyberdomenet og cybermakt er relevant for FN-paktens interesser i en globalisert verden. Vi kommer til å få mer innsyn i hvordan den globaliserte verden har endret på krigføringen.

Innhold

1.0 Innledning

Fokus-rapporten fra Etterretningstjenesten er en årlig trussel- og risikovurdering som belyser utvalgte tema som kan ha betydning for Norge og norske interesser. Fokus 2017 har blant annet valgt å fokusere på trusselen i det digitale rom. Truslene mot politiske, militære og økonomiske mål øker og E-tjenesten forventer omfattende etterretningsoperasjoner mot Norge i 2017. (E-tjenesten 2017) Cyberdomenet utgjør et nytt område for militær makt og stiller staten ovenfor et nytt trusselbilde. jfr. datamaterialet på Forsvarets Forskningsinstitutts sider «Strategisk kommunikasjon og cyberforsvar» (2017) Det sikkerhetspolitiske landskapet har over de siste årene gjennomgått store endringer og utfordringene er mer komplekse enn noen gang. Nasjonalstatenes sikkerhetsinteresser utfordres og øker usikkerheten globalt. Det skjer «betydelige endringer, både geopolitisk og gjennom globaliseringens nye usikkerhet. (St.meld. nr. 15 (2008-2009), 2009, s. 10) Økt politisk globalisering har ført med seg ukonvensjonelle sikkerhetsutfordringer i det digitale rom som får «konsekvenser for global stabilitet, sikkerhet og utvikling.» (Meld. St. nr. 37. (2014-2015), 2015, s. 9) Dette fører til økende uforutsigbarhet mellom statene og et mer komplekst trusselbilde. (St.meld. nr.15 (2008-2009.), 2009, s. 11) Cyberdomenet utfordrer sikkerhetspolitikken til nasjonalstatene.

I denne oppgaven vil vi belyse ulike hendelser og angrep i cyberdomenet og sette de i lys av FN-pakten og dens bestemmelser. De hendelsene vi har valgt ut for å belyse problemstillingen bærer preg av å være angrep på en stats infrastruktur eller demokratiske prosesser. Hendelsene bærer i tillegg et preg av å ha blitt utført av en annen stat.
Det har skjedd ulike hendelser som, tjenestenektangrepene mot Estland i 2007, Cyberelementene under konflikten i Georgia 2008, Stuxnet-ormen som ble avslørt i 2010 og Presidentvalget i USA 2017. (Johnsen & Kveberg, 2013). Dette kan betraktes som hendelser som har åpnet øynene for cybermakt hos mange nasjonalstater. Samtidig som det er en stødig strøm med avsløringer av mer avanserte etterretningsoperasjoner som sannsynlig kun kan gjennomføres av stater. (E-tjenesten 2017) I de siste årene har ulike hendelser innen cyberkrigføring som bekrefter at dette er et domene i utvikling. (E-tjenesten 2017) Informasjon- og kommunikasjonsteknologien har i løpet av de siste 20 årene endret samfunnet. På den ene siden oppstår det nye utfordringer av

cyberkriminalitet, trusler mot personvernet og ivaretakelse av individuelle rettigheter. (Sabbagh et al. 2012)

1.1 Problemstilling

«Hvordan påvirker politisk globalisering og cyberkrigføring de tradisjonelle forbudene mot intervensjon og maktforbudet?»

Den teknologiske utviklingen har ført til ulike utfordringer innen internasjonale relasjoner. Med den økte globaliseringen blir grensene mer og mer visket ut og den teknologiske utviklingen har endret konseptet tid og rom. I de siste årene har det vært økt fokus på cyberangrep og trusselbildet har endret seg. Trusselen i det digitale rom øker. Etter hvert som samfunn har blitt mer avhengig av informasjonsteknologi, har de også blitt mer sårbare. Angrep i det digitale rom er i dag en av de raskest voksende truslene mot samfunnssikkerheten. (Meld. St. nr. 36. (2014-2015), 2015. s. 21) Det internasjonale samfunnet kan på mange måter sees på som et anarki uten en overordnet myndighet. Likevel har statene forhandlet frem ulike avtaler og reguleringer. FN er et eksempel på dette. FN-pakten er det grunnleggende dokumentet som FN er grunnlagt på. Paktens formål er å fremme internasjonal fred og sikkerhet. Reguleringene mellom stater kan vi blant annet finne i intervensjonsforbudet og maktforbudet som er kodifisert i pakten. Den teknologiske utviklingen og globaliseringen utgjør en utfordring ved at teknologien utvikler seg raskere enn avtaler og pakter kan formes. Reguleringene har vanskeligheter med å holde tritt med teknologien. Problemstillingen vår vil sette lys på de reguleringene som er satt med tanke på intervensjon og maktbruk mellom stater sett i lys av politisk globalisering og den teknologiske utviklingen. Ved å ta for oss denne problemstillingen mener vi at vi får en oversiktlig og et helhetlig bilde av utfordringene, samt fordelene og ulempene ved digitale internasjonale relasjoner og fordelene ved å utvikle en digital forsvarsstrategi i det internasjonale samfunnet.

1.2 Metodevalg

Undersøkelsesmetoden i denne oppgaven vil være en analyse av dokumenter. Vi baserer denne oppgaven på å analysere hvordan politisk globalisering og cyberkrigføring påvirker de tradisjonelle forbudene mot intervensjon og maktforbudet.

Dag Ingvar Jacobsen beskriver at hensikten med forskning er å frambringe gyldig og troverdig kunnskap om virkeligheten. Metode er som sagt en måte å gå fram på for å samle inn empiri, eller det vi kaller data. Det vil si at vi bruker metoden som et hjelpemiddel til å gi en beskrivelse av virkeligheten. (Jacobsen 2015, 15 & 21) Uansett hvilken empiri det dreier seg om, bør den alltid tilfredsstille to krav. For det første må empirien være valid, det vil si gyldig og relevant. For det andre må empirien være reliabel, det vil si pålitelig og troverdig. Med gyldig og relevant mener vi at empiren vi samler inn gir svar på problemstillingen vår. Etter som vi skal finne kilder til bruken av cyberkrigføring, hacking og cyberdomenet som trussel, er det viktig med relevante og gyldige kilder til oppgaven. Det som kan være problematisk er at oppgaven bygges på pågående situasjoner, derfor kan påliteligheten i artiklene variere, og det er viktig å se på de med kritisk blikk da feil eller ufullstendig informasjon kan forekomme.

1.2.1 Dokumentanalyse

Dokumentanalyse er en metode hvor setninger, forteller og ordene er nedtegnet av andre. «Forskere kan benytte seg av offentlige dokumenter, nettsider, blogger, årsrapporter for en bedrift, politiske selvbiografi, aviser og mye mer» (Jacobsen 2015, 170) Metoden vi benytter i denne oppgaven er dokumentanalyse av sekundærdata, det vil si data som andre har samlet inn. Dette innebærer at informasjonen ofte er samlet inn til et annet formål – en annen problemstilling enn den vi ønsker å belyse. Historieforskning må nesten alltid basere seg på denne typen data, i alle fall om vi studerer hendelser som har skjedd før eller som er pågående. Ut ifra denne beskrivelsen ser vi at det er en mengde utvalg av hva vi kan benytte oss av som kilde. Mye av dokumentasjonen vi analyserer i denne oppgaven kommer fra Forsvarets Forskningsinstitutt (FFI), Etterretningstjenesten (E-tjenesten), Stortinget og ulike nyhetskilder. De offentlige institusjonene tar utgangspunktet i norske interesser og forutsetninger. Eksemplene vi tar opp gjennom oppgaven berører ikke direkte Norge, men i lys av den økte globaliseringen ser vi at vurderingene gjort av norske

myndigheter kan anvendes i tilfeller som omfatter andre stater. Det ligger i oppgavens natur at det vil være vanskelig å samle inn primærdata for å besvare problemstillingen vår. Kildene befinner seg i posisjoner hvor det vil være veldig vanskelig å få tilgang til de. Men også alle andre samfunnsvitenskaper benytter seg av sekundærdata, slike data kan både være kvalitativ og kvantitativ. Men i denne metoden tar vi for oss kvalitative sekundærdata, der vi samler inn tekster og tar for oss eksisterende fortellinger og historier og forsøker å fortolke disse. (Jacobsen 2015, 170)

I lys av at vi analyserer FN pakten som er et juridisk dokument, kunne det vært naturlig å benyttet juridisk metode. Men bakteppet til problemstillingen i oppgaven er teorien om politisk globalisering, og i det juridiske aspektet i dokumentene vil det ikke være hensiktsmessig i forhold til å få svar på problemstillingen vår.

1.2.2 Kvalitativ analyse

Vår analyse av nettaviser, FN-pakten, artikler og rapporter vil være å fokusere på ordlyden og konteksten. Dette er sentralt ved dokumentanalyse. Det første spørsmålet vi må stille oss selv etter å ha samlet inn ulike kilder, er «hvordan vi skal trekke ut det fornuftige av informasjonsmengden?» Jacobsen nevner at vi må forsøke å redusere noe av kompleksiteten. Poenget med å redusere og strukturere er å få samlet inn det viktigste fra ulike perspektiver, nyanser og synspunkter. Etter å ha samlet inn all informasjon vi trengte for å belyse problemstillingen, satt vi med mye kunnskap som vi ville bruke, men samtidig ble informasjonen for omfattende. Etter å ha sett igjennom hva som gikk igjen av informasjon og hva som var nødvendig å ta med, klarte vi å strukturere dokumentene. Gjennom å sammenstille forskjellige dokumenter kan det påpekes spesielle avvik, mønstre, regulariteter og underliggende årsaker. Det er de sentrale detaljene som trekkes fram, de som kan gi ny innsikt i situasjonen eller et fenomen. (Jacobsen 2015, 197)

1.2.3 Styrker og svakheter ved dokumentanalyse

Offentlig versus private kilder

Jacobsen nevner et sentralt aspekt når vi skal vurdere en kildes pålitelighet. Det er å analysere hvilken mottaker informasjonen var rettet mot opprinnelig. Her gjøres det et skille mellom det vi kan kalle private og offentlige kilder. (Jacobsen 2015, 189)

FN- pakten, FFI- rapporter, Melding til Stortinget og FOKUS 2017 – rapporten, er rettet mot offentligheten og politiske myndigheter. Derfor fremstår disse med høy troverdighetsgrad. Dette er offentlige dokumenter som er i gjenstand for faglig debatt og høring.

Personlige versus institusjonelle kilder

I tillegg til å analysere hvem som mottar informasjonen, må vi også analysere hvem avsenderen av informasjonen er. Her går det et vanlig skille mellom personlig og institusjonelle kilder. (Jacobsen 2015, 190) Ved personlig kilde, er det ett enkeltmenneske som står som avsender. Fordelen med personlige kilder er at man ser klart hvem sine synspunkter som kommer frem. Ved institusjonelle kilder, står det en kollektiv enhet bak informasjonen. Det kan være organisasjoner, foreninger eller en gruppe mennesker. En av problemene med den institusjonelle, er at det er mer uklart. Det blir vanskeligere å se hvem sine synspunkter som kommer frem. FN-pakten og Melding til Stortinget kan man se på som institusjonelle kilder. Mens FFI- rapporten som er skrevet av to, er det mer personlige synspunkter, på den andre side står FFI bak rapporten og må regnes som institusjonell.

Vurdering av generell kvalitet ved kilden

Til slutt nevner Jacobsen (2015) at man må foreta en vurdering av hvilken kvalitet kilden har. Den er først og fremst knyttet til kunnskapen og kompetansen til den som har skrevet ned informasjonen, har. FN-pakten, Melding til Stortinget, FFI og Forsvaret har troverdige kilder. For å finne ut kvaliteten til kilden, kan man se på språket og informasjonen. Validiteten til en kilde er basert på avsender. Man må alltid være kritisk til kvaliteten, og man burde som regel ha flere kilder, som kan balansere hverandre. I oppgaven bruker vi også informasjon fra TV2 og New York Times. Språket til disse kildene er ofte tilpasset allmennheten. Dette er for at informasjonen skal være lettere å forstå. Nettaviser blir sett på som offentlige dokumenter som er for allmenheten, det er de som informerer om nyhetene rundt om i verden. Derfor kan man se på de som pålitelige kilder.

2.0 Hoveddel

Landegrensene viskes ut og trusselbildet blir mer og mer uoversiktlig. Økt globalisering fører til at cyberangrep kan utføres fra andre siden av kloden fra ukjente fiender. Dette krever en endring i fokus og prioritering i sikkerhetspolitikken. Siden sikkerhetsarkitekturen i det internasjonal samfunnet er basert på FN-pakten spiller denne en sentral rolle i interaksjonen mellom stater. (Meld. St. nr. 36. (2016-2017), 2017, s. 11) Stortingsmelding 15 (2008-2009) hevder at FN-systemet spiller en viktig rolle for å «ivareta en rettslig basert internasjonal orden.» Likevel belyser den også viktigheten av å erkjenne det økende gapet mellom «globale styringsutfordringer og FN-systemets kapasitet og evne til problemløsning.» (St.meld. nr. 15. (2008-2009), 2009, s. 11) I denne oppgaven vil vi se på ulike hendelser i det internasjonale samfunnet som har tatt plass i cyberdomenet og er av en problematisk natur. Center for Cyber and Information Security ved NTNU forklarer at de ulike «miljøene bruker ulik terminologi om det samme og samme terminologi om ulike ting.» Terminologien er blant annet informasjonssikkerhet, cybersikkerhet, datasikkerhet, IT-sikkerhet, IKT-sikkerhet, datasikkerhet og disse begrepene betyr ikke det samme. Men de brukes ofte om hverandre. (CCIS 2017) Vi velger å benytte cyberdomenet som en fellesnevner for all aktivitet knyttet til IKT-sikkerhet. I de eksemplene vi har valgt å se på er kriteriet at angrepet eller hackingen er utført mot infrastrukturen eller den demokratiske prosessen til en nasjonalstat og at det er indikasjoner på at det ble utført av en annen stat. Det er vanskelig å direkte attribuere et cyberangrep til en stat. Med attribusjon velger vi å benytte samme kvalifikasjoner som Forsvarets forskningsinstitutt. «Med attribusjon menes her å kunne fremstille ugjendrivelige bevis på at en spesifikk aktør står bak en handling.» (Johnsen & Kveberg, 2013). Denne problemstillingen er kjent problematikk i cyberdomenet. Utfordringene man står ovenfor i å bevise opprinnelsen for et cyberangrep er tekniske utfordringer som knytter seg til å spore seg frem til opprinnelsen for angrepet og andre utfordringer som å vite hvem som står bak eller har handlet på vegne av. (Johnsen & Kveberg, 2013) På grunn av problematikken rundt å bevise at en stat står bak de ulike angrepene lager vi en hypotese om at konfliktene i cyberdomenet er mellom to stater.

Som populært kalt «Web War 1» ble, ifølge Leif Hamnes for Teknisk ukeblad, Estland angrepet i cyberdomenet i 2007. Han forklarer at en «estisk/russisk krangel om rivningen av russiske krigsminnesmerker i Tallinn utløste et massivt tjenestenektangrep» som

resulterte i at nær all nettbasert informasjon i Estland stoppet opp. Parlamentet, departementene, sentrale banker, aviser og tv-kanaler ble rammet. (Hamnes 2012) Tallin-manualen, en analyse i problemstillingen om hvordan eksisterende folkerett kan benyttes i situasjoner i cyberdomenet, ble opprettet i etterkant men selv om det var klare indikasjoner på at Russland sto bak kunne det ikke bevises og det ble konkludert med at det ikke var brudd på maktforbudet. Konflikten mellom Georgia og Russland eskalerte til cyberdomenet i august 2008, og nasjonale medier og statlige nettsider ble utsatt for et massivt tjenestenektangrep fra Russland. Hamnes skriver at «det ble som vanlig ikke funnet noen offisielle, formelle bånd mellom angriperne og en konkret nasjonalstat.» I 2010 ble det avdekket at amerikanske myndigheter i en årrekke har utviklet en kraftig dataorm, populært kalt Stuxnet, som ifølge Hamnes var «viruset som gjorde dataangrep anerkjent som en høyst virkelig og fysisk krigføringsmetode.» (Hamnes 2012) Ormen ble sendt inn i et atomkraftverk i Iran og utløste eksplosjoner i uransentrifuger og fikk ødelagt 1000 av 6000 sentrifuger før det ble oppdaget. (Zero Days, 2016) NOU 2015:13 hevder at «analysen av Stuxnet-angrepet viser at tradisjonelle beskyttelsestiltak som holdningskampanjer, sikkerhetsoppdateringer og antivirusbeskyttelse har liten effekt på denne typen sofistikerte angrep.» (NOU 2015:13, 138-139) NRK-dokumentaren «Zero Days» intervjuer forskjellige kilder i amerikansk etterretning og disse hevder at Stuxnet-ormen ble utviklet av USA og Israel under dekknavnet Olympic games. Det har blitt spekulert om andre stater kan være involvert i det vi kaller cyberkrigføring. Etter at Stuxnet ble kjent i mediene, har nå statene fått opp øynene for den nye krigføringen, og flere stater har gjort store endring når det gjelder opprettelse av cyberavdeling, og bruk av flere ressurser til avdelingene innenfor militærbruk og selvforsvar. Dette er tilfeller som er preget av ødeleggelse av infrastruktur og angrep som kan skade befolkningen. Den siste saken vi har sett på derimot er Presidentvalget i USA i 2017. Demokratenes e-post server ble hacket og e-poster som førte til FBI-etterforsking av presidentkandidat Hillary Clinton ble lekket. Russland har ikke tatt på seg skylden men der finnes klare bevis for at det er russisk intervensjon.

> *Russland gjennomførte omfattande digitale operasjonar for å påverke valkampen i USA, og ein kan ikkje sjå bort frå at framande makter også kan forsøkje å påverke valet på ulike måtar her i Noreg og andre stader i Europa i 2017. (Generalløytnant Morten Haga Lunde, sjef Etterretningstjenesten. Fokus 2017, 6)*

Kanskje spesielt de siste årene har cyberkig og spionasje/hacking havnet høyt på agendaen i internasjonal politikk. (Johnsen & Kveberg, 2013) Historisk sett er arbeidet med informasjonssikkerheten en gammel tradisjon, nært forbundet med sikkerhetsbehov i krig og for opprettholdelse av sentralmakten. Historien om utviklingen og bruk av kryptering og steganografi (skjult skrift) illustrerer dette. Stadig mer informasjon blir lagret i komplekse informasjonssystemer og vi blir samtidig avhengige av flere digitale tjenester, noe som gjør at vår generasjon er mer sårbare enn før. Det blir mer og mer fokus på dataangrep (hacking), cybervåpen og datasikkerhet. Flere storstater har allerede erklært krig gjennom cyberdomene, som Russland og Kina (E-tjenesten 2017)

Globale sikkerhetsutfordringer er «større, grenseoverskridende fenomener som truer sikkerheten til individer, samfunn eller stater.» (Meld.St. nr. 37(2014-2015) 2015, s. 9) I forsvarets Fokus 2017 blir det trukket frem tre kategorier av digitale trusler; etterretning, sabotasje og påvirkning. Etterretning blir brukt til å hente ut og utnytte digital informasjon. Etterretningsoperasjonene er ofte rettet mot ulike mål av nasjonalstatlige interesser. Sabotasje omfatter skade, ødeleggінger og forstyrringer mot ulike mål som infrastruktur og ulike kommunikasjonssystem. Påvirkning innebærer manipulering av virkeligheten gjennom nyhetsmedium og sosiale medium. Formålet er å «diskreditere de statlige styresmaktene, forvirre innbyggerne og eventuelt demoralisere militært personell.» (E-tjenesten 2017) Sikkerhetsutfordringer i det digitale rom er ikke et nytt fenomen men den teknologiske utviklingen og økt globalisering har ført til at de har fått «mer alvorlige grenseoverskridende og globale konsekvenser.» (Meld.St. nr. 37. (2014-2015), 2015 s. 9) I følge Forsvarets forskningsinstitutt holder Norge fast ved at folkeretten er tilstrekkelig til å dekke også for hendelser og konflikter i cyberdomenet. FN-pakten slår fast at væpnet makt kan benyttes i selvforsvar, jf. artikkel 51, eller når Sikkerhetsrådet anser det som nødvendig for å bevare internasjonal fred og sikkerhet, jf. artikkel 42. Til tross for at hacking og cyberangrep har blitt utført i økt grad de siste årene har ikke folkeretten blitt benyttet i forbindelse med noen av de. (Johnsen & Kveberg, 2013) Etter angrepet på Estland i 2007 ble Tallinn-manualen opprettet. Tallinn-manualen er en utredning med formål å forstå hvordan eksisterende lover og normer for konflikt kan benyttes i saker der hendelser og konflikter oppstår i cyberdomenet og ble gitt ut av Cambridge University Press i 2013. Tjenestenektangrepene i Estland ble ikke ansett som et angrep i henhold til folkeretten. Spørsmålet vi vill stille oss da er hvorfor folkeretten ikke er benyttet i de ulike sakene vi tar for oss i denne oppgaven. Forsvarets forskningsinstitutt hevder at

cyberdomenet i langt større grad enn fysiske domener er folkerettslig uregulert, og at nasjonalstater ikke har monopol på cyberdomenets maktmidler. «Cyberdomenet fremstår som et domene *sui generis*, da det på noen områder hverken er under nasjonal eller global suverenitet» (Johnsen og Kveberg, 2013) Dette betyr at det er et helt nytt domene.
Det er vanskelig å ha klare grenser for statssuvereniteten i cyberdomenet, derfor kommer det eksisterende internasjonale lovverket til å bli utfordret. FFI hevder det ikke finnes en internasjonal konsensus for hvordan man kollektivt kan svare på denne utfordringen, og at «man kan si at det foregår en maktkamp i internasjonale fora mellom to relativt steile fronter.» (Johnsen og Kveberg, 2013) I melding til stortinget blir problemstillingen rundt effekten av digital krigføring belyst. Den forklarer at siden det kan oppnås stor effekt med relativt begrensede midler er digitale etterretningsoperasjoner og digital krigføring et satsingsområder for mange moderne forsvar. «Muligheten for å skjule eller tilsløre egen identitet gjør slike metoder attraktive også i fredstid.» Meldingen belyser også at innblanding i «demokratiske prosesser er et voksende problem.» (Meld.St. nr. 36, (2016-2017), 2017, s. 21)

> *Det digitale rom kjennetegnes av uoversiktlige strukturer og stor grad av privat flernasjonalt eierskap, noe som gjør det vanskelig for myndighetene å holde tritt med utviklingen og beskytte sårbar kritisk infrastruktur. (Meld.St. nr. 36, (2016-2017), 2017, s. 21)*

2.1 Politisk globalisering

Ordet «globalisering» er blitt et populært ord i senere tid. Manfred B. Steger forklarer at globalisering er blitt «the buzzword of our time.» (Steger 2013, 1) Steger tar for seg fire dimensjoner av globalisering: politisk, økonomisk, kulturell og økologisk. Denne oppgaven vil fokusere på den politiske dimensjonen av globalisering og utfordringer den økende globaliseringen fører med seg i det internasjonale sikkerhetspolitiske samfunnet. Den økte populariteten av ordet globalisering kan være et signal om at verden er i konstant endring. Det eksiterer et reelt behov for et generelt begrep for å beskrive de mangfoldige og mangesidige måtene verden i økende grad er sammenvevet på. Globalisering er et utrykk for økende grad av samhandling, integrasjon, påvirkning og gjensidig avhengighet mellom folk og stater innenfor områder som økonomi, samfunn, teknologi, kultur, politikk og økologi. Globaliseringsprosesser bidrar til å redusere betydningen av avstander og

statsgrenser. Enten vi ser på global kapitalisme, trender i forbruksvaner, transnasjonalmigrasjon og identitetspolitikk eller online-kommunikasjon, har globaliseringsprosessene i det sene 20. og tidlige 21. århundret en del fellestrekk. Thomas Hylland Eriksen nevner åtte nøkkelbegreper innenfor globalisering; frakobling, akselerasjon, standardisering, sammenveving, mobilitet, blanding, sårbarhet og tilbakekobling. Vi har valgt å fokusere å fokusere på frakopling og sårbarhet som er relevant for denne oppgaven.

2.1.1 Frakopling og sårbarhet ved den politiske globaliseringen

Det første nøkkelbegrepet vi tar for oss blir frakopling, en minimumsdefinisjon av globalisering kan kanskje avgrenses til at prosessene i samtiden bidrar til gjøre avstanden irrelevant. Globaliseringen innebærer at tid og sted blir irrelevant, relativt eller i det minste mindre viktig. Ideer, sanger, bøker, investeringskapital, arbeid, mote og cyberdomene reiser raskere enn noen gang enn noen gang tidligere og stedet der de befinner seg er mindre relevant enn det tidligere. Dette aspektet ved globalisering har teknologiske og økonomiske endringer som sin viktigste drivkraft, men har også kulturelle og politiske implikasjoner. (Eriksen 2015, 21) En stat trenger ikke å være fysisk tilstede om de vil påvirke andre stater. Cyberdomenet har gjort det mulig å bruke cyberangrep tvers av landegrenser, og her viskes tid og rom ut. Det som muligens kan være farlig med dette, er at man vet aldri når og hvor et angrep vil skje.

Videre tar vi for oss nøkkelbegrepet sårbarhet, som kommer av den negative siden ved cyberdomenet.

Eriksen skriver at innenfor globalisering, har vi ulike dimensjoner. Den politiske dimensjonen er rettet mot oppgaven og der kan vi se en klar helhet med det vi har skrevet om videre i oppgaven. Politisk globalisering viser til en intensivering og utvidelse av politiske forhold på tvers av kloden. Politisk globalisering handler om utenrikspolitikkens inntreden på nær sagt alle områder, eventuelt opphørt av skillet mellom innenriks og utenrikspolitikken. Prosessen reiser viktige problemstillinger rundt utfordringene hver suverene stat står ovenfor. Opphavet til den suverene staten kan spores til freden i Westphalen i 1648, fordi etableringen av selvstendige nasjonalstater tradisjonelt er knyttet til denne begivenheten som danner avslutningen på tredveårskrigen. På en ene siden bruker

politikerne mer av sin tid på deltakelse i internasjonale eller globale institusjoner hvor overnasjonale strategier og spilleregler diskuteres og samkjøres. På den andre siden finnes det i dag knapt et saksfelt hvor politikerne utelukkende kan forholde seg til et rent nasjonalt perspektiv. Politisk globalisering er prosessen der politiske interaksjoner intensiveres og ekspanderer globalt. Denne prosessen fører til en rekke problematikker rundt politiske spørsmål som handler om staters suverenitet, den økende innvirkningen av mellomstatlige organisasjoner og de fremtidige prospektene for regionalt og globalt styre. (Steger 2013, 60) I stortingsmelding 15 (2008-2009) står det at statene ikke er i ferd med å dø ut selv om globaliseringen i større grad hvisker ut grensene mellom ulike land. De sier at det heller ikke er slik at «nasjonale symboler, perspektiver og interesser, eller lokal tilhørighet, forsvinner.» Grunntrekkene til nasjonalstatene består fremdeles. Likevel står statene ovenfor et nytt og kompliserende sikkerhetsparadoks:

> *De samme globale sammenhengene og kreftene som i dag gjør samfunn rike, frie og trygge, åpner opp for nye risikoer og farer som både kan undergrave globaliseringen og skade de samfunnene som er vevd inn i globaliseringsprosessene, og samtidig redusere statsmaktens samlede styringskapasitet. (St.meld 15 (2008-2009) 2009, s. 23)*

To stater som har kanskje spesielt gode forutsetninger for cybermakt er USA og Russland. (Johnsen & Kveberg, 2013) De har spesialisert seg innenfor cyberangrep og investerer i cyberavdelingene, som de har opprettet muligens grunnet hacking og cyberangrepene som skjedd de siste årene og spesielt i 2016 og 2017. (Johnsen og Kveberg, 2013 & E-tjenesten 2017) Ved bruk av cyberdomene sitter man med mye makt. Makt er et viktig begrep for å forstå den politiske dimensjonen. Helt generelt kan man si at makt er en aktørs evne til å nå sine mål. Ved fokus på cyberdomene, så er det de som har økonomi og mulighet til å infiltrere seg inn i infrastruktur og databasene til andre stater via nett, som sitter med makten. Østerud forklarer at globalisering er en utfordring mot staten både som beslutningsarena og som ramme om politisk fellesskap. Globalisering kan beskrives som en prosess der betydningen av territorial avgrensing og nasjonalstatlig forankring viskes ut. (Østerud 2004, 109)

2.2 FN-pakten

FN-pakten ble i 2005 bekreftet av verdens statsledere. 50 år etter at FN ble opprettet i San Fransisco i 1945 bekreftet verdens statsledere troen på paktens prinsipper. FN-pakten er bygget på fred og sikkerhet, utvikling og menneskerettigheter. FN ble opprettet i kjølevannet av annen verdenskrig. Formålet var at de brutale ødeleggelsene og overgrepene aldri skulle kunne skje igjen. I paktens fortale heter det at pakten skal virke i «å redde kommende slektledd fra krigens svøpe som to ganger i vår livstid har brakt usigelig sorg over menneskeheten» og «å forene våre krefter for å opprettholde internasjonal fred og sikkerhet.» (FN-pakten)

2.2.1 Intervensjonsforbudet

For å opprettholde internasjonal fred og sikkerhet og opprettholde det internasjonale rettssystemets relevans, må de nye utfordringene også «integreres og løses innenfor systemet.» (Johnsen & Kveberg, 2013) En av de viktigste prinsippene i folkeretten er suverenitetsprinsippet. Suverenitetsprinsippet beror seg i utgangspunktet i at alle stater er suverene og selvstendige. Stater kan selv velge å la seg binde av traktater og avtaler, i tillegg til å være bundet av folkerettslig sedvane. Historisk sett har suverenitetsprinsippet i hovedsak blitt sett på som et forbud mot maktbruk mellom statene. Intervensjonsforbudet ble utledet direkte fra suverenitetsprinsippet og er forbudet mot å intervenere i andre staters anliggende. Forbudet ble utdypet i Generalforsamlingens resolusjon «Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations.» (Resolusjon 2625 1970) Denne resolusjonen fastslår at ingen stat har rett til å intervenere i andre staters interne eller eksterne forhold. Dette gjelder væpnet intervensjon så vel som enhver annen form for innblanding eller trusler mot en stats politiske, økonomiske eller kulturelle institusjoner. Intervensjonsforbudet har i lang tid vært omstridt. I 1986 trakk Den internasjonale domstolen (ICJ) opp en grense mellom det som anses som ulovlig intervensjon og forbudet mot bruk av makt i *Nicaragua-saken.* Saken fastslo at bevæpning og trening av opprørsgrupper i en annen stat ble ansett å stride mot maktforbudet, men finansiering av opprørsgrupper ble sett på som brudd på intervensjonsforbudet. (Ruud og Ulfstein 2014, 191) Som tidligere nevnt har folkeretten i

Det spekuleres hvorvidt Russland var involvert i hacking av USA-valget. Men det har i senere tid blitt gransket, og kommet frem at sjefen for Nasjonal sikkerhetsmyndighet (NSM), CIA og FBI at Russland har vært involvert og dermed er en stor trussel mot stater ved å intervenere seg. Christian Pretorius, leder for NSMs Cybersikkerhetsavdeling, og understreker ovenfor TV 2 at han baserer sine uttalelser på det som allerede har blitt kjent gjennom amerikanske medier. Det som er nytt ved denne hackingen er at aktørene alltid har skjult hva de har fått tak i. Det spekuleres i at poenget med hackingen var å svekke tilliten til valgsystemet. I fortrolige samtaler med amerikanske toppolitikere skal representanter for CIA og FBI ha gitt utrykk for at Russlands motiv ikke bare var å hjelpe Trump med å vinne valgkampen, men at de også ville svekke tilliten til det amerikanske valgsystemet. På den andre siden skal Trump ha gjentatte ganger avvist påstanden om russisk innblanding. (Perse, 2016) Det er viktig å analysere hendelsene som har skjedd og unngå at noe lignende skjer i fremtiden. Det burde bekymre de fleste stater, ettersom en storstat som USA har blitt angrepet. De fleste moderne stater forbereder bruk av digitale operasjoner som ett av flere virkemidler i mellomstatlige konflikter, dette inkluderer utvikling av skadevare som kan brukes til å sabotere infrastruktur eller å forstyrre kritiske samfunnsfunksjoner. (Meld. St. 37 (2014-2015), s. 28)

Skandalen som preget det amerikanske presidentvalget ved at demokratenes servere ble hacket og e-poster lekket til offentligheten, og følgende FBI etterforsking av presidentkandidat Hillary Clinton, var en påminnelse for det globale samfunnet om at selv de mest demokratiske prosesser kan vakle. Spekulasjonene om Kremls hånd i spillet skaper et stort problem sett fra intervensjonsforbudet i folkeretten. Det er uten tvil en innblanding i en annen stats politiske institusjon og demokratiske prosess. Hacking brukt på denne måten er en avansert form for intervensjon og er nesten umulig å sanksjonere mot. For stormaktstatene med et velutviklet cyberarsenal er dette en relativt trygg måte å styre demokratiske prosesser i andre stater på. I denne saken var motparten en annen stormakt, men i andre stater som er i startfasen av økt digitalisering uten det avanserte cyberforsvaret kan dette føre til stor sårbarhet og et sikkerhetspolitisk mareritt.

2.2.2 Maktforbudet

> *Intet i denne Pakt skal innskrenke den naturlige rett til individuelt eller kollektivt selvforsvar når et væpnet angrep er blitt foretatt mot et medlem av de Forente*

> *Nasjoner, inntil Sikkerhetsrådet har truffet de tiltak som er nødvendige for å opprettholde internasjonal fred og sikkerhet. (FN-pakten artikkel 51)*

FN-pakten artikkel 2 (4) sier at «alle medlemmer skal i sine internasjonale forhold avholde seg fra trusler om eller bruk av væpnet makt mot noen stats territoriale integritet eller politiske uavhengighet eller på noen annen måte som er i strid med de Forente Nasjoners formål.» Denne bestemmelsen handler om maktbruk mot andre stater. I Iran-saken sender USA et virus inn i systemet til et atomkraftverk i Iran og utløser eksplosjoner og får det til å se ut som menneskelig eller teknisk svikt. Dette kan sees gjennom FN-pakten som et brudd på forbudet mot maktbruk der USA angriper Irans infrastruktur. Alle stater har rett til å verne om sin egen suverenitet og FN-pakten artikkel 51 fastslår retten til selvforsvar. Dette er det eneste unntaket til artikkel 2 (4). Artikkel 51 fastslår at en stat har «rett til individuelt eller kollektivt selvforsvar når et væpnet angrep er blitt foretatt» men sier ingenting om hvordan dette kan skje. ICJ har i Caroline-saken vedtatt noen begrensninger i selvforsvarsretten. Det settes krav til umiddelbarhet, nødvendighet og proporsjonalitet. En utøvelse av selvforsvarsretten må følge som et direkte svar, det må begrenses til det nødvendige og forsvaret må stå i proporsjoner til angrepet (Ruud og Ulfstein 2014 , 200). Om vi fastslår at USA har utført et væpna angrep mot Iran, hvordan kan Iran svare på dette? Iran oppdaget at USA sto bak angrepet mange år i ettertid. Om begrensingen i selvforsvarsretten er umiddelbarhet, hvordan kan de forsvare seg mot et angrep som ingen vet hvor kommer fra og som senere viser seg å være en annen stat? Og om begrensingen også er proporsjonalitet, kan de sende raketter tilbake eller gjelder proporsjonalitet at man må svare med samme mynt? Her skal vi ikke gjette noe om Irans cybervåpenarsenal men få stater har et like godt cyberforsvar som USA. Utviklingen og mangel på klare reguleringer innen cyberkrigføring kan føre til en stor skjevhet i forsvarsevnen til mindre stater mot stormaktene innen teknologi som USA, Russland og Kina.

Når de folkerettslige ansvarsreglene i stor grad bygger på folkerettslig sedvanerett får vi et "problem" når det er snakk om hacking og cyberangrep. Når nye metoder blir brukt, er det vanskelig å lene seg på sedvane. Sedvane bygger seg opp gjennom tid og er ikke kodifisert. Et av problemene ved sedvaneretten man muligens står ovenfor i dag, kan være hacking og cyberangrep. Operasjon Olympic Games, eller Stuxnet som den blir kalt er dekknavnet til cyberoperasjonen som skapte overskrifter i media rundt angrepet på atomkraftverket til Iran. Olympic games representerte på mange måter startskuddet for et

internasjonalt kappløp der hacking og cyberangrep ikke bare brukes til etterretning og rekognosering, men også som ledd i offensiv angrep. Viruset har nå kommet ut på svartebørsen og det er fritt frem for alle å kjøpe den. Forsvarets forskningsinstitutt forklarer at det som i Norge blir definert som cyberkrigføring er i russiske og kinesiske øyne en del av en informasjonskrigføring. De sier videre at Russland har vedtatt å etablere en egen avdeling for cyberkrigføring og anser Internett som et mulig stridsdomene. «Dette signaliserer et klart skifte fra tidligere ordelag fra russisk side» (Johnsen og Kveberg, 2013) For å hacke et datasystem er det viktig å kjenne til sårbarheten til systemet. Forsvarets forskningsinstitutt skriver at «ukjente sårbarheter kalles ofte nulldagssårbarheter, eller zero-days.» Det har oppstått et marked for kjøp og salg av disse sårbarhetene og foreløpig er det nasjonalstater som har økonomi og vilje til å benytte seg av disse. (Johnsen og Kveberg, 2013) Østerud hevder at det er «mange overdrivelser i den politiske og populære debatten om globalisering.» Dette er overdrivelser om hvor langt utviklingen er kommet, og om hvor uavvendelig den er. (Østerud 2004, 14) Dette ble uttalt i 2004 og den teknologiske utviklingen gjør at det internasjonale sikkerhetsbilde blir stadig utviklet, og man kan kun spekulere i hvor langt ulike stormakter har kommet i utviklingen av cyberarsenal. Forsvarets forskningsinstitutt hevder at det er i norsk interesse at «cyber integreres i det internasjonale systemet og organisasjonene Norge ønsker skal styrkes i fremtiden, som for eksempel FN og Nato.» (Johnsen og Kveberg, 2013) I en melding til stortinget står det at respekt for felles spilleregler gir et godt og effektivt internasjonalt samarbeid og at folkeretten er den rettslige rammen for dette. (Meld. St. 36 (2016-2017), s. 39) Sakene vi har gått innom i denne oppgaven viser at stater kan oppnå stor skade med minimal risiko for å bli straffet av det internasjonale samfunnet. Som tidligere nevnt er det offisielle standpunktet til den norske regjeringen at folkeretten er tilstrekkelig til å være førende i saker der cyberangrep er benyttet. Ser vi på utviklingen derimot, der nasjonalstater kjøper og benytter sårbarheter i et uoversiktlig og uregulert marked. Folkeretten må «videreutvikles når samfunnsutviklingen skaper nye reguleringsbehov.» (Meld. St. 36, (2016-2017), s. 39) Historisk sett har krig funnet sted og blitt avgjort i det fysiske domenet, vanligvis mellom to parter. Påvirkning og villedning har i noen grad vært benyttet, men etter kampen på slagmarken har det stort sett vært klart hvem som har vunnet.

Opprustningskappløpet pågikk i flere tiår før ICJ behandlet lovligheten av bruk eller trusler om bruk av atomvåpen, men dommen gir ikke noen klar entydig konklusjon. Det er

ikke utarbeidet noen konvensjoner som forbyr bruken av atomvåpen. Med tanke på ødeleggelsene et atomvåpen kan gjøre kan det virke uforståelig at dette ikke er klart å utarbeide. Å sammenligne atomvåpen med cybervåpen kan kanskje virke som å strekke seg langt, men i et samfunn, som for eksempel Norge, der store deler av infrastrukturen er styrt av teknologi kan en fiendtlig stat skape stor harme og kaos ved å utføre digitale angrep.

3.0 Konklusjon

Spørsmålet om hvordan den politiske globaliseringen og cyberkrigføring påvirker de tradisjonelle forbudene mot intervensjon og maktforbudet er et komplisert spørsmål med mange ulike aktører. Spørsmålene vi har tatt opp i denne oppgaven skal sette lys på om FN-pakten er en rettskilde som kan benyttes for å beskytte suvereniteten til nasjonalstatene når utviklingen og bruken av cyberkrigføring og den politiske globaliseringen øker. Som tidligere nevnt slår norske myndigheter fast at globaliseringen fortsetter og virkningen på samfunnet er betydelig. Trusselbildet i internasjonal politikk er i stadig endring og sakene som har kommet opp de siste årene viser et bilde av ulike nasjonalstater som i stor grad utvikler og bruker cyberangrep. FN-paktens bestemmelser er ment til å kunne bli anvendt i alle tilfeller der brudd på intervensjonsforbudet eller maktforbudet er spørsmålet. Ordlyden i pakten skal kunne anvendes uansett hvilke metoder eller våpen som er brukt. Til tross for dette har vi sett mange saker de siste årene der statene intervenerer eller angriper en annen stat i cyberdomenet. Teknologien utvikler seg raskt og det kan være vanskelig for globale internasjonale organ som FN å holde følge. Dagens kriger finner sted i et uoversiktlig trusselbilde hvor påvirkning gjennom cyberdomenet spiller en stor nøkkelrolle. Hvilke konsekvenser får dette for verden i dag? På samme måte som luftfart endret verden på begynnelsen av 1900- tallet endrer informasjonsteknologi verden i dag. (Johnsen og Kveberg, 2013) Med endringen i sikkerhetsbildet burde rammen for den internasjonal fred og sikkerhet også endre seg.

4.0 Referanseliste:

Center for Cyber and Information Security. Forskningsinstitutt. Hentet fra: https://ccis.no/nb/informasjonssikkerhet-cybersikkerhet-datasikkerhet-hva-er-forskjellen/

Clausewitz, Carl von (1832) *On War*. Oversatt av Michael Howard & Peter Paret (1976). Princeton, New Jersey: Princeton University Press.

Etterretningstjenesten. (2017). *«FOKUS2017»* Hentet fra: https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus2017.pdf#page=16

Eriksen, T. H. (2008). *Globalisering: Åtte nøkkelbegreper*. Oslo, Universitetsforlaget. 2008

FN-pakten, 1945

FM-Sambandet. 2017. «FN-pakten, art. 2» http://www.fn.no/FN-informasjon/Avtaler/FN-pakten/FN-pakten (Lest: 11.03.2017)

FN-Sambandet. 2017. «FN-pakten, art. 51» http://www.fn.no/FN-informasjon/Avtaler/FN-pakten/FN-pakten (Lest: 11.03.2017)

Forsvaret. 06.02.2017 *«Digitale rom»* http://forsvaret.no/fakta/undersokelser-og-rapporter/fokus2017/digitale-rom (Lest: 20.03.2017)

Forsvarets forskningsinstitutt. 07.01.2015 *«Cyber- og informasjonssikkerhet»* http://www.ffi.no/no/Forskningen/Avdeling-Cyber-og-EK/Sider/IKT-sikkerhet.aspx (Lest: 01.03.2017)

Forsvarets forskningsinstitutt. 28.02.*2017 «Strategisk kommunikasjon og cyberforsvar»* http://www.ffi.no/no/Forskningen/Avdeling-Cyber-og-EK/Sider/Strict.aspx (Lest 01.03.2017)

Gibney, Alex ”Zero Days” Dokumentar. Av Nrk. https://www.nrk.no/ytring/trusselen-fra-cyberspace-1.13285105 (Sett: 28.02.2016)

Greg, Miller, Nakashima, Ellen & Tate. Julie. 2012, 19. *“U.S., Israel developed Flame computer virus ti slow Iranian nuclear efforts, officials say”* Av The Washigton Post, National Security-https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html?utm_term=.4302ce3331d2
(Lest: 01.03.2017)

Hamnes, Leif. 2012 *«Cyberangrep og datavirus- 16 spektakulære cyberangrep» Av Teknisk ukeblad.* https://www.tu.no/artikler/16-spektakulaere-cyberangrep/244245
(Lest: 17.05.2017)

Hovi & Malnes (red.) (2011). *Anarki, makt og normer, Innføring i internasjonal politikk.* Oslo: Abstrakt forlag AS 2011

Jacobsen, Dag Ingvar. (2015). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode, 3. utgave.* Oslo: Cappelen damm AS 2015.

Johnsen, Roger. 2013. *«Cyberkrigføring og Forsvarets operative evne».* Internasjonal politikk 71, (2): 241-251. (Lest: 02.03.2017)
https://www.idunn.no/ip/2013/02/cyberkrigfoering_og_forsvaretsoperative_evne

Johnsen, Siw Tynes *«Norway, NATO and cyber defense»* (FFI-rapport 14/01328)
Hentet fra: http://www.ffi.no/no/Rapporter/14-01328.pdf

Johnsen, Siw Tynes & Kveberg, Torbjørn *«Cyberdomenet, Cybermakt og norske interesser»* (FFI-rapport 13/02712)
Hentet fra: https://www.ffi.no/no/Rapporter/13- 02712.pdf

Lewis, James A. (2011) *Cyberwar Thresholds and Effects*. IEEE security and privacy, 9 (5): 23-29

Mingst, Karen A. og Arreguìn-Toft, Ivan M. (2014): *«Essentials of International Relations»*, 6. utgave, W. W. Norton & Company

NATO Cooperative Cyber Defence Center Of Excellence. Organization. Hentet fra: https://ccdcoe.org/tallinn-manual.html

Perse, Kjell. 2016 *«Cybersjef om russisk hacking av USA-valget: - Første gang vi har sett dette»*. Av Tv2, http://www.tv2.no/a/8802988 (Lest:15.03.2017)

Ruud, Morten & Ulfstein, Geir. (2014). *Innføring i folkerett, 4. utgave*. Oslo: Universitetsforlaget 2011.

Sabbag, Karim et al. (2012) *Maximizing the Impact of Digitization*. I soumitra Dutta & Benat Bilbao-Osorio (red.) *The Global Information Technology Report 2012*. Geneca: World Economic Forum

S.A. Miller. 2017, 11. «Trump bolsters cybersecurity effort, says he's keeping campaign promise to Americans». Av Washington Times, http://www.washingtontimes.com/news/2017/may/11/donald-trump-launches-cyber-security-effort/ (Lest: 17.05.2017)

Sandvik, Kristin Bergbora 2013. *«Cyberkrig og internasjonal rett»*. Internasjonal politikk 71, (2): 242-262 https://www.idunn.no/ip/2013/02/cyberkrig_og_internasjonal_rett (Lest: 02.03.2017)

Sanger, David E. 2012 *«Obama Order Sped Up Wave of Cyberattacks Against Iran»*. *Av The New York Times*, 01.06.2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (Lest: 01.03.2017)

Steger, Manfred B. (2013). *Globalization, A very short introduction.* United Kingdom: Oxford University press.

Szoldra, Paul. 2016, 07. *«A new film gives a frightening look at how the US used cyberwarfare to destroy nukes*». Av Business insider, http://www.businessinsider.com/zero-days-stuxnet-cyber-weapon-2016-7?r=US&IR=T&IR=T (Lest: 01.03.2017)

The White house, 2017.11.05. Goverment. Hentet fra: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

Østerud, Øyvind. (2004). *Globalisering og nasjonalstaten.* Oslo: Gyldendal Norsk Forlag AS 1999.