Bacheloroppgave

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

Rikke Simonsen Ellingsen

Begynnelsen på slutten av det unipolare øyeblikket?

Hvilken rolle har utviklingen av cyber som avskrekking på maktbalansen mellom USA og Kina?

Bacheloroppgave i Statsvitenskap
Veileder: Kristian Bernhof Ellinggard
Mai 2020

NTNU
Kunnskap for en bedre verden

Rikke Simonsen Ellingsen

Begynnelsen på slutten av det unipolare øyeblikket?

Hvilken rolle har utviklingen av cyber som avskrekking på maktbalansen mellom USA og Kina?

Bacheloroppgave i Statsvitenskap
Veileder: Kristian Bernhof Ellinggard
Mai 2020

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

NTNU
Kunnskap for en bedre verden

Sammendrag

Hensikten med denne oppgaven er å gi en innsikt i dynamikken mellom USA og Kina i utviklingen av fremmedelementet cyber som avskrekking. Dette blir gjort med dokumentanalyse som metode. Ved hjelp av teorien om strukturell realisme og mer tradisjonelle maktforståelser samt nyere forskning på cyberfenomenet, debatteres det om Kina er på tur å ta igjen USA, som etter den kalde krigen har blitt regnet som en global hegemon, og hvilken rolle cyber kan ha i denne utviklingen. Studien synes å konkludere med at cyber gir en økning i kinesiske maktressurser og kapabiliteter som ifølge strukturell realisme gjør at de tar på seg mer oppgaver på den internasjonale arena, men at en retning bipolar orden enda debatteres om og trenger å forskes mer på, samtidig som at det enda er for tidlig å si.

Innholdsfortegnelse

1.0 Introduksjon

Flere forskere hevder at USA, etter den kalde krigen, fungerer mer eller mindre som en hegemon og et internasjonalt politi på den globale arena, bl.a Waltz (2000, s. 30). Layne (2012, s. 203) hevder at denne perioden av unipolaritet er over, noe Waltz også predikerte. Kina blir sett på som en av de største utfordrerene til denne såkalte «amerikanske freden» også kalt Pax americana, da Kina i lang tid har hatt en formidabel utvikling, særlig i form av økonomi og teknologi (Knutsen 2016, s. 451). I kjølvannet av denne utviklingen har det i tillegg oppstått et fremmedelement, cyber. Hvilken rolle spiller dette fremmedelementet på maktbalansen mellom USA og Kina? I denne besvarelsen vil nettopp dette spørsmålet bli sett i lys av Waltz og strukturell realisme og mer tradisjonelle maktforståelser, som på den ene siden hevder at slike fremmedelement i liten grad har noe å si på hvordan stater forholder seg til hverandre (Waltz 2000, s. 5). Spørsmålet vil også bli sett i lys av nyere forskning, som på den andre siden blant annet sammenligner utviklingen av cyber nærmest som en ny kald krig, som for eksempel Hjortdal (2011) og Lindsay (2014/15).

En av motivasjonsfaktorerne for dette temaet er den proteksjonistiske utenrikspolitikken til president Donald Trump. USAs tendens til mulitlateral tilbaketrekking er et interessant element i spørsmålet om maktbalanse. Dette blir kommentert nærmere i oppgavens empiri. I tillegg ser man at Kina satser høyt på cyberteknologi (Hjortdal 2011, s. 5). I spørsmålet om cyber og maktbalanse hadde også stater som Russland og Japan fortjent sin plass, men for å avgrense og stå i stil med problemstillingens relevans, har jeg valgt å fokusere på USA og Kina. Det er ingen offisiell definisjon på cyber eller cyberspace, men dette er definisjonen det blir tatt utgangspunkt i for å forklare fenomenet. “Cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems” (Ottis og Lorents 2010, s. 268).

Jeg har valgt å strukturere besvarelsen på følgende måte: Helt først kommer en begrepsavklaring og et teoretisk rammeverk der teorien om strukturell realisme blir presentert og begrep som sikkerhetspolitikk, avskrekking og maktbalanse blir redegjort. Dette gjør det lettere å forstå oppgavens hoveddel. Deretter kommer et historisk bakteppe, som setter problemstillingen i kontekst, der man allerede ser en endring i dynamikken mellom USA og Kina som stormakter. I neste kapittel som er empiridelen av besvarelsen, blir den amerikanske

og kinesiske cyberstrategien sett nærmere på samt et eksempel på et historisk cyberangrep som har som rolle i denne besvarelsen å illustrere konsekvensene av et cyberangrep, Stuxnet-viruset, som kan sies å ha endret debatten rundt cyber og cyberkrigføring. Før diskusjonen vil valg av metode bli presentert, som er dokumentanalyse. Heretter kommer en diskusjon og konklusjon der man kan se at overvekten av argumenter viser at cyber i stor grad har supplert kinesiske kapabiliteter og dermed maktressurser. Som ifølge strukturell realisme ser ut til å øke oppgavene på internasjonalt nivå (Waltz 2000, s. 34). Litteraturgrunnlaget blir presentert i slutten av oppgaven.

2.0 Begrepsavklaring og teori

Først blir begrepet *sikkerhetspolitikk* presentert, dette fordi avskrekking er et sikkerhetspolitisk instrument og avskrekking blir presentert senere i kapittelet. Deretter blir teorien om *strukturell realisme* presentert, under samme delkapittel blir begrepene *makt, avskrekking og maktbalanse* redegjort for. Dette på grunn av at disse er sentrale begrep innenfor strukturell realisme. Tilslutt i kapittelet blir det sett nærmere på konseptet *cyberkrigføring,* som kan sees på som et «fremmedelement» hos de mer tradisjonelle teoriene.

2.1 Sikkerhetspolitikk

Sikkerhetspolitikk er et sentralt begrep som blir ofte brukt i oppgavens hoveddel, da det blir forkus på det sikkerhetspolitiske aspektet ved cyberteknologi og cyberkrig. I denne besvarelsen vil avskrekkings-delen av sikkerhetspolitiske instrumenter bli lagt stor vekt på. Ved å forstå dette begrepet vil vi være i stand til å få en bedre forståelse av hvorfor sikkerhetspolitikk er en kilde til avskrekking, og hva som gjør det til et viktig instrument spesielt med tanke på besvarelsens problemstilling. Jeg har først valgt følgende definisjon på sikkerhetspolitikk:

> [..]Å oppnå beskyttelse for eget land mot fysisk maktbruk og vold utenfra, praksis ofte væpnet, militær maktbruk. Slik maktbruk kan bli rettet mot eget land fra en annen stat eller fra en ikke-statlig organisasjon eller gruppe (Hovi og Malnes 2011, s. 102).

Dette er den tradisjonelle definisjonen til Hovi og Malnes (2011), en utvidet definisjon av begrepet blir også presentert, der de blant annet ser på om det skal gjelde maktbruk innenfra også, eller mer kollektivt anliggende, der de også tar med miljø, fiske, marked osv. Denne tradisjonelle definisjonen av sikkerhetspolitikk kan man tolke som at væpnet og militær maktbruk legitimeres, både mot stater og ikke-statlige aktører/organisasjoner, i beskyttelsen av

sitt eget. Dette er en definisjon som legger relativt mer vekt på makt i motsetning til annen kjent litteratur i Statsvitenskap, som for eksempel *Utenrikspolitikk og norsk krisehåndtering* (2014) av Gunnar Fermann (red). Fokuset på makt kan dermed i større grad gjøre definisjonen mer analytisk fruktbar med tanke på tema om avskrekking i denne besvarelsen, der militær makt og forsvar står sentralt i forhold til avskrekking som et sikkerhetspolitisk instrument. Man kan derimot se at definisjonen ikke tar for seg begrepet "cyber" på noen vis. De skriver "praksis ofte væpnet", som kan tolkes å gi rom for andre trusler. Sikkerhetspolitikk kan sees på som en underkategori for utenrikspolitikk.

2.2 Strukturell realisme

Strukturell realisme er en sentral teori når det kommer til maktbalanse og hvordan stater forholder seg til hverandre på den globale arena. I motsetning til klassisk realisme som mener at det er menneskets natur som skaper maktkamp (Jackson og Sørensen 2016, s. 62), mener strukturell realisme at det er arkitekturen i det internasjonale systemet som tvinger stater til å søke etter makt (Mearsheimer 2006, s. 72). I et anarkisk system der det ikke finnes en garanti for at man blir angrepet eller ikke, er det naturlig for stater å ville bli så mektig at de kan beskytte seg selv, og stormakter blir tvunget til å konkurrere mot hverandre hvis de skal overleve (Mearsheimer 2006, s. 72). Strukturell realisme ignorerer kulturelle forskjelligheter og regimetyper, strukturen i systemet legger samme føringer for makt for både demokratiske og ikke-demokratiske stater (Mearsheimer 2006, s. 72).

Strukturell realisme skiller mellom defensive og offensive realister, der førstnevnte mener systemet vil til slutt straffe dem hvis man får for mye makt og sistnevnte som tenker motsatt. At det er strategisk lurt å skaffe så mye makt som mulig, og hvis muligheten er der, oppnå hegemoni (Mearsheimer 2006, s. 72). De hevder også at makt er basert på materielle kapabiliteter og at maktbalansen er basert på ting som militære evner og atomvåpen. Stater har imidlertid også en mer usynlig makt, de samfunnsøkonomiske ingrediensene som må ligge til grunn for å bli en stor militærmakt. Krig er dermed ikke den eneste måten å skaffe makt på, man kan også gjøre det ved å øke størrelsen på befolkningen og deres andel av global velferd, noe som Kina har gjort de seneste årene (Mearsheimer 2006, s. 72). Waltz (2000, s. 34) sier at eksterne faktorer som gir nok press, kan ha en påvirkning på hvordan stater oppfører seg. Det skal nevnes at Mearsheimer tilhører den offensive biten av strukturell realisme, dette skiller han

fra Waltz. Makt, avskrekking og maktbalanse er sentrale begreper i strukturell realisme og vil videre bli presentert hver for seg.

2.2.1 Maktbegrepet

«Power depends upon context, and the rapid growth of cyber space is an important new context in world politics» (Nye, Jr. 2010, s. 1). Før begrepet maktbalanse blir redegjort, er det greit å få en bedre forståelse for hva som menes med *makt* i statsvitenskapen. I tillegg blir det gått gjennom hva som menes med hard og myk makt, da dette også er et vanlig skille av makt innen internasjonal politikk og utøvelse av utenrikspolitikk. Dette fordi selve maktbegrepet er omstridt og defineres på ulike måter hos ulike forskere. En av de mest kjente definisjonene av makt kommer fra den amerikanske statsviteren Robert A. Dahl. Hans formulering sier at A har makt over B i den grad han/hun kan få B til å gjøre noe han ellers ikke ville gjort (Grindheim 2010). Dette er en av de vanligste anvendte definisjonene i statsvitenskap.

Både Østerud (2014) og Hernes (1975) mener imidlertid at Dahls definisjon av makt er for snever. I boken *Makt og Avmakt* (1975) utvikler Hernes en egen definisjon av makt. «A har makt over B når A har kontroll over de ressursene som kreves for å avgjøre utfall som aktørene har interesse av» (Grindheim 2010). Hvis man anvender denne definisjonen, i motsetning til Dahls definisjon, kan man tolke det sånn at det åpner for flere typer maktbruk (overtalelse, trusler og lignende). Man ser at Hernes har en mer interesseorientert definisjon enn Dahl som tar utgangspunkt i at interessekonflikten er åpenbar (Grindheim 2010). Dermed man tenke seg til at Hernes definisjon av makt passer bedre med tanke på besvarelsens problemstilling.

Det er som nevnt vanlig å skille mellom *hard* og *myk* makt. Joseph S. Nye, Jr hevder at det er tre grunnleggende måter å oppnå makt på, og det er tvang, betaling og attraksjon. Her forklarer han de to første som hard makt og den siste som myk makt (Nye, Jr. 2009, s. 160). Med attraksjon kan man tenke seg til at stater kan sette en slags agenda for andre stater og fungerer mer som et «forbilde», enn ved hard makt der man enten benytter militær makt eller økonomiske sanksjoner for eksempel. For det om stater kan ha mer å tjene på ved å bruke myk makt ovenfor hard, så vil ikke myk makt alene stoppe personer som Osama bin Laden, antageligvis. Nye, Jr (2009, s. 163) foreslår dermed at man må kombinere de to typene av makt til noe han kaller *Smart power*. Cyber kan sees på som en arena som er åpen for både hard og myk makt, noe som blir nærmere diskutert senere i oppgaven.

2.2.2 Avskrekking

Cyber åpner for en ny arena der stater kan avskrekke hverandre. Når det kommer til avskrekking som et sikkerhetspolitisk instrument, eller som Hovi og Malnes kaller det: en metode i sikkerhetspolitikken, er målet med avskrekking i bunn og grunn å hindre uønsket atferd, *før* det har skjedd (Hovi og Malnes 2011, s. 116). For å ta et annet eksempel på begrepet kan man tenke på "enkle" kriminelle handlinger som for eksempel promillekjøring. En vet at hvis man blir tatt i å kjøre i fylla så blir man straffet med bot og kanskje også fengselsstraff. Dette gjør at de fleste vil unngå å sette seg selv i den situasjonene, det lønner seg ikke.

Major og Mölling (2016) har en annen formulering av begrepet avskrekking. De forklarer avskrekking som en strategi der militære trusler og militære midler blir brukt. "Opponents are deterred from attacking by the threat of forceful retaliation and demonstrated military readiness" (Major og Mölling 2016, s. 1). De har altså en mer spisset definisjon av avskrekking enn Hovi og Malnes (2011), ved at de bare fokuserer på militære virkemidler. Målet er å overbevise motstanderen om at kostnadene og konsekvensene av å gå til angrep trumfer fordelene. De tar også opp to typer avskrekking, avskrekking ved fornektelse (denial) og avskrekkring ved straff (punishment). Der førstnevnte handler om å eliminere motstanderens utsikter til å nå målet deres, og der sistnevnte metode handler om å ha en skremmende militær gjengjeldelse i tilfelle motstanderen skulle angripe (Major og Mölling 2016, s. 2). Det er altså en metode for å hindre krig, som hovedsaklig fungerer psykologisk. I tillegg nevner de sikkerhetsdilemmaet, som også er et kjent begrep i statsvitenskap. "This is the classical security dilemma: everyone attempts to produce more security for themselves, which paradoxically leads to less security for all" (Major og Mölling 2016, s. 2). Dette sikkerhetsdilemmaet er et av begrepene som blir sentral i videre analyse og diskusjon. Essensen av dette dilemmaet forklarer Mearsheimer (2006, s. 75) er at de fleste skritt en stormakt tar for å styrke sin egen sikkerhet, reduserer sikkerheten til andre stater.

I dette tilfellet vil fokuset på avskrekking være i form av å hindre uønsket atferd med tanke på militære angrep og aggresjon, der man også kan tolke dette som en del av cyberdomenet og ikke bare væpnet militær makt. Ut i fra det kan man se på formuleringen av avskrekkings begrepet fra Major og Mölling (2016) som passende i form av relevans til besvarelsen.

2.2.3 Maktbalanse

Som en del av et teoretisk rammeverk for denne besvarelsen vil det være gunstig med en grundigere forståelse av begrepet maktbalanse.Verden har alltid bestått av et statssystem med anarkisk struktur bestående formelt av uavhengige/suverene stater. Statene består av en politisk autoritet og en egen befolkning i et avgrenset territorium (Østerud 2014, s. 226). Fermann (2014, s. 31) forklarer anarki som samhandling som den uregulerte maktkampen i det globale rommet. De suverene statene er derimot, av naturlige årsaker, ikke helt like enheter. Statene varierer i både størrelse, indre struktur og betydning. Noe som gjør at statene plasserer seg på ulik skala når det kommer til verdenspolitikken. USA har naturligvis mer makt på den internasjonale arena enn for eksempel Norge og Liechtenstein (Østerud 2014, s. 226). Noe som fører til at USA kan føre en mer proaktiv utenrikspolitikk enn småstater som Norge. Eller som Thykidid formulerte det «Den sterke gjør som han makter, den svake lider det han må» (1972:406, sitert i Fermann 2014, .s 31).

Når man begynte å ta i bruk ordet «Supermakt» etter andre verdenskrig, ble det ikke bare definert som en forsvarsevne som kan avskjerme ethvert angrep, men i moderne tid, en gjenjeldelsesevne som kan *ødelegge* aggressoren (Østerud 2014, s. 226). Med moderne tid mener man spesielt den kjernefysiske terrorbalansen, som betraktelig endret dimensjonen av verdenspolitikken. Dette er basert på troverdighet og anerkjennelse på den internasjonale arena, makten behøver med andre ord ikke å være særlig demonstrert. Dette kjenner man igjen i teorien om avskrekking i forrige delkapittel.

Det som avgjør en stats posisjon i systemet, som blir betraktet som et hierarki, er den relative fordelingen av ressurser og den strategiske bruken av dem. Her tar man organisasjonsprinsippet som forutsetning, verden er anarkisk. Dermed får man internasjonal orden og stabilitet gjennom fordelingen av makt og kontroll samt samarbeid og gjensidig avhengighet (Østerud 2014, s. 227). Det er her uttrykket maktbalanse kommer fra. Statssystemene gjennom tidene har alltid hatt en form for maktbalanse, men denne balansen har naturligvis ikke beskyttet mot krig og ekspansjon. Maktbalanse kan være både bevisst og ubevisst (Østerud 2014, s. 228).

Et begrepet som henger sammen med maktbalanse er *polaritet.* Såkalte «poler» er et eksempel på et systemtrekk i en internasjonal struktur. Disse polene er balanserende stormakter/supermakter i et maktbalansesystem (Østerud 2014, s. 212). Det finnes andre

eksempler på systemtrekk, men i denne besvarelsen og i lys av problemstillingen, vil fokuset være på polaritet. Maktbalansen man først kjente til var en såkalt multipolar orden, som bestod av en flyt mellom fem europeiske stormakter. Deretter, under den kalde krigen, var maktbalansen bipolar, som består av to stabile maktpoler/blokker. I 1980-årene, da den såkalte østblokken gikk i oppløsning og Sovjetunionens oppløsning i 1991, var den bipolare ordenen over (Østerud 2014, s. 228). Etter dette er det USA som har hatt størst makt, og som fungerer som den dominerende aktør i utenrikspolitikken. Dette kommenteres nærmere i neste kapittel av besvarelsen.

2.3 Cyberkrigføring

Som President Barack Obama sa i Mai 2009 "It´s the great irony of our information age- the very technologies that empower us to create and to build also empower those who would disrupt and destroy" (som sitert i Stevens 2012, s. 148). Her refererer han til utviklingen av cyberteknologi. Cyberteknologi og cyberrommet har utviklet seg i en relativ kort periode som har skapt en ny plattform og slagmark for krigføring. Da dette har utviklet seg så fort samtidig som man er usikker på langtidseffekten, befinner besultningstakerne (i dette tilfellet politiske aktører) seg et steg bak cyberdomenet, der det som oftetst er lett å være etterpåklok (Stevens 2012, s. 148). En av de største bekymringene her er de potensielle konsekvensene dette kan ha for både kritisk infrastruktur og nasjonal sikkerhet. Hva som menes med kritisk infrastruktur er, ifølge en rapport fra Direktoratet for samfunnsikkerhet og beredskap, blant annet elektrisk kommunikasjon, transport, kraft og finans, bare for å nevne noen (Dsb 2012, s. 9). Dette er områder det er mulig å påvirke ved hjelp av cyberteknologi og hackerangrep, noe som gjør en moderne stat sårbar. Her kan man allerede få en idè om hvordan en cyberkrig kan utfolde seg. Et hackerangrep kan forstås, i lys av nasjonal sikkerhet, som "[..]adversial computer-mediated actions against critical information infrastructures (CII) and other ICT-networked national assets, including those of the military and security services" (Stevens 2012, s. 151).

Stevens (2012) skiller mellom to typer cyberkrigføring: «Information warfare» og «Knowledge warfare». Førstnevnte ser på informasjon som et våpen i seg selv, innenfor dette skiller han igjen mellom to typer «Information warfare». Der skiller han mellom «netwar» og «cyberwar» der førsnevnte utgjør en samfunnsidealistisk konflikt formidlet av nettbaserte ICTs (Information and communication technology), på et strategisk nivå. Sistnevnte som en operativ-taktisk form for informasjonskonflikt mellom organiserte stats militærer (Stevens 2012, s. 149).

Den andre typen cyberkrigføring kaller han «Knowledge warfare». Her vil begge parter forsøke å forme fiendens handlinger ved å manipulere strømmen av etteretning og informasjon (Stevens 2012, s. 150).

I lys av dette kan man se at cyberkrigføring kan foregå på en større og mindre skala. Der man i den ene enden finner økonomisk spionasje (informasjonshenting) for eksempel, og i den andre enden et angrep på kritisk infrastruktur som for eksempel transport og kraft. Der sistnevnte får store direkte konsekvenser for sivile. Mer konkrete eksempler på cyberkrigføring blir presentert i oppgavens empiridel.

3.0 Historisk bakteppe

Denne delen av besvarelsen består av et historisk bakteppe. Først blir det en redegjørelse av hva som menes med "Pax americana", dette er relevant da det gir en forklaring på det som kalles "det unipolare øyeblikket" som står svært sentralt i besvarelsen med tanke på maktbalanse. Andre punkt i denne delen tar for seg Kinas økonomiske utvikling, dette er relevant for oppgaven da Kina kan sees på som en stor utfordrer til det unipolare øyeblikket, og på grunn av Kinas fokus på cyberteknologi.

3.1 Pax Americana

En av motivasjonsfaktorene til denne bachelor besvarelsen er som nevnt den proteksjonistiske utenrikspolitikken, særlig i lys av nåværende presidentskap (2016-2020) med Donald Trump. Grunnen til at denne politikken er interessant, er fordi det kan sies å være «uvanlig» når det kommer til USAs posisjon på den internasjonale arena. Helt siden slutten på andre verdenskrig i 1945, har USA involvert seg betraktelig i politikken på andre siden av Atlanterhavet. Både i kampen for å hindre sovjetisk kommunisme og innflytelse under den kalde krigen, men også for å hindre terrorister i å få tilgang til masseødeleggelses våpen (Knutsen 2016, s. 434). Dette var også USAs mulighet for et globalt hegemoni.

USA brukte denne muligheten, og den internasjonale arena endret seg gradvis mot en orden der Amerikanske ideer og normer rådet. Disse ideene inkluderte liberale ideer som favoriserte et åpent marked, transnasjonale samarbeid og demokratiske verdier (Knutsen 2016, s. 435). Man kan se på det som en demokratisering av Vesten under amerikansk regi. Dette ble også godt tatt

imot blant Europeiske land. Det viste seg at jo flere stater som innførte demokrati, jo mindre konflikter/kriger oppstod. Dette sto i stil med Huntingtons «tredje demokratiske bølge» og Fukyamas «End of history» (Huntington 1991, s. 12). Oppsummert vil det si at man hadde gått inn i en demokratisk bølge på den internasjonale arena bestående for det meste av demokratier som i følge den demorkatiske freden ikke kriger mot hverandre. Dette har Fukyama kalt «End of history». "There is now no ideology with pretentions to univerisality that is in position to challenge liberal democracy, and no universal principle of legitimacy other than the sovereignty of the people" (Fukuyama, sitert i Knutsen 2016, s. 440). Dette er bagkrunnen for utrykket *Pax Americana,* også kalt «Den amerikanske freden» (Layne 2012, s. 203). Etter den kalde krigen fungerer USA som en global hegemon og som et nærmest fungerende «Internasjonalt politi», som opprettholder relativ fred og en stabil verdensorden.

3.2 Kinas utvikling

En annen motivasjonsfaktor for denne besvarelsen er Kinas formidable utvikling siden 80-tallet, da de åpnet opp for en ny økonomisk reform. De har skaffet seg hundrevis av milliarder på utenlands investering, og trillioner av dollar på private innenlands investeringer (Bijian 2005, s. 18). Kina har uvtiklet seg raskere enn noen andre stater, fra og med 2011 lå Kina på andreplass blant de største økonomieme i verden. Kina har en rikere økonomi enn alle de europeiske landene og Japan, til sammen (Knutsen 2016, s. 451). De har basert moderniseringsprosessen hovedsakling på innenrikse ressurser, og har hatt fokus på ideologiske og institusjonelle innovasjoner samt industriell omstilling. De har blant annet gjort om borgernes personlige innsparinger til investeringer, noe som har ført til at økonomien har økt så raskt (Bijian 2005, s. 20).

I 2017 hevder Bloomberg-spaltist Smith (2017) at Kina er *den* største økonomien i verden. I 2019 og i skrivende stund har derimot den økonomiske veksten til Kina minket, og blir sett på som den svakeste veksten på nærmere 30 år (Sin et.al. 2020). Kina har drastisk forbedret både velferd og militærmakt over de siste 20 årene sammenlignet med andre stater. USA har imidlertid et større forsvarsbudsjett enn Kina, der Kina ligger på andreplass (Knutsen 2016, s. 451). En rekke forskere og observatører mener at Kina dermed er den største trusselen til *Pax americana* og det unipolare øyeblikket. På grunn av veksten i produktivitet og militære kapabiliterer (Knutsen 2016, s. 451). Enkelte hevder til og med at dagens verdensorden ikke

kan kalles unipolar, da Kinas maktposisjon og kapabiliteter tilsier at ordenen heller kan kalles bipolar (Tunsjø 2018, s. 50). Dette blir videre diskutert senere i besvarelsen.

Når det kommer til Cyberdomenet har Kina i likhet med økonomisk vekst også hatt en drastisk utvikling i cyberteknologi. Kina er det landet som har den største veksten innen internett-økonomi og har en av de mest aktive cyber programmene (Lindsay 2014/15, s. 7). Konsekvensene av dette vil også bli nærmere diskutert senere i besvarelsen.

4.0 Empiri

Dette kapittelet tar for seg besvarelsen empiriske funn. Først blir kinesisk cyberstrategi presentert, etterfulgt av amerikansk cyberstrategi. Hvordan forholder statene seg til cybertrusselen og hva fokuserer de på når det kommer til cybersikkerhet? Til slutt blir Stuxnet-viruset fremlagt, dette for å illustrere konsekvensene av et cyberangrep. De empiriske funnene vil videre bli diskutert i besvarelsens analysedel.

4.1 Kinas Cyberstrategi

Utfordringen med cyber-sikkerhet er spesielt akutt i stater som Kina, som har et av verdens mest voksende internett-økonomi, og som har en av de mest aktive cyber operasjons programmene (Lindsay 2014/15, s. 7). Før man går nærmere inn på Kinas cyberstrategi kan det være gunstig å få en bedre forståelse av hva som menes med strategisk ledelse. Her blir en definisjon av Fermann (2014) brukt, sett i en storpolitisk sammenheng:

> [..]handler strategisk ledelse om statens evne til å mobilisere politiske, økonomiske, militære, etterretningsmessige og administrative ressurser på en slik måte at staten settes i stand til å kunne konkurrere om knappe goder og viktige posisjoner på den globale arenaen." (Fermann 2014, s. 51).

Man kan tolke denne definisjonen som en mer offensiv definisjon i motsetning til en bredere definisjon som også er presentert av Fermann (2014). Kinas cyberstrategi kan sees på som mer offensiv enn defensiv, noe som også blir videre diskutert, derfor passer denne definisjonen her. Siden Kina blir sett på som den største utfordreren til pax americana, er det ikke rart at mye av litteraturen til Kinas håndtering og strategi i cyberdomenet blir sett fra et amerikansk perspektiv. Det blir med andre ord ofte sammenlignet med USA, noe Lindsay (14/15) i en viss grad også gjør.

Hjortdal (2011, s. 1) ser imidlertid på Kinas cyberstrategi på en litt mer nøytral måte, men kommer ikke foruten å sammenligne med USA til en viss grad. Han forklarer at cyberrommet er og vil fortsette å være et svært viktig element i Kinas strategi for innflytelse på den interasjonale arena. En grunn til at Kina opprettholder en agressiv cyberstrategi er det faktum at Kina har mer å vinne på det, enn de fleste andre aktører. Kina har for eksempel mye å vinne når det kommer til militær makt og kapabiliteter samtidig som at de generelt ligger bak USA på det teknologiske plan. Dermed vil de ha stor nytte av å spionere og skaffe seg informasjon i disse sektorene, slik at det også kan bidra til et økonomisk overtak (Hjortdal 2011, s. 4).

Cyberrommet og cyberkapabiliteter er noe PLA (People`s liberation Army) satser på. Som på norsk betyr folkets frigjøringshær, altså en bevæpnet styrke, som er under det kommunistiske partiet i Kina (Hjortdal 2011, s. 5). Dette er et essensielt satsingsområde hvis Kina ønsker å utfordre USA som hegemon, samtidig som at de forsøker å avskrekke USA. Den strategiske ledelsen i Kinas militær ser på cyberkapabiliteter som en viktig asymmetrisk mulighet i avskrekkingen (Hjortdal 2011, s. 5). En overlegenhet av informasjon vil også kunne føre til en militær overlegenhet, ifølge PLA. «Whoever strikes first prevails» (Lindsay 2014/15, s. 31). Med dette mener PLA at de vitale målene for en slik teknologisk motstander som USA er informasjonssystemene. Dermed ved å angripe informasjonssystemene er det mulig å bremse eller lamme fiendens organisering, strategiske beslutningstaking og nasjonal økonomi (Lindsay 2014/15, s. 31). På denne måten kan man skape overlegenhet over et sterkere militære, så lenge man angriper informasjonssystemene tidlig i en konflikt.

PLA tildeles mye ressurser som skal brukes i utviklingen av cyberrommet, og disse forbedringene er synlige. De har etablert evner til informasjonskrigføring, med et spesielt fokus på cyberkrigføring som i deres doktrine kan brukes i fredstid. PLA tar til orde for bruk av cyberangrep som kan bremse og overraske fienden (Hjortland 2011, s. 6). Iasiello (2017, s. 1) beskriver Kinas cyberstrategi som en informasjonsstrategi. Sett i lys av Hjortdal og Lindsay kan det se ut som at dette er en passende beskrivelse. En annen ting Iasiello (2017) peker på er Kinas lokale satsing i cyberdomenet. Kritikere av Kinas utkast av en cybersikkerhets lov hevder at Kina forsøker å få kontroll på egne innbyggere sin internettaktivitet og informasjonen som flyter gjennom det, samtidig som de beskytter lokale bedrifter fra utenlandsk konkurranse. Et slags «Acting locally, thinking globally» perspektiv (Iasiello 2017, s. 1). De har altså integrert cybersikkerhet inn i alle aspekter ved nasjonal strategi.

Det byråkratiske hierarkiet i Kina har i sin natur mange små grupper bestående av innflytelsesrike embetsmenn som tar viktige politiske beslutninger, de dekker alt fra økonomi til propaganda. Denne prosessen er ikke særlig transparent. En direktør for et kinesisk politisk institutt hevder at disse små gruppene bestemmer heller enn regjeringsdepartementene selv i vitkige politiske saker (Iasiello 2017, s. 5). President Xi Jinping ga i 2014 gruppen "Central Internet Security and Informatization Leading Group" ansvaret for Kinas cybersikkerhet. Et av målene til gruppen, ifølge CCTV (et kinesisk overvåkningsselskap) er å ha kontroll over opinionen i Kina. Gruppen har et nært forhold til Kinas statsråd gjør at endringer kan skje raskt. Gruppen har full autoritet over all online aktivitet, både sosialt, kulturelt, militært og politisk (Iasiello 2017, s. 5).

Et eksempel på et cyberangrep fra Kina, som var til å skaffe informasjon var på Angela Merkel, den tyske rikskansleren. Hennes egen pc ble hacket og det ble kopiert sensitive data som ble sendt til Kina (Hjortdal 2011, s. 10). Dette viser hvor sofistikert cyberkapabilitetene til Kina er. De ble anklaget for å stjele industrielle hemmeligheter og være i stand til å påvirke og sabotere infrastruktur. En tysk etteretningsagent Walter Opfermann mente i etterkant av dette angrepet at det ikke bare kunne være en fare for Tyskland men for kritisk infrastruktur verden over (Hjortdal 2011, s. 5). Dette er bare et av mange eksempler på cyberangrep fra Kina.

Hvem står bak Kinas cyberkrigføring? På den offentlige siden er cyberkrigføringen PLAs genrelle stabs ansvar (Hjortdal 2011, s. 11). Det fjerde departementet «Electronic Countermeasures and Radar» og det tredje departementet «Signals Intelligence and Technical», som nesten kan sammenlignes med USAs «National Security Agency». Trening i cyberoperasjoner foregår på tvers av hele PLA, fra kommando til selskapssnivå. Cyber regnes som en kjernekompetanse for alle kampenheter (Hjortdal 2011, s. 11). PLA samarbeider også med private hackere, både formelle og uformelle samarbeid. PLA sponser derfor utvalgte universiteter i Kina til forskning av utvikling til informasjonskrig (Hjortdal 2011, s. 11).

4.2 USAs Cyberstrategi

Sett i lys av Kinas offensive cyberstrategi, baserer amerikansk cyberstrategi seg på å kunne forsvare og håndtere angrep. USA har en mer defensiv tilnærming til cyberrommet. Etter 2018 foregikk det en strategisk reorientering i amerikansk cyberstrategi. Strategien fokuserer på «Superiority through persistence» (Smeets 2020, s. 445). Med andre ord, å skape overtak ved

et utholdende cyberforsvar. Man skal kunne ta i mot alle type angrep. Smeets (2020, s. 445) deler cyberrommet inn i tre forskjellige fargesoner: Blue space (områder i cyberrommet kontrollert av USA), Red space (områder i cyberrommet kontrollert av motparten) og Grey space (alle beskrivlser/områder som ikke passer i kategorien blue eller red space). Det må også nevnes at ulike aktører kan ha forskjellige definisjoner når det kommer til kontroll i cyberrommet.

En viktig del av amerikansk cyberstrategi er at de sikter etter globale avtaler for å skape et bærekraftig nettverk. De vil samarbeide med andre liksesinnede aktører som gjør at cyber*forsvar* blir lettere enn cyber*angrep* (Healey 2016, s. 16). Dette gjelder også ikke-statlige aktører. En grunn til dette er at det hjelper aktører med lite cyberkapabiliteter med å forsvare seg mot aggressorer. Ansvaret for håndtering av cyberrommet i USA ligger hos «US Cyber Command» og forsvarsdepartemantet (Smeets 2020, s. 446). USA har lenge hatt en observatørrolle når det kommer til cyberaktivitet utenfor sitt eget såkalte «blue space», der de skaffer informasjon fra motparters aktivitet (Smeets 2020, s. 446). Disse etatene har imidlertid endret strategi, noe som endrer militærets oppførsel i cyberrommet. Cyber command ønsker å være mer aktiv i cyberrommet, det vil si å forstyrre, benekte eller ødelegge «red» og «grey space» (Smeets 2020, s. 446). Et eksempel på dette er at US cyber command fjerner IS (Islamsk Stat) propaganda fra en server i Tyskland. Dette gjør de selv om Tyskland ikke har godkjent dette for fullt, noe som har ført til frustrasjon (Smeets 2020, s. 446).

Et annet kjennetegn for amerikansk cyberstrategi er at det ikke finnes en egen klar strategi, noe som gjør det vanskelig å balansere konkurrerende prioriteter (Healey 2016, s 16). Wilner (2020, s. 256) hevder imidlertid at selv om en full strategi ikke er klar, så eksisterer det deler og biter av en strategi spredt utover forskjellige departement. I samsvar med president Donald Trumps generelle tretthet av mulitilateralisme (samarbeid mellom flere stater), og FN generelt så kan det se ut til at USA mest sannsynlig trekker seg mer tilbake når det kommer til å skape globale cyber normer. USA vil heller få frem sine egne røde linjer og skape bilaterale (avtale mellom to stater) avtaler som gagner amerikanske interesser i større grad (Wilner 2020, s. 268).

Healey (2016) presenterer noen punkt som kjennetegner amerikansk politikkutforming i cyberdomenet, som man også kan tolke som noe kritisk. Først og fremst trekker Healey frem at det som sagt ikke er en klar strategi. Han snakker også om en pågående militarisering av cyberpolitikk, der Forsvarsdepartementet har hovedrollen, og ikke byråer som har fokus på

innovasjon og økonomi slik som Handelsdepartementet (Healey 2016, s. 16). Politikkutformingen blir også kritisert for å misforstå dynamikken i en cyber konflikt, som fører til en overvekt av den taktiske og tekniske biten istedenfor den mer strategiske og langsiktige understrømmene. De har også et mer kortsiktig syn på når det kommer til nasjonal sikkerhet (Healey 2016, s. 16). USA har også fått kritikk på ha for stor tro på offentlig sektor når det kommer til cyber og problemene det medfører. Det blir også gitt kritikk på at USA er uforberedt på det offensive cyberrommet og at det kan utvikle seg til å bli en større trussel enn det det er i dag. Som igjen gjør at de er uforberedt på plutselige «cyber-sjokk» (Healey 2016, s. 16).

Hvis USA og den strategiske ledelsen skal håndtere disse punktene, må strategien basere seg rundt tre hovedpunkt: fremme velstand, være symbolsk for Amerika og deres verdier og gi nye verktøy for å følge tradisjonell nasjonal sikkerhet (Healey 2016, s. 17). Det andre punktet handler blant annet om at USA kan bruke denne muligheten til myk makt. Dette skal føre til en såkalt ikke-statlig sentrisk cyberstrategi.

4.3 Stuxnet-viruset

Før analysedelen i denne besvarelsen vil det være gunstig å ta for seg et kjent eksempel på et cyberangrep som i realiteten har blitt utført. Dette for å få et nærmere innblikk i cyberkrigføringens slagmark og for å sette angrepets konsekvenser i perspektiv. Som eksempel på et cyberangrep blir «Stuxnet-viruset» brukt. Som også har blitt kalt «Stuxnet-ormen». Førstnevnte blir brukt i denne besvarelsen. I cyberlitteraturen er det vanlig å se på cybertrussel *før* og *etter* Stuxnet-viruset, noe som gir en indikator på at cyberangrepet var historisk omfattende.

I 2009 oppdaget sikkerhetsanalytikere verden over et virus som hadde angrepet og mest sannsynlig gjort ødeleggelser på det Iranske atomvåpen anlegget. Angrepet var sannsynligvis gjort gjennom anleggets industrielle kontrollsystem, noe Iran senere bekreftet (Porche, Sollinger og McKay 2011, s. 1). Denne typen virus og angrep er ikke den første av sitt slag, men skilte seg ut fra tidligere angrep i form av kapabilitet, og ikke minst, sysselsetting. Noe som har gjort dette cyberangrepet til et av de mest kjente cyberangrepene gjennom tidene, og som muligens har endret etablerte normer i cyberdomenet (Porche, et.al 2011, s. 1).

Å lage og gjennomføre Stuxnet-angrepet har måttet kreve store ressurser, kompetanse og informasjon. Det er derfor umulig at én genial hacker har gjort dette alene. Ressursene som har blitt anvendt kan antyde et tilfelle av spionasje, som kan implisere til etteretningsbyråer (Porche, et.al 2011, s. 6). Forskere antyder også at det må ha vært mange personer med eksepsjonelle ferdigheter involvert og at det har tatt månedsvis å utvikle dette sofistikerte viruset, både ingeniører og programmerere (Porche, et.al 2011, s. 7). Stuxnet, ifølge det som har blitt rapportert, var et selvreplikerende malware (skadelig programvare) som setter seg inn i Siemens software som deretter har evnen til å kontrollere hardware (de industrielle kontrollsystemene) (Porche, et. al 2011, s. 7).

Stuxnet-viruset var til og med programmert til å avlede ved å skjule aktiviteter gjennom falsk informasjon til skjermene som overvåket systemet. Dette er bare ett eksempel på hvor elegant og sofistikert angrepet er, og det hevdes også at viruset fortsatt plager iranske regjeringers operasjoner (per 2011) (Porche, et.al.2011, s. 8). Porche, Sollinger og McKay presenterer minst fire grunner til at dette Stuxnet-viruset er bekymringsfullt. (1), For det første så avslutter dette angrepet debatten om at et slikt virus er mulig, det er reelt og kan gjøre fysisk skade. (2), For det andre viser den sofistiskerte naturen og ressursene som krevdes for å skape dette viruset, at dette må ha vært statsstøttet. (3), Den tredje grunnen er at andre kontrollsystemer enn kjernekraftverk lett kan angripes, som kan skape langvarige skader og konsekvenser (F.eks. elektrisitet, jernbane, vann og avløp osv.). Med andre ord, Stuxnet hendelsen bekreftet at disse systemene er sårbare. (4), Den fjerde og siste grunnen er utfordringen med å koordinere defensive aktiviteter da både privat og offentlig sektor er innblandet i dette fenomenet. Dette gjør at forsvaret av cyberangrep blir alles problem (Porche, et.al 2011, s. 8).

I ettertid har det blitt kjent at det var USA og Israel som stod bak Stuxnet-viruset, under hemmelig ordre fra President Barack Obama, som ville bremse iransk fremgang i å lage en atombombe uten å sette i gang et tradisjonelt militærangrep. Totalt ødela angrepet nesten 1000 av irans 6000 sentrifuger som beriker uranium, noe som er et viktig steg i prosessen med å lage en atombombe (Nakashima og Warrick 2012). Ut ifra litteraturgrunnlaget har USA og Israel formelt ikke tatt på seg ansvaret for angrepet, men i denne oppgaven blir det tatt i betraktning av de stod bak.

> "The idea was to string it out as long as possible," said one participant in the operation. "If you had wholesale destruction right away, then they generally can figure out what happened, and it doesn't look like incompetence." (Nakashima og Warrick 2012).

Med dette som bakgrunn kan man også tenke seg til at det som har blitt gjort én gang, kan også bli gjort igjen. Med andre ord kan virus som Stuxnet også true viktige industrier og infrastruktur i USA, og selvføgelig mindre aktører.

5.0 Metode

I dette kapittelet blir forskningsmetoden som blir brukt i denne besvarelsen tatt for seg, det blir også satt noen kritiske blikk ved metoden. Da problemstillingen var bestemt, ble en kvalitativ forskningsmetode på denne oppgaven mer naturlig enn en kvantitativ forskningsmetode. Innenfor kvalitativ forskningsmetode ble dokumentstudier, også kalt dokumentanalyser best egnet til besvarelsens problemstilling. "Document analysis is a systematic procedure for reviewing or evaluating documents—both printed and electronic (computer-based and Internet-transmitted) material" (Bowen 2009, s. 27). Theis (2002, s. 352) kaller den samme metoden for en «kvalitativ historisk analyse», og forklarer det som en metode der man tar i bruk primære historiske dokumenter eller historikernes tolkninger derav til tjeneste for teoriutvikling og testing.

I denne besvarelsen er kildene hovedsakelig hentet fra forskningsdokumenter (artikler, rapporter, bøker osv). I havet av informasjon og dokumenter som finnes på internett er det viktig å være kritisk til kildene man velger å bruke. Dokumentene er derfor hovedsaklig fagfellevurdert, noe som styrker reliabiliteten til forskningen. Når det kommer til litteratur om cyberstrategier og cyberkapabiliteter er dette et tema som stater ikke diskuterer åpent, da det sjeldent er en fordel for en stat å meddele at man spionerer på en annen stat som får nettverket deres til å skru av (Hjortdal 2011, s. 4). Dette har også vært en av utfordringene til besvarelsen på denne problemstillingen, og har gjort at man må sette kritiske blikk ved litteraturgrunnlaget.

En tendens i kapittelet om kinesisk cyberstrategi er at mye av litteraturen er sett i et amerikansk perspektiv samt skrevet av amerikanere. Selv om det finnes en del kilder på samme tema, er mye av argumentene og innholdet likt. Til tross for dette ble anerkjente forskere og forfattere i litteraturen om internasjonal politikk og statsvitenskap forsøkt å være overlegen i denne besvarelsen. Som F.eks. Fermann (2014), Østerud (2014) og Waltz (2000). Dette er en del av en selekteringsprosess, som også er en utfordring med dokumentanalyse som metode. En fordel

med metoden er at man kan finne så mange ulike kilder at det blir lettere å unngå partiskhet (Bowen 2009, s. 28). Samtidig må man også ta egen forskersubjektivitet i betraktning, særlig ved dokumentanalyse. Som er forskerens personlige påvirkning på forskningen (Tjora 2017, s. 258).

6.0 Diskusjon

I denne delen av oppgaven blir empirien sett i lys av teori og begreper. Diskusjonen vil ta for seg den strukturelle realismen i stor grad, og sette det opp mot nyere forskning på cyber og avskrekkings effekten det kan føre med seg. Hvordan kan man forvente at utviklingen av Kina skal utarte seg i et cyberstrategisk perspektiv?

Historisk sett har konflikter mellom øst og vest endt i tragedie, men etterhvert som atomvåpen kom på banen har eierne endret oppførsel og blitt mer forsiktige, slik at kriser ikke kommer ut av kontroll (Waltz 2000, s. 36). Er det grunn til å tro at eierne blir like forsiktige når det kommer til cyber kapabiliteter? Hvis man sammenligner cyber med atomvåpen vil det med første øyekast være naturlig å se på atomvåpen som en mye større trussel. Men, hvis man ser på konsekvensene ved et cyberangrep som Stuxnet, der man kan gjøre fysiske skader mer eller mindre uoppdaget og den potensielle påvirkningen hos staters kritiske infrastruktur i betraktning, så kan man se at gapet mellom atomvåpen og cyberangrep minskes betraktelig. Mye av det empiriske grunnlaget på cyber sammenligner cyber med atomvåpen. Dermed er det grunn til å tro at cyber også kan ha en balanserende effekt mellom USA og Kina. I tillegg til dette kan cyber i mye større grad brukes til myk makt, noe som er et av de tre hovedpunktene til Healey (2016, s. 17) når det er snakk om amerikansk cyberstrategi. At det skal være symbolsk for Amerika og deres verdier. Man ser også en tendens til at myk makt har blitt mer fremtredende med årene.

Når det er sagt, har USA en lang historie med å gripe inn i svake stater, ofte med hensikt å bringe demokrati til dem (Waltz 2000, s. 29). Noe som også gjenspeiler seg i USAs cyberstrategi. I et svar på en av president Clintons taler om amerikansk cyberstrategi, uttalte det kinesiske statlig eide *Global Times,* at amerikansk strategi inneholder aggressiv retorikk mot stater som ikke følger deres verdier (Stevens 2012, s. 160). Dermed kan man se at Kina ser på USA og liberale verdier som en trussel. I følge Waltz (2000, s. 11) og strukturell realisme fremmer demokratier krig fordi de bestemmer at måten å bevare fred på er å beseire ikke-

demokratiske stater og gjøre dem demokratiske. Hva om Kina delte samme verdier som USA? Ville det vært en like stor utfordrer som det er idag? Ikke ifølge Mearsheimer (2006, s. 72) og strukturell realisme. Dette fordi verdenssystemet skaper føringer for å oppnå makt på tvers av kulturer og regimetyper. Det samme gjør ubalansert makt, som lar svakere stater føle seg urolige og gir dem grunn til å styrke sine posisjoner (Waltz 2000, s. 29).

I så fall kan det virke som Kina bruker dette fremmedelementet, cyber, for alt det er verdt. Cyber har jo som nevnt skapt en ny dimensjon krigføring. Ifølge Iasiello (2017, s. 3) har Kina ett mål med kinesisk cyberstrategi, at det kinesiske kommunist-partiet skal ha makten. Dette kan også sammenlignes med den offensive delen av strukturell realisme. I lys av strukturell realisme så har stormakter en tendens til å ta på seg mer oppgaver på internasjonalt nivå jo mer ressurser de har (Waltz 2000, s. 34). Nå er USA den dominerende aktøren på den internasjonale arena, men man har som nevnt sett en tendens til en mer proteksjonistisk politikk fra USA sin side. Kan man da forvente at Kina tar mer og mer plass? Samtidig kan man ikke sammenligne en proteksjonistisk politikk med tap av makt. Lindsay (2014/15, s. 9) hevder at en krig mellom USA og Kina er høyst usannsynlig, og ifølge strukturell realisme samt historisk sett vil nye ordener etablere seg når riket har falt, med andre ord i slutten av en krig. Slik som skjedde etter den kalde krigen og det ble mer eller mindre en unipolar orden. I så fall ville en dreining i retning bipolar orden skje på et mer fredfullt vis enn tidligere, der makten er mer ressurs og innflytelsebasert.

Cyberangrep som trussel og cyber som statlig spionasje (knowledge warfare) er noe som foregår på hverdagslig basis, og det kan gå lang tid før det blir oppdaget samtidig som at det er mye som ikke blir oppdaget i det hele tatt. Her ligger et stort skille hvis man skal sammenligne cyber og atomvåpen som eksterne faktorer. Statlig spionasje er noe som har forekommet lenge før avansert cyberteknologi, men det blir enklere å gjennomføre samtidig som at man slipper å sette egne spioner/mennesker i like stor fare. Hvis cyberangrep skjer så og si hele tiden, kan man da forvente at det bryter ut en krig eller en krise? Ifølge Lindsay (2014/15, s. 37) er en misoppfatning av offensiv cyberdominans i tillegg til lite transparens når det kommer til cyberkapabiliteter på begge sider, en oppskrift på ustabilitet mellom USA og Kina. Dermed er det selvfølgelig rom for at slike dagligdagse cyberangrep oppdages og misforstås for en større trussel. Det har et opptrappingspotensial. Som for eksempel når USA opererte fra en server i Tyskland, uten Tysklands fulle samtykke og dette førte til frustrasjon (Smeets 2020, s. 446).

Som nevnt ser Kina på cyberkapabiliteter som en vikitig asymmetrisk mulighet i avskrekkingen (Hjortdal 2011, s. 5). Hvis Kina skal ta igjen USA militært og fører en såkalt informasjonskrig med USA, vil de ikke da bruke de militære «hemmelighetene» til USA og anvende de selv? Hvis Kina skal bli like avansert som USA når det kommer til militæret og avhengigheten til elektroniske systemer, vil jo dette undergrave asymmetrien som først og fremst skulle være en fordel (Lindsay 2014/15, s. 35). Etter Stuxnet-viruset som USA og Israel antageligvis stod bak har USA demonstrert deres evner i cyberspace og villigheten til å operere med cyber i en krigføring (Lindsay 2014/15, s. 35). Dette er en såkalt «deterrence by punishment» strategi fra USA sin side, de har demonstrert hva de er kapable til. Dette må Kina ta i betrakning om de skal planlegge en cyberkrig med USA. Hvis cyberkrigføring er så effektivt som Kina tror, men undervurderer kostnadene, er dette en stor ulempe for PLA. Asymmetrien av cyberkrigføring som egentlig blir sett på som en fordel for den svakere makten, fungerer egentlig motsatt hevder Lindsay (2014/15, s. 35) og gir den sterkeste makten med det mest erfarne forsvaret fordelen.

Når det er sagt, har man sett et skifte i den amerikanske cyberstrategien. Fra et fokus på «deterrence by denial» under president Bush, til en «punishment» basert strategi under president Obama og Trump (Wilner 2017, s. 270). Kina har en mer offensiv cyberstrategi og en mer offensiv strategi generelt hvis man skal se det i et strukturelt realistisk perspektiv. Nå som USA ser ut til å skjerpe cyberstrategien til en mer aktiv strategi, kan det være en mulighet for at Kina undervurderer kostnadene. Kina ser ut til å ikke diskutere konsekvensene i like stor grad som USA (Lindsay 2014/15, s. 36). Når det kommer til den politiske dimensjonen, gjenspeiler cyberstrategiene forholdet mellom USA og Kina, en dypt økonomisk avhengighet, men mistillit og rivalisering på den sikkerhetspolitiske arena. Internett har beriket både USA og Kina, men friksjonen i cyberrommet er en pris å betale (Lindsay 2014/15, s. 45).

Ifølge strukturell realisme så kan eksterne forhold forme hvordan stater forholder seg til hverandre, så lenge presset er stort nok (Waltz 2000, s. 34). Utviklingen av cyber som avskrekking kan man se på som et stort eksternt press, ikke minst med tanke på usikkerheten rundt cyberrommet. Spørsmålet blir jo hva dette fører til? Dette spørsmålet forblir ubesvart inntil videre, men man kan se på tendenser og sette det opp mot teorier. Lindsay (2014/15, s. 46) hevder at mønstrene i USA og Kinas cyber aktiviteter er i overenssetemmelse med logikken fra den kalde krigen stabilitets paradokset, men i en litt annen form. Cyberrommet åpner for mer utradisjonelle sikkerhetsdilemmaer, som for eksempel diskriminering av menneskerettigheter. Noe stormakter vanligvis ignorerer og heller fokuserer på å beskytte

økonomi og militære midler (Lindsay 2014/15, s. 47). En full skala cyberkrig mellom USA og Kina er som nevnt høyst usannsynlig inntil videre, men det har et opptrappings potensial som kan gjøre at man kommer nærmere og nærmere en krise. Med krise tenker man i hovedsak på angrep på kritisk infrastruktur. Dette fremmedelementet er en klar utfordring til den strategiske ledelsen, og krever et viss samarbeid slik at ting ikke kommer ut av kontroll (Lindsay 2014/15, s. 47).

7.0 Konklusjon

Denne oppgaven har hatt til hensikt å se nærmere på fremmedelementet cyber, og hvilken rolle det har når det kommer til dynamikken mellom stormaktene USA og Kina, og maktbalansen mellom dem. Studien ble gjort med dokumentanalyse som metode. Det teoretiske rammeverket bygger på strukturell realisme og mer tradisjonelle forståelser av makt og avskrekkings elementet av makt. For å oppsummere noen av de viktigste resultatene fra dette studiet, kan man se at i en allerede tilbaketrekking av amerikansk involvering på den internasjonale arena og Kinas formidable utvikling, så har Kinas satsing i cyberrommet supplert kinesiske kapabiliteter. Som ifølge den strukturelle realismen gjør at Kina får et større fotfeste og tar på seg mer oppgaver på den internasjonale arena. Dette er svært interessant. Ut i fra oppgavens empiri vil dette være det nærmeste man kommer en endring i maktbalanse. Cyber kan ha gjort at Kina trår mer i hælene til USA når det kommer til kapabiliteter og makt, men det debatteres enda hvorvidt dette vil føre til en dreining i en bipolar verdensorden.

8.0 Litteraturliste

Bijian, Z. (2005). China's "Peaceful Rise" to Great-Power Status. *Foreign Affairs, 84*(5), 18-24. doi:10.2307/20031702

Bowen, G. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal, 9*(2), 27-40. DOI 10.3316/QRJ0902027

Direktoratet for samfunnssikkerhet og beredskap (DSB). (2012). *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner– modell for overordnet risikostyring.* (1. delrapport). Hentet fra: https://www.dsb.no/globalassets/dokumenter/rapporter/sikkerhet-i-kritisk-infrastruktur.pdf

Fermann, G. (red). (2014). *Utenrikspolitikk og Norsk Krisehåndtering.* Oslo: Cappelen Damm Akademisk.

Grindheim, J.E. (2010). Makt. *Stat & Styring 04* (20). Hentet fra: https://www.idunn.no/stat/2010/04/art12

Healey, J. (2016). A NON-STATE STRATEGY FOR SAVING CYBERSPACE. *Journal of International Affairs, 70*(1), 13-20,11. Hentet fra: https://search.proquest.com/docview/1855797087?accountid=12870

Hjortdal, M. (2011). China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security, 4*(2), 1-24. Hentet fra: www.jstor.org/stable/26463924

Hovi, J. & Malnes, R. (red). (2011). *Anarki, makt og normer - innføring i internasjonal politikk.* Oslo: Abstrakt forlag.

Huntington, S.P. (1991). Democracy's Third Wave. *Journal of Democracy 2*(2), 12-34. doi:10.1353/jod.1991.0016

Iasiello, E. (2017). China's Cyber Initiatives Counter International Pressure. *Journal of Strategic Security, 10*(1), 1-16. DOI: http://doi.org/10.5038/1944-0472.10.1.1548

Jackson, R. & Sørensen, G. (2016). *Introduction to - International relations - Theories and Approaches.* Oxford: Oxford university press.

Mearsheimer, J. (2006). Structural Realism. I Dunne, T., Kurki, M., & Smith, S. (2007). *International relations theories: Discipline and diversity*. Oxford: Oxford University Press. Press, 2006), pp. 71–88. Hentet fra: https://www.commackschools.org/Downloads/8_mearsheimer-_structural_realism.pdf

Knutsen, T. (2016). *A history of international relations theory* (3 utg.). Manchester: Manchester University Press.

Layne, C. (2012). This Time It's Real: The End of Unipolarity and the "Pax Americana". *International Studies Quarterly, 56*(1), 203-213. Hentet fra: www.jstor.org/stable/41409832

Lindsay, J.R. (2014). The Impact of China on Cybersecurity: Fiction and Friction. *International Security 39*(3), 7-47. Hentet fra: https://www.muse.jhu.edu/article/571041

Major, C., & Mölling, C. (2016). (Rep.). *Rethinking Deterrence: Adapting an Old Concept to New Challenges*. German Marshall Fund of the United States. Hentet fra: www.jstor.org/stable/resrep18842

Nakashima, E. & Warrick, J. (2012, 2 juni). Stuxnet was work of U.S. and Israeli experts, officials say. *The Washington Post*. Hentet fra: https://cyber-peace.org/wp-content/uploads/2013/06/Stuxnet-was-work-of-U.S.pdf?fbclid=IwAR2NN8_v-3UWoAHLmciYjZBNZN0og4w0RMKq7RCj8uPbq22SeLexmSv1QWw

Nye, J.S. (2009). Get Smart: Combining Hard and Soft Power. *Foreign Affairs, 88*(4), 160-163. Hentet fra: www.jstor.org/stable/20699631

Nye, J.S. (2010) Cyber Power. Harvard Kennedy School, Hentet fra: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf

Ottis, R., & Lorents, P. (2010). *Cyberspace: Definition and implications*. Reading: Academic Conferences International Limited. Hentet fra: https://search.proquest.com/docview/869617247?accountid=12870

Porche, I., Sollinger, J., & McKay, S. (2011). A Cyberworm That Knows No Boundaries. I *A Cyberworm that Knows No Boundaries,* (s. 1-18). Santa Monica, CA; Arlington, VA; Pittsburgh, PA: RAND Corporation. Hentet fra: www.jstor.org/stable/10.7249/op342osd.8

Sin, N. Yao, K. Westbrook, T. Sano, H. Leussink, D. & Uetake, T. (2020, 17 januar). Instant View: China's economic growth slows to 6.1% in 2019, near 30-year low. *Reuters.* Hentet fra: https://www.reuters.com/article/us-china-economy-gdp-instantview/instant-view-chinas-economic-growth-slows-to-6-1-in-2019-near-30-year-low-idUSKBN1ZG092?fbclid=IwAR2sWeguJlJan3UACRMA2Zy06eDWKC-xGs1UbYJhQqxukBwU1jNzbcxBnmU

Smeets, M. (2020). US cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection, *Intelligence and National Security, 35*(3), 444-453, DOI: 10.1080/02684527.2020.1729316

Smith, N. (2017, 18 oktober). Who Has the World's No. 1 Economy? Not the U.S. *Bloomberg Opinion.* Hentet fra: https://www.bloomberg.com/opinion/articles/2017-10-18/who-has-the-world-s-no-1-economy-not-the-u-s

Stevens, T. (2012). A Cyberwar of Ideas? Deterrence and Norms in Cyberspace, *Contemporary Security Policy, 33*(1), 148-170. DOI: 10.1080/13523260.2012.659597

Tunsjø, Ø. (2018*). The Return of Bipolarity in World Politics: China, the United States, and Geostructural Realism*. New York: Columbia University Press.

Waltz, K. (2000). Structural Realism after the Cold War. *International Security*, 25(1), 5-41. Hentet fra: www.jstor.org/stable/2626772

Østerud, Ø. (2014). *Statsvitenskap – Innføring I politisk analyse*. (5 utg.). Oslo: Universitetsforlaget.

NTNU

Kunnskap for en bedre verden