Strategisk avskrekking i det digitale rom

Finnes det rasjonelle strategier for små stater?

Stig Tore Aannø

Masteroppgave

Forsvarets høgskole

Vår 2018

Forord

Denne masteroppgaven er et resultat av en av de undringene jeg har båret rundt på de senere årene av min profesjonelle hverdag. Albert Einstein sa at man ikke kan løse problemer med det samme tankesettet som skapte dem. Gjennom Øystein Tunsjøs gode forelesninger innenfor modulen Geopolitikk, sikkerhet og militærmakt oppdaget jeg konturene av et tankesett som kunne bidra til å gi svar på en disse undringene. Kåre Dahl Martinsen, som ledet an i metodefaget var positiv og motiverende når problemstillingen og metodevalg for dette prosjektet ble presentert, etter det var siktene stilt inn og troen på at prosjektet kunne gjennomføres på plass. Takk til begge for inspirasjon og motivasjon. Kersti Larsdotter som senere ble utpekt som min veileder fikk dermed en kandidat som i stor grad hadde valgt alle de store valgene, med de utfordringene det bærer med seg. Takk for konstruktive veiledninger.

Reisen denne oppgaven har representert for meg har vært interessant, lærerik men også krevende. Valget om å benytte meg av spillteori har kostet meg uker i ekstra pensum, streamede forelesninger på Internett og støtte av programvaren Gambit som har fungert som en fasit og et bevis ovenfor meg selv at jeg etterhvert behersket metoden. Takk til de som deler forelesninger og til de som skriver fri programvare. Prosessen har tatt meg dit at jeg ovenfor meg selv har et akseptabelt svar på den undringen denne reisen startet med. Jeg håper at de som er faglig interessert i denne problemstillingen også får noe igjen av å lese denne studien.

Skriving av en individuell masteroppgave innenfor det som vanligvis er ens egen fritid, er i realiteten et teamarbeid. For meg har det forutsatt en positiv, fleksibel og støttende kone, og jeg er dypt takknemlig for at både hjemmestøtten og forståelsen alltid har vært der Ingvild. Min sønn Lukas som fram til de siste månedene av og til har gitt uttrykk for å glede seg til voksenlivet, ettersom det for han har sett ut som en leksefri tilværelse, har nå endret mening og lært seg å sette pris på å være barn en stund til. Arbeidet med denne masteroppgaven har med andre ord allerede skapt noen positive ringvirkninger. Når han om en del år selv skal vurdere å søke høyere utdanning, håper jeg derimot at han har glemt alt, litt naivitet kan hjelpe et godt stykke på veien, enten man skal velge et krevende utdanningsløp, eller en metode som ikke var en del av pensum.

Sammendrag

Denne studien undersøker hvordan ulike strategier for avskrekking gjennom det digitale rom kan understøtte eller undergrave en småstats overordnede sikkerhetspolitiske målsettinger. Studien støtter seg på strukturell realisme for å forstå aktørene i det internasjonale systemet, og tar utgangspunkt i klassisk avskrekkingsteori for å identifisere aktuelle strategier. Disse teoriene drøftes så i relasjon til det digitale domenet og dets egenskaper. Dette danner så grunnlag for å utvikle modeller for gjennomføring av en spillteoretisk analyse, der hensikten er å avdekke hvorvidt de ulike avskrekkingstrategiene understøtter eller undergraver småstatens overordnede strategiske målsettinger. Studien viser at avskrekking gjennom det digitale rom er krevende uavhengig av om vi ser på hegemoner, stormakter eller småstater. Videre viser studien at småstater har et mindre handlingsrom, ettersom avskrekkingsstrategier i ulike tilfeller kan føre til en bilateral eskalering mellom partene. Dette undergraver i praksis småstatens overordnede strategiske målsetting. På tross av at avskrekking framstår som et krevende konsept, viser studien at det finnes rasjonelle strategiske muligheter som støtter seg på særegenhetene i det digitale rom. Disse særegenhetene gir forutsetninger for at det er mulig å endre offensiv-defensiv balansen til fordel for defensiven, samtidig som faren for eskalering forblir lav.

Nøkkelord: cyber, avskrekking, småstat, spillteori, strategi, digitale rom

Summary

This study investigate how different cyber deterrence strategies can support or undermine a small states national security policy. The study uses structural realism as the basis of understanding national states which are the actors in the international system and deterrence theory in order to identify the relevant deterrence strategies. The theories are furthermore discussed in relation to the inherent properties of the cyber domain. This acts as the basis for forming game theoretical models which are then analyzed with an objective of discovering whether the deterrence strategies supports or undermines the small states strategic goals. The study show that achieving cyber deterrence is a demanding goal regardless of the state being a hegemon, a great power or a small state. Furthermore, the study show that small states have fewer available options since deterrence strategies can lead to a bi-lateral escalation, creating a possible conflict, which again will undermine the small states strategic goals. Despite the fact that cyber deterrence is difficult concept, the study show that there are strategies available for small states, that supported by the properties of the cyber domain, have the potential to shift the offense-defense balance in favor of the defense. Changing the offense-defense balance in favor of the defense, can then change the cost-benefit analysis of offensive actor towards cooperation without the risk of escalating into a bi-lateral conflict.

Key words: Cyber deterrence, small state, game theory, strategy

Innholdsfortegnelse

Illustrasjoner og figurer

1 Innledning

1.1 Bakgrunn

Etteretningstjenestens årlige rapport for 2018 - Fokus, viser at Russisk aktivitet mot Norge i det digitale rom er et økende problem og rapporten sier videre:

> Det digitale rom gir statlige aktører en rekke nye muligheter til å sabotere både sivile og militære mål i andre stater. Sivile mål kan være systemer som er av kritisk betydning i moderne, industrialiserte samfunn, som styrings- og administrasjonssystemer for kraft, telekommunikasjon, transport og finansielle tjenester. Typiske militære mål er systemer for kommando og kontroll, kommunikasjon, navigasjon og overvåking (Etteretningstjenesten, 2018, s. 31)

I hvilken grad er samfunnet avhengig av denne digitale dimensjonen? Generelt kan vi si at all samfunnskritisk infrastruktur i dag er styrt av datamaskiner, den store majoriteten av disse datamaskinene er direkte eller indirekte tilknyttet Internett. Det betyr at de er sårbare for påvirkning gjennom det digitale rommet. Strøm, vann, telekommunikasjon, bank og finans, helse og flyt av varer og tjenester er områder som kan utsettes for sabotasje. En påvirkning på en eller flere av disse områdene kan gi svært negative konsekvenser og kan sette et moderne samfunn ut av funksjon og i ytterste konsekvens true liv og helse. Verdens penge- og aksjeverdier er bokført av banker og finansinstitusjoner på datamaskiner, penger flyter fra forbrukere til butikker - videre til leverandører og produsenter i det digitale rom, så lite som 8% av verdens pengevolum eksisterer som fysisk valuta (Chang, 2017). Verdens verdiskapning støtter seg i dag for alle praktiske formål på det menneskeskapte digitale rommet og denne verdiskapningen dermed også sårbar for digitale angrep.
Ved siden av kritisk samfunnsinfrastruktur, skapes det og forvaltes store verdier i det digitale rommet.
Ser vi nærmere på Apple, et selskap uten egen produksjonsinfrastruktur eller eksklusiv tilgang til naturressurser, er på tross av dette i stand til generere en årlig inntjening på nesten $230 milliarder og oppnådde i 2017 en aksjeverdi på over $900 milliarder (Nasdaq, 2018) (Shen, 2017). Denne store verdiskapningen er i hovedsak forankret i selskapets intellektuelle verdier og menneskelige kapital. Hvis man ser på hvor denne inntjeningen plasseres Apple i forhold til nasjonalstaters BNP i 2016, plasserer selskapet på en 44. plass, som er plassen under

Finland og over Bangladesh. Apple er ikke alene, selskaper som Alphabet[1], Facebook, Amazon og Microsoft er eksempler på andre selskaper som baserer sin verdiskapning på informasjon, det digitale rom og som har et økonomisk fotavtrykk som kan sammenlignes med verdens nasjonalstater. Næringskjeder som dette er sårbare for industrispionasje og konkurransefordeler kan vris fra ett selskap til ett annet. Den potensielle gevinsten eller -tapene er så store at nasjonalstaters potensiale for verdiskapning blir påvirket i vesentlig grad.

Fokus peker også på et annet forhold som er blitt aktualisert spesielt gjennom det amerikanske presidentvalget i 2016 der Donald Trump gikk seirende ut:

> I økende grad formidles vår opplevelse av virkeligheten via digitale systemer. Utviklingen er ikke begrenset til infrastruktur, industrielle prosesser og tjenesteproduksjon, men omfatter også meningsdannelse og sosial interaksjon. Den økende betydningen utfordrer fysiske grenser og den strukturelle maktbalansen (Etteretningstjenesten, 2018, s. 32).

Sosiale medier er blitt en integrert del av menneskers hverdag. Interaksjon med mennesker gjennom det digitale rom bygger relasjoner og kan ha stor innflytelse på individers tanker og meninger. Sosiale medier har utviklet forretningsmodeller der de genererer inntekter gjennom å levere målrettet reklame mot brukerne. Forretningsmodellen kan ved siden av produktreklame også benyttes til målrettede informasjonskampanjer som rekker på tvers av landegrenser og er et svært effektivt middel for å påvirke store befolkningsmasser.

Trusler mot en nasjonalstat kan ut ifra dette kategoriseres i tre hovedkategorier; *sabotasje*, *etterretning* og *påvirkning*. Etteretningstjenestens årlige fokusrapport sier at Russisk aktivitet i det digitale rom er en økende utfordring for vestlige demokratier (Etteretningstjenesten, 2018, s. 32). Trusselen dette representerer er høyt oppe på den politiske agendaen hos statsledere over hele verden. Framveksten av Internett og informasjonssamfunnet har de siste tiårene ledet til at det digitale rommet er blitt selve lerretet det moderne industrialiserte informasjonssamfunnet et er malt på.

Norge som en småstat må også ta hensyn til denne trusselen og utvikle strategier som har til hensikt å minimere konsekvensen av slik påvirkning. Ettersom det digitale domenet er relativt ungt og dynamisk, eksisterer det i liten grad sannheter om hvordan disse utfordringene kan

1 Alphabet Inc. er Googles morselskap.

løses. Det finnes heller ingen empiriske eksempler på avskrekkingsstrategier som har fungert og det er derfor naturlig å stille spørmål om det er mulig å få det til å fungere. Vi skal derfor se helt konkret på nasjonalstaten som aktør og hvilken effekt avskrekking kan gi som et virkemiddel for å opprettholde handlefrihet i det digitale domenet. Videre skal vi se problemet fra et småstat-perspektiv – altså finnes det grunnlag for en småstat å utvikle en avskrekkingsevne gjennom det digitale domenet for ivareta egen suverenitet og handlefrihet, eller må småstaten finne seg i å lide det den må?

1.2 Problemstilling

Er det mulig for en småstat å avskrekke sterkere nasjonalstater innenfor det digitale rom?

Hensikten med å besvare problemstillingen er å utvikle teori om små staters avskrekkingsevne i det digitale rom. En slik teori kan være en brikke som er med på å legge til rette for hvordan svakere stater velger å utforme en nasjonal cyberstrategi for å lykkes med avskrekking innenfor en sikkerhetspolitiske kontekst.

I problemformuleringen finner vi tre elementer vi må forstå før vi kan anvende en metode for å svare på problemstillingen. Først har vi behov for å forstå nasjonalstater og hvordan disse påvirkes av ulike faktorer innenfor det internasjonale systemet. Videre trenger vi å forstå begrepet avskrekking, hva omfatter det, og hvilke forutsetninger må være til stede for å oppnå avskrekking? Det siste elementet vi trenger å forstå, er det digitale rom. Siden det digitale rom i historisk kontekst er en nyvinning og som fremdeles er under stor utvikling, er det nødvendig å forsøke å forstå hvordan dette domenet virker i relasjon til nasjonalstaten og avskrekking. Når vi har dannet oss et bilde av hvordan disse tre henger sammen har vi forutsetning for å identifisere ulike avskrekkingsstrategier. Disse strategiene kan så danne en hypotese som vi tester. Her er det utfordrende å støtte seg på empiri ut i fra to faktorer. Først, samfunnets avhengighet til det digitale rom har i historisk sammenheng eksistert i så kort tid at det er vanskelig å trekke ut nok empiri til å underbygge svar på problemstillingen. I praksis er det vanskelig å vise til tilfeller der avskrekkingsstrategier i det digitale så langt gang har fungert etter hensikten. Målet med en avskrekkingsstrategi handler ofte om å kunne opprettholde en normaltilstand, eller status-quo. Nummer to, normaltilstanden kan ofte være stabil over tid uten tilstedeværelse av vellykket avskrekking. Dette kan vanskeliggjøre muligheten for å konkludere om hvorvidt en avskrekkingsstrategi i det digitale domenet basert på datagrunnlaget. I et forsøk på å omgå disse empiriske utfordringene skal vi i stor grad støtte oss på spillteori i metoden for å gi svar på problemstillingen.

1.3 Avgrensing

Selv om en avskrekkingsevne antageligvis også påvirker kost-nytte-regnskapet hos hacker-, terror, eller kriminelle organisasjoner, vil studien ikke berøre disse i særlig grad. Årsaken til dette er at disse grupperingene normalt er underlagt et nasjonalt lovverk i motsetning til nasjonalstater som i hovedsak opererer i et det internasjonale systemet som i følge en realismetilnærming er anarkisk av natur. Dette fører til at instrumentene for å påvirke kost-nytte-regnskapet hos disse aktørene vurderes til å være vesentlig annerledes enn de som benyttes mellom nasjonalstater. Som en konsekvens ville både teorigrunnlaget og spillene utvides vesentlig i omfang for å dekke disse ikke-statlige aktørene. Oppgaven vil heller ikke dekke etteretningsvirksomhet mellom nasjonalstater gjennom det digitale domenet. Dette er en praksis som er de fleste stater selv bedriver og i stor grad aksepterer (Wilner, 2017, s. 315). Denne studien begrenser seg dermed til å se på nasjonalstaten i en sikkerhetspolitisk kontekst. Når vi omtaler små stater finnes det ikke en omforent definisjon for hvor stor eller liten denne er. I enkelte sammenhenger benyttes Nederland som målestokk med om lag 16 millioner innbyggere, mens verdensbanken setter grensen ved 1,5 millioner innbyggere (Areng, 2014, s. 1). Det er ikke vesentlig for denne studien å trekke en klar grense for hvilke kriterier som infris for at en nasjonalstat faller innenfor kategorien småstat. Det som er vesentlig er at det eksisterer en vesentlig maktasymetri mellom det vi i denne studien omtaler som en stormakt og en småstat.

1.4 Tidligere forskning

Aktivitet mot nasjonalstater i det digitale rom er et økende problem. Stater med moderne samfunnssystem har i de senere årene utviklet nasjonale cyberstrategier for å på best måte håndtere denne utfordringen. Det finnes så langt ikke noe belegg for at en nasjon så langt har klart å utvikle en nasjonal cyberstrategi. Behovet for forskning er stort og et søk på den akademiske søkemotoren Google Scholar viser at det er om kring 1200 akademiske arbeider som omfatter temaet. Litt over halvparten av disse er skrevet etter 2014. Hvis vi ser nærmere på dette utvalget er det kun noen få av disse arbeidene undersøker strategiske avskrekkingen i det digitale rom i en relasjon til små stater. Det første er et working paper med tittelen *Cyber deterrence in Singapore: Framework & Recommendations*. Denne studien tar en bred tilnærming til avskrekking der den ser på hele bredden av trusselaktører og virkemidler. Studien konkluderer med noen generelle anbefalinger, men har et vesentlig problem knyttet til sin tolkning av avskrekking gjennom nektelse. Her beskriver studien at avskrekking gjennom nektelse i det digitale domenet handler om å nekte en annen stat tilgang til teknologi på en

tilsvarende måte som man nekter stater muligheten til å bygge atombomber ved å hindre tilgang til anriket uran (Tan, 2018, s. 4). Studien konkluderer ut i fra denne tolkningen at avskrekking gjennom nektelse i det digitale domenet ikke er en relevant strategi for Singapore. Vi skal senere se at avskrekking gjennom nektelse inkluderer andre potensielle handlemåter enn det den singaporske studien baserer sine konklusjoner på.

NUPI har et pågående forskningsprosjekt innenfor temaet: «Upholding the NATO cyber pledge: What does cyber deterrence and cyber resilience mean for NATO and Norway?» Forskingsprosjektet har så langt utarbeidet et policy paper som konkluderer med at det er behov for at NATO endrer sin tankegang fra tradisjonelle avskrekkingsmodeller. Dagens NATO modeller hevder policy paperet, er basert på atom- og konvensjonell avskrekking fra den kalde krigen. Det er dermed behov for at denne endres en mer fleksibel og dynamisk prosess og poengterer at avskrekking ikke begrenser seg til to tilstander, suksess eller total svikt, men at avskrekking i det digitale rom er en kontinuerlig prosess (NUPI, 2017, s. 4).

Ser vi på forskning som ikke ser spesielt på småstatperspektivet er Martin C. Libicki en stor bidragsyter og utga allerede i 2008 boken *Cyberdeterrence and Cyber War* og fulgte i 2017 opp med boken *Cyberspace in Peace and War.* Dette er så langt det mest omfattende arbeidet som er gjort for å tette gapet mellom strategi- og teknologiperspektivet i det digitale rom. Libickis forskning har et amerikansk perspektiv på problemstillingene. Konklusjonene han trekker er derfor ikke alltid like relevante for små stater, samtidig er mye av grunnlaget hans konklusjoner støtter seg på helt relevante. Generelt kan man si at Libicki har en forsiktig holdning til avskrekking i det digitale rom. Hans største bidrag er å trekke fram hvilke faktorer og relasjoner er av betydning for en strategi det digitale rom uten å være preskriptiv. Libicki beskrev allerede i 2008 at avskrekking har en annen dynamikk i det digitale domenet enn tilfellet er innenfor atom- og konvensjonell avskrekking. Det samme poenget NUPI gjør i sitt policy paper fra 2017.

Joseph Nye (2017) argumenterer for at man i tillegg til begrense seg til å se på de to klassiske avskrekkingskategoriene, også bør inkludere to nye: «deterrence by entanglement» og «deterrence by norms». Nye peker dermed på et viktig poeng ved at det finnes virkemidler utenfor det digitale rom som også kan påvirke påvirke nasjonalstatenes handlinger innenfor dette domenet.

2 Teoretiske rammeverk

Vi skal i dette kapittelet se nærmere på teorier som kan understøtte en metodisk tilnærming til å besvare problemstillingen. For å få til dette må vi kunne analysere nasjonalstaters strategiske valg og hvordan disse påvirker hverandre. Spillteori er et vitenskaplig felt som bruker en metodiske tilnærminger som har til hensikt å analysere og rangere ulike strategiske valg rasjonelle aktører kan foreta seg ut ifra definerte scenario. Ved siden av at aktøren er rasjonelle, så er det også nødvendig å ta stilling til hva aktøren ønsker å oppnå. Hva er aktørens preferanser og ønskede sluttilstand? Spillteori forutsetter altså enhetlige rasjonelle aktører og det er dermed en forutsetning at vi finner en modell for nasjonalstaten som oppfyller dette kravet.
I stedet for å forsøke å utvikle denne modellen så har jeg valgt å støtte meg på strukturelt realisme, som er en teori innenfor internasjonal politikk. Det er flere forhold som gjør det naturlig å velge realisme for å beskrive aktørene i denne oppgaven. Først er det avgjørende at realisme ser på nasjonalstaten som selve aktøren. Videre er det i følge realismeteori nasjonalstater rasjonelle aktører som primært handler ut ifra en målsetting om å øke eller opprettholde egen sikkerhet og overlevelsesevne (Williams, Lobell, & Jesse, 2012, s. 11). Et strukturelt realismeperspektiv på internasjonal politikk ser dermed ut som hensiktsmessig grunnlag for å beskrive aktørene innenfor metoden vi anvender. Vi skal se nærmere på strukturell realisme i neste del.

Ved siden av å ha en teori som beskriver aktøren, har vi også behov for teori som beskriver selve virkemidlet - avskrekking. Hva er avskrekking, hvilke forutsetninger må være til stede for å oppnå avskrekking? En forståelse for hvilke muligheter og begrensninger som finnes innenfor avskrekkingsteori, samt en forståelse av virkemidlene i det digitale domenet er en forutsetning for å å ta tak i problemstillingen.

2.1 Internasjonal politikk – strukturell realisme

> We have no facts about the future, since the future has't happened yet. We need a theory.
>
> John Mearsheimer

En forståelse av aktørene i spillet er en forutsetning for å vurdere hva som er relevante strategier og hvilken konsekvens de ulike strategiene vil ha for aktørene. Her er det naturlig å se nærmere på teori innenfor internasjonal politikk for å skape tilstrekkelig aktørforståelse. Fagområdet internasjonal politikk er preget av en rekke ulike skoler som betrakter det

internasjonale systemet ut ifra ulike forutsetninger. Her er det nødvendig å gjøre et valg i forhold til hvilken teori som er mest hensiktsmessig å støtte seg på. Avskrekking er for nasjonalstater først og fremst et strategisk sikkerhetsspørsmål. Vi trenger derfor en teori som i tilstrekkelig grad klarer å beskrive nasjonalstatens perspektiv på sikkerhet. Videre at en kapasitet for avskrekking gjennom det digitale domenet, kan være en form for makt som kan benyttes målrettet for å påvirke andre stater. Teoriene må videre gi forutsetning for å utlede hvilke preferanser staten har i forhold til ulike strategiske utfall. Sist at en nasjonalstat kan betraktes som en rasjonell og enhetlig aktør. Dette er viktig for å redusere kompleksiteten i modellene til et omfang som er praktisk håndterlig. Realisme gir tilstrekkelig svar på disse områdene og gir spesielt gode forutsetninger når det gjelder det siste punktet som bidrar til å redusere kompleksiteten i modellene til et praktisk håndterbart omfang.
Vi skal nå se nærmere på strukturell realisme og hva den sier om aktørene som er berørt av problemstillingen i denne teksten.

I følge realisme er det makt som er valuta i internasjonal politikk og stormaktene er hovedaktørene i det internasjonale systemet. Stormaktene følger nøye med på hvor mye økonomisk og militær makt de har i relasjon til andre og forsøker aktivt å hindre tap av terreng ovenfor de andre aktørene (Mearsheimer, 2013, s. 78). Dette perspektivet på makt samt fokuset på å ikke tape relativt til andre aktører i den internasjonale systemet, blir således et sentralt moment for å forstå aktørens målsetting og preferanser. Vi ser at det innenfor realismeteorien er stormaktene som er i fokus, men Waltz hevder at dette ikke betyr det samme som at man ikke ser mindre stater. I følge Waltz er det avgjørende å ha fokus på stormaktene for å kunne forstå småstatenes skjebne (K. N. Waltz, 1979, s. 73). Teorien omhandler dermed også mindre stater, men deres handlingsrom er altså sterkt influert at stormakene. Tar vi utgangspunkt i dette, betyr det at realismeteori kan være tilstrekkelig for å forstå både stormakter og småstater som aktører i spillanalysene vi kommer tilbake til senere i kapittel 4. av denne oppgaven.

Hvis vi ser nærmere på realismeteori, ser vi at det finnes ulike avgreninger. En av de fundamentale forholdene som skiller de ulike grenene er deres perspektiv på spørsmålet: hvorfor ønsker stater makt? Klassiske realister som Morgenthau mente at dette var forankret i menneskets natur (Mearsheimer, 2013, s. 77). I følge Morgenthau er ønsket om makt en medfødt egenskap hos alle mennesker. Denne medfødte egenskapen fører dermed til at nasjoner ledes av mennesker som har et slags innebygd ønske om å øke egen og dermed nasjonens makt. Strukturelle realister mener på en annen side at årsaken til at stater ønsker

makt, ikke har så mye å gjøre med menneskets natur. I stedet hevder strukturell realisme at ønsket om makt er knyttet til strukturen i det internasjonale systemet. Kjernen i argumentet henger sammen med at det internasjonale systemet er anarkisk av natur. Det betyr at det ikke finnes en overordnet lov og - makt som binder stater og som straffer stater som ikke retter seg etter denne loven. Konsekvensen av dette er at ingen stat har en garanti for at den ikke kan bli angrepet av den annen stat. Dette fører så til at en hver stat har et sterkt insentiv til selv å ha nok makt til å kunne ta vare på sin egen sikkerhet, ettersom dette er det eneste virkemidlet de har for å sikre egen overlevelse.
Denne dynamikken binder stater inn i en kontinuerlig maktkamp som altså har sitt opphav i ønsket om å overleve. Betraktninger knyttet til påvirkning fra kulturelle- eller statslederes personlige preferanser i utformingen av nasjonalstatenes strategiske valg er dermed i følge strukturell realisme irrelevant, ettersom den internasjonale systemet skaper like insentiver for stater, uavhengig av andre forutsetninger (Mearsheimer, 2013, s. 78).
Ved å støtte oss på strukturell realisme, er vi dermed ikke avhengig av å drøfte kulturelle faktorer eller faktorer knyttet til personligheten til en aktuell statsleder. Videre åpner det også for at vi kan se på nasjonalstater i en mer generisk tilnærming, uten å måtte se på statens interne forhold.

Et annet spørsmål som skiller innenfor realismeretningene, og som også er relevant for å forstå nasjonalstaten som selve aktøren er: hvor mye makt er nok makt? Defensive strukturelle realister som Waltz mener at det vil være uklokt av en stat å forsøke å maksimere sin egen makt. Konsekvensen er i følge Waltz at det internasjonale systemet vil komme til å straffe en slik adferd hvis de oppnår for mye makt ved at andre stater vil balansere mot denne staten (Mearsheimer, 2013, s. 81).
Mearsheimer som representerer offensiv strukturell realisme mener på sin side at det gir god mening når stater forsøker å maksimere sin relative makt og videre søke hegemoni om dette er mulig. Rasjonale for dette er i følge Mearsheimer at det å være en overlegen makt gir best sikkerhet. Insentivet for en stat om å øke sin egen relative makt for å oppnå mer sikkerhet fører videre til et kjent og mye omtalt mekanisme som er omtalt som sikkerhetsdilemmaet. Sikkerhetsdilemmaets sentrale poeng er at når en stat øker sin egen sikkerhet gjennom å øke sin relative makt, så reduserer den samtidig sikkerheten til andre stater (Jervis, 2013, s. 90). Denne dynamikken kan videre være en utløsende faktor for våpenkappløp mellom nasjoner. Tidligere amerikansk president Barack Obama advarte om at et våpenkappløp er et mulig scenario i det digitale domenet (Politico, 2016). Er det ut ifra det sannsynlig at vi står ovenfor

et våpenkappløp mellom stater i det digitale domenet? Hvis det er tilfelle, vil det gi føringer for at småstater også må øke sine evne til å beskytte seg i det digitale rom.

Vi må også ta stilling til hvordan offensiv–defensiv-balansen fungerer i det digitale rom. Hvis det digitale domenet favoriserer offensiven, vil det kunne drive stater til å utvikle offensive virkemidler og gjennom det forsterke effenkten av sikkerhetsdilemmaet. På den annen side, hvis maktmidlene er av en slik karakter at de kun kan benyttes i en defensiv rolle for den staten som anskaffer de, vil det redusere intensiteten i sikkerhetsdilemmaet, samtidig som staten øker sin egen sikkerhet. Utfordringen er at det i enkelte sammenhenger ikke er mulig å sikre seg gjennom kun å satse på defensive virkemidler (Jervis, 2013, s. 105). Konsekvensen av dette er at det ikke alltid finnes handlingsrom for en stat å øke sin egen sikkerhet uten samtidig å øke intensiteten i sikkerhetsdilemmaet. I følge tidligere amerikansk viseforsvarsminister William J. Lynn favoriserer cyberdomenet offensiven (Saltzman, 2013, s. 43). Dette underbygges også av at Canada, som kan defineres som en status-quo makt, velger å etablere en offensiv kapasitet i cyberdomenet. Begrunnelsen er at de vurderer at en defensiv kapasitet alene ikke er tilstrekkelig for å ivareta egen sikkerhet i dette domenet (International Institute for Strategic Solutions, 2013, s. 45). Mange hevder at det i dag allerede pågår et våpenkappløp i det digitale domenet, hvis dette stemmer, så understøtter dette også Lynns påstand om at det digitale domenet favoriserer offensiven (Paletta mfl., 2015). Selv om maktmidler i det digitale domenet ser ut til å ha trekk som stemmer med tenkning rundt offensiv – defensiv balanse, er det også klart at Jervis teori ikke omtaler det digitale domenet direkte. Teorien er i sin helhet tuftet på makt i form av kinetiske våpen, det betyr ikke at den ikke kan gi oss relevant innsikt når vi ser på hvordan makt i det digitale domenet kan påvirke intensiteten i sikkerhetsdilemmaet, men det understreker at vi må være varsom når vi betrakter teoriens relevans i tilknytning til oppbygging av makt i det digitale domenet.

Militærmakt er et helt sentralt tema innenfor realismeteori. Realismen er klar på hvilke faktorer som utgjøre en nasjonalstats makt. Waltz introduserte i sin bok *Theory of international politics*, seks faktorer som
bedømmer en nasjons kapabilitet (styrkeforhold) (1979, s. 131). Disse faktorene er; størrelse og befolkning, naturressurstilgang, politisk stabilitet, kompetanse, økonomisk evne og til slutt militær makt.
I forhold til militærmakt kan vi ikke uten videre vurdere at dette begrepet også dekker en nasjons makt i det digitale domenet. En årsak til dette er at det digitale domenet og dets rolle har oppstått etter at hovedtrekkene av teorien strukturell realisme er kommet på plass. Det kan

også være utfordringer knyttet til å direkte innlemme makt i det digitale rom i realismens militærmaktbegrep omhandler i hovedsak en fysisk form for makt som kan true en nasjons geografiske integritet og suverenitet. På en annen side er det mulig å se på makt i det digitale domenet som en del av nasjonens maktpotensiale gjennom at den kan forsterke en nasjonalstats økonomi. Samtidig kan makt i det digitale domenet også forsterke effekten av å bruke militær makt på samme måte som luftmakten kan gi landstyrkene luftstøtte. Hvis vi trekker denne støttende rollen videre og ser det i relasjons til småstatsperspektivet er det å gjennomføre offensive landoperasjoner i liten grad et relevant virkemiddel for en småstat. Kan da offensiv makt i det digitale domenet være relevant for en småstat?
Når vi ser nærmere på de andre kapabilitetene, er evnen for en nasjon til utvikle sin makt i det digitale domenet mest avhengig av kapabiliteten kompetanse, men forutsetter også at nasjonen har tilstrekkelig økonomisk evne. Dette er kapabiliteter relativt små stater bør kunne ha tilstrekkelig med ressurser innenfor til å prioritere en betydelig evne, som videre kan bety at offensiv makt i det digitale domenet er mulig å utvikle, selv for en småstat. Et eksempel på en småstat som har en betydelig evne i det digitale rom er Israel (Balance, 2018, s. 342). I motsetning til tradisjonell militærmakt er det også utfordrende å kvantifisere hvor mye makt en nasjon besitter innenfor dette domenet. I tilfellet Israel kan en vurdering av maktpotensialet underbygges av at Israel lykkes i å hacke et av verdens største sikkerhetsselskaper Kapersky Lab. Som en del av denne operasjonen avslørte de det som antas å være russisk infiltrering av firmaets sikkerhetsprodukter som de senere varslet sin allierte – USA om (Perlroth & Shane, 2017). Israel skal også ha vært en sentral aktør i utviklingen av Stuxnet, som var en skadevare som ble spesielt utviklet for å infiltrere Irans urananrikingsanlagg i Natanzs, der skadevaren lykkes i å ødelegge anrikingssentrifugene (Nakashima & Warrick, 2012). Israel har altså på tross av sin status som småstat klart å komme i posisjon som en av de mektigste aktørene innenfor det digitale domenet. På tross av at det er vanskelig å kvantifisere makt i det digitale domenet, så underbygger Israel at en småstat kan velge å utvikle offensiv virkemidler og bli ansett som en sterk aktør innenfor dette domenet.

Realismeteori tilsier at maktdynamikken i internasjonal politikk tenderer mot å være et nullsumspill (Mearsheimer, 2007; K. N. Waltz, 1979, s. 70). Det blir dermed en forutsetning og vil også påvirke- og reflekteres i spillmodellene vi skal se på senere. Hvis en stormakt på den ene siden øker sin makt, taper andre nasjoner sikkerhet.

2.2 Polaritet

Polaritet er en beskrivelse av hvordan makt er fordelt mellom stater i det internasjonale systemet. Polaritet benyttes ofte som et rammeverk i når stabiliteten i det internasjonale systemet drøftes. Det internasjonale systemet har etter den kalde krigen blitt regnet som unipolart (Ikenberry, Mastanduno, & Wolforth, 2009, s. 1). I et unipolart system er makten i stor grad konsentrert hos en stat, som ofte blir omtalt som systemets hegemon. Hegemonen i det internasjonele systemet etter den kalde krigen har vært USA, men vi ser at denne statusen utfordres av Kina. Polariteten i systemet er altså ikke stabilt over tid. Under den kalde krigen fantes det to stormakter: USA og Sovjetunionen dominerte andre stater og konkurrerte seg i mellom i et bipolart system. Hvis vi så ser tilbake til det internasjonale systemet før den andre verdenskrig, fantes en rekke stater som Storbritannia, Frankrike, Tyskland, Italia, Russland og USA som alle var stormakter, kunne vi observere et multipolart system.
Et unipolart system slik vi ser det i dag vil i følge realismeteori ikke kunne opprettholdes over tid. Andre stater vil begynne å balansere for å motvirke makten til hegemonen. Kinas makt vokser og vil etterhvert kunne være sterk nok til å utfordre USA (Tunsjø, 2014, s. 3). Tidligere sjef for NSA, Gen. Keith Alexander har uttalt at industrispionasje gjennom det digitale domenet utgjøre historiens største overføringen av rikdom mellom nasjonalstater (Rogin, 2012). Teknologi for å utføre denne type aktivitet er relativt billig og er tilgjengelig for både småstater og ikke-statlige aktører. Gjennom sin ressursrikdom og teknologi blir hegemonenen i systemet et mål for en stor del av disse aktørene, og utfordringen med å verne om sin egen økonomiske maktbase utfordrende (Huesken, 2012, s. 48). Det ser altså ut til at framveksten av det digitale rom og dets rolle i verdiskapning påvirker maktpolaritet ved å distribuere makt til de svakere aktørene, på de sterkeste aktørenes bekostning. En amerikansk rapport fra DOD Defence science board peker også på risikoen av «death by a 1 000 hacks», der den akkumulerte effekten av all aktiviteter, der hver enkelt er relativt ubetydelig, til slutt kan få store negative konsekvenser (Defence Science Board, 2017, s. 9). Det ser dermed ut til at det er polene i det internasjonale systemet som naturlig blir målet for en betydelig del av denne aktiviteten. En småstat er i denne konteksten mindre interessant og kan dermed ha en fordel ved å være et mindre attraktivt mål. Ut i fra en slik mekanisme er det mulig å forutsette at det for de offensive aktørene gir lavere utbytte å bruke sin kapasitet mot små stater. Dette fører videre til at små stater kan nøye seg med å påføre den potensielt offensive staten en lavere kostnad for å oppnå avskrekking, enn tilfellet er for en stormakt eller hegemon.

2.3 Geopolitikk.

Strukturell realisme gir et grunnlag for å forstå målsettingen for nasjonene innenfor det internasjonale systemet, men det er også slik at ulike nasjoner er gitt ulike geografiske betingelser. Geopolitikk er en teori som viser til at geografi i kombinasjon med andre faktorer har innflytelse på internasjonal politikk (Knutsen, 2012, s. 264). Det digitale domenet er i seg selv i begrenset grad påvirket av geografi. Det er mulig å hevde at vår verden er for liten til at den har påvirkning på det digitale rom, ettersom informasjonen flytter seg på tvers av verden i løpet av millisekunder, dermed blir avstand en relativt uvesentlig faktor. En stat kan gjennom det digitale domenet ramme en annen stat ved å gjennomføre offensive operasjoner mot denne, uavhengig av geografisk avstand. På den andre siden er det mulig å hevde at det digitale domenet består av en fysisk infrastruktur som i høyeste grad er forankret i den fysiske verden. Det digitale domenet er altså ikke i seg selv påvirket av geografi, men infrastrukturen har en grad av sårbarhet, også fra de fysiske domenet. Enkelte nasjonalstater slik som USA, har en større del av de Internetts kritiske byggestener innenfor egne landegrenser, men generelt er infrastrukturen bygget med relativt stor redundans. Det vanskeliggjør i praksis at en nasjonalstat i vesentlig grad skal kunne ramme resten av verden, gjennom å påvirke infrastruktur innenfor de geografiske grensene av egen nasjonalstat.

Bruk av offensiv makt i det digitale domenet kan på en annen side eskalere over i det fysiske domenet. I slike tilfeller vil geopolitiske betraktninger være av vesentlig betydning. Geografiske relasjoner til andre stater påvirker i stor grad hva en stat kan tillate seg i det digitale domenet (Sheldon, 2014, s. 287). En småstat har eksempelvis mindre handlingsrom når det kommer til hva den kan foreta seg av operasjoner mot en stormakt hvis stormakten deler en felles grense med småstaten. Årsaken til dette er at stormakten i et slikt tilfelle er godt posisjonert til å gjengjelde handlingen med andre midler. Offensive operasjoner utført av en småstat har i et slikt tilfelle en risiko for å eskalere en situasjon inn i de tradisjonelle domenene. For småstaten er dette sjelden ønskelig, da den typisk vil være underlegen en større aktør. Geografi har derfor en sterk innflytelse på hvordan og mot hvem en småstat bør anvende makt i det digitale domenet. En generell betraktning relatert til geopolitikken er at avstand vil gi økt handlefrihet, mens nærhet vil reduserer den. Geopolitiske betraktninger kan med det spille inn på spillmodellenes mulige utfall og dermed også spillernes preferanser. Konsekvensen av dette er at generiske spillmodeller basert på en strukturell realismetolkning av stormakt-småstat relasjonen og deres preferanser, ikke nødvendigvis fanger opp alle de vesentlige faktorene som påvirker aktørenes preferanser i modellen. Det kan derfor være nødvendig å gjøre geopolitiske forutsetninger i spillmodellene, eller bruke konkrete

nasjonalstater slik at det er mulig å analysere de geopolitiske faktorene og hvordan de påvirker de mulige utfallene og statenes preferanser.

2.4 Avskrekking

> Deterrence, in its broadest sense, means persuading an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs and risks (Mearsheimer, 1983).

Påvirkning av en aktørs kost-nytte-vurdering er altså det sentrale temaet innenfor avskrekkingsteori. Det en nasjon risikerer å tape ved å utføre en handling, må overgå nytten ved å utføre handlingen. Avskrekking handler altså om intensjoner – ikke bare det å prøve å forstå en annen aktørs intensjoner, men å påvirke dem.
En evne til å påføre en potensiell motstander skade avhenger ikke av en evne til å kunne beseire den samme motstanderen (Schelling, 2008, s. 22). Schellings påstand åpner for at avskrekking ikke bare bare er et virkemiddel for de sterkeste. Avskrekking åpner for at det er en strategi som er et realistisk virkemiddel for en småstat å bruke ovenfor en sterkere stat. Et eksempel som benyttes til å illustrere denne mekanismen er fotgjengeren som går ut i veien, foran en buss og dermed påvirker denne til å senke farten eller til å med stoppe. Det er ingen tvil om at fotgjengeren er den svake parten, men fra bussens side er ulempen ved å kjøre over fotgjengeren så stor at den høyeste preferansen likevel er å stoppe. I praksis er dette ukontroversielt og henger også sammen men hvorfor den store majoriteten av småstater utruster seg med militære forsvar. Ettersom det eksisterer et asymmetrisk maktforhold ovenfor den staten som skal avskrekkes, spiller alliansepolitikk også inn som en vesentlig komponent for å forsterke avskrekkingen (Tamnes mfl., 2015, s. 78).
Effektiv avskrekking krever at tre forhold er til stede. For det første må aktøren ha en faktisk evne til å gjennomføre det den truer med (evne). Ser vi eksempelvis på atomvåpen, er prøvesprenginger en effektiv måte å demonstrere denne evnen på. Sprenger en nasjon en atombombe er det liten tvil om at aktøren har evnen. Hvordan demonstrerer en nasjon en slik evne i det digitale rom? Forhold knyttet til evne skal vi se nærmere på når vi redegjør for hva det vil si å ha en offensiv evne i det digitale domenet senere i denne teksten. For det andre må det være troverdig at denne evnen kan bli benyttet mot aktøren som er ment å avskrekkes (troverdig). Ser vi igjen på historien knyttet til avskrekking med atomvåpen, ble det etterhvert stilt spørsmål til troverdigheten ved USAs doktrine «Massive retaliation» som tilsa at et et hvert overtramp mot NATO, ville besvares med en massiv gjengjeldelse med atomvåpen.

Denne reaksjonen manglet i mange scenarier proporsjonalitet og dette ga dermed grobunn for å stille spørsmål ved troverdigheten til doktrinen. Det tredje og siste forholdet som må på plass er klar kommunikasjon. Aktøren som ønsker å avskrekke må kommunisere klart hvor grensen går for hvor avskrekkingmiddelet kommer til anvendelse (Jasper, 2017, s. 9). Kommunikasjonen må lykkes med å «trekke en linje i sanden» der hvor en overtredelse medfører gjengjeldelse. Disse tre forutsetningene er altså avgjørende for å oppnå en effektiv avskrekking, men som vi skal se senere, synes dette mer krevende innenfor det digitale domenet enn hva tilfellet er med atommakt.

Bernard Brodie poengterte så tidlig som i 1946 at hensikten med å besitte atomvåpen var å ikke bruke dem, men å hindre den andre parten å bruke sine. Dette oppnås ved å true den potensielle motstanderen med at; om han noensinne velger å benytte sine våpen, så ville det gjengjeldes (Libicki, 2016, Kapittel 21). Dette underbygger et sentralt poeng innenfor klassisk avskrekkingsteori; målsettingen er å aldri måtte benytte den avskrekkende kapasiteten. Avskrekking er altså et defensivt virkemiddel som har til hensikt å påvirke kost-nytte-vurderingen til en aktør slik at han vurderer det som sin egen beste interesse å ikke krysse den kommuniserte grensen. Velger han likevel å krysse denne grensen, har hensikten med avskrekkingen mislyktes. Når avskrekkingen har mislyktes står den defensive aktøren i praksis igjen med to uønskede valg. Det første er å bruke avskrekkingsmiddelet, som med stor sannsynlighet vil kunne eskalere situasjonen, eller å avstå fra å bruke det, som vil føre til at avskrekkingen taper sin troverdighet. Dette viser viktigheten av at terskelen for hvor avskrekkingsmiddelet kommer til anvendelse, settes på et nivå der konsekvensen i stor nok grad legitimerer middelet. I tilfeller der en småstats avskrekking feiler ovenfor en stormakt vil valget om å realisere avskrekkingsmiddelet kunne være irrasjonelt ettersom den mektigste av de to partene sannsynligvis vil kunne komme best ut av en eventuell eskalering ut i de fysiske domenene. Dette forholdet smitter også over på troverdigheten om hvorvidt småstaten er villig til å bruke avskrekkingsmiddelet. Paradoksalt nok kan det lønne seg for en den svakere parten å framstå irrasjonell og uforutsigbar for at avskrekkingen skal være troverdig (Schelling, 2008, s. 36). Denne mekanismen kan for eksempel til en viss grad underbygge en påstand om at Nord Koreas truende framtreden og retorikk ovenfor stormakten USA er rasjonell, hvis Nord Koreas primære målsetting er å gjøre sin avskrekkingstrussel troverdig. Et annet relevant perspektiv knyttet til dette er at det nok ikke er like lett for småstater som eksempelvis Norge, som hvert år deler ut fredsprisen å høste troverdighet for tilsynelatende irrasjonelle avskrekkingstrusler om straff mot en eventuell sterkere nasjonalstet. Finland på en annen side kan muligens på tross av å framstå som rasjonell småstat ha bedre forutsetning

med en avskrekkingsstrategi forankret i sin historie fra vinterkrigen og Sisu[2]. Finland kan altså støtte seg på en kultur og et etos om å stå i mot uansett hvor håpløs situasjonen ser ut. Avskrekking må altså være troverdig for å ha en effekt, ikke alle stater, spesielt ikke småstater har lik forutsetning for å etablere en troverdig trussel mot en overmakt.

Atomavskrekking var under den kalde krigen i prinsippet ikke-repeterbar og symetrisk. Den er ikke-repeterbar basert på at konsekvensen ved å utløse virkemiddelet vil føre til en så stor endring i tilstanden, at det kan forutsettes at det ikke vil være mulig eller nødvendig å bruke avskrekkingmiddelet om igjen. Den er symetrisk ettersom begge sider har tilsvarende evne eller kapasitet til å straffe. Hvis vi sammenligner dette med kriminalitetsavskrekking, er denne repeterbar og asymetrisk. Den er repeterbar ettersom kriminelle som har sonet sin straff og sluppet fri, om de bryter loven på nytt, kan de også bli straffet på nytt. Den er asymetrisk da evnen til å straffe i hovedsak ligger hos den ene parten som i dette tilfellet er staten. Hvis vi betrakter avskrekkingmiddelet i det digitale rom, så vil også denne være repeterbar, siden gjennomføring av avskrekkingsmiddelet sannsynligvis ikke vil frata partene evnen til å gjenta handlingene. Samtidig er avskrekking i det digitale domenet symetrisk basert på at begge parter kan ha denne evnen (Libicki & Project Air Force (U.S.), 2009, s. 30). Avskrekking i det digitale rom avviker altså vesentlig med atomavskrekking ved at den er repeterbar, som den har til felles med avskrekking mot kriminelle handlinger. Samtidig eksisterer den i det internasjonale systemet, som er anarkisk og alle stater har dermed tilsvarende mulighet til etablere en slik kapasitet og bruke den. Her er det mulig å trekke en parallell til disputer mellom europeiske stater før atomvåpentrusselen, der statene hadde en form for ikke-utslettende avskrekking som kunne brukes om og om igjen. Innenfor dette systemet oppsto det til dels hyppige kabinettkriger (K. Waltz, 1979, s. 64). Dette gir grunnlag for å spørre i hvilken grad det er mulig å avskrekke innenfor et repeterbart og symmetrisk system. Hvis vi legger til at vi spesielt ser på avskrekking i en småstat-stormakt-relasjon, så er ikke styrkeforholdet symmetrisk hvis vi beveger oss over i de fysiske domenet. I det fysiske domenet har stormakten en asymmetrisk maktfordel. Stormakten kan dermed dominere om situasjon i det digitale domenet eskaleres ut til det fysiske. Dette blir dermed en faktor som småstaten må ta stilling til når den velger sine handlinger i det digitale domenet.

Hvis vi ser nærmere på klassisk avskrekkingsteori beskriver denne i hovedsak to avskrekkingsstrategier. Avskrekking gjennom straff (deterrence based on punishment) og avskrekking gjennom nektelse (deterrence based on denial) (Mearsheimer, 1983). Avskrekking gjennom straff handler om å etablere en troverdig trussel om at en hver aktør som krysser den kommuniserte grensen vil bli møtt med en overveldende gjengjeldelse.

2 Sisu er et finsk uttrykk som handler om pågangmot og indre kraft.

Denne formen for gjengjeldelse er assosiert med trussel om bruk av atomvåpen, men dekker også bruk av konvensjonelle våpen. Avskrekking gjennom nektelse handler om en strategi som vil hindre en aktørs muligheter til å nå sine målsettinger. Strategiens mål er å kunne kontrollere situasjonen tilstrekkelig, slik at aktøren er forhindret fra å bruke enkelte handlingsmåter, framfor å tvinge han til en bestemt oppførsel (Muller & Stevens, 2017, s. 2). Hvis vi ser forbi de to tradisjonelle hovedkategoriene for avskrekking har de senere år blitt argumentert for nye strategier. Eksempler på dette er avskrekking gjennom «entanglement» eller avskrekking gjennom normer (Nye, 2017, s. 60). Disse strategiene faller utenfor dette arbeidets problemstilling, ettersom virkemidlene i disse strategiene i liten grad er basert på virkemidler innenfor den digitale sfæren. Det er allikevel viktig å ta disse perspektivene med i betraktningen når en stat utvikler en helthetlig avskrekkingsstrategi, da de kan utgjøre elementer som kan styrke helheten av en nasjonal strategi.

I dette kapittelet har vi systematisk sett på ulike teorier der hensikten er å forstå nasjonalstaten som aktør i det internasjonale systemet. Videre har vi sett på teorier som hjelper oss med å forstå mekanismer i dette systemet og som gir føringer for aktørenes strategiske valg. Til slutt har vi sett nærmere på avskrekkingsteori der vi videre skal anvende ulike avskrekkingsstrategier i spillmodellene der hensikten er å avgjøre i hvilken grad de er anvendelige for en småstat. Før vi er klare for å utvikle spillmodellene, er det viktig å forstå det digitale domenet i konteksten av det internasjonale systemet og avskrekkingsteori. Vi beveger oss i neste kapittel derfor over i å se nærmere på det digitale domenet.

3 Digitalt handlingsrom

3.1 Moderne samfunns sårbarhet

Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren definerer det digitale rom som: *Fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data. Det digitale rom er synonymt begrep med cyberdomenet (2014, s. 4)*. Internett utgjøre den største delen av det digitale rom, men det digitale rom omfatter også systemer som ikke er direkte sammenkoblet med Internett. For systemer som ikke er koblet direkte til Internett kan man i stor grad forutsette at de i dag er indirekte tilkoblet. Alle informasjonssystemer er eksempelvis avhengige av ulike programvareoppdatering og kilden for disse er i dag Internett. Videre er det i de fleste systemer behov for å løfte informasjon inn og ut av systemet. Mye av denne informasjonen kommer fra, eller vil etterhvert ende opp på Internett. Både programvareoppdateringer og informasjon som flyttes fram og tilbake kan således benyttes som en bro mellom de åpne internettet og de indirekte tilkoblede systemene. Dette kan videre benyttes til å introdusere skadevare i systemene, samt å løfte utilsiktet informasjon ut av systemet. Det betyr i praksis at så godt som ingen systemer kan ekskluderes fra det digitale rom og så godt som ingen systemer kan unntas fra de sårbarhetene og truslene som følger av det.

Cyberdomenet er av mange i dag anerkjent som et femte operasjonsdomene, på linje med; land-, sjø-, luft- og rom-domenet (North Atlantic Treaty Organisation, 2016, s. 15). På grunn av dets unge alder preges mye av kunnskapen knyttet til domenet av umodenhet, dette forsterkes ytterlig av at domenet også er under rask utvikling, ikke bare innenfor domenet, men også av selve domenet. Dette avviker fra de tradisjonelle domenene, der selve domenet er statisk og dermed mer forutsigbar ramme enn tilfellet er med cyberdomenet. Domeneperspektivet er heller ikke delt av alle stater. Russland og Kina som begge er betydelige maktfaktorer i det digitale rom, kategoriserer det som informasjonsoperasjoner, eller informasjonskrigføring, samtidig har de ikke etablert et tilsvarende rammeverk der de ser på det digitale domenet som et eget operasjonsdomene (Inkster, 2017, s. 32). Det finnes derfor ikke ett unisont perspektiv på det digitale rom som deles på tvers av alle nasjonalstater.

Hva er det så mennesker kan frykte av aktiviteter i det digitale domenet? Vi har tidligere beskrevet hvordan det digitale domenet er blitt en bærebjelke og en forutsetning for at at det

et moderne samfunn kan fungere. Det moderne mennesket har klart seg uten datamaskiner i tusenvis av år, men har de siste tiårene gjort seg avhengig av det moderne samfunnet som igjen er avhengig av datamaskiner. Fjerner vi datamaskiner fra det moderne samfunnet slutter det å fungere. Et slikt scenario kan starte med at samfunnet mister tilgang til elektrisitet som tar med seg oppvarming, evne til å kjøle og lagre mat utover en dag, dette stopper så drivstoffpumper på bensinstasjoner som medfører at det meste av transport, inklusive tog og fly vil stå i løpet av timer eller dager. Mangelen på evne til å flytte varer og tjenester vil føre til at butikker vil være tomme for varer etter noen dager. Mangelen på elektrisitet vil også føre til at det etter en tid ikke vil være mulig å kommunisere over vesentlige avstander og man vil raskt miste oversikten over tilstanden innenfor en nasjonalstat. Den politiske ledelsen i en nasjonalstat vil ikke kunne danne seg et riktig situasjonsbilde og vil uten tilgang til informasjonsteknologi og kommunikasjonsmidler ha svært dårlig kontroll og svært begrenset evne til å styre og lede mottiltak. Sykehus vil være i stand til å opprettholde prioritert funksjoner en kort tid, men vil etter en tid ikke kunne støtte seg på de teknologiske hjelpemidlene de er avhengige når drivstoff til nødaggregater tar slutt. Politi og forsvarorganisasjoner vil etter en tid ha svært begrenset evne til å kommunisere med befolkningen og seg i mellom. Mangel på drivstoff vil føre til at mobiliteten i samfunnet forsvinner. Evnen til å betale er avhengig av elektrisitet, fysiske penger vil fungere, men det vil ikke være mulig å omsette penger på konto til fysiske penger. Betalingssystemet bryter dermed også sammen. Den tiltakende mangelen på mat kan videre lede til at det oppstår plyndring av det som finnes av mat og andre livsviktige ressurser. Lovløshet bryter ut uten at politi er i stand til å håndtere det. Totalt sett ser vi en kaskade av konsekvenser som river ned byggestenene i det moderne samfunnet og konsekvensen av det hele er kaos.

Scenariet jeg har forsøkt å beskrive over er en kjede av av konsekvenser som oppstår ved å nekte et moderne samfunn elektrisitet. Det faktum at mennesket har levd i tusener av år uten datamaskiner og elektrisitet, og dermed er i stand til å leve uten disse tingene, betyr ikke det samme som en brå overgang tilbake til denne virkeligheten, ikke vil bære med seg menneskelig katastrofe. Sammen med denne menneskelige katastrofen, kan også tilliten til nasjonens øverste ledelse være et offer og kan dermed medføre at hele nasjonalstatens eksistensgrunnlag er svekket. Hvor realistisk er det at en nasjons elektrisitetsforsyning kan rammes gjennom det digitale domenet? I den pågående konflikten mellom Ukraina og Russland har vi sett at vesentlige deler av Ukrainas energiforsyning er tatt ned to ganger. Først i 2015, to dager før julefeiringen, mistet en kvart million ukrainere bosatt i Ivano-Frankivsk-regionen i den vestre delen av Ukraina strømmen. Ukrainsk etterretning har pekt på Russland

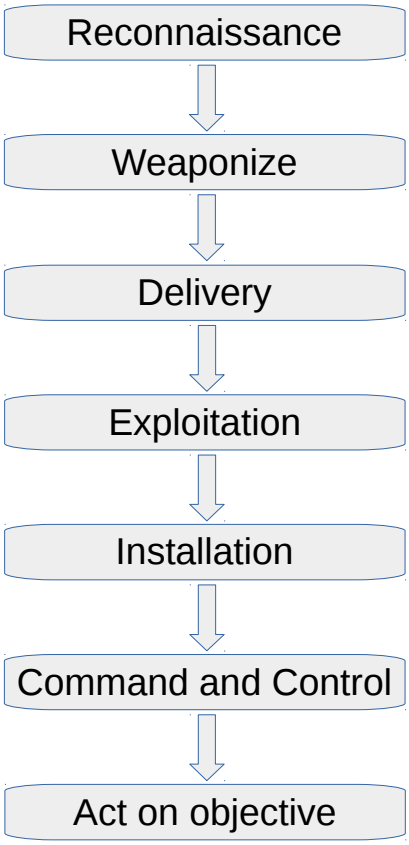
som aktøren, men har ikke vært i stand til å produsere håndfaste bevis. Strømmen var tilbake etter så kort tid som 6 timer, men det skulle ta så lang tid som 2 måneder før de rammede styringssystemene var gjenopprettet. Hovedårsaken til at man var i stand til å gjenopprette strømforsyningen på relativt kort tid tilskrives at den ukrainske strøminfrastrukturen fremdeles kan opereres manuelt (Zetter, 2016). Om lag ett år senere blir Kiev, Ukrainas hovedstat mørklagt, denne gangen kom strømmen tilbake allerede etter en time. Igjen var dette muliggjort av at stasjonen som ble rammet kunne opereres manuelt. Etter nærmere undersøkelse av hendelsen viser det seg at angrepet var langt mer sofistikert enn mørkleggingen som skjedde året før. Det spekuleres også i at aktøren hadde lagt begrensninger på seg selv slik at omfanget ikke skulle bli for stort. I mer vestlig orienterte land er tilsvarende infrastruktur i enda større grad automatisert, og en tilsvarende type angrep ville kunne gitt alvorligere konsekvenser enn tilfellet var i Ukraina. Energisektoren er bare ett av flere sektorer som er blitt rammet i Ukraina de siste årene, andre områder som finans-, media-, transport-, forsvar- og politisk sektor er også blitt rammet (Greenberg, 2017). Enkelte hevder at Ukraina er Russlands treningsfelt for å utvikle og teste sine egne kapasiteter innenfor det digitale domenet. Selv om andre stater ikke er rammet på samme måte som Ukraina, så er det klare indikatorer som tilsier at tilsvarende aktør er i ferd med å etablere seg i vestlige lands kritiske infrastruktur (US-CERT, 2018). Dette har videre ført til offisielle sanksjoner mot Russland (Borger, 2018). Det er derfor sannsynlig at en aktør som Russland er i ferd med å posisjonere seg slik at de også er i stand til å påvirke kritiske infrastruktur i vestlige land. I sluttrapporten fra *Defence Science Board – Task force on Cyber deterrence*, som var utnevnt av det amerikanske forsvarsdepartementet kan vi lese at:

> Although progress is being made to reduce the pervasive cyber vulnerabilities of U.S. critical infrastructure, the unfortunate reality is that, for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructures. The U.S. military itself has a deep and extensive dependence on information technology as well, creating a massive attack surface (2017).

Vi ser altså at USA som av mange regnes som den sterkeste nasjonalstaten i det digitale domenet, anser sin kritiske infrastruktur å være gjennomgående sårbar i forhold til en sofistikert aktør, og peker spesielt på Russland og Kina som aktører med en slik offensiv evne.

Trusselen ser i høyeste grad ut til å være reell ettersom Russland angivelig allerede har forsøkt å infiltrere USAs kritiske infrastruktur og at USA har sanksjonert mot disse handlingene. Paradoksalt nok ser vi altså at den sterkeste aktøren i det internasjonale systemet rammes, som kan tolkes til at realismens påstand om at økt makt gir økt sikkerhet i dag ikke omfatter det digitale domenet på den samme måte.

3.2 Kostnaden av å gjennomføre komplekse operasjoner i det digitale domenet



Illustrasjon 1: Cyber kill chain

Selv om aktiviteter i det digitale rom i mange sammenhenger skjer nærmest umiddelbart, er prosessen knyttet til et målrettet angrep både tidkrevende og ressurskrevende. Den såkalte Cyber kill chain-modellen viser naturlige steg som må gjennomføres før en aktør er i posisjon til å utføre den skadelige handlingen (Yadav & Rao, 2015). Cyber kill chain-modellen gir oss et klart bilde av det store omfanget fra etterretning og analyse av målsystemet til at den ønskede handlingen kan utføres. I det hele tatt er prosessen tidkrevende, ressurskrevende og kunnskapskrevende. Kunnskap om ellers ukjente sårbarheter i datasystemer er ofte en forutsetning der en avansert motstander skal rammes.

Offensive handlinger i det digitale domenet mot en forberedt aktører vil derfor kunne kreve fra flere måneder til år å planlegge og gjennomføre. Når en offensiv aktør først har etablert et brohode i infrastrukturen til målet, kan på en annen side den ødeleggende handlingen gjennomføres akkurat når den offensive aktøren ønsker det.

For å kunne iverksette en handling raskt i det digitale domenet, er det i de fleste tilfeller en forutsetning å ha iverksatt handlinger som gir tilgang til et potensielt mål på et tidlig tidspunkt[3]. Dette gir aktører insentiv til å forsøke å skaffe seg priviligert tilgang i en tidlig fase. Dette har gitt grobunn for aktører som blir referert til som «Advanced persistent threats» (APT). Disse aktørene er ofte antatt å være støttet av en stat og arbeider kontinuerlig med å

3 Det finnes enkelte typer offensive handlinger som tjenestenektangrep som kan gjennomføres mer eller mindre umiddelbart, men denne typen angrep er kun i stand til å oppnå en konsekvens av et begrenset omfang.

opprettholde tilgangen på infrastruktur de allerede har klart å få kontroll over. I tillegg arbeider de kontinuerlig med å skaffe seg tilgang til ny infrastruktur. Mandiant, som er et anerkjent amerikansk sikkerhetsselskap har offentliggjort en detaljert rapport på aktøren APT1 som de identifiserte som en kinesisk aktør etter å ha observert aktiviteten deres nært over en lengre periode. Rapporten avslører at APT1 i snitt opprettholdt sin tilgang til målets infrastruktur i 354 dager, mens det lengste tilfellet var tallet 1764 dager (Mandiant, 2013, s. 3).

Det foregår altså en konstant offensive handlinger i det digitale rom der en vesentlig del av det med stor sannsynlighet er understøttet av en nasjonalstat.

3.3 Under terskelen av væpnet angrep

Illustrasjon 2: Grad av krigshandling

Martin Libicki har utarbeidet en modell som plasserer offensive handlinger mot en annen stat i et spekter der diplomati og atommakt danner to ytterpunktene (2009, s. 29). Cyber ligger her på et sted mellom diplomati og fysisk makt der diplomati på den ene siden benyttes innenfor rammen av fred, mens fysisk makt mellom stater oftest konstituerer en krigshandling. Cyber ligger i grenselandet mellom disse to, der det på den ene siden eksisterer en rekke offensive handlinger som havner under terskelen for en krigshandling, mens det også i det øvre spekteret av cyber finnes handlinger som kan kategoriserer som et væpnet angrep. Det er internasjonal enighet om at krigens folkerett også gjelder for operasjoner i det digitale rom, samtidig er ikke dette alltid helt uproblematisk da folkeretten ikke er utviklet med operasjoner i digitale rom i tankene. For å passere terskelen for hva som kan regnes som et væpnet angrep i det digitale rom, stiller folkeretten krav at til at angrepet forårsaker død eller skade på personell eller skade eller ødeleggelse på objekter (Forsvarets høgskole, 2013, s. 189–190) (Schmitt & NATO Cooperative Cyber Defence Centre of Excellence., 2017, s. 375). Krigens folkerett gir dermed betydelig rom for operasjoner under terskelen av en krigshandling og gir med dette insentiver for at nasjonalstater bygger opp kapasiteter for å utnytte dette handlingsrommet til sin fordel. I 2007 ble Estland rammet av et stort tjenestenektangrep[4] som lammet landets myndigheter og finansinstitusjoner. Etter noen dager ble landet tvunget til å koble ned sine forbindelser til

4 Et tjenestenektangrep er en enkel form for angrep i det digitale domenet som potensielt kan gjøre felles tjenester utilgjenglige ved å oversvømme denne med forespørsler.

Internett for å gjenopprette tilgang til tjenester innenfor landet (Libicki, 2016, s. 11). Selv et angrep med denne konsekvensen førte ikke til at NATO iverksatte en straffereaksjon (Kello, 2017, s. 203). Det var usikkerhet knyttet til om det var den russiske staten, russiske innbyggere eller russiske innbyggere i Estland som sto bak angrepene. En indikator på hvem som sto bak ser man muligens ved å observere at Georgia, allerede året etter ble rammet at tilsvarende type angrep, like før russiske styrker beveget seg inn i Sør-Ossetia.

Stormaktene har spesielt gode forutsetninger for å operere under terskelen for hva som vil tolkes som et væpnet angrep. Deres relative styrke innenfor mer tradisjonelle militære maktdisipliner gir en lav risiko for at aktørene de operer mot vil risikere å eskalere situasjonen inn i de fysiske domenene. Lav risiko betyr derimot ikke det samme som ingen risiko. President Trump har den senere tiden igangsatt tiltak i retning av en handelskrig mot Kina som svar på urettferdig handelspraksis, tyveri av intellektuell eiendom[5] og cyberangrep (Fullerton, 2018). Vi ser at USA altså svarer med økonomiske mottiltak, hvorvidt de også svarer med tiltak i det digitale rom finnes det ingen uttalt trussel om, eller indikasjoner på. Sanksjonene mot både Kina og Russland viser at begge aktører driver betydelig aktivitet i det digitale rom mot USA, som totalt sett er antatt å være den sterkeste aktøren i det digitale domenet. Når stormaktene tillater seg et så stort handlingsrom ovenfor hverandre, må vi samtidig gå ut ifra at de ikke legger spesielle begrensinger på seg selv ovenfor å operere mot mindre stater, skulle de ha en interesse av det.

Ukrainakrisen sammen med USAs reaksjon på det de hevder er Russiske forsøk på å infiltrere energiforsyningsinfrastrukturen i USA, peker også i retning av at det er en bevissthet hos statsledere om at det er mulig å skade en nasjonalstat gjennom bruk av makt i det digitale rommet. Realister mener at makt er selve valutaen i det internasjonalse systemet (Dunne, Kurki, & Smith, 2013, s. 77). Det har alltid vært i staters interesse å ha kunnskap om hvor mye makt andre nasjoner besitter. For størstedelen av historien har tendensen vært at stater hemmeligholder slik informasjon, mens i løpet av den kalde krigen har deling av slik informasjon blitt viktig for å beroliggjøre den andre parten om at et strategisk overfall ikke er i ferd med å skje (Inkster, 2017, s. 28). Dette har vært praktisert i forhold til både atomvåpen og konvensjonelle våpen. Digitale kapasiteter og -våpen er på en annen side vanskelig å måle og kvantifisere på meningsfulle måter. Et digitalt våpen kan i stor grad miste sin verdi hvis det vises fram, ettersom den andre aktøren i praksis blir satt på sporet av hva han bør beskytte seg mot og kan iverksette mottiltak. Framveksten av det digitale domenet har dermed introdusert

5 Tyveri av intellektuell eiendom foregår også i stor grad gjennom det digitale rom. General Keith Alexander, US Cyber Command uttalte at den pågående blødningen av industrielle hemmeligheter er den «største overføringen av rikdom i historien» (Jon R. Lindsay, Tai Ming Cheung, 2015)

ny kompleksitet knyttet til det å måle en nasjonalstats makt. Dette gir videre utfordringer knyttet til det å etablere en avskrekkingsevne i det digitale domenet. Hvordan kommuniserer man at man har en evne uten å samtidig å svekke den? Hvis vi ser på hvordan denne avskrekkingen ble etablert innenfor atommakt, var prøvesprengninger avgjørende for å demonstrere den ødeleggende evnen. Videre viste ballistiske missiler med evne til å løfte satellitter ut i rommet, at atomvåpnene kunne leveres hvor som helst på jordens overflate uten at det var mulig å forsvare seg. I det digitale rom finnes det ikke en ekvivalent til en atombombe på et ballistisk missil. Det finnes altså ikke en digital ladning som vil kunne ødelegge det den pekes mot og det finnes ikke en universal transportmetode som vil bære det digitale våpenet gjennom digitale- brannmurer og sikringstiltak for å ramme målet med den universelle digitale ladningen. Et angrep gjennom det digitale rommet ligner langt mere på en spesialoperasjon der et spesialtrent mannskap etter en tids rekognosering og trening forsøker å trenge seg usett inn i en infrastruktur for å plassere spesialtilpassede ladninger som vil kunne ramme det aktuelle målet. Et eksempel på dette er Stuxnet, skadevaren som ødela sentrifuger som anriket Uran på Natanz fasiltiten i Iran. Denne skadevaren ble oppdaget på et tidspunkt da den hadde infisert over 100 000 tilfeldige datamaskiner tilknyttet internett (Libicki, 2016). I starten var det uklart hva denne skadevaren hadde som hensikt da det ikke var åpenbart om den gjorde noe i det hele tatt mot de infiserte maskinene. Senere ble det kjent at skadevaren var spesialutviklet for å nå et helt konkret mål, anrikingssentrifugene i Natanz, og var dermed helt ufarlig for den store majoriteten av datamaskinene som ble rammet.
Hvis vi så ser på helheten av dette, kan vi påstå at ulikhetene mellom atommakt og makt i det digitale rom er langt større enn likhetene. Det vil også kunne bety at avskrekking innenfor det digitale domenet også vil være annerledes, som vi nå skal se litt nærmere på.

3.4 Attribusjonsproblemet

Attribusjon er et område som skaper særskilte utfordringer i det digitale rom. Det åpne internettet skaper forutsetninger for at enhver aktør kan operere ut ifra infrastruktur i ett annet land enn det aktøren selv opererer fra eller representerer. Dette kan gjøre det vanskelig å avgjøre med sikkerhet hvilken aktør som står bak de faktiske handlingene. Evnen til å attribuere med sikkerhet utgjør for en avskrekkingsstrategi forskjellen mellom å kunne kommunisere, «ikke gjør dette», mot noe som sier, «ikke bli tatt hvis du gjør dette» (Libicki, 2016, Kapittel 23). Evne til å attribuere blir dermed en forutsetning for en troverdig avskrekkingsevne samtidig som feilattribuering kan føre med seg egne problemer. Eskalering ved uhell er en vesentlig risiko i dette domenet (Borghard & Lonergan, 2017, s. 457). På et mellomstatlig nivå kan det få svært uønskede konsekvenser om man iverksetter

gjengeldelsestiltak mot feil aktør, eller lar være å utføre avskrekkingtiltaket med bakgrunn i «plausible deniability». Det vil i det første tilfellet bety en uønsket eskalering, i det andre tilfellet tap av troverdigheten i avskrekkingsstrategien. For en småstat er det ikke nok å være overbevist om at man har rett, men er også helt avhengig av å kunne bevise at man har rett ovenfor alliansepartnere, ettersom disse kan bli trukket inn i en eventuell eskalering av situasjonen. Hvis eksempelvis en småstat velger å gjengjelde en offensiv handling i det digitale rom mot en stormakt uten tilstrekkelige bevis, kan det åpne for at småstaten i praksis eskalerer situasjonen og skaper en bilateral konflikt der alliansepartnere kan ende opp med å vurdere at det var deres eget alliansemedlem som skapte konflikten. Attribusjonsutfordringen åpner også for at en tredjepart kan agere som en annen aktør for å sette i gang en konfrontasjon mellom to stater. En offensiv avskrekkingstrategi (avskrekking gjennom straff) kan derfor være risikabel og kontraproduktiv, om den defensive staten ikke har en sterk evne til å attribuere de handlingene som er over terskelen for å iverksette en gjengjeldelse. Siden det er forskjell på å utpeke en aktør basert på motiver og det å bevise at den samme aktøren var den som utførte handlingen, er attribusjonproblemet en sentral problemstillingen i forhold til å ha en troverdig avskrekkingsstrategi. Sammenligner vi det med for eksempel forutsetninger atommakt har i forhold til attribusjon er det her for det første ni stater som besitter atomvåpen og opphavet til våpnene kan i stor grad identifiseres gjennom isotopiske indikatorer (Nye, 2017, s. 50). Attribusjonsproblemet er derfor i stor grad spesielt krevende i det digitale rom, videre undergraver dette troverdigheten av en strategi basert på avskrekking gjennom straff.

3.5 Offensivens domene

> In cyberspace, the offense has the upper hand. The Internet was designed to be collaborative and rapidly expandable and to have low barriers to technological innovation; security and identity management, were lower priorities. For these structural reasons, the U.S. government's ability to defend its networks always lags behind its adversaries' ability to exploit U.S networks' weaknesses (Lynn, 2010, s. 99)

Det er altså klart at en strategi basert på avskrekking gjennom straff har sine særegne utfordringer i det digitale domenet. På en annen side, hvis Lynns påstand om at det digitale rom favoriserer offensiven er riktig, bør det også eksistere utfordringer knyttet til en

avskrekkingstrategi basert på nektelse, som i all hovedsakt baserer seg på defensive tiltak, som dermed vil være underlegne de offensive.
En nektelsesbasert beskyttelse av kritisk infrastruktur kan være kostbart og ineffektivt når man betrakter omfanget av det som skal beskyttes. Dette fører til at man stå ovenfor en situasjon der kostnadene kan bli uakseptabelt store, uten at de garanterer for at strategien er effektiv. For en småstat kan den totale risikoen allikevel vise seg å være lavere gjennom at en slik strategi fjerner muligheten for feilattriburing og gjengjelde mot feil aktør. For en småstat vil det være svært uheldig å gjengjelde mot en stormakt, spesielt om den aktuelle aktøren er geografisk plassert for å gjenghelde handlingene gjennom et av de fysiske domenene. Geopolitikk påvirker altså handlingsrommet innenfor det digitale domenet. Småstaten kan potensielt risikere å ende opp i et bilateral konflikt, der dens allierte partnere vurderer at alliansepartneren selv er skyld i eskaleringen og dermed lar han stå alene.
På den andre siden finnes det også skeptikere som tviler på det digitale domenet favoriserer offensiven gjennom å poengtere at et målrettet angrep med stor virkningsgrad vil være så kostbart å gjennomføre at sannsynligheten for at det skjer er lav (Kello, 2017, s. 59). Denne kostnaden, som vi også har sett i cyber-kill-chain-modelen, tilser at å maksimere denne kostnaden ytterligere er et mulig konsept for en effektiv nektelsesstategi.

Det synes tydelig at det er vesentlige ulikheter mellom avskrekking i det digitale rom, og mer tradisjonell avskrekking gjennom atomvåpen, eller konvensjonelle våpen. Den vesentligste faktoren er attribusjonsproblemet, men det er også et vesentlig problem knyttet til at en straffereaksjon oftest vil være tidkrevende å realisere. Det siste kan lede til at aktøren som utløste straffereaksjonen ikke nødvendigvis vil kunne se på den som en straffereaksjon til sin egen handling. Denne uklarheten kan forsterkes ytterligere ved at det i det digitale domenet nærmest er en konstant offensiv aktivitet, spesielt mot systemer tilknyttet Internett. Den store majoriteten av denne aktiviteten er lite sofistikert og oppleves nærmest som en støy, men denne tilstanden er med på å lage et bilde av bare gråtoner, som igjen kan gjøre det vanskelig å skille den konstante pågående aktiviteten fra aktivitet som er ment som en straffereaksjon fra en nasjonalstat mot en annen. Eller et sofistikert forsøk på infiltrasjon av kritisk infrastruktur.

Vi har tidligere sett på snøballeffekten som bryter ned det moderne samfunnet om eksempelvis energiforsyningen faller bort. Konsekvensene er store, samtidig er det grunn til å stille spørsmål til om et angrep gjennom det digitale rom kan gjøre så ugjenkallelig skade, eller om situasjonen alltid vil begrense seg til det vi har sett i Ukraina der

elektrisitetsforsyningen ble gjenopprettet etter timer. Hva som er realistisk er likevel ikke av like stor betydning som hva som er den kognitive oppfattelsen av trusselen i konteksten av avskrekking. Det essensielle er som vi har sett å kunne skape en kognitiv frykt for konsekvensene, ettersom det er denne oppfattelse som til slutt påvirker kost-nytte-analysen hos aktøren som skal avskrekkes. Hvis vi benytter amerikansk etterretnings trusselvurderinger som et referansepunkt, så er det mulig å observere at trussel gjennom det digitale domenet ikke er nevnt så kort tid tilbake som i 2007, mens i 2015 er det rangert som den største trusselen (Nye, 2017, s. 45). Det underbygger at det over få år har skjedd en stor endring i oppfattelsen av potensialet av konsekvensene denne trusselen representerer.

3.6 Småstatens forutsetninger

> ... in the cyber domain some animals are, in the words of George Orwell, more equal than others, and cyber power is only really meaningful when it is taken together with other means for exercising and projecting influence (Inkster, 2017, s. 32)

Hva kan så en småstat håpe på å oppnå? Hvis vi er på Inksters betraktning om at cybermakt gir mening om man kombinerer med andre virkemidler, synes det også slik at dette ytterligere er i disfavør småstaten. Det vil være utfordrende for en småstat å kombinere det med tradisjonelle former for militærmakt da man må forutsette at han er underlegen større aktører. Vi har sett at avskrekking gjennom straff er en utfordrende strategi for alle aktører, men spesielt utfordrende for småstater med tanke på faren for å utilsiktet eskalere situasjonen.

Avskrekking gjennom nektelse er en langt mer tiltalende strategi for småstaten ettersom faren for en uønsket eskalering er betydelig lavere, samtidig er det vanskeligere å skape en troverdig avskrekking da ser ut som det eksisterer en generell aksept for at det digitale domenet favoriserer offensiven. Fokus på en nektelsestrategi må derfor være å maksimere den opplevde kostnaden for den offensive aktøren. En måte å maksimere den offensive aktørens kostnad er en strategi der nektelse kombineres med avledning (Heckman, Stech, Schmoker, & Thomas, 2015). En kombinasjon av nektelse og avledning kan lede den offensive aktøren til å bruke vesentlige ressurser konstruerte blindspor, samtidig som dette gir den defensive parten en god forutsetning for å analysere den offensive aktørens metoder og virkemidler. Hvis den defensive aktøren i tillegg åpent deler den offensive aktørens metoder og virkemidler vil dette

i vesentlig grad kunne avvæpne den offensive aktøren ettersom andre da kan beskytte sin ressurser mot denne type offensiv virksomhet. Hvorvidt denne nektelsesstrategien har potensiale til å påføre den offensive aktøren en uakseptabel kostnad vil avhenge av en rekke variabler og kan ikke generaliseres. En av de vesentlige variablene er evne og kapasitet hos den defensive aktøren til å utføre en slik strategi og vanskelighetsgraden ved å lykkes med en slik strategi kan lett undervurderes. Målet er uansett å bygge opp en defensiv kapasitet basert på nektelse og avledning som kan tippe offensiv-defensiv balansen i fordel for defensiven ved å avlede, analysere og avvæpne offensive aktører. Ulempen med en slik transparent strategi er at den kan kompromittere den defensive kapasiteten i nektelsestrategien og gi den offensive aktøren hint om hvilke metoder han bør satse på. På den andre siden er «security through obscurity»[6] en sikkerhetsstrategi som etterhvert har stor anerkjennelse for å være feilslått i datasikkerhetssammenheng. De store aktørene innfor IKT-tjenester har i stor grad beveget seg fra en praksis der de har møtt personer som har påpekt svakheter i sikkerhetsimplementasjoner med søksmål (Meunier, 2006), til i dag å dele ut generøse belønninger for det samme (Finkle, 2016). Konsekvensen er at sikkerheten i systemer i dag er langt bedre, samtidig er det en etablert sannhet blant de fleste sikkerhetseksperter at komplekse datasystemer alltid vil ha sikkerhetsutfordringer. Angrepsflaten og trusselen mot den vil dermed fortsatt være der, på tross av teknologiske framskritt.

3.7 Avskrekkingsstrategier

I neste del skal vi se nærmere på hvilke handlingsalternativer vi finner innenfor de to strategiene avskrekking gjennom straff, og - nektelse i det digitale rom. Problemstillingen binder oss til å se på relevante avskrekkingvirkemidler som implementeres gjennom det digitale domenet.

3.7.1 Avskrekking gjennom straff i det digitale domenet

Avskrekking gjennom straff i det digitale domenet forutsetter for det første at det finnes gode angripelige mål, dernest må det være mulig å skape en tilstrekkelig konsekvens ved å ramme disse målene. Hvis vi først vurderer tilgangen på gode mål er det her tildels store forskjeller mellom nasjonene. Land med et lavt teknologisk utviklingsnivå vil knapt være mulig å ramme, mens et høyteknologisk land har antageligvis et utvalg av mål som vil gi en markant

6 Security through obscurity – handler om å ivareta sikkerhet gjennom å tilsløre hvordan ting fungerer. I dag er det bred enighet om at dette er en feilslått strategi. Sikkerhetsmekanismer skal tåle dagens lys, og at deling kan bidra til å forberede sikkerheten ved at flere kan bidra til å identifisere og utbedre svakheter.

konsekvens hvis de rammes. Hvis vi tar den beste forutsetningen og har et mål om å avskrekke en nasjon med et høyteknologisk moderne samfunn, er det flere forhold skaper utfordringer i forhold til å lykkes med å gjennomføre en hurtig og målrettet gjengjeldelse. For det første har IKT-systemer en begrenset levetid og byttes ut hyppig. I tillegg er det vanlig praksis å gjennomføre sikkerhetsoppgradering av programvare regelmessig. Dette fører til at de potensielle målene er i stadig endring (Libicki, 2016, Kapittel 25). Konsekvensen av dette er at terrenget en offensiv aktør vil operere i endrer seg. Det blir dermed svært usikkert i hvilken grad det er mulig å forehåndsidentifisere gode angripelige mål. Hvis det er slik at man avdekker et angripelig mål må det ha tilstrekkelig konsekvens å ramme det, slik at det kan påvirke kost-nytte vurderingen til denne aktøren i tilstrekkelig grad. Hvis vi trekker paralleller til luftmakt der Gen. Giulio Douhet som tidlig argumenterte for at strategisk luftmakt ville kunne undergrave en nasjons evne til å føre krig ved å straffe befolkningen. Strategisk luftmakt og bombing av byer så etterhvert bred anvendelse under den andre verdenskrig, uten at det gav den forutsette effekten (Borghard & Lonergan, 2017, s. 477). Denne bombingen kan bedre kategoriseres som tvangsmakt, men eksempelet illustrerer at avskrekkingsmiddelet antageligvis må ha en svært høy konsekvens om det skal påvirke kost-nytte vurderingen til den som kan bli rammet. Hvis vi samtidig vurderer avskrekking med atomvåpen, er det lett å se at når en stat ved å bruke atomvåpen kan risikere å utslette seg selv i prosessen, er det en kraftfull konsekvens som har langt bedre forutsetninger for å påvirke denne statens kost-nytte-analyse i ønsket retning . Vi har sett at det finnes et betydelig skadepotensiale som kan oppnås gjennom det digitale domenet, men det er klart at empiri fra de fysiske domenet legger listen svært høyt for hva som er tilstrekkelig straff for å avskrekke eller tvinge.

3.7.2 Avskrekking gjennom nektelse i det digitale domenet

I sin enkleste form kan avskrekking gjennom nektelse være å sikre og overvåke alle systemer på en så god måte at alle forsøk på inntrengning er nytteløse, eller vil kunne avverges i tid. Det handler altså om å bygge en form for forsvarsmur rundt alle systemer som er så sterk at det vil oppleves som nytteløst for alle som har kartlagt muren. En slik tilnærming til å forsvare kritisk infrastruktur i det digitale domenet kan se enkelt og attraktivt ut. Utfordringen med denne tilnærmingen er at utbredelsen og kompleksiteten på den kritiske infrastrukturen kan gjøre det urealistisk å lage en mur som har forutsetning for å ivareta alt. Kostnaden for en offensiv aktør for å patruljere denne digitale muren for å finne eventuelle svakheter er også lav (Libicki, 2016, Kapittel 26). Hvis vi igjen trekker fram Douhet, er et av hans mest kjente sitater at «the bomber will always get through» dette er også en relevant påstand når det

kommer til å forsvare digital infrastruktur. Som forsvarer må man lykkes i å stoppe alle angrep, som angriper trenger man potensielt kun lykkes en gang. Dette gir dermed gode insentiver for den offensive parten til å fortsette å prøve.
Hvis vi ser utover denne enkle tilnærmingen finnes det metoder som kan øke kostnaden og usikkerheten hos den offensive aktøren. Et eksempel på dette er at det implementeres fabrikerte sårbarheter i tilknytning til den kritiske infrastrukturen som avleder og binder opp sofistikerte offensive aktører. Når en aktør forsøker å utnytte en slik fabrikkert sårbarhet, vil den forsvarende parten umiddelbart kunne bli varslet og kan monitorere og analysere den offensive aktørens metoder og virkemidler. Her vil forsvareren også kunne binde opp den offensive aktøren over lengre tid og gi aktøren en opplevelse av at den har lykkes i å infiltrere infrastrukturen. Ettersom den defensive aktøren lærer om den offensive aktørens metoder og virkemidler, kan denne informasjonen deles med tredjeparter i den hensikt å «avvæpne» den offensive aktøren. En slik nektelsesstrategi vil kunne påføre den offensive aktøren økte kostnader knyttet til ressursbruk og introdusere usikkerhet om hvorvidt aktøren egentlig har lykkes å infiltrere den defensive partens virkelige infrastruktur, eller er lokket inn i en avledning.

3.7.3 Oppsummering av avskrekkingsstrategier

For å oppsummere og kategorisere relevante avskrekkingsstrategier ut ifra drøftingen ser vi først en strategi basert på straff. Denne strategien forutsetter at den defensive aktøren etablerer en kapasitet til å attribuere og slå hardt tilbake mot et offensiv aktør som har passert grensen for hva den defensive parten aksepterer.
Nummer to er en ren nektelsestrategi der den defensive aktøren klarer å etablere en infrastruktur som er så motstandsdyktig mot offensive operasjoner, at aktørene som opererer mot den, vil konkludere med at det er sløsing med ressurser. Denne strategien har ingen konkrete virkemidler til å slå tilbake mot en offensiv aktør innenfor det digitale domenet.
Til slutt har vi sett på en strategi basert på nektelse og avledning, som har til å hensikt å maksimere kostnaden av offensive operasjoner i det digitale domenet for en avansert aktør.

4 Metode

Valget av spillteori som kjernen i denne studiens metode er basert på at dagens situasjonen i det digitale rom har likheter til situasjonen man sto ovenfor på 60-tallet med atomvåpen. I begge tilfeller eksisterte det en strategisk kapasitet med stor betydning for nasjonal sikkerhet, samtidig er det ikke umiddelbart klart hvordan kapasiteten best passer inn i en nasjonal sikkerhetsstrategi. Den nye kapasiteten var den gang som i dette tilfellet, ulik alt som hadde eksistert tidligere. Mangelen på empiri gir dermed utfordringer når man skal utvikle teori. Spillteori ble den gang videreutviklet og brukt for å underbygge avskrekkingsteori som igjen er grunnlaget for den amerikanske atomstrategien. Denne strategien har så langt opprettholdt sine målsettinger. Det er derfor interessant å se hva en spillteoretisk analyse kan gi av svar for å understøtte et svar på denne studiens problemstilling som har tilsvarende empiriske forutsetninger, men er et annet problem med ulike forutsetninger.
Kapittelet introduserer og forklarer den spillteoretiske metoden. I denne delen skal vi beskrive en spillmodell som reflekterer aktørene og deres preferanser relatert til det digitale domenet og dets særegenheter. Hensikten med spillmodellen er helt konkret å teste de utvalgte avskrekkingsstrategiene og belyse de ulike utfallene det kan ha for en småstat å implementere dem. Dette vil danne et grunnlag for å vurdere hvorvidt avskrekkingsstrategien kan understøtte småstatens strategiske målsetting.

Avskrekkingsstrategiene blir således hypoteser som vi tester ved hjelp av spillteori og analyserer opp i mot den evnen hver av hypotesene har for å understøtte småstatens målsetting.

4.1 Spillteori

Spillteori er teorien om interaksjon mellom rasjonelle aktører (Hovi, 2008, s. 11). Litt mer konkret kan vi si at det er et studie av matematiske modeller som forsøker å gjenspeile konflikt og samarbeid mellom intelligente og rasjonelle aktører og som har til hensikt å identifisere kvaliteter ved ulike strategier. Spillteori har sitt opphav hos John Von Neumann og Oskar Morgenstern som publiserte boken *The_theory of games and economic behaviour* i 1944. Et spill i denne sammenhengen er en interaksjon mellom to eller flere aktører hvor aktørene står ovenfor ulike definerte valg, som hver for seg gir ulik gevinst for aktøren. Spillteori kan anvendes innenfor en rekke ulike disipliner, slik som statsvitenskap, sosiologi, økonomi, kybernetikk, militærstrategi og internasjonal politikk. Rasjonell i denne

sammenhengen betyr at aktørene har til hensikt å optimalisere sin egen gevinst. Gevinsten henger sammen med det vi har identifisert som aktørens strategiske målsetting og ettersom aktørene i denne oppgaven er nasjonalstater, kan vi ved å støtte oss på realismeteori innenfor internasjonal politikk for å forstå en stats sikkerhetspolitiske målsetting.

For å kunne anvende spillteorien så må vi også forstå hvilke ulike handlemåter aktørene og dermed hvilke valgmuligheter som finnes i spillet. Vi må også analysere situasjonen for å klassifisere hvilken type spill vi analyserer. Her har vi allerede avdekket de vesentlige forholdene gjennom avskrekkingsteori og relevante egenskaper ved det digitale domenet som hjelper oss å forstå hvilke handlingsalternativer som er mulig.

Innenfor spillteori har det utviklet seg ulike grener som er tilpasset å løse ulike typer strategiske situasjoner. Vi kan dele opp disse grenene i to hovedkategorier, statiske spill og dynamiske spill. Hver av disse to hovedgrenene kan vi igjen delen inn i spill med fullstendig informasjon og spill med ufullstendig informasjon.
Analysen av spillene har som hensikt å avdekke likevekter. Spillteorien operer med et til dels stort antall likevektsbegreper. De fleste er basert på Nash-likevekten som er utviklet for statiske spill med fullstendig informasjon av nobelprisvinner i økonomi, John Nash. Andre relevante likevektsbegreper er delspilllperfekt likevekt og bayesiansk likevekt.

	Statiske spill	Dynamiske spill
Fullstendig informasjon	Nash-likevekt	Delspillperfekt likevekt
Ufullstendig informasjon	Bayesiansk Nash-likevekt	Bayesiansk perfekt likevekt

Tabell 1: Oversikt over ulike likevekter innenfor spillteorien

En Nash-likevekt er et valg der en individuell spiller ikke kan oppnå et bedre resultat ved å endre sin strategi, forutsatt att alle de andre spillernes valg er konstante (Bennett, 1995, s. 23). Delspillperfekt likevekt er en videre raffinering av Nash-likevekt og benyttes typisk i dynamiske spill sammen med baklengs induksjon for å finne spillets løsning (Stone, 2001, s. 221).
Vi skal senere benytte oss av delspillperfekt likevekt når vi analyserer modellene i denne studien.

Hvis man skal benytte spillteori for å analysere en strategisk situasjon må man først avklare hvilken type spill som skal analyseres.

En spillteoretisk analyse består i følge Jon Hovi av (2008, s. 27):
1. Hvem er spillere?
2. Hvilke handlingsvalg kan spillere foreta?
3. I hvilken rekkefølge foretar spillerne sine valg?
4. Hvilken informasjon har aktørene når de velger handlinger?
5. Hvilke resultater (utfall) følger av bestemte kombinasjoner av handlinger?
6. Hvilke preferanser har aktørene over spillets mulige utfall?
7. Kan aktørene fremsette endelige selvbindinger, herunder inngå bindende avtaler?
8. Hva er spillets likevekter?
9. Hvilken likevekt er spillets «løsning»?
10. (Er løsningen pareto-optimal?)[7]

Trinn 1 – 7 omfatter her modellbeskrivelsen, mens trinnene 8 – 10 representerer selve analysen av spillet.

Vi avklarer altså først hvem som er aktører (spillere). Noen eksempler på aktører kan være individer, stater, koalisjoner eller firma. Forutsetningen er at det er mulig å identifisere aktørenes målsetting og at de forfølger denne målsettingen på en rasjonell måte. I enkelte typer spill, kan det også være aktuelt å inkludere en ekstra aktør som representerer eksterne usikkerhetsfaktorer som påvirker spillet.
Når spillerne er identifisert er det naturlig å vurdere hvilke handlingsvalg de kan foreta, samt hvilken rekkefølge disse valgene foretas i . Tas valgene av begge spillerne samtidig, eller foretas valgene i sekvens? Hvorvidt spillerne foretar valgene samtidig eller i sekvens påvirker også hvilken informasjon de baserer disse valgene på. Informasjonen spillerne har på det tidspunktet de foretar valgene er avgjørende for hvilke valg som er preferert.

Videre må vi også ta stilling til hvilket utfall hvert av valgene vil lede til og hvilke preferanse de ulike spillerne har til de ulike utfallene. Her er det ofte tilstrekkelig å rangere spillernes preferanse fra høyst til lavest. Gevinsten reflekterer preferansen der høyeste poengsum tilsvarer høyeste preferanse. Til slutt vurderes andre forhold som kan påvirke spillet som

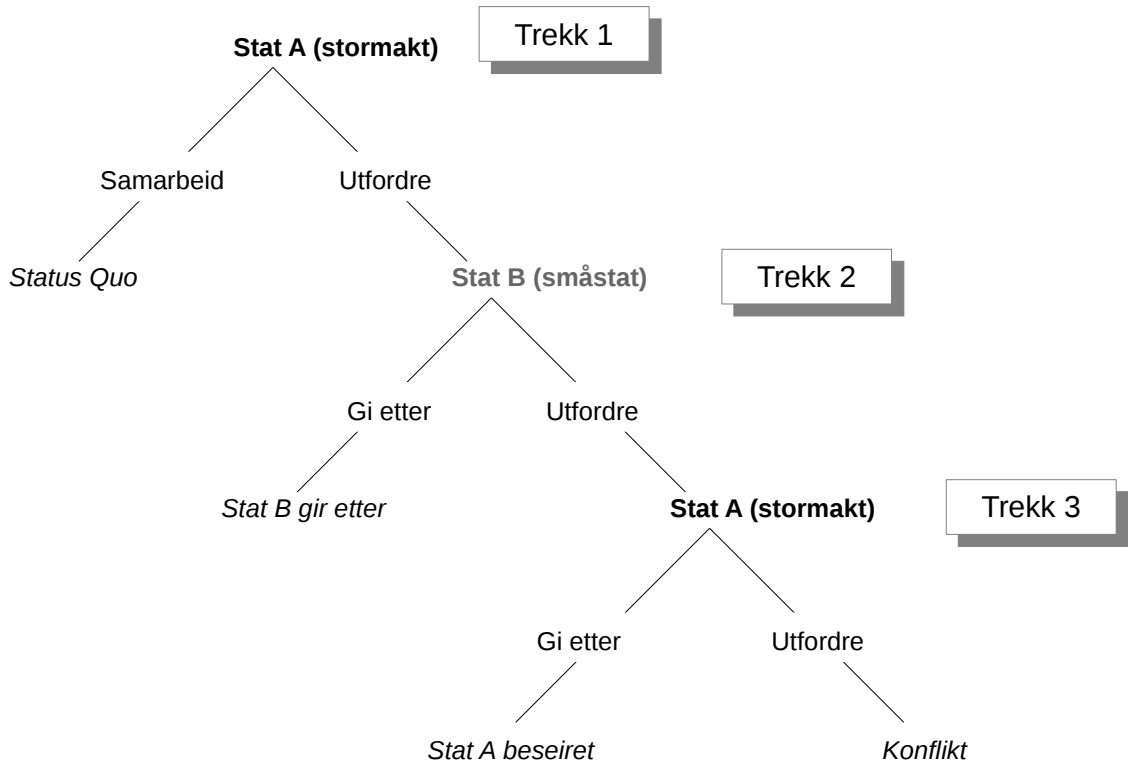
7 Pareto-optimalitet er et konsept knyttet til samarbeidsspill og er ikke relevant i denne studien.

selvbindinger og avtaler[8]. Slike avtaler kan eksempelvis lede til at det ikke vil være mulig å velge konkrete strategier som bryter med disse avtalene (Bennett, 1995, s. 27).
Denne delen av analysen danner altså grunnlaget for selve modellen som representerer spillet, mens resten av analysen handler om å løse spillet ved å identifisere likevekter for så å avklare hva som er spillets løsning. Denne danner videre grunlaget for en drøfting om hvorvidt spillet peker på en relevant strategi for en småstat.

4.2 Konseptuell modell for å analysere en småstats avskrekkingsevne.

Vi skal nå beskrive den overordnede modellen vi skal benytte i analysen av de ulike avskrekkingsstrategiene.
Først må vi avklare hvem som er aktørene i modellen. Her er de to sentrale aktørene to nasjonalstater der Stat A representerer stormakten og Stat B representerer småstaten. Utover dette kunne det ha vært aktuelt å trekke inn en tredje aktør som representerer en allianse, eller en alliert av småstaten ettersom vi ut ifra teorien har sett at småstater tenderer til å balanserer mot andre stater og danne forsvarsallianser for å ivareta sin sikkerhet. Argumentet mot at dette er nødvendig henger sammen med at vi ser at man innenfor det digitale domenet opererer under terskelen av det som regnes som et væpnet angrep. Konsekvensen av dette er at en forsvarsallianser sannsynligvis ikke er villige til å anvende makt før et væpnet angrep er et faktum. Modellen vil dermed begrenses til to aktører, en stormakt (Stat A) og en småstat (Stat B).
Vi forutsetter ved spillets start at småstaten allerede har implementert en avskrekkingsstrategi. Stormakten står derfor ovenfor spillets første valg som handler enten å opprettholde status-quo eller ønsker å utfordre småstaten og samtidig trosse avskrekkingsmiddelet. Forutsatt at Stat A velger å utfordre, og at småstaten på et senere tidspunkt avdekker at stormakten har krysset grensen som er satt for å benytte avskrekkingsmiddelet må småstaten ta stilling til om den ønsker å realisere det den har truet med eller å gi etter. Hvis småstaten i dette trekket velger å utfordre stormakten ved å å gjennomføre avskrekkingstiltaket vil det etter dette være stormakten som igjen velger hvordan om han ønsker å besvare denne reaksjonen.
Ut ifra dynamikken i disse trekkene ser vi at vi står ovenfor et sekvensielt spill der stormakten (Stat A) velger det første trekket ettersom småstatens strategiske målsetting er å opprettholde status-quo og dermed preferer utgangstilstanden.

8 Selvbindinger eller avtaler er ikke inkludert i modellene i denne studien.



Illustrasjon 3: Unilateralt avskrekkingsspill i ekstensiv form

Sekvensielle spill modelleres ofte i en ekstensiv form som gir en beskrivende illustrasjon av hvilken aktør som velger handlemåte i hvert trekk og hvilke handlemåter det er mulig å velge mellom. Modellen som er illustrert over beskriver således aktørene, hvilken rekkefølge trekkene foretas i og hvilke handlingsalternativ aktørene kan velge mellom i hvert trekk.

Spillet viser de to aktørene Stat A som representerer stormakten som står ovenfor det første valget om hvorvidt den ønsker å utfordre den mindre staten som er representert av Stat B. I første trekk ser vi altså at stormakten - Stat A, står oven et valg mellom å opprettholde en normaltilstand (Status quo) med den svakere Stat B. Hvis Stat A velger å utfordre Stat B i dette trekket har i praksis avskrekkingen feilet. Det andre trekket skal så utføres av Stat B har to valgmuligheter; gi etter ved å etterkomme Stat A sitt krav, eller utfordre Stat A gjennom å realisere avskrekkingsmiddelet. Hvis Stat B velger å gi etter, har Stat A oppnådd sin målsetting med minimum av anstrengelse. Dette er typisk det optimale utfallet for Stat A samtidig som Stat B har undergravd troverdigheten av eget avskrekkingsmiddel som i praksis kan bety en høyere risiko for å bli utfordret i framtiden. Hvis Stat B heller velger å utfordre Stat A ved å effektuere avskrekkingsmiddelet betyr det at Stat B har tatt en avgjørelse som har stort potensiale for å eskalere situasjonen. I det tredje trekket er det avgjort at Stat A ikke har oppnådd sin optimale løsning ettersom valget nå står mellom å gi etter for en svakere part,

eller eskalere til konflikt. Det å gi etter for den svakere parten på dette tidspunktet vil eksempelvis kunne føre til tap av anerkjennelse og respekt i det internasjonale systemet. Hvis den sterkere Stat A velger å etablere konflikt, kan det også være mindre optimalt ettersom en eventuell seier potensielt kan få en langt høyere kostnad enn det utbyttet rasjonelt kan rettferdiggjøre.

Vi har nå beskrevet hovedtrekkene av et avskrekkingsspill som vi vil bruke bruke videre for å analysere hvordan ulike kapasiteter kan virke inn på småstaten evne til å avskrekke i det digitale domenet. Ved å identifisere likevekter vil vi kunne få verdifulle indikatorer på hvilken effekt ulike avskrekkingsstrategier kan ha for en småstat.

I modellene skal vi angi hvilken avkastning begge aktørene i alle de mulige utfallene. Dette skal vi gjøre ved å rangere de ulike resultatene ut ifra aktørenes preferanse. Det minst ønskede utfallet vil få verdien 1, det nest minst ønskede vil få verdien 2, det tredje minst ønskede vil få verdien 3. Den høyeste avkastningen vil dermed avhenge av hvor mange resultater modellen kan gi. Det vil også kunne eksistere resultater der det ikke er praktisk mulig å rangere mellom de to alternativene, i disse tilfellene vil løsningene gi lik avkastning. Ved å vekte aktørenes preferanse på denne måten, vil det gi et godt grunnlag for å analysere strategiene innenfor en modell, samtidig har verdiene ingen funksjon utover dette (Tadelis, 2013, s. 5).

En vanlig framgangmåte for å analysere et spill i ekstensiv form er å gjennomføre en baklengs induksjon. Det betyr at man bestemmer strategien ut ifra å se hva som vil skje i siste trekk, og nøste opp derifra. Etter å ha vurdert hvert trekk hver for seg, vurderer man helheten og rangerer avkastningen i de ulike løsningene (Tadelis, 2013, s. 23). Vi finner alstå den delspillperfekte likevekten i de siste delspillene i hver gren av beslutningstreet først, for så å ta med oss resultatene fra hvert av delspilllene ettersom vi nøster inn i mot det første delspillet.

4.3 Kritikk av metoden

> ... like all social science theories my theory is a rather crude instrument I believe that the social science theories get it right about 75% of the time and let's make the generous assumption that my theory is one of the better ones in social science and therefore gets it right 75% of the time. Let's just assume that if that's true it still means that I'm wrong 25% of the time ... («Harper Lecture with John J. Mearsheimer: Can China Rise Peacefully? - YouTube», 2013)

Metoden støtter seg på teorier som strukturell realisme og avksrekkingsteori, i tillegg anvendes spillteori for å analysere ulike avskrekkingstrategier for å kunne avdekke hvorvidt avskrekkingstrategiene er i stand til å støtte opp under aktørenes målsetting. Samtlige av disse tre hovedelementene har styrker og svakheter i forhold til å predikere aktørene og dynamikken i det internasjonale systemet. Realisme kan for det første kritiseres for å ha flere ulike avgreninger som på tross av å være basert på like grunnprinsipper, ender opp med å uenige på vesentlige områder. Mearsheimer kritiserer eksempelvis defensiv strukturell realisme for å ikke kunne forklare de to verdenkrigene på 1900-tallet der Tyskland og Japan forsøkte å bli regionale hegemoner og mislykkes. Defensive realister erkjenner at teorien ikke forklarer disse krigene, men understreker at de ikke ble startet på et rasjonelt grunnlag. For å kompensere for teoriens manglende forklaringevnen henviser Waltz til å supplementere teorien med en annen teori som peker på innenrikspolitiske forhold som en årsak til disse krigene. Mearsheimer understreker videre at dette teorisupplementet ikke er en strukturell realisme teori (Mearsheimer, 2013, s. 83). Mearsheimers poeng svekker dermed den defensive strukturelle realismens validitet ved at den ikke evner å forklare de to største mellomstatlige krigene som har oppstått etter dagens statssystem oppsto etter freden i Westfalen. Mearsheimers offensive strukturelle realisme evner å forklare disse to krigene uten å peke på andre teorier, men Mearsheimers gren av realisme er heller ikke uten kritikere. Defensiv strukturell realisme argumenterer at stater forsøker å oppnå sikkerhet ved å balansere makt og at en maksimering av makt vi være kontraproduktivt og potensielt lede til våpenkappløp. På den andre siden argumenterer offensiv strukturell realisme for at det internasjonale systemet skaper en forutsetning som fører til at alle stater i praksis ikke har noe annet valg enn å maksimere sin makt, enten de ønsker det eller ikke. Innenfor offensiv strukturell realisme er altså stormakter i hovedsak revisjonistiske stater som søker etter mulighet for å øke sin relative makt, mens innenfor defensiv strukturell realisme er stater i hovedsak status-quo makter som i hovedsak søker å opprettholde en maktbalanse (Snyder, 2002, s. 157). Gapet mellom de to teoriene er her så stort at det er åpenbart at begge teorier ikke evner å komme til samme konklusjon gitt like forutsetninger. Mearsheimers offensive realisme blir kritisert for å ha en slagside i sitt valg av empiri som omfatter Japan fra 1868 til 1945; Tyskland fra 1862 til 1945; Sovjetunionen fra 1917 til 1991; Italia fra 1861 til 1943; Storbritannia fra 1792 til 1945; og USA fra 1800 til 1990 (Snyder, 2002, s. 159). De fleste av de omtalte case-studiene omhandler stater som i tidsperioden i stor grad var på utkikk etter muligheter til å utvide sin egen makt. Snyder konkluderer videre med offensiv strukturell realisme ikke kan ses på som en teori som i sin helhet kan erstatte defensiv strukturell realisme men kan være egnet til å

utvide strukturell realisme til å gi en bedre forklaringskraft bla. knyttet til revisjonistiske stater (Snyder, 2002, s. 173).
Ved siden av at denne studiens metoden støtter seg på teori, som i følge Mearsheimer i beste fall har en 75% sannsynlighet for å forutse hva som som vil skje, framfor konkret empiri innenfor det området vi undersøker bærer teorien i seg selv med seg en vesentlig del av usikkerhet knyttet til resultatet.

Hvis vi i tillegg trekker inn spillteori som basert på denne teorien konstruerer beslutningsmodellene som danner grunnlaget for analysen av de aktuelle avskrekkingsstrategiene, så er det her mulighet for å introduserer ytterlig usikkerhet. Spillteori har i seg selv ingen forklaringevne og kan ikke forutse fenomen mellom aktørene hvis vi ikke støtter oss på empiri eller teori. De forutsetningene vi legger til grunn i spillmodellene er derfor avgjørende for at resultatene skal ha verdi. Problemer kan oppstå om vi tar med for mange detaljer i form av aktører (brikkene) og valg (brikkenes mulige bevegelser). Her vil spillet etter ganske få trekk bli for omfattende å analysere (Guner, 2012). Det er derfor en målsetting at spillets omfang er innenfor et håndterbart omfang og strukturell realisme bidrar således til å redusere omfanget ettersom aktørene begrenser seg til stater. Spillteori har også høstet en del kritikk der metoden brukes i en preskriptiv sammenheng ettersom det viser seg at mennesker ikke alltid velger de mest rasjonelle handlingsmåtene. I denne studien bruker vi på den annen side spillteori i en normativ kontekst og unngår dermed denne svakheten. Strukturell realisme, maktbalanse-, polaritet- og avskrekkingsteori kommer alle til kort som teorier som gir en helt riktig beskrivelse av aktører og mekanismer i det internasjonale systemet. Teoriene er i essens et overslag på å forklare virkeligheten og når man kombinerer flere ulike overslag i den samme metoden vil det kunne øke usikkerheten på svarene som kommer ut av metoden. Et eksempel som kan illustrere dette er en spillteoretisk analyse av spillet Sjakk. På tross av at spillet har et klart definert sett av regler og spillernes målsetting er klar, fører det enorme antallet valgmuligheter etter hvert trekk at spillet blir for krevende å analysere.
Noen kritikere kritiserer spillteori for å være for kvantitativ i sin tilnærming og metoden er således avhengig av at alt må kunne måles for at det er mulig å anvende matematikk for å finne spillets løsning. Dette er i stor grad en oppfatning som er basert på en misforståelse ettersom spillteori i mange sammenhenger kun krever at det er mulig å rangere spillernes preferanser. Denne rangeringen støtter seg på kvalitative vurderinger om gjøres gjennom analysen av spillerne, deres målsettinger og de valgmulighetene som spillerne står ovenfor (Bennett, 1995, s. 28). Tallene representerer derfor kvalitative vurderinger og ikke

kvantitative målinger. Løsningen av spillet støtter seg deretter på rasjonelle valg og logiske bindinger.

Hvis vi er konkret på svakheter med baklengs induksjon, som i utgangspunktet er en intuitiv og enkel analysemetode, er det forhold som kan føre til at denne analysemetoden produserer usannsynlige løsninger. Utfordringene oppstår i midlertidig først når antallet aktører, handlinger og forutsetninger blir uoversiktlige (Spaniel, 2011, s. 168). I modellene vi skal analysere har imidlertid få aktører og et begrenset antall handlingsalternativer, som tilsier at baklengs induksjon er en godt egnet analysemetode. Metoden hviler dermed på de forutsetningene som legges inn i spillmodellene. I følge Mearsheimer er teoriene innenfor internasjonal politikk grove verktøy og de beste kan etter hans vurdering forutse en utvikling med 75% sannsynlighet. Ettersom metoden baserer seg på disse grove verktøyene har den de samme begrensingene, men ettersom problemstillingen søker ett svar som ligger på et overordnet og prinsipielt nivå, vil metoden kunne gi verdifull innsikt som bidrar til å svare på problemstillingen.

5 Analyse av spillmodeller

I dette kapittelet skal vi modellere hver av de identifiserte avskrekkingstrategiene og finne løsningen for hver av spillmodellene. Spillmodellenes løsning vil så danne grunnlaget for å vurdere i hvilken grad avskrekkingstrategien kan underbygge småstatens overordnede målsetting.

5.1 Avskrekking gjennom nektelse.

5.1.1 Beskrivelse av modellen

Forutsetninger:

- De to statene har i en normaltilstand lite samarbeid og svake økonomiske bånd.
- Det digitale domenet favoriserer offensiven og dermed vil en offensiv aktør alltid, gitt nok tid, lykkes i å infiltrere deler av en annen stats kritiske infrastruktur (offensiv-defensiv-balanse).
- Den svakere staten er kjent med at stormakten har en evne og - ambisjon i det digitale rom.
- Småstaten har kommunisert tydelig for hvor den setter grensen for hva som er akseptabelt.
- Småstaten har en god og troverdig evne til å ivareta sin kritiske infrastruktur.

Modellen gjenspeiler en strategi basert på ren avskrekking gjennom nektelse. Den overordnede situasjonen kan beskrives som normaltilstand der de to aktørene ikke er i konflikt med hverandre. På tross av at statene er i en normaltilstand er de alltid på jakt etter å øke sin egen relative makt for å bedre kunne ivareta sin egen sikkerhet. Den sterke staten ønsker i dette tilfellet å erverve seg tvangsmidler ovenfor den svakere staten gjennom å infiltrere denne statens kritiske infrastruktur. Den svakere staten på sin side ønsker å optimalisere sin egen evne til å forsvare seg mot en offensiv aktør i det digitale rom. Den svakere staten arbeider målrettet med en passiv sikring i sin kritiske informasjonsinfrastruktur der hensikten å redusere risikoen for at en offensiv aktør lykkes i å infiltrere statens kritiske infrastruktur. Den svakere staten har en tydelig kommunikasjonsstrategi knyttet til sin strategi og ønsker med dette å kunne påvirke kost-nytte-analysen til flest mulig aktører, slik at de ikke truer integriteten til den svakere statens kritiske infrastruktur. Den svakere staten baserer altså sin avskrekkingsstrategi på to forhold. Den første er god sikring av egen infrastruktur som vil gjøre det mer ressurskrevende for den sterkere staten å lykkes med å infiltrere den svakere

statens infrastruktur. Hvis den sterkere staten på tross av sterke sikringstiltak likevel lykkes i å infiltrere kritisk infrastruktur, har den svakere staten ingen andre virkemidler i det digitale domenet å falle tilbake på. Utenfor det digitale domenet kan staten velge å bruke klassiske virkemidler som diplomati og økonomiske sanksjoner, men ettersom den her er den svakere parten i situasjonen, vil en slik handling kunne føre til en eskalering mot en konflikt som undergraver den svakere nasjonens hovedmål om å opprettholde status-quo.

Første trekk:

Den sterke staten, Stat A har i første trekk initiativet siden den svakere staten, Stat B først og fremst ønsker å opprettholde status-quo. Her må den sterkere staten gjøre en kost-nytte-analyse for å avgjøre om den ønsker å utfordre den svakere staten gjennom å forsøke å infiltrere og få kontroll på den svakere statens infrastruktur. Hvis den sterke staten i dette trekket konkluderer med at den potensielle kostnaden ved å forsøke å infiltrere den svakere nasjonens kritiske infrastruktur er større enn den potensielle nytten, vil han velge å opprettholde status-quo. Hvis vurderingen er motsatt vil han velge å utfordre Stat B gjennom å forsøke å infiltrere statens infrastruktur.

Andre trekk:

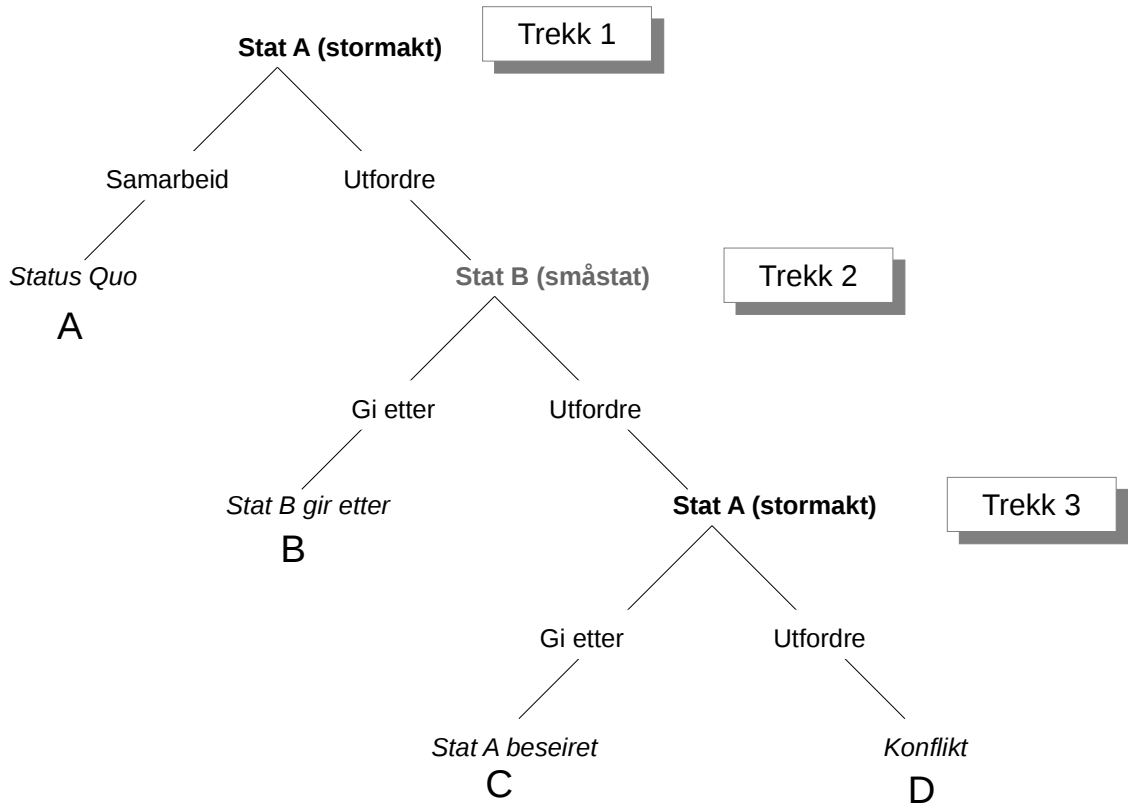
Den svakere staten, Stat B må her gjøre et valg. Den sterke staten, Stat A, har nå valgt å iverksette offensive operasjoner mot den svakere staten, mens den svakere staten sikre sine kritiske systemer på best mulig måte. Gitt at den sterkere parten bruker nok ressurser, vil den etterhvert lykkes med å infiltrere deler kritisk infrastruktur ut ifra forutsetningen om at offensiv-defensiv-balansen generelt er vurdert til å favoriserer offensiven i det digitale rom. Etterhvert vil den svakere staten bli bevisst på at den er mål for den offensive operasjonen, eller den oppdager at en uønsket aktør har skaffet seg kontroll over deler av statens kritiske infrastruktur. Den svakere staten står da ovenfor to valg: I det første alternative handlingsvalget kan den svakere staten velge å begrense seg til å reetablere kontroll på egen kritiske infrastruktur i den hensikt å sikre seg mot et angrep som benytter tilsvarende operasjonsmetode og virkemidler i framtiden. I det andre strategiske alternativet kan den svakere staten velge å utfordre den offensive aktøren. Ettersom en inntrengning i kritisk infrastruktur som vi har sett er under terskelen for hva som regnes som et væpnet angrep i det digitale rom, vil det ikke være mulig for den svakere staten å støtte seg på en forsvarsallianse som eksempelvis NATO for å gjennomføre en gjengjeldelse. Staten er dermed begrenset til å håndtere saken bilateralt, fortrinnsvis gjennom å bruke diplomatiske eller økonomiske

virkemidler. Ettersom den svakere staten har valgt en avskrekkingsstrategi basert på nektelse, er det ikke en aktuell opsjon å gjengjelde med makt gjennom det digitale domenet.

Tredje trekk:

Det siste trekket utføres av den sterke staten og kommer om den svakere staten har valgt å besvare den sterkere statens handlinger med diplomatiske og økonomiske sanksjoner. Den sterkere staten må her beslutte hvorvidt den ønsker å besvare den svakere statens sanksjoner, eller gi etter for det diplomatiske presset. Beslutningen vil her påvirkes av hvor stor suksess de offensive operasjonene har vært i forhold til å infiltrere kritisk infrastruktur og konsekvensen av de sanksjonene den svakere staten har besluttet å gjennomfører. Ettersom vi har forutsatt at de to statene til daglig har lav gjensidig avhengighet, har sannsynligvis diplomatiske sanksjoner begrenset konsekvens for den sterkere staten. Ut ifra denne forutsetningen vil den sterke staten måtte foreta ett av to valg: det første strategiske valget kan den velge å gi etter, avslutte de offensive operasjonene og «beklage» ovenfor den svakere staten. I det andre alternativet kan de velge å besvare de diplomatiske eller økonomiske sanksjonene med tilsvarende eller mer omfattende styrke tilbake.

5.1.2 Vurdering av preferanser



Illustrasjon 4: Avskrekking gjennom nektelse -løsningsalternativer

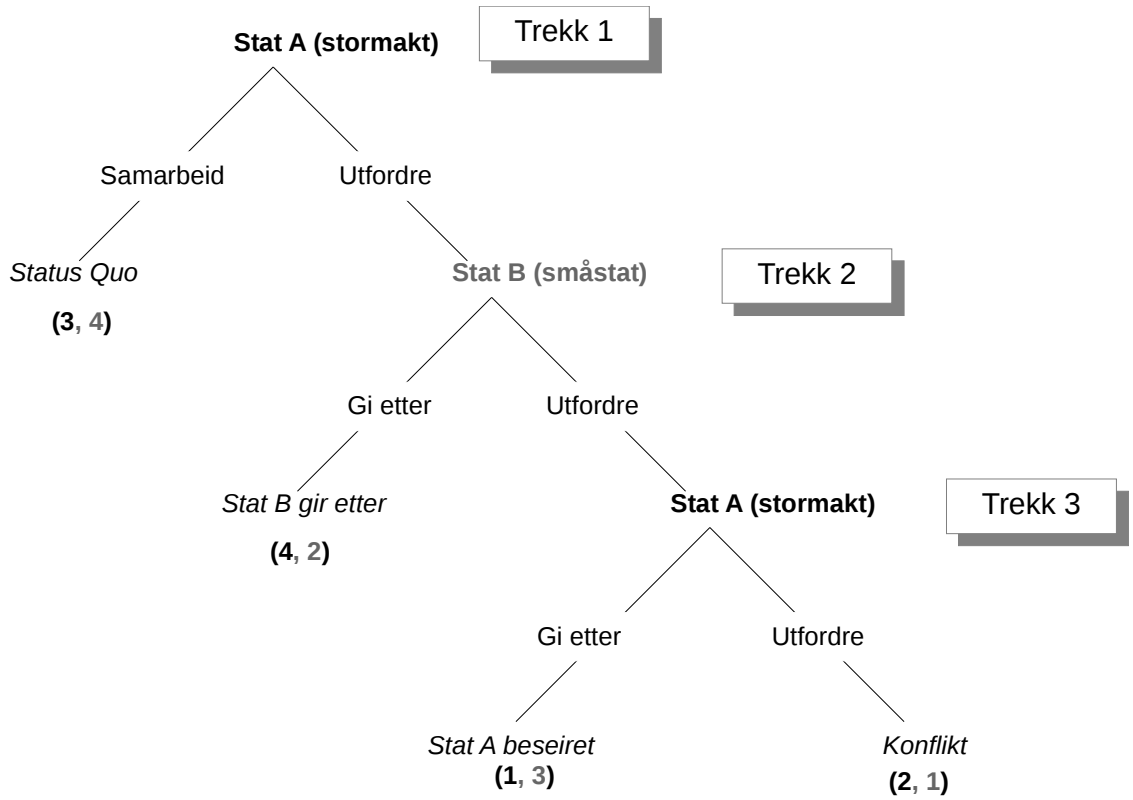
Preferanser og gevinster *Stat A (stormakt)*

Vi skal nå vurdere og rangere de to statenes preferanser. Hvis vi starter med den sterkeste av de to statene - Stat A, kan vi si med relativt stor sikkerhet at en løsning der den sterkeste staten må gi etter for den svakere statens sanksjoner er den minst prefererte løsningen for Stat A (C). Dette utfallet vil føre til at den sterkeste staten framstår som svak ettersom den velger å bøye av for en klart svakere stat. Altså er C=1. Den nest laveste rangeringen er utfallet der statene havner i en konflikt med hverandre (D). Årsaken til at dette utfallet har en lav preferanse er at det ikke understøtter Stat A sin overordnede målsetting om å infiltrere Stat B sin kritiske infrastruktur for å oppnå en relativ maktfordel. Konsekvensen av dette utfallet er at Stat A havner i en bilateral konflikt med Stat B. Altså er D=2. Da gjenstår det bare å avgjøre rekkefølgen på et utfall der status-quo (A) opprettholdes, eller der Stat B i praksis lar Stat A komme unna med sin aktivitet knyttet til å infiltrere Stat B sin kritiske infrastruktur (B). Her er det klart at Stat A ville foretrekke løsningen der det er mulighet for å øke sin relative makt framfor å opprettholde status-quo. Det gir B=4 og A=3.

Stat A sine preferanser og gevinster blir dermed: B=4, A=3, D=2, C=1

Preferanser og gevinster Stat B (småstat)

Den svakere statens minst prefererte utfall er å havne i en konflikt med den sterkere staten (D), ettersom den ved dette utfallet i praksis har alt å tape og lite å vinne. Altså D=1. Videre er det nest dårligste utfallet å gi etter og ikke utfordre Stat A i trekk 2, dersom den oppdager at Stat A har infiltrert egen kritiske infrastruktur. Altså er B=2. Til slutt gjenstår å avgjøre preferansen mellom status-quo i trekk 1 eller at den sterkere staten, stat A gir etter for Stat B sine diplomatiske virkemidler i trekk 3. Stat B sin primære målsetting er som småstat å opprettholde status-quo (A) ovenfor den sterkere staten, men hvis det ikke er mulig er den nest høyeste preferansen at Stat A i trekk 3 bøyer av for Stat B sine sanksjoner (C). Altså C=3 og A=4.
Stat B sine preferanser og gevinster blir dermed: A=4, C=3, B=2, D=1



Illustrasjon 5: Avskrekking gjennom nektelse - preferanser

5.1.3 Baklengs induksjon og løsning av delspill-perfekt likevekt

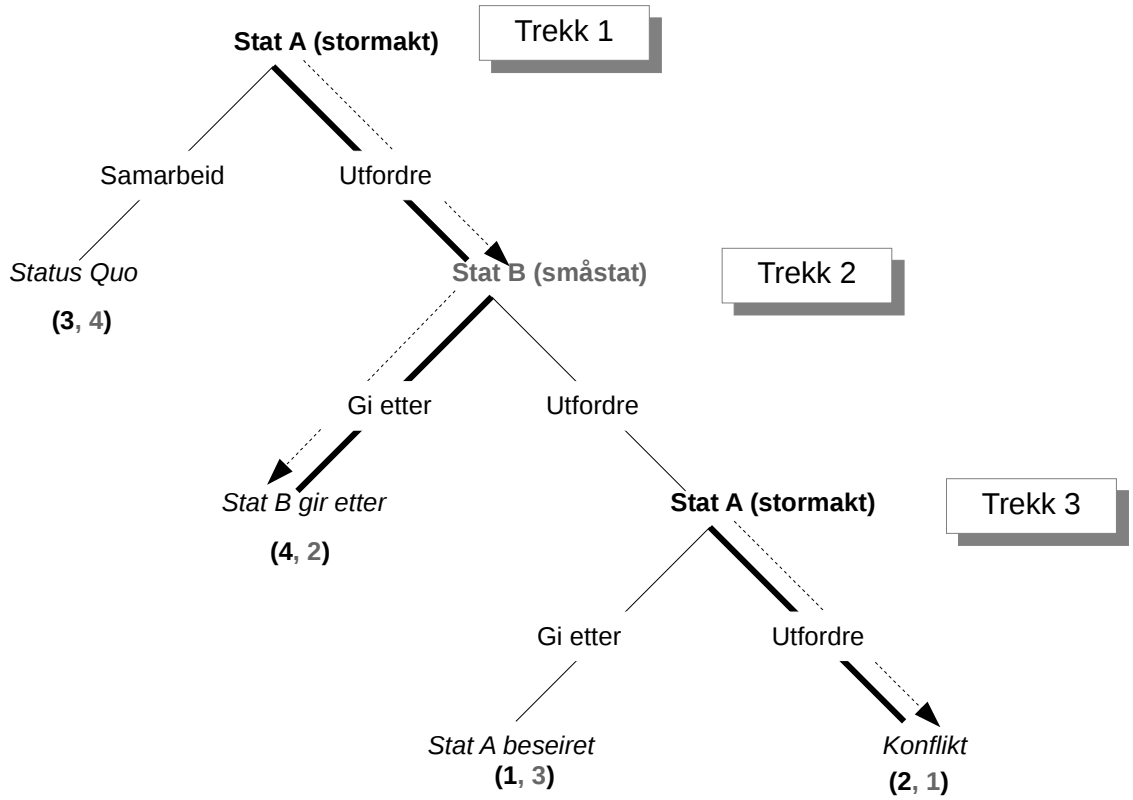
Basert på denne rangeringen av preferanser kan vi gjennomføre en baklengs induksjon for å identifisere delspillikevekter.

Først ser vi på Trekk 3 hvor det er den sterkere staten - Stat A som skal foreta valget, står den ovenfor et valg om å *gi etter* (1) eller *utfordre* stat B (2). Det rasjonelle valget for Stat A i Trekk 3 blir dermed å *utfordre* Stat B

Dernest ser vi på Trekk 2 der den svakere staten skal velge mellom å *gi etter* ved å ikke reagere på Stat As infiltrering (2), eller utfordre Stat A med sanksjoner. Ettersom vi allerede har avklart at Stat A vil velge strategien *utfordre* i trekk 3, så kan vi altså utlede at stat B her i praksis vil velge sluttilstanden *konflikt* (1) om den velger å utfordre Stat B med sanksjoner. Det rasjonelle valget for Stat B i Trekk 2 vil dermed være å *gi etter* (2).

Når vi da til slutt ser på Tekk 1 hvor den sterkere staten - Stat A står ovenfor et valg mellom å opprettholde status quo (3), eller *utfordre* Stat B ved å forsøke å infiltrere kritisk infrastruktur, har vi allerede sett at det rasjonelle valget for Stat B i Trekk 2 vil være å *gi etter* (4). Det betyr at i Trekk 1 vil det strategien *utfordre* gi den høyeste gevinsten (4), og dermed være det mest rasjonelle valget.

Løsningen på spillet er dermed:



Illustrasjon 6: Avskrekking gjennom nektelse - løsning

<Stat A>, <Stat B>
<Utfordre, Utfordre>, <Gi etter>

5.1.4 Delkonklusjon avskrekking gjennom nektelse

Vi ser ut ifra løsningen av spillet at den sterkere staten, Stat A her vil foretrekke å gjennomføre offensive operasjoner mot den svakere staten, Stat B. Det betyr den svakere statens avskrekkingsstrategi har mislykkes. Det er to forhold i denne avskrekkingsmodellen som undergraver den svakere statens avskekkingsstrategi. For det første støtter strategien seg på å ensidig operere defensivt i et domene der empiri tilsier at offensiven har en fordel ovenfor defensiven. Dette taler altså for at en stat som ønsker å øke sin relative makt ut ifra en rasjonell vurdering vil velge å operere offensivt mot en stat på tross av at denne jobber aktivt med å sikre sin egen kritiske infrastruktur. Før den offensive staten iverksetter operasjoner mot den svakere statens infrastruktur må den imidlertid vurdere eventuelle andre reaksjoner fra den svakere staten om den blir avslørt. Her er det to faktorer som svekker den svakere statens evne til å avskrekke. Den første og viktigste faktoren er at en gjengjeldelse der den

svakere staten gjennomfører diplomatiske eller økonomiske sanksjoner mot den sterkere staten, sannsynligvis vil føre til eskalering. Dette vil i så fall kunne ramme den svakere staten i større grad enn det rammer den sterkere staten. I tillegg kan det for den svakere staten også være utfordrende å attribuere den sterkere staten, som igjen kan undergrave støtte til den svakere staten fra allierte eller partnere. Infiltrasjon av en stats kritiske infrastruktur er under terskelen for hva som tolkes som et væpnet angrep mot en stat. Dette tilsier at den svakere staten her står ovenfor en bilateral situasjon med den sterkere staten der avskrekkingsmiddelet vil kunne føre til en eskalering og dermed en krise i relasjonen mellom de to statene. Denne konsekvensen avviker mest med den svakere statens målsetting om å opprettholde status-quo, dermed er avskrekkingsmiddelet irrasjonelt. Avskrekkingteori sier at det ikke er diskvalifiserende for en avskrekkingsstrategi å true med å gjennomføre en straff som i seg selv er irrasjonell, men her er det en forutsetning at denne straffen i isåfall har en vesentlig avskrekkende effekt for aktøren den er rettet mot. Samtidig er det avgjørende at den truende staten må kunne skape troverdighet i forhold til at den kommer til å gjennomføre disse handlingene, på tross av at den til slutt vil sannsynligvis vil koste den truende parten mer enn den truede. I modellen vi har presentert avskrekkingsmiddelet i form av diplomatiske eller økonomiske virkemidler antageligvis for svakt til å framstå som særlig avskrekkende. Når et svakt virkemiddel sannsynligvis også vil påføre størst negative konsekvenser for den parten som iverksetter det, er det heller ikke troverdig at det vil benyttes.
Totalt ser en avskrekkingsstrategi basert på ren nektelse i det digitale domenet ut til å være for svak til å oppnå en effektiv avskrekking av en sterkere stat, som søker å infiltrere den svakere statens kritiske infrastruktur.

5.2 Avskrekking gjennom straff

5.2.1 Beskrivelse av modellen

Forutsetninger:

- De to statene har i en normaltilstand lite samarbeid og svake økonomiske bånd.
- Det digitale domenet favoriserer offensiven og dermed vil en offensiv aktør gitt nok tid lykkes i å skaffe seg tilgang til deler av en annen stats kritiske infrastruktur.
- Den svakere staten er kjent med at den sterke staten har en offensiv evne og ambisjon i det digitale rom.
- Småstaten har kommunisert tydelig for hvor den setter grensen for hva som er akseptabelt og at den vil reagere tydelig om denne grensen krysses.

- Småstaten har en god og troverdig evne til å gjennomføre offensive operasjoner i det digitale rom.

Modellen gjenspeiler en strategi basert på avskrekking gjennom straff. Den overordnede situasjonen kan på starttidspunktet beskrives som normaltilstand der de to aktørene ikke er i konflikt med hverandre. På tross av at statene er i en normaltilstand er de på jakt etter å øke sin egen makt for å bedre kunne ivareta sin egen sikkerhet. Den sterke staten ønsker i dette tilfellet å erverve seg tvangsmidler ovenfor den svakere staten ved å infiltrere denne statens kritiske infrastruktur. Den svakere staten ønsker på sin side å påvirke kost-nytte-analysen til stater som forsøker å skaffe seg kontroll på dens kritiske infrastruktur. Dette gjør han gjennom å true med gjengjeldelse som videre vil gi store negative konsekvenser for den offensive aktøren. Den svakere staten har kommunisert tydelig at denne gjengjeldelsen vil finne sted om det avdekkes at en aktør har skaffet seg urettmessig kontroll over kritisk infrastruktur. Den svakere staten har demonstrert evne til gjengjeldelse ved at den over tid har bygget vesentlig kompetanse innenfor relevante fagfelt. Staten kan vise til svært høy kompetanse innenfor sikkerhetsområdet, både i form av utdanningsinstitusjoner og industri. Denne kompetansen kan også knyttes til landets militære forsvar. Den svakere staten kan også vise til å støttet allierte med vellykkede offensive cyberoperasjoner mot «failed states» og terroristorganisasjoner. Den svakere staten har altså en troverdig evne, kommunisert klart hvor den setter grensen for gjengjeldelse og troverdige gjennom at den har benyttet maktmiddelet mot andre stater tidligere. Ressursene den svakere staten binder opp i det å opprettholde en troverdig avskrekkingstrussel gjennom straff, øker til dels risiko for at det ikke er nok ressurser til å beskytte alt av kritisk infrastruktur på en optimal måte, men den svakere staten avveier at økningen i risiko på dette området blir mer en kompensert for ved å ha evne til å fremstå med en potent og troverdig straff å slå tilbake med.

Første trekk:

Den sterke staten har i første trekk initiativet siden den svakere staten først og fremst ønsker å opprettholde status-quo. Her må den sterkere staten i sin egen kost-nytte-analyse først ta stilling til konsekvensene av å utløse en gjengjeldelse fra den svakere staten. Relevante faktorer som må tas stilling til er egen kritiske infrastrukturs sårbarhet ovenfor en eventuell gjengjeldelse fra den svakere staten, og egen evne til å gjenopprette normaltilstand etter å ha blitt rammet. Det er allerede nå aktuelt å vurdere hvordan en eventuell konflikt med den aktuelle staten vil understøtte, eller skape utfordringer for den sterkere statens overordnede strategi i det internasjonale systemet. Hvis den sterke staten i dette trekket konkluderer med at

den potensielle kostnaden ved å iverksette offensive cyberoperasjoner er større enn den potensielle nytten, vil han velge å opprettholde status-quo, mens motsatt sluttning vil tilsi at det vil være en bedre strategi å iverksette offensive operasjoner mot den svakere statens infrastruktur.

Andre trekk:

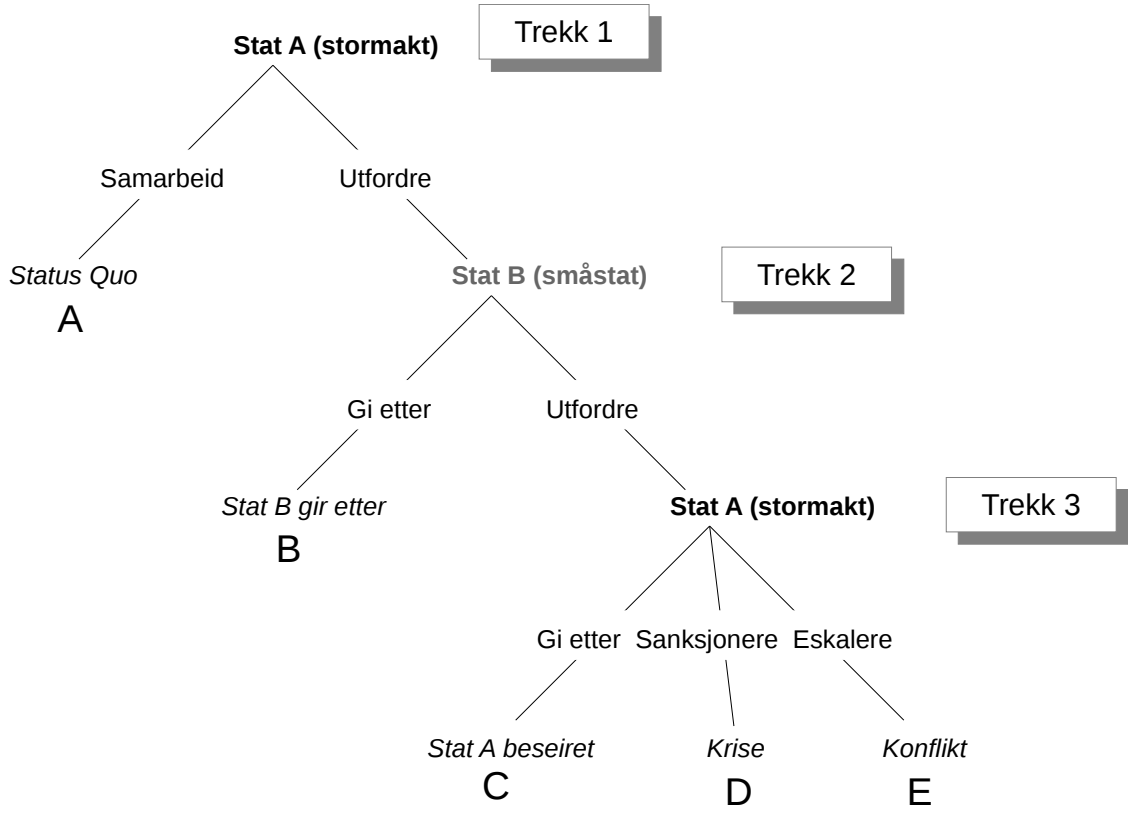
Den svakere staten er den neste som må ta et strategisk valg. Den sterke staten har på dette tidspunktet lykkes i å infiltrere deler av den svakere statens kritiske infrastruktur og den svakere staten har oppdaget infiltrasjonen. Den svakere staten har gode indikasjoner på hvem som står bak infiltrasjonen, men har ikke sterke nok bevis til å underbygge denne påstanden «utover en hver tvil». Den sterkere staten benekter tilknytning til infiltrasjonen. Den svakere staten står her ovenfor to strategiske valgmuligheter: I det første valget begrenser den svakere staten seg til å reetablere kontroll på egen kritiske infrastruktur å sikre seg mot et tilsvarende angrep i framtiden. På denne måten unngår den svakere staten faren for å eskalere situasjonen med den sterkere staten, samtidig vil den undergrave troverdigheten til sin egen avskrekkingsstrategi, som videre vil gi en økt risiko for å bli rammet av ytterlig infiltrasjon på et senere tidspunkt. I det andre strategiske valget kan den svakere staten velge å utfordre den offensive aktøren som i dette tilfellet er den sterkere staten. Ettersom en inntrengning i kritisk infrastruktur er under terskelen for hva som regnes som et væpnet angrep i det digitale rom vil det sannsynligvis ikke være mulig å støtte seg på en forsvarsallianse som eksempelvis NATO. Den svakere staten er i et slikt tilfelle sannsynligvis begrenset til å håndtere saken bilateralt. Den svakere staten står ovenfor et valg om å gjennomføre et angrep på en sterkere statens kritiske infrastruktur for å opprettholde troverdigheten til egen avskrekkingsstrategi, etter at den samme strategien i utgangspunktet har mislyktes i å avskrekke den sterkere staten. Denne handlingen kan videre føre til en eskalering og en krise eller konflikt mellom de to statene. Denne krisen eller konflikten kan også bevege seg over til det fysiske domenet, der den sterkere staten er overlegen. Den potensielle situasjonen kan forverres ytterlig dersom de to nasjonene er geografisk tilknyttet hverandre og konflikten kan bevege seg over i det geopolitiske området. Dersom den svakere staten velger å gjengjelde infiltrasjonen gjennom å rette et angrep tilbake mot kritisk infrastruktur, kan det ha en svært negativ kostnad for staten ettersom gjengjeldelsen med stor sannsynlighet vil utløse en bilateral konflikt med en sterkere stat. Gjengjeldelsen fra den svakere staten kan også oppleves som uproposjonal ettersom den utløsende handlingen – den påståtte infiltrasjonen, ikke hadde påført den svakere staten målbare negative konsekvenser. I prinsippet står den svakere staten her ovenfor et valg som er vanskelig å argumentere for ut ifra rasjonelle betraktninger. Hvis målet for staten er å ivareta

eller øke sin egen sikkerhet er det tvilsomt om valget om å gjengjelde gjør annet enn å bidra vesentlig i negativ retning.

Tredje trekk:

Det siste trekket utføres av den sterke staten og kommer etter at den svakere staten har valgt å besvare den sterkere statens med gjengjeldelse mot hans kritiske infrastruktur. Den sterkere staten må her håndtere konsekvensene av gjengjeldelsen og deretter beslutte hvorvidt den ønsker å besvare den svakere statens offensive handlinger. Beslutningen vil her påvirkes av konsekvensen av gjengjeldelsen den svakere staten har gjennomført. Ettersom den svakere staten direkte eller indirekte har truet den sterkere statens sikkerhet, hjemler dette et sterkt svar. Hvis objekter eller menneskeliv er gått tapt som en konsekvens av den svakere statens gjengjeldelse kan det også, i følge krigens folkerett, tolkes som et væpnet angrep, og den sterkere staten har dermed en legitim rett til å gjengjelde angrepet med eksempelvis bruk av våpenmakt. Ut ifra denne forutsetningen vil den sterke staten måtte foreta ett av tre valg: Det første strategiske valget kan han velge å gi etter, avslutte de offensive operasjonene og «beklage» ovenfor den svakere staten. I det andre alternativet kan han velge å besvare med diplomatiske og økonomiske sanksjoner hvis målet er å reagere, men returnere til normaltilstand. I det tredje alternativet kan han velge å eskalere situasjonen ved å bruke fysiske makt som han kan hevde er legitimt i henhold til krigens folkerett.

5.2.2 Vurdering av preferanser



Illustrasjon 7: Avskrekking gjennom straff - løsningsalternativer.

Preferanser og gevinster Stat A (stormakt)

Vi skal nå vurdere og rangere de to statenes preferanser. Hvis vi starter den sterkeste av de to statene, Stat A, kan vi nok si med relativt stor sikkerhet at en løsning der den sterkeste staten må gi etter for den svakere statens sanksjoner er den minst prefererte løsningen for Stat A ettersom den framstår som svak om den gir etter for en småstat. Altså er C=1. Den nest laveste rangeringen er situasjonen der statene havner i en eskalerende konflikt med hverandre. Stat A sitt overordnede mål er å infiltrere Stat Bs kritiske infrastruktur for å oppnå en maktforskyving i egen favør, ikke ende opp i en bilateral konflikt. Altså er E=2. Det å gjennomføre sanksjoner (D) understøtter heller ikke målsetningen Stat A siktet mot når den først velger å forlate status-quo (A), på en annen side har det mindre negative konsekvenser enn den hardere reaksjonen *eskalere* (E) dermed foretrekkes D framfor E.[9] Altså er D=3. Da gjenstår det bare å avgjøre rekkefølgen på et utfall der *status-quo* (A) opprettholdes, eller der Stat B i praksis lar Stat A komme unna med sin aktivitet knyttet til å infiltrere Stat B sin kritiske infrastruktur (B). Her er det klart at Stat A ville foretrekke løsningen der det er mulighet for å øke sin relative makt framfor å opprettholde status-quo. Det gir B=5 og A=4.

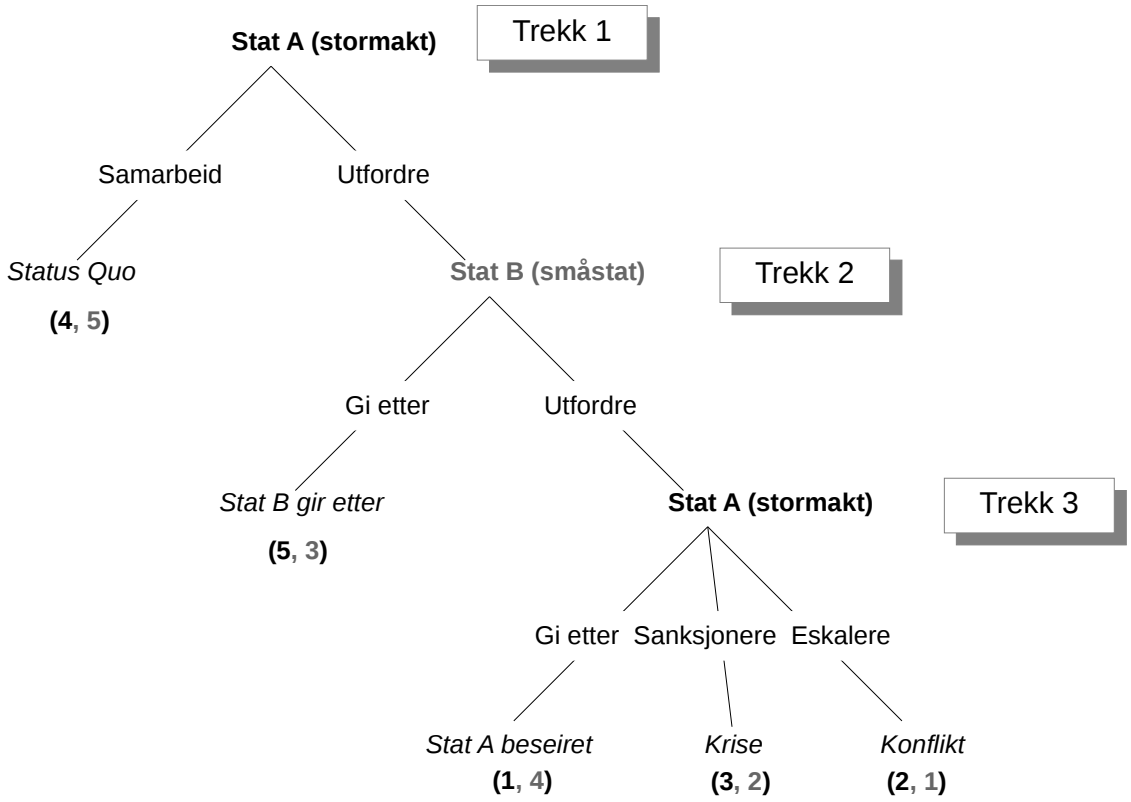
9 Denne preferansen avhenger av hvor sterk Stat B sin gjengjeldelse Stat B har gjennomført. Om Stat B hadde gjengjeldt på en hard måte, ville Stat A kunne foretrukket Konflikt (E) framfor Sanksjonere (D).

Stat A sine preferanser og gevinster blir dermed: B=5, A=4, D=3, E=2 og C=1

Preferanser og gevinster Stat B (småstat)

Den svakere statens minst prefererte utfall er å havne i en skarp konflikt med den sterkere staten A, hvor statens sikkerhet vil være truet på en alvorlig måte. Altså E=1. Videre er det nest dårligste utfallet å bli pålagt sanksjoner av Stat A. Dette vil kunne redusere statens sikkerhet og handlefrihet i det internasjonale systemet samt påføre Stat B økonomiske tap. Altså D=2. Det tredje minst foretrukne utfallet vil være å gi etter og ikke utfordre stat A i trekk 2 når Stat B oppdager at Stat A har infiltrert egen kritiske infrastruktur. Altså er B=3. Til slutt gjenstår status-quo i trekk 1 eller at den sterkere staten, Stat A gir etter for Stat B sine virkemidler i trekk 3. Her vil en løsning der den sterkere staten gir etter for den svakrere statens press, være den nest mest prefererte løsningen for den svakere staten B. Status-quo som er sammenfallende med Stat B sin overordnede målsetting vil dermed være den mest foretrukne. Altså A=5 og C=4.
Stat Bs preferanser og gevinster blir dermed: A=5, E=4, B=3, D=2 og E=1

5.2.3 Baklengs induksjon og løsning av delspill-perfekt likevekt



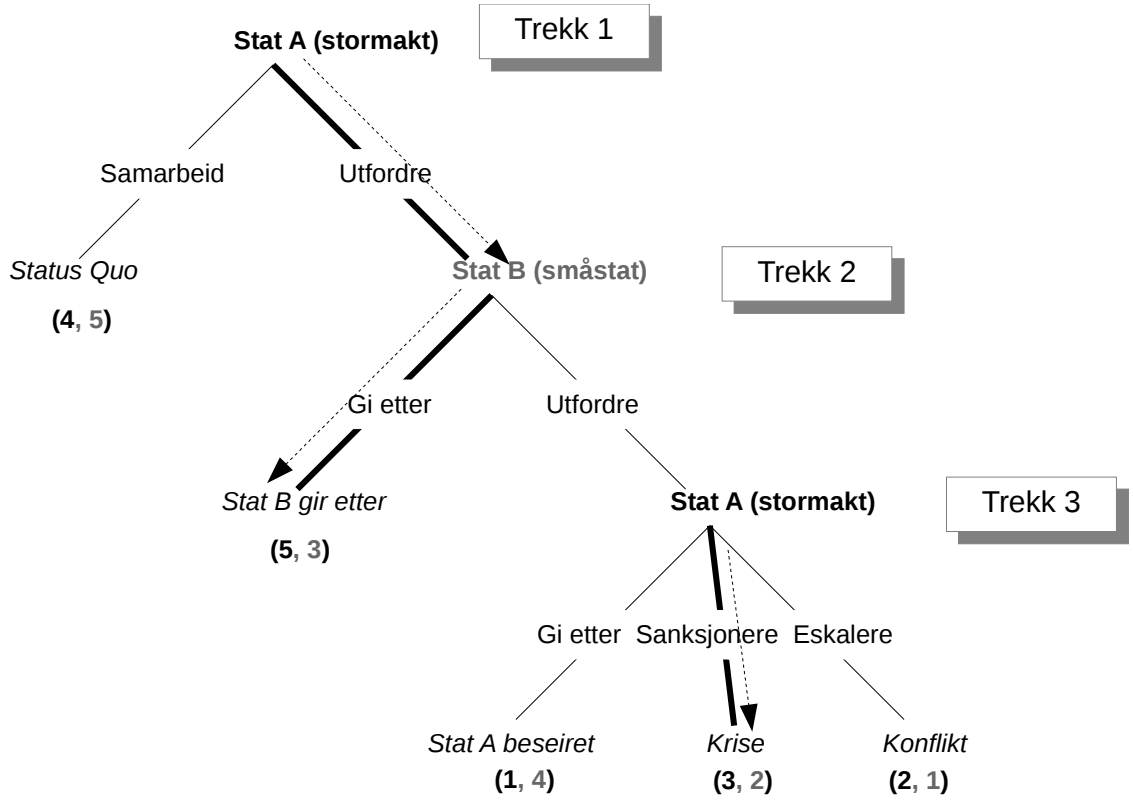
Illustrasjon 8: Avskrekking gjennom straff - preferanser

Basert på denne rangeringen av preferanser kan vi gjennomføre en baklengs induksjon for å identifisere delspillikevekter. Først ser vi på Trekk 3 hvor det er den sterkere staten - Stat A som står ovenfor tre valg. Det første er å gi etter (1), nummer to er å eskalere til en konflikt (2), det siste er å sanksjonere som kan lede til en krise (3). Det rasjonelle valget for Stat A i Trekk 3 blir dermed å sanksjonere (3) ovenfor Stat B.

Dernest ser vi på Trekk 2 der den svakere staten, Stat B, skal velge mellom å *gi etter* ved å ikke realisere avskrekkingsmiddelet på Stat As infiltrering (3), eller realisere avskrekkingsmidlene ved å *utfordre* Stat A med sanksjoner. Ettersom vi allerede har avklart at Stat A vil velge strategien S*anksjonere* i trekk 3, kan vi altså utlede at Stat B her i praksis vil velge sluttilstanden Krise (2) om den velger å utfordre Stat B med sanksjoner. Det rasjonelle valget for Stat B i Trekk 2 vil dermed være å *gi etter* (3).

Når vi da til slutt ser på Tekk 1 hvor den sterkere staten - Stat A står ovenfor et valg mellom å opprettholde status-quo (4), eller utfordre Stat B ved å forsøke å infiltrere kritisk infrastruktur, så har vi allerede sett at det rasjonelle valget for Stat B i Trekk 2 vil være å *gi etter* (5). Det

betyr at i Trekk 1 vil strategien *utfordre* gi den høyeste gevinsten (4), og dermed være det rasjonelle strategiske valget.
Løsningen på spillet er dermed:



Illustrasjon 9: Avskrekking gjennom straff - løsning.

<Stat A>, <Stat B>
<Utfordre, Sanksjonere>, <Gi etter>

5.2.4 Delkonklusjon avskrekking gjennom straff

Vi ser i dette spillet at det er en irrasjonell strategi for den svakere staten å avskrekke den sterkere staten gjennom å true den sterkere aktørens kritiske infrastruktur. En av hovedutfordringene er at når man betrakter hele spillet og de sannsynlige utfallene, er det tydelig at den svakere staten har mest å tape på å gjengjelde en infiltrasjon mot egen infrastruktur. Hvis vi ser på infiltrasjonen som er handlingen som utløser en potensiell gjengjeldelse fra den svakere staten, så har den i prinsippet ingen skadelige konsekvenser så lenge den sterkere staten ikke tar ned eller forstyrrer den infrastrukturen den har infiltrert. Hvis den svakere staten svarer på en infiltrasjon med et angrep mot den sterkere statens infrastruktur for å opprettholde sin troverdighet knyttet til avskrekkingstrusselen, blir dette raskt en handling som ikke står i proposjon til den handlingen som utøste den. Dette lager

forutsetninger for at den sterkere staten legitimt kan eskalere situasjonen og i ytterste konsekvens reagere med våpenmakt. Den uproposjonale reaksjonen fra den svakere staten kan også skape en oppfattelse av at den er den aggressive parten, og dermed være i en dårlig posisjon ut ifra etiske og moralske betraktninger. Den svakere staten vil dermed stå igjen med en svært begrenset politisk handlefrihet, mens den sterkere staten har sannsynligvis fått økt sin egen betraktelig.

Denne typen avskrekkingsstrategi fra en småstat legger også opp til at den sterkere staten kan bruke denne mekanismen bevisst om den ønsker å skape en bilateral krisetilstand for i neste omgang kunne presse den svakere staten i relevante saker.

Dette er dermed en uheldig strategi for å småstat å forfølge da den for det første er lite troverdig da den spiller det meste av initiativet over til den sterkere parten. Hvis den svakere staten likevel velger å gjengjelde en infiltrasjon med noe som vil bli oppfattet som en uproposjonal reaksjon, vil dette med stor sannsynlighet føre til en eskalering, uten garanti for at en alliansepartner som eksempelvis NATO vil kunne involvere seg. Småstaten kan dermed befinne seg i en bilateral krise eller konflikt med en stormakt, der stormakten kan være i en situasjon der det kan være legitimt å svare med militærmakt ovenfor småstaten. Løsningen på spillet tilsier dermed at avskrekking gjennom straff er en avskrekkingsstrategi som i liten grad er i stand til å understøtte småstatens overordnede politiske målsetting. Konsekvensen av å implementere en slik strategi kan med stor sannsynlighet føre til en svekkelse av småstatens sikkerhet.

5.3 Avskrekking gjennom nektelse og avledning.

Forutsetninger:

- De to statene har i en normaltilstand lite samarbeid og svake økonomiske bånd.
- Den svakere staten er kjent med at den sterke staten har en offensiv evne og ambisjon i det digitale rom.
- Småstaten en kommunikasjonsstrategi der den tydelig beskriver sin policy som at den vil dele objektiv informasjon om sofistikerte offensive aktørers metoder og virkemidler.
- Småstaten har en evne til å utføre gjennomføre aktive defensive tiltak som å avlede og analysere en sofistikert aktør.
- Småstaten har en god og troverdig evne til å ivareta sin kritiske infrastruktur.

Modellen gjenspeiler en strategi basert på avskrekking gjennom nektelse, men i tillegg implementerer strategien virkemidler som maksimerer den totale kostnaden for aktører som

gjennomfører offensive operasjoner gjennom det digitale rom mot den svakere staten. Den overordnede situasjonen kan beskrives som normaltilstand der de to aktørene ikke er i konflikt med hverandre. På tross av at statene er i en normaltilstand er de alltid på jakt etter å øke sin egen relative makt for å bedre kunne ivareta sin egen sikkerhet. Den sterke staten ønsker i dette tilfellet å erverve seg tvangsmidler ovenfor den svakere staten ved å infiltrere denne statens kritiske infrastruktur. Den svakere staten har utviklet aktiv sikring sin kritiske informasjonsinfrastruktur. Hensikten med den aktive sikringen er at avledningstiltakene skal skape et falskt bilde av sårbarhet for infiltrasjon i det digitale rom. Et antall av sårbarhetene en offensiv aktør finner er i realiteten simulerte for at den offensive aktøren skal bli lokket inn i en del av infrastrukturen der de ikke vil gjøre skade, men kan observeres og analyseres av den defensive staten. Informasjonen om aktørene, handlemåtene og eventuelle virkemidler som benyttes, deles av den svakere staten på en åpen, objektiv og nøytral måte. Målsettingen med dette er todelt, på den ene siden ønsker den svakere staten å bidra til at tredjeparts aktører er i stand til å beskytte seg mot tilsvarende angrep. På den andre siden er målet å øke den faktiske kostnaden for den offensive aktøren å gjennomføre offensive operasjoner mot småstaten. Vi har tidligere sett at det å lykkes med et målrettet angrep i det digitale rom mot en dyktig aktør er ressurskrevende. Denne strategien spiller på dette forholdet og forsterker det ytterlig ved at den offensive parten bruker ressurser på noe som for han ser ut som en sårbarhet det er mulig å utnytte, men som i praksis er kontraproduktiv da den er et avledningsmiddel. Samtidig deles alt av informasjon om potente aktører, operasjonsmetode og virkemidler som benyttes. Dette vi kunne gi en slags avvæpningseffekt, der aktøren med større hyppighet må utvikle nye våpen, som er svært ressurskrevende. Den svakere staten har i denne modellen en bevisst og upolitisk kommunikasjonsstrategi knyttet til denne handlemåten, slik at informasjonen som blir formidlet i størst mulig grad er objektiv og troverdig. I praksis sier den svakere staten til andre aktører at: «ingen kan hindre noen i å forsøke å ramme oss med digitale våpen, men vi vil for hver gang se til at våpenet blir betraktelig sløvere hvis det brukes mot oss». Hensikten er å påvirke kost-nytte-analysen den offensive aktører, samtidig som faren for eskalering holdes på et lavt nivå.

Første trekk:

Den sterkere staten har i første trekk initiativet siden den svakere staten ønsker å opprettholde status-quo. Her må den sterkere staten gjøre en kost-nytte-analyse for å avgjøre om den ønsker å utfordre den svakere staten gjennom å forsøke å infiltrere og få kontroll på den svakere statens infrastruktur. Hvis den sterke staten i dette trekket konkluderer med at den potensielle kostnaden ved å iverksette offensive operasjoner gjennom det digitale domenet er

større enn den potensielle nytten, vil han velge å opprettholde status-quo. Den sterkere staten vil her kunne observere at den andre aktøren fremstår med en rekke sårbarheter, og avhengig av kjennskap til den svakere statens strategi og kommunikasjon kunne konkludere at den står ovenfor et sårbart mål der det vil være gode muligheter for at offensive tiltak vil kunne gi avkastning. På den andre siden, hvis aktøren er kjent med at den svakere staten har en strategi om å framstå svakere enn den i realiteten er, for å eventuelt påføre den offensive parten en ekstra kostnad, står den offensive aktøren ovenfor et dilemma. Hvis tidligere erfaring tilsier at den svakere staten har en reell evne til å kompromittere operasjonsmetode og virkemidler, vil dette telle i retning av at den sterkere staten vil velge å opprettholde status-quo. Hvis den sterkere staten tviler på at den svakere staten har denne evnen, vil dette telle i retning av å utfordre den svakere staten.

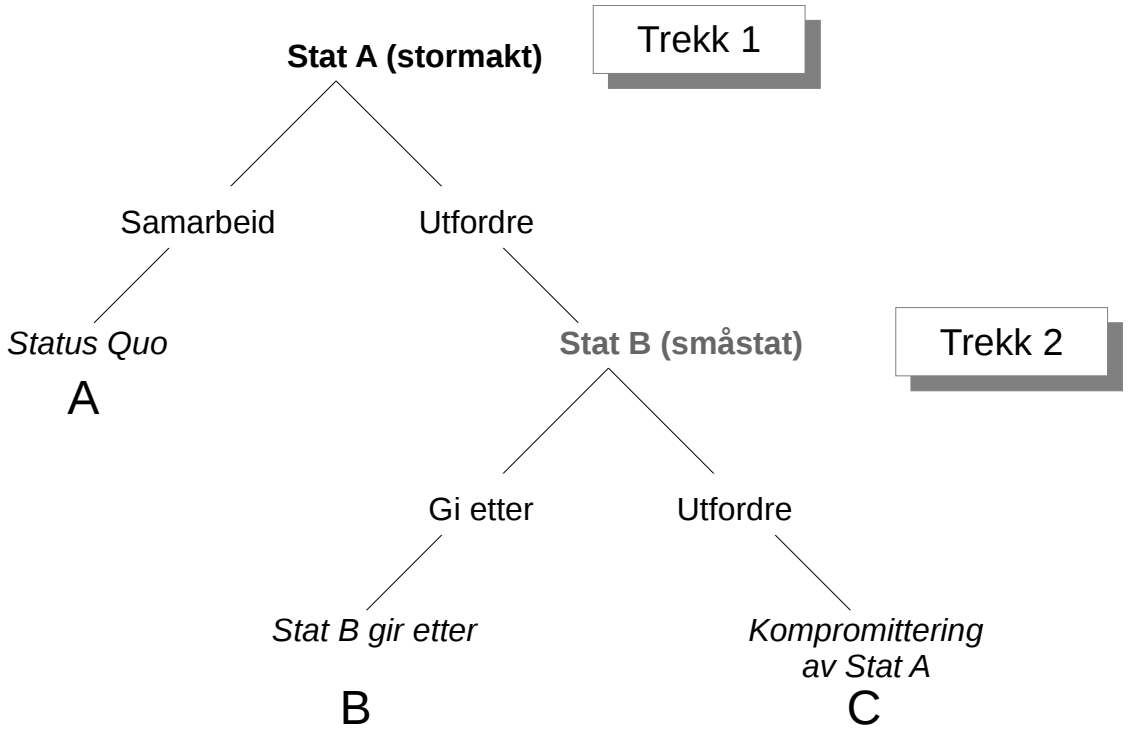
Andre trekk:

Den svakere staten er den neste som må ta et strategisk valg. Den sterke staten har nå valgt å iverksette offensive operasjoner gjennom det digitale domenet mot den svakere staten, mens den svakere staten vil sikre sine kritiske systemer på best mulig måte. Den offensive aktøren kan nå enten lykkes i å trenge inn i kritisk infrastruktur gjennom en faktisk sårbarhet, eller den vil operere mot fabrikkerte sårbarheter som er etablert av den svakere staten. I det første tilfellet vil det kunne ta tid for den svakere staten å detektere inntrengingen, men den defensive strategien tilsier at den over tid vil kunne detekterer og analysere infiltrasjonen. I det andre tilfeller der den sterkere staten begynner å operere mot den falske sårbarheten, vil den svakere staten få en umiddelbar deteksjon, samt gode forutsetninger for å analysere den offensive aktøren og avdekke operasjonsmetoder og eventuelle virkemidler. Den svakere staten står da ovenfor to strategiske valgmuligheter: I det første strategiske valget begrenser den svakere staten seg til å reetablere kontroll på egen kritiske infrastruktur og sikre seg mot et tilsvarende angrep i framtiden. Her vil vi unngå en eventuell eskalering mot den sterkere staten, og vil samtidig kunne maksimere kostnaden det vil ha for den sterkere staten å opprettholde sine offensive operasjoner. I den andre strategiske handlemåten, velger den svakere staten å påføre den offensive aktøren ytterlig kostnader gjennom å frigi informasjon som vil ha stor verdi for tredjeparts aktører, som da kan sikre seg mot den sterkere aktørens metoder og virkemidler. Denne reaksjonen vil typisk være godt under terskelen for å eskalere situasjonen, spesielt om den svakere staten velger å ikke attribuere hendelsen til den sterkere staten. En slik attribusjon er heller ikke nødvendig for påføre den sterkere staten kostnader ettersom en deling av objektiv informasjon i prinsippet også vil kunne nøytralisere den offensive statens operasjonsmetoder og virkemidler.

Tredje trekk (gjentakelse av første trekk):

Som vi har sett så søker denne nektelsesstrategien å påføre offensive aktører kostnader som er direkte tilknyttet den offensive handlingen og som søker å unngå en involvering av et politisk nivå. Det betyr i praksis at denne modellen, som vi har sett i de foregående modellene, ikke har et tredje trekk der den sterkere staten vurderer en form for eskalering mot den svakere staten. I stedet vil dette bli en gjentagende modell der vi etter det andre trekket igjen starter på det første trekket. Det som endrer seg mellom hver av disse rundene, er den sterkere statens oppfattelse av hvor god den svakere statens nekelsesstrategi er. Hvis den sterkere staten erfarer at de offensive operasjonene mot den svakere statens infrastruktur gir resultater, vil den velge å fortsette å utfordre den svakere staten. Hvis den på den andre siden erfarer at den bruker mye ressurser mot fabrikerte sårbarheter som ikke materialiserer seg, samtidig som dens metoder blir kompromittert, er det større sannsynlighet for at kost-nytte-analysen lander på at en opprettholdelse av status-quo er den mest hensiktsmessige valget.

5.3.1 Vurdering av preferanser



Illustrasjon 10: Avskrekking gjennom nektelse og avledning -løsningsalternativer.

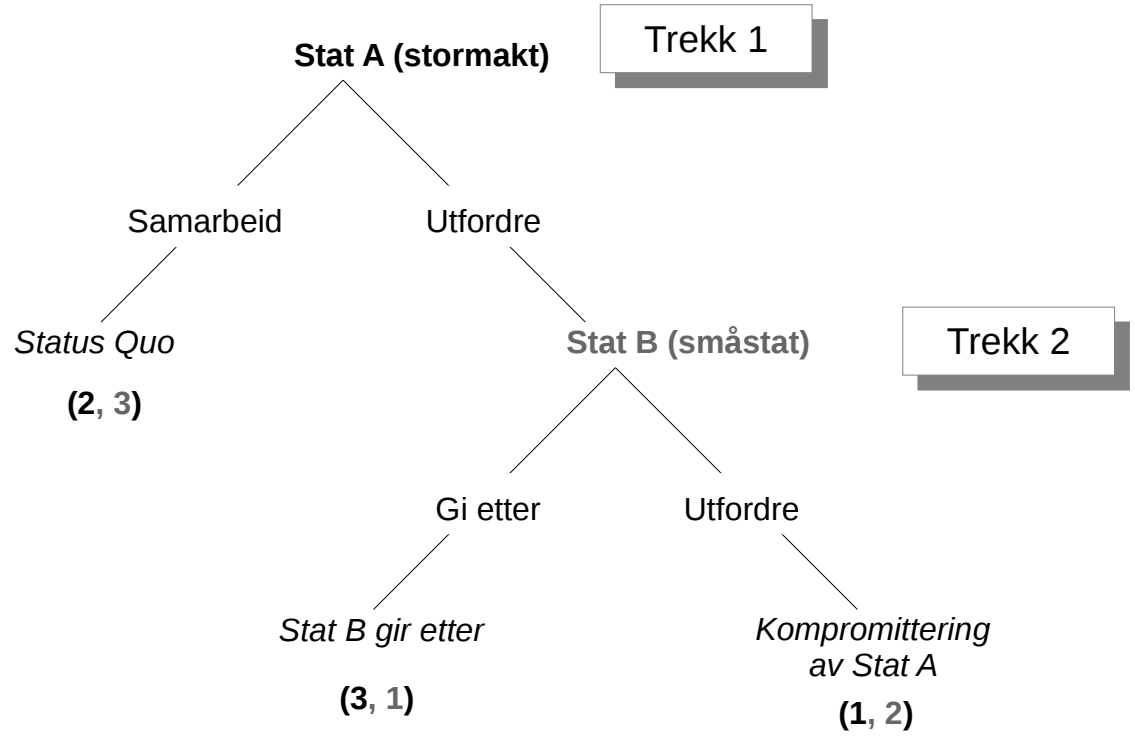
Preferanser og gevinster Stat A (stormakt)

I denne modellen har vi tidligere i analysen kommet fram til at Stat B sitt virkemiddel ikke har en eskalerende effekt. I praksis betyr det at modellen er gjentagende etter trekk 2, mens gevinstene kan endre seg mellom hver iterasjon av spillet. Hvis vi ser på Stat A sine preferanser ut ifra modellbeskrivelsen før den første iterasjonen, kan vi si at en kompromittering av handlemåte og virkemidler (C) er den minst prefererte for Stat A. Altså C=1. Stat A sitt mål er fremdeles å infiltrere Stat B sin kritiske infrastruktur og *samarbeid* for å opprettholde status-quo (A) understøtter dermed ikke denne målsettingen. Altså er A=2. Til slutt står vi igjen med det den prefererte løsningen der Stat B i trekk 2 gir etter for Stat A, uten å påføre den kostnad i form av å kompromittere operasjonsmetoder og virkemidler (B). Stat A sin foretrukne løsning er dermed B=3.
Stat A preferanser og gevinster blir dermed: B=3, A=2 og C=1

Preferanser og gevinster Stat B (småstat)

Den minst prefererte løsningen for Stat B i denne modellen er å *gi etter (*B) for stat A i trekk 2 da dette leder til størst mulighet for at Stat A lykkes i å kompromittere stat B sin kritiske infrastruktur og reduserer småstatens relative makt. Altså er B=1. Den nest minst prefererte løsningen er å utfordre og kompromittere Stat A i trekk 2 da dette ikke er i henhold til Stat B sin overordnede målsetting. Altså er C=2. Den prefererte løsningen dermed *samarbeid* og opprettholdelse av status quo (A). Altså er A=3.
Stat B preferanser og gevinster blir dermed: A=3, C=2 og B=1

5.3.2 Baklengs induksjon og løsning av delspill-perfekt likevekt

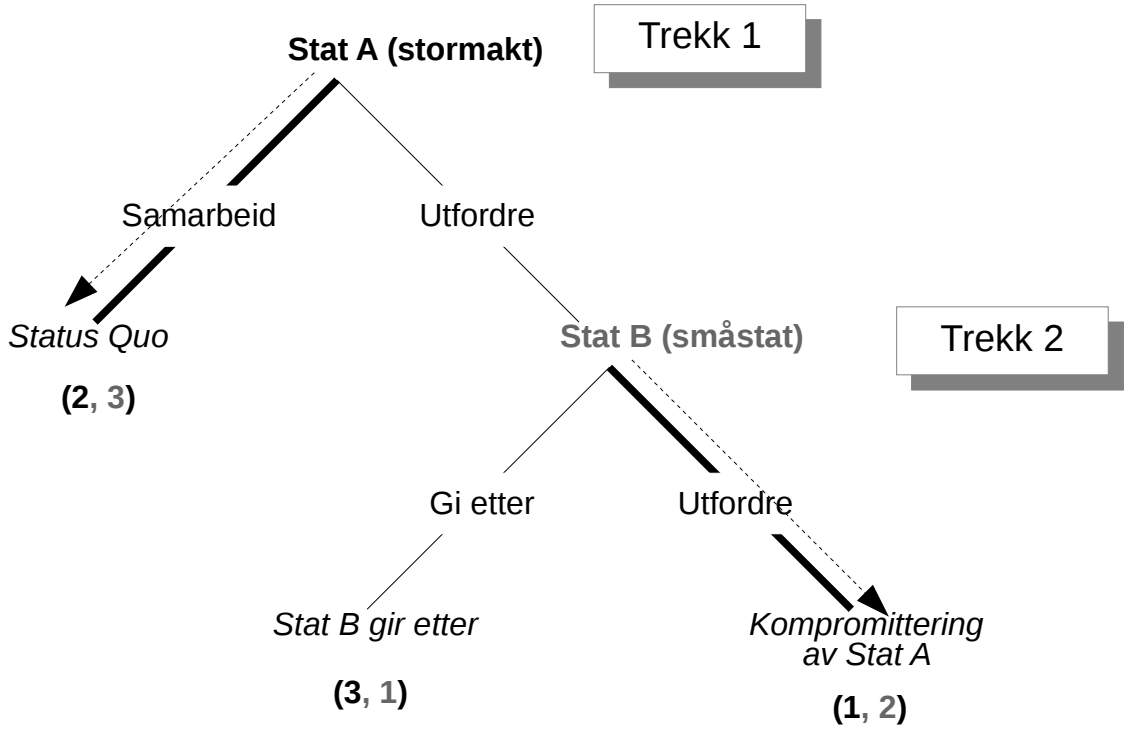


Illustrasjon 11: Avskrekking gjennom nektelse og avledning – preferanser.

Basert på denne rangeringen av preferanser kan vi gjennomføre en baklengs induksjon for å identifisere delspillperfekte likevekter. Først ser vi på Trekk 2 hvor det er den svakere staten - Stat B som skal foreta valget, står den ovenfor et valg om å *gi etter* (1) ved å ikke påføre Stat A kostnaden ved å kompromittere operasjonsmetode og virkemidler, eller utfordre stat A (2). Ettersom *utfordre* (2) er større enn å gi etter (1) er det rasjonelle valget for Stat B i trekk 2 å utfordre Stat A.

Når vi så ser på trekk 1 hvor den sterkere staten - Stat A står ovenfor et valg mellom å opprettholde status-quo (2), eller utfordre Stat B ved å forsøke å infiltrere hans kritiske infrastruktur, har vi allerede sett at det rasjonelle valget for Stat B i Trekk 2 vil være å utfordre (2) Stat A. Det betyr at Stat A i trekk 1 står ovenfor et valg mellom samarbeid (2) som videre status-quo eller å bli utfordret (1) av Stat B i trekk 2. Ettersom *samarbeid* (2) er større enn *utfordre* (1) i trekk 1 er det rasjonelle valget for Stat A her å velge *samarbeid* (2) og dermed opprettholde status-quo.

Løsningen på spillet er dermed:



Illustrasjon 12: Avskrekking gjennom nektelse og avledning – løsning.

<Stat A>, <Stat B>
<Samarbeid>, <Utfordre>

5.3.3 Delkonklusjon avskrekking gjennom nektelse og avledning

Vi ser i dette spillet at den svakere staten er i stand til å opprettholde status-quo og avskrekke de offensive operasjoner som har til hensikt å infiltrere den svakere statens kritiske infrastruktur. En viktig forutsetning må være til stede for at det skal være mulig å oppnå dette og det er at den defensive aktøren må være i stand til å demonstrere at den påfører den offensive aktøren en tilstrekkelig kostnad. I praksis betyr det at den svakere staten må være i stand til å påvirke offensiv-defensiv balansen til å bli en fordel for defensiven. Strategien forsøker å oppnå dette gjennom en kombinasjon av å framstå med mange fabrikkerte sårbarheter som har til hensikt å binde opp ressurser hos den offensive aktøren. Samtidig kan den defensive aktøren analysere aktiviteten som foregår mot de fabrikkerte sårbarhetene og dermed sette seg selv i stand til å kompromittere den offensive aktørens metoder og virkemidler. Den defensive aktøren øker også sin forutsetning for å lykkes gjennom å unngå virkemidler som kan eskalere det bilaterale forholdet med den offensive staten. Ved å unngå

eskalering gjøres spillet om til et gjentakende spill, der den defensive staten i stedet for å havne i en bilateral konflikt, får mulighet til å utvikle sin defensive kapasitet fram til et punkt der den offensive staten erfarer at det ikke lengre er hensiktsmessig å videreføre offensive operasjoner. Ved unngå å eskalere situasjonen utnytter i praksis denne defensive strategien at vi her står ovenfor en repeterbar og symetrisk avskrekking. Offensive operasjoner og gjengjeldelse er altså repeterbare i det digitale domenet ettersom en offensiv handling ikke vil slå ut den defensive aktørens evne til å reagere. Maktforholdet er derimot asymmetrisk dersom situasjonen eskalerer over i det fysiske domenet, ettersom vi har en stormakt som handler ovenfor en småstat. Gjennom åpen deling av informasjon om offensive aktørers metoder og virkemidler, er også småstaten i en posisjon der den støtter både statlige og ikke-statlige aktører.

Dette spillet viser altså at en avskrekkingsstrategi basert på nektelse, kombinert med ulike tiltak som maksimerer kostnaden for en offensiv aktør, kan endre offensiv-defensiv-balansen til fordel for defensiven. Hvis de kostnadspåførende tiltakene også unngår å eskalere mellomstatlige relasjonener i negativ retning, har vi et gjentakende spill der den svakere staten kontinuerlig kan lære og forbedre avskrekkingsmiddelet.

6 Konklusjon

> ... right, as the world goes, is only in question between equals in power, while the strong do what they can and the weak suffer what they must?
> Thucydides

Hensikten med denne studien var å søke å svare på om det er rasjonelt grunnlag for å utvikle en avskrekkingsevne i det digitale rom for en småstat. Ettersom dette domenet er relativt ungt, finnes det i praksis lite empiri studien kan støtte seg på. Mangelen på empiri forsterkes ytterlig av at domenet fortsatt preges av høy grad dynamikk og utvikling, både innenfor teknologi, doktriner og nasjonalstaters strategi. Studien har derfor utviklet hypoteser i form av tre ulike avskrekkingsstrategier og testet disse gjennom å anvende spillteori. Spillmodellene støtter seg på relevant teori innenfor internasjonal politikk.

Studien er relevant ettersom det digitale domenet de siste årene har vært en aktuell problemstilling høyt på politiske agendaer hos alle nasjonalstater med en moderne samfunnsstruktur. Årsaken til dette er at en fungerende digital infrastruktur i dag er en forutsetning for at samfunnsystemet fungerer, samtidig som at den digital infrastrukturen er sårbar for påvirkning fra eksterne aktører. De fleste nasjonalstater arbeider i dag med å begrense disse sårbarhetene og de siste årene er det gjennomført mye forskning knyttet til avskrekking av trusler mot den kritiske infrastrukturen. Det unike ved denne studien er at den ser nærmere på avskrekking i det digitale rom i konteksten av en småstat. Studien avgrenser seg til å se på avskrekkingsvirkemidler i det digitale domenet og nasjonalstater som aktører.

Den generelle oppfattelsen om at domenet i dag favoriserer den offensive parten, skaper et insentiv for at stater utvikler offensive kapasiteter i det digitale domenet. Ettersom domenet gir rom for å operere offensivt under terskelen for hva som regnes som et væpnet angrep, kan slike operasjoner påvirke maktbalansen mellom stater ved å stjele en stats intellektuelle eiendom, eller true kritisk infrastruktur i en aktuell stat i fredstid.

Strukturell realismeteori sier at nasjoner søker makt for å ivareta sin egen sikkerhet, samtidig ser vi at USA som av mange i dag regnes som hegemonen i et unipolart system, i vesentlig grad er et offer for offensiv aktivitet gjennom det digitale domenet. Når hegemonen i et system ikke lykkes med sin avskrekkingsstrategi, er det i seg selv grunnlag nok til å stille spørsmål om hvorvidt avskrekking for en småstat kan lykkes.

Denne studien skal svare på om hvorvidt det er rasjonelt for en småstat å forfølge en avskrekkingsstrategi. Hvis strategien skal være rasjonell må det finnes en rimelig

sannsynlighet for at den skal kunne lykkes i å oppnå avskrekking, og samtidig ha lav sannsynlighet for å undergrave småstatens øvrige strategiske målsettinger.
Denne studien har testet avskrekkingsteori ved å spillmodellere avskrekking gjennom nektelse og avskrekking gjennom straff, for å vurdere potensialet disse har for en småstat. Hensikten med disse modellene er ikke å være preskriptive for hvordan en stat bør utforme sin avskrekkingsstrategi, men å avdekke hvordan vesentlige faktorer påvirker ulike avskrekkingsstrategier for en småstat og hvorvidt det forutsatt disse faktorenes påvirkning, fremdeles er rasjonelt å utvikle en avskrekkingsstrategi. Ettersom teoriene vi støtter oss på i analysen er relativt unøyaktige erstatninger for virkeligheten, må vi også forutsette at vi kun kan trekke grove konklusjoner ut av denne studien.
Studien viser at avskrekking i det digitale rom er generelt krevende, og er sannsynligvis mere krevende for en småstat. En felles utfordring for alle avskrekkingsstrategier er at det digitale rom i dag har egenskaper som tilbyr et handlingsrom under terskelen for hva som kan defineres som et væpnet angrep, samtidig som attribusjonsproblemet gir forutsetninger for at den offensive parten kan skjule, eller benekte innblanding. Det digitale rom kan benyttes til å påvirke maktbalansen i favør den offensive parten ved at den offensive staten skaffer seg evne til å degradere andre staters kritiske infrastruktur, eller stjele deres intellektuelle eiendom og dermed redusere deres evne til å generere rikdom. Dette er til sammen sterke insentiver for at offensive operasjoner i det digitale rom har stor nytteverdi. Avskrekkingens rolle er dermed å påføre en offensiv aktør en kostnad som opphever denne nytteverdien.

En avskrekking basert på nektelse gjennom passiv beskyttelse av egen infrastruktur har fordel ved at den har et lavt potensiale for å være eskalerende. Ulempen er at det i dag ansees som svært vanskelig å sikre hele den kritisk infrastruktur på en god nok måte. Angrepsflaten og mulighetene den representerer for en offensiv part er stor. Samtidig er kostnadene ved å kontinuerlig forsøke å lete etter sårbarheter relativt lave. En strategi basert på passiv beskyttelse vil med høy sannsynlighet kreve oppfølging med diplomatiske virkemidler når hendelser oppstår. Denne strategien har således en svak eller ingen avskrekkende effekt. Passiv beskyttelse av infrastrukturen er en grunnsikring og dermed en forutsetning for å ha neon som helst sikring av kritisk infrastruktur, men som avskrekkingsstrategi er den med høy sannsynlighet for svak.

En avskrekkingsstrategi basert på straff gjennom å true med gjengjeldelse har på en annen side et høyere potensiale for i tilstrekkelig grad å påvirke kost-nytteanalysen til en offensiv aktør. Det finnes ennå i dag lite empiri på at maktbruk gjennom det digitale domenet har gitt

konsekvenser som gir vesentlig grunnlag for å avskrekke en offensiv aktør, men det finnes et viss teoretisk grunnlag som kan understøtte at det er mulig. For en småstat er likevel hovedutfordringen med denne strategien at den med stor sannsynlighet vil føre til en eskalering av situasjonen som med stor sannsynlighet vil være i disfavør en småstat. En avskrekkingsstrategi basert på straff vil for en småstat for det første framstå som irrasjonell. Dette er nødvendigvis ikke diskvalifiserende for en avskrekkingsstrategi, men mer problematisk da den antageligvis vil ha lav troverdighet. Alt i alt kan en avskrekkingsstrategi basert på straff skape flere problemer for en småstat enn den potensielt løser, dermed er det en dårlig løsning.

En avskrekkingsstrategi basert på nektelse og avledning, er en modell som representerer en mer aktiv form for beskyttelse som søker å maksimere muligheten for at den offensive parten bruker tid og ressurser på aktiviteter som ikke gir avkastning. Videre legger strategien opp til å skaffe informasjon om sofistikerte aktørers metoder og virkemidler og dele dette åpent og objektivt for redusere potensialet for at metodene kan gjenbrukes. Dette påfører den offensive aktøren en ytterlig kostnad ved at andre potensielle mål lærer å beskytte seg mot metodene. Til slutt tilfører den usikkerhet hos den offensive aktøren der den må stille spørsmål om den egentlig har infiltrert den defensive aktørens infrastruktur, eller om den er fanget i en avledning. Strategien øker dermed kostnaden samtidig som den også senker nytten for en offensiv aktør, da aktøren er usikker på om den egentlig har infiltrert en kritisk infrastruktur, eller om den er fanget i et avledningstiltak. Ved at strategien kun påfører kostnad til den offensive operasjonen eller selve angrepet fører også til at den gir lav eskalerende effekt. Vi har sett at avskrekking i det digitale rom skiller seg fra avskrekking med eksempelvis atommakt ved at den er repeterbar. En avskrekkingsstrategi basert på nektelse og avledning utnytter dette ved at den i stedet for å eskalere situasjonen gir mulighet til å gjenta «spillet». For hver iterasjon av spillet har den offensive og den defensive aktøren «lært» av foregående iterasjon. Det betyr at avskrekkingsstrategien kan utvikle seg til å fungere på tross av at den ikke fungerer i starten. Den kan bli toverdig på tross av at den ikke er troverdig fra starten. Den kan dermed oppnå avskrekking etterhvert, på tross av å ikke være avskrekkende nok fra starten. Strategien synes dermed å spille bedre på det digitale domenets særegenheter. På tross av at strategien ser ut til å være anvendbar for en småstat, er det likevel ingen garanti for et den vil være tilstrekkelig da vi har sett på dette ut ifra teoretiske betraktninger. Det finnes ikke empiri på at denne strategien er effektiv, men heller ingen empiri på det motsatte.

Denne studien konkluderer dermed med at avskrekking i det digitale rom i dag generelt sees på som krevende, og er sannsynligvis mer krevende for en småstat som må unngå strategier som kan føre til eskalering. Domenet skaper rom for at en offensiv aktør kan operere mot en annen stat under terskelen for det som regnes som et væpnet angrep og vil dermed ikke etablere en krigstilstand. Små stater kan dermed ikke forutsette støtte fra en eventuell forsvarsallianse. På tross av dette ser vi at det er mulig å forme en avskrekkingsstrategi for en småstat ved at den støtter seg på særegenheter ved det digitale rom. Konklusjonen er dermed at det er rasjonelt for en småstat å etablere en avskrekkingsstrategi i den grad strategien evner å ta hensyn til småstatens begrensinger og samtidig klarer å utnytte det digitale rommets særegenheter.

7 Litteraturliste:

Areng, L. (2014). Lilliputian States in Digital Affairs and Cyber Security. *Tallinn Paper*, (4).

Balance, T. M. (2018). Chapter Seven: Middle East and North Africa. *The Military Balance*, *118*(1), 315–374. http://doi.org/10.1080/04597222.2018.1416983

Bennett, P. G. (1995). Modelling Decisions_Bennett.pdf. *Mershon International Studies Review*.

Borger, J. (2018). US accuses Russia of cyber-attack on energy sector and imposes new sanctions | US news | The Guardian. Hentet 17. mars 2018, fra https://www.theguardian.com/us-news/2018/mar/15/russia-sanctions-energy-sector-cyber-attack-us-election-interference

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

Chang, S. (2017). Here's all the money in the world, in one chart - MarketWatch. Hentet 5. mars 2018, fra https://www.marketwatch.com/story/this-is-how-much-money-exists-in-the-entire-world-in-one-chart-2015-12-18

Defence Science Board. (2017). *Task force on Cyber Deterrence*.

Dunne, T., Kurki, M., & Smith, S. (2013). *International Relations Theories Disipline and Diversity* (Third Edit). Oxford: Oxford University Press.

Etteretningstjenesten. (2018). Fokus 2018.

Finkle, J. (2016). Apple offers big cash rewards for help finding security bugs. Hentet 14. april 2018, fra https://www.reuters.com/article/us-cyber-blackhat-apple/apple-offers-big-cash-rewards-for-help-finding-security-bugs-idUSKCN10F2TX

Forsvarets høgskole. (2013). Manual i krigens folkerett. Oslo.

Forsvarsdepartementet. (2014). Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren. Oslo: Forsvarsdepartementet.

Fullerton, J. (2018). China's threat to fight trade war «to the end» sends Asian markets tumbling after Trump escalates tariffs row. Hentet 26. mars 2018, fra https://www.telegraph.co.uk/business/2018/03/23/chinas-threat-fight-trade-war-end-sends-asian-markets-tumbling/

Greenberg, A. (2017). Russia's Cyberwar on Ukraine Is a Blueprint For What's to Come | WIRED. Hentet 17. mars 2018, fra https://www.wired.com/story/russian-hackers-attack-ukraine/

Guner, S. (2012). A Short Note on the Use of Game Theory in Analyses of International Relations. Hentet fra http://www.e-ir.info/2012/06/21/a-short-note-on-the-use-of-game-theory-in-analyses-of-international-relations/

Harper Lecture with John J. Mearsheimer: Can China Rise Peacefully? - YouTube. (2013). Hentet 5. februar 2016, fra https://www.youtube.com/watch?v=0DMn4PmiDeQ

Heckman, K. E., Stech, F. J., Schmoker, B. S., & Thomas, R. K. (2015). Denial and Deception in Cyber Defense. *Computer*, *48*(4), 36–44. http://doi.org/10.1109/MC.2015.104

Hovi, J. (2008). *Spillteori En innføring*. Oslo: Universitetsforlaget.

Huesken, F. W. (2012). International Systems, Polarity, Cybertechnology, and Stability. *SYNESIS*, 40–51.

Ikenberry, J., Mastanduno, M., & Wolforth, W. (2009). Introduction: Unipolarity, State Behavior, and Systemic Consequences. I *World Politics* (Bd. 61, s. 1–27). Cambridge University Press. Hentet fra http://www.jstor.org/stable/40060219

Inkster, N. (2017). Measuring Military Cyber Power. *Survival*, *59*(4), 27–34. http://doi.org/10.1080/00396338.2017.1349770

International Institute for Strategic Solutions. (2013). Chapter Three: North America. *The Military Balance*, *113*(1), 49–88. http://doi.org/10.1080/04597222.2017.1271209

Jasper, S. (2017). *Strategic cyber deterrence : the active cyber defense option*. Lanham: Rowman & Littlefield. Hentet fra https://www.amazon.com/Strategic-Cyber-Deterrence-Active-Defense-ebook/dp/B072JXFFJ8/ref=sr_1_4?s=digital-text&ie=UTF8&qid=1521744662&sr=1-4&keywords=deterrence

Jervis, R. (2013). Offense, defense, and the security dilemma. *International politics*, (11), 1689–1699.

Jon R. Lindsay, Tai Ming Cheung, D. S. R. (2015). *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press.

Kello, L. (2017). *The virtual weapon and international order.*

Knutsen, T. (2012). Mr. Geopolitics. I *Internasjonal politikk* (70. utg., s. 245–266). Universitetsforlaget.

Libicki, M. C. (2016). *Cyberspace in peace and war*. Annapolis: Naval Institute Press. Hentet fra https://books.google.no/books?id=m4f9DAAAQBAJ&printsec=frontcover&dq=cyberspace+in+peace+and+war&hl=no&sa=X&ved=0ahUKEwjM04vT-NvZAhVHJ5oKHUGlAGcQ6AEIKDAA#v=onepage&q=cyberspace in peace and war&f=false

Libicki, M. C., & Project Air Force (U.S.). (2009). *Cyberdeterrence and cyberwar*. RAND.

Lynn, W. J. (2010). Defending a New Domain the Pentagon's Cyber Strategy. *Foreign Affairs*, *89*(5), 97–108. Hentet fra http://www.scribd.com/doc/36500793/Defending-a-New-Domain-the-Pentagon-s-Cyber-Strategy

Mandiant. (2013). *Mandiant, APT1: Exposing One of China's Cyber Espionage Units*. *Report*. Hentet fra http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Mearsheimer. (2007). *The Tragedy of Great Power Politics*. Academic Internet Pub Incorporated. Hentet fra https://books.google.com/books?id=JReUPQAACAAJ&pgis=1

Mearsheimer, J. J. (1983). *Conventional deterrence*. Cornell University Press. Hentet fra https://books.google.no/books?id=lNwZDgAAQBAJ&printsec=frontcover&dq=conventional+deterrence&hl=no&sa=X&ved=0ahUKEwjI_K-fr9jZAhWGDuwKHYzmD8cQ6AEIKDAA#v=onepage&q=conventional deterrence&f=false

Mearsheimer, J. J. (2013). Structural Realism. I *International Relations Theories Disipline and Diversity2* (Third Edit, s. 77–). Oxford: Oxford University Press.

Meunier, P. (2006). Reporting Vulnerabilities is for the Brave - CERIAS - Purdue University. Hentet 14. april 2018, fra https://www.cerias.purdue.edu/site/blog/post/reporting-vulnerabilities-is-for-the-brave/

Muller, L. P., & Stevens, T. (2017). Upholding the NATO cyber pledge Cyber. *Policy Brief 5 / 2017*. NUPI. Hentet fra http://www.nupi.no/en/About-NUPI/Projects-centres-and-programmes/Cyber-Security-Centre/Upholding-the-NATO-cyber-pledge

Nakashima, E., & Warrick, J. (2012). Stuxnet was work of U.S. and Israeli experts, officials say - The Washington Post. Hentet 25. februar 2018, fra https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.4aeb95ef200f

Nasdaq. (2018). Apple Inc. (AAPL) Income Statement - NASDAQ.com. Hentet 5. mars 2018, fra https://www.nasdaq.com/symbol/aapl/financials?query=income-statement

North Atlantic Treaty Organisation. (2016). Warsaw Summit Communiqué, (July), 1–30. Hentet fra http://www.nato.int/cps/en/natohq/official_texts_133169.htm

NUPI. (2017). Upholding the NATO cyber pledge: What does cyber deterrence and cyber resilience mean for NATO and Norway? - Forskningsprosjekt | NUPI. Hentet 21. april 2018, fra http://www.nupi.no/Om-NUPI/Prosjekter-sentre-og-programmer/Upholding-the-NATO-cyber-pledge-What-does-cyber-deterrence-and-cyber-resilience-mean-for-NATO-and-Norway

Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), 44–71.

Paletta, D., Yadron, D., Valentino-DeVries, J., Palette, D., Yadron, D., & Valentino-DeVries, J. (2015). Cyberwar Ignites a New Arms Race. Hentet 21. februar 2018, fra https://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128

Perlroth, N., & Shane, S. (2017). How Israel Caught Russian Hackers Scouring the World for U.S. Secrets - The New York Times. Hentet 25. februar 2018, fra https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html

Politico. (2016). Obama warns of cyber «arms race» with Russia - POLITICO. Hentet 7. april 2018, fra https://www.politico.com/story/2016/09/obama-russia-cyber-arms-race-227732

Rogin, J. (2012). NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history" – Foreign Policy. Hentet 8. april 2018, fra http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/

Saltzman, I. (2013). Cyber posturing and the offense-defense balance. *Contemporary Security Policy*, *34*(1), 40–63. http://doi.org/10.1080/13523260.2013.771031

Schelling, T. C. (2008). *Arms and influence*. Hentet fra https://books.google.no/books?id=TX_yAAAAQBAJ&dq=arms+and+influence&hl=no&sa=X&ved=0ahUKEwjQpuTeydnZAhWE26QKHT97BHQQ6AEIKDAA

Schmitt, M. N., & NATO Cooperative Cyber Defence Centre of Excellence. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge: Cambridge University Press. Hentet fra https://books.google.no/books?id=n9wcDgAAQBAJ&printsec=frontcover&dq=tallinn+manual+2.0&hl=no&sa=X&ved=0ahUKEwj_zND11PraAhWD1ywKHWWkCMgQ6AEIKDAA#v=onepage&q=tallinn manual 2.0&f=false

Sheldon, J. B. (2014). Geopolitics and Cyber Power: Why Geography Still Matters. *American Foreign Policy Interests*, *36*(5), 286–293. http://doi.org/10.1080/10803920.2014.969174

Shen, L. (2017). Apple Nears $1 Trillion Thanks to iPhone X | Fortune. Hentet 5. mars 2018, fra http://fortune.com/2017/11/08/apple-stock-amazon-trillion-aapl-iphone-x/

Snyder, G. H. (2002). Mearsheimer's World: Offensive Realism and the Sruggle for Security. *International Security*, *27*(1), 149–173.

Spaniel, W. (2011). *Game theory 101 : the complete textbook*. Hentet fra https://books.google.no/books?id=4d2xoAEACAAJ&dq=game+theory+101&hl=no&sa=X&ved=0ahUKEwiwwsyuxeTaAhVwhaYKHfKrBsEQ6AEILjAB

Stone, R. W. (2001). The Use and Abuse of Game Theory in International Relations: The Theory of Moves. *The Journal of Conflict Resolution*, *45*(2), 216–244. Hentet fra http://www.jstor.org/stable/3176277

Tadelis, S. (2013). *Game theory : an introduction*. Princeton University Press. Hentet fra https://books.google.no/books/about/Game_Theory.html?id=eLkOJPwAdu8C&redir_esc=y

Tamnes, R., Bundt, K. H., Grytting, T., Hoel, A. H., Matlary, J. H., Toje, A., & Wilhelmsen, J. (2015). Et felles løft, 1000.

Tan, E. E. (2018). *Cyber Deterrence in Singapore : Framework & Recommendations*. Singapore. Hentet fra http://hdl.handle.net/10220/44634

Tunsjø, Ø. (2014). The Return of Bipolarity (s. 41).

US-CERT. (2018). Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors | US-CERT. Hentet 17. mars 2018, fra https://www.us-cert.gov/ncas/alerts/TA18-074A

Waltz, K. (1979). *Theory of international politics*. *Addison-Wesley Publishing Company*. Hentet fra https://www.press.umich.edu/pdf/9780472099818-ch1.pdf

Waltz, K. N. (1979). Theory of International Politics. (Bd. 78, s. 60–78). McGraw-Hill.

Williams, K. P., Lobell, S. E., & Jesse, N. G. (2012). *Beyond great powers and hegemons : why secondary states support, follow or challenge*. Stanford University Press.

Wilner, A. (2017). Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation. *Comparative Strategy*, *36*(4), 309–318. http://doi.org/10.1080/01495933.2017.1361202

Yadav, T., & Rao, A. M. (2015). Technical aspects of cyber kill chain. *Communications in Computer and Information Science*, *536*, 438–452. http://doi.org/10.1007/978-3-319-22915-7_40

Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid | WIRED. Hentet 17. mars 2018, fra https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/