MASTEROPPGAVE

Emnekode: SO330S

Navn: Thomas Frost

Norges strategiske respons i møte med russiske cyberangrep - *nederlandske lærdommer og utviklingen av nytt cyberstrategisk konsept*

Dato: 12. november 2023

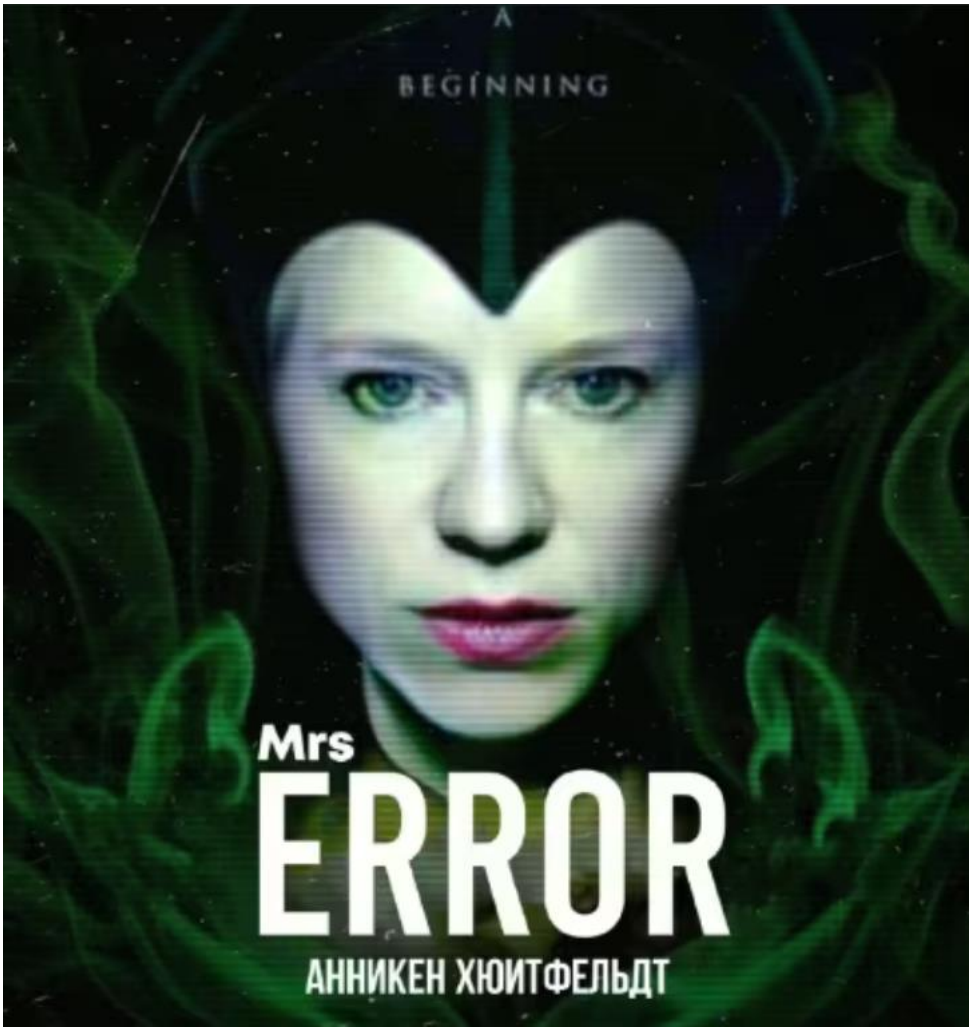
Totalt antall sider: 84

NORD universitet

www.nord.no

«Jeg leder nå en regjering som egentlig er under angrep»

Jonas Gahr Støre, 7. august 2023



FORORD

Denne oppgaven markerer slutten på min mastergrad i samfunnsvitenskap med fordypning i internasjonale relasjoner. Tidligere har jeg sagt at jeg aldri skal ta en mastergrad. For en absurd tanke! På tross av det, sitter jeg nå med en ferdig oppgave. Det har vært en inspirerende prosess som har inneholdt de fleste sinnsstemninger. Fra enorm arbeidslyst og motivasjon, til dyp frustrasjon og mangel på både tid og energi. Å gjennomføre et masterstudie samtidig med småbarnstilværelse og fulltidsjobb har periodevis medført en krevende prosess. Nå er jeg endelig ferdig.

Jeg vil gjerne takke dyktige og dedikerte forelesere ved Nord Universitet for noen meget spennende og inspirerende år. En særlig takk går også til veileder Torbjørn Pedersen for profesjonalitet, faglig kompetanse, nyttige innspill, samt verdifulle tilbakemeldinger.

Den aller største takken må likevel gå til dere på hjemmebane. Takk til alle jeg har spurt om råd, som har lest igjennom, kommet med innspill og bidratt til gode diskusjoner.

Selv om skriveprosessen har vært individuell, har det i realiteten vært en laginnsats. En særlig takk må derfor rettes til min kone Anette for utelukkende støtte og forståelse. Til slutt en stor takk og bamseklem til min datter Martine, som innimellom har tvunget meg til å koble av og bare være pappa. Vi er et godt team!

God lesning.

November 2023

Thomas Frost

SAMMENDRAG

Norge har de siste årene jevnlig blitt rammet av cyberangrep. Som følge av økt digitalisering og teknologisk avhengigheter, har denne utviklingen bidratt til et mer sårbart samfunn. Denne studien undersøker Norges evner til avskrekking mot cyberangrep, spesifikt fra russiske statlige aktører. For dette formålet vil jeg sammenligne Norges cyberstrategi med Nederlands, fordi de har valgt en annen, mer offensiv tilnærming. Studien støtter seg på teoretiske perspektiver rundt avskrekking, attribusjon og spillteori for å identifisere hvorvidt det foreligger et ikke-utnyttet avskrekkingspotensiale for norske myndigheter. Gjennom en komparativ analyse av cyberstrategiene og spillteoretiske modelleringer av tre ulike spill, har hensikten vært å avdekke hvorvidt dagens avskrekkingsstrategi er tilstrekkelig og hvordan den eventuelt kan forbedres.

Studien viser at avskrekking innen cyberdomenet er svært utfordrende, spesielt fordi cyberangrep er fordekt av natur. Studiens analyser av avskrekkingsstrategiene om straff og nektelse peker på at Norge i mange tilfeller vil være best tjent med å forholde seg passive, da mottiltak vil kunne føre til uforholdsmessig eskalering. Utfordringen med dette, er at manglende responser igjen kan skape et farlig handlingsrom hvor Russland får være premissleverandøren for hva som er akseptabel atferd innen cyberdomenet.

På tross av utfordringene avskrekking medfører innen cyberdomenet, har Nederland de siste årene endret sin strategi, hvor de nå i større grad går inn for en mer offensiv tilnærming. I tillegg har Nederland hatt et betydelig fokus på å styrke egen resiliens. Det kan se ut til at dette har bidratt til en positiv utvikling i antallet rapporterte alvorlige cyberangrep sammenliknet med andre land. I tillegg blir nå Nederland av mange sett på som en betydelig aktør innen cybersikkerhet. Dette styrker deres målsetning om å fremstå som et lite attraktivt land å angripe.

Videre viser studien at Norge vil kunne ha en positiv effekt av i større grad å benytte seg av avskrekkingsstrategien «aktivt cyberforsvar» – et samspill mellom å etablere robuste systemer og offensive destruktive kapasiteter.

SUMMARY

In recent years, Norway has regularly been hit by cyber-attacks. As a result of increased digitization and technological dependencies, this development has contributed to a more vulnerable society. This study examines Norway's deterrence capabilities against cyber-attacks, in particular from Russian state actors. To do so, Norwegian cyber strategy has been compared to the Netherlands, as they have chosen a different, more offensive approach. The study relies on theoretical perspectives around deterrence, attribution, and game theory, to identify whether there is unsolved deterrence potential for the Norwegian authorities. Through a comparative analysis of the cyber strategies and game-theoretic modeling of three different games, the purpose has been to reveal whether the current deterrence strategy is sufficient, and how it can possibly be improved.

The study shows that deterrence in the cyber domain is incredibly challenging, especially because cyber-attacks are covert by nature. The study's analyses of the deterrence strategies of punishment and denial show that in many cases, Norway will be best served by being passive, as countermeasures could lead to disproportionate escalation. The challenge in such an approach is that a lack of response can once again create a dangerous room for action where Russia ends up being the agenda setter for what is acceptable behavior within the cyber domain.

Despite the challenges that deterrence entails in the cyber domain, the Netherlands has, in recent years, changed its strategic starting point, where they now express a more offensive approach. In addition, the Netherlands has had a significant focus on strengthening its own resilience. It may appear that this has contributed to a positive development in the number of reported serious cyberattacks compared to other countries. In addition, the Netherlands has achieved a better status and is now seen by many as a significant player in cyber security, thus strengthening their objective of appearing as an unattractive country to attack.

Furthermore, the study shows that Norway will potentially have achieved a positive effect by making greater use of the deterrence strategy “active cyber defense” – an interaction between establishing robust systems and offensive destructive capacities.

INNHOLDSFORTEGNELSE

DEL I: INNLEDNINGSKAPITLER

1.1 Introduksjon

Datoen er 24. juli 2023. På nytt har det blitt offentlig kjent at Norge er rammet av et cyberangrep. Denne gangen mot IKT-plattformen til tolv departementer. Hvilken aktør som står bak, er ennå ikke kjent. Det som derimot er klart, er at statsminister Jonas Gahr Støre to uker etter at angrepet ble kjent, karakteriserte det som et angrep mot regjeringen (Aftenposten, 2023). En slik beskrivelse fremstår uvanlig krass i norsk målestokk.

Cyberangrep mot Norge har de siste årene blitt hverdagskost. Selv om forebyggende sikkerhet tar ned den digitale risikoen, bør Norge sørge for å fremstå som et lite attraktivt land å angripe (NSM, 2022b). Evnen til å avskrekke en motstander fra å iverksette cyberangrep er derfor viktig – en strategisk kommunikasjon Norge i mange år har kombinert med beroligelse (FFI, 2022b, s. 45). Derimot skaper den raske utviklingen i det digitale domenet nye og mer komplekse utfordringer når det gjelder evnen til å avskrekke en motstander (NOU 2015: 13, s. 15). Det er også bakteppet for denne oppgaven.

Tradisjonelt sett har militære operasjoner hovedsakelig foregått i de tre konvensjonelle domenene for krigføring; til lands, på havet og i luften, senere også i verdensrommet. Selv om det i lang tid også har eksistert ukonvensjonelle metoder som for eksempel falsk flagg-operasjoner og desinformasjon ved bruk av propaganda, har trusselbildet i vesentlig grad endret seg som følge av digitalisering (NOU 2015: 13, s. 15). Digitaliseringen kan ses på som et to-egget sverd. Det er både en kilde til innovasjon, men også kilde til økt sårbarhet. Man står nå ovenfor en ny type trussel, ofte fra en ukjent trusselaktør, og som vi senere skal se, ofte med uklare respons- og håndhevingsmuligheter. Skadepotensialet ved bruk av cyberoperasjoner kan være betydelig. Strømnett kan kobles ut, kommunikasjonssystemer kan settes ut av spill, og mye annen kritisk infrastruktur kan ødelegges eller gjøres utilgjengelig for en periode (Friis, 2020, s. 30)

Russland har lange tradisjoner i å operere innen cyberdomenet. Som følge av dette har russiske cyberaktiviteter vært diskutert blant vestlige akademikere siden slutten av 90-tallet for eksempel i forbindelse med deres operasjoner i både Tsjetsjenia og Georgia (Fridman, 2018, s. 115). Russlands sikkerhetspolitiske prioriteringer har utviklet seg drastisk siden den kalde krigen. Til å være en hegemonisk utfordrer til USA under den kalde krigen utviklet det seg tidlig på 2000-tallet en diskusjon om mulig russisk medlemskap i NATO. Derfra har

polariseringen mellom øst og vest blitt forverret etter at Putin tok plass i presidentstolen i 2000. I takt med den negative trenden har også NATOs forhold til Russland utviklet seg, stort sett utelukkende i negativ retning. Dette var også en av hovedårsakene, i tillegg til Russlands krigføring i Ukraina, at NATO i 2022 endret sitt strategiske konsept. For første gang ble Russland presentert som den mest signifikante og direkte trusselen mot NATO og dens allierte (NATO, 2023, s. 3-4). I tillegg pekte NATO på at Russland har satt den europeiske sikkerhetsordenen i fare, og at det er Russland alene som er ansvarlig for å sørge for de-eskalering i den hensikt å gjenopprette et nytt samarbeid med NATO (NATO, 2023, s. 3-4).

Bruken av avskrekking bygger på en grunnleggende forståelse om at en motstander frykter en potensiell respons. Man kan finne tradisjonelle og dype historiske spor etter avskrekkingens effekter både i Bibelen og hos Thukydid som skrev om Peloponneskrigen mellom Sparta og Athen (Nye, 2017, s. 45 og Lebow, 2007). Avskrekking, sammen med beroligelse, har vært sentrale sikkerhetspolitiske kommunikasjonsbegreper, spesielt i etterkant av 2. verdenskrig og under den kalde krigen. NATO har for Norges del siden dens stiftelse tilbake i 1949 vært et av de mest betydningsfulle avskrekkingsmidlene, hvor medlemskap i alliansen har sikret Norge en legitim militær evne. Beroligelse av ikke-allierte skulle derimot skje gjennom dialog, diplomati og åpenhet (FFI, 2022b, s. 45).

Oppgaven tar utgangspunkt i Norges avskrekkingsevner i møte med russiske cyberangrep, og hvorvidt Norge har noe å lære av tilnærmingen Nederland har valgt for å håndtere de samme utfordringene. Det eksisterer en god del kunnskap fra et norsk utgangspunkt om dette temaet fra før, spesielt når det gjelder avskrekkingsteoriens potensial innen cyber (Aannø, 2018, Wilhelmsen, Larsen, Soldal Lund, Svenungsen og Aannø, 2021, Svenungsen, 2022; Pedersen 2023). I tillegg til de overnevnte, har blant annet Liebetrau, 2023; Muller, 2019; Smeets, 2022 analysert og vurdert Nederlands tilnærming og cyberstrategi. Relevant empiri tar derimot ikke i så stor grad for seg alternativer til de tradisjonelle avskrekkingsteoriene. Scott Jasper, en amerikansk akademiker spesialisert innen cyberpolicy og strategi, har etablert et forslag til ny avskrekkingstrategi, *aktivt cyberforsvar* (Jasper, 2017). Aktivt cyberforsvar vil i denne oppgaven være utgangspunktet for vurderingen av Norges avskrekkingsevner i møte med russiske cyberangrep.

Formålet med oppgaven er å forsøke å identifisere hvorvidt det ligger et ikke-utnyttet potensiale for norsk avskrekking mot cyberangrep ved å se på relevante strategier for avskrekking.

Dette gjøres gjennom å besvare og analysere følgende problemstilling:

Har Norge noe å lære av den nederlandske cyberstrategien i møte med russiske cyberangrep?

1.2 Operasjonalisering

Operasjonalisering av en problemstilling innebærer prosessen fra det generelle til det konkrete. Gjennom målrettet avgrensning av det området man har fokus på, samt konkretisering av hvordan problemstillingen kan gjøres forskbar, skal operasjonaliseringen forsøke å gi et presist meningsinnhold (Johannessen, Christoffersen & Tufte, 2011, s. 63-64).

Utgangspunktet for operasjonaliseringen er min problemstilling som tar utgangspunkt i Norges avskrekkingspotensial i møte med cyberangrep. For å gjøre problemstillingen forskbar søker jeg å dele analysen i to. Den første delen innebærer en sammenlikning mellom Nederlands og Norges nyeste cyberstrategier. Årsaken til at Norges strategi sammenliknes med Nederlands, er fordi deres tilnærming til avskrekking i det digitale domenet er svært annerledes, selv om landene i mange tilfeller er sammenlignbare. Bakgrunnen til dette kommer jeg nærmere tilbake til senere i oppgaven. Den andre delen inneholder spillteoretiske modelleringer av tre ulike scenarioer, for å identifisere det norske avskrekkingspotensialet med tre ulike avskrekkingsstrategier, *nektelse, straff* og *aktivt cyberforsvar*.

1.3 Oppgavens oppbygning

Oppgaven består av totalt tre hoveddeler. Del I -- «Introduksjon» -- består av innledningskapitlene, hvor oppgaven, problemstilling og operasjonalisering, samt nødvendige avgrensninger og begrepsavklaringer, blir presentert. Videre redegjør jeg for hvilke metoder jeg har benyttet i oppgaven. Formålet er å gi et overblikk over valg av fremgangsmåte, og prosessen som har foregått i forbindelse med arbeidet med oppgaven. Kapittelet avsluttes med et kritisk syn på oppgavens validitet og relabilitet. Avslutningsvis vil jeg redegjøre for noen teoretiske forutsetninger. De består av avskrekkingsteori, attribusjonsteori, gjennomgang av Norges og Nederlands cyberstrategi, samt et overordnet innsyn i spillteori og de spillteoretiske forutsetningene som legges til grunn for den videre analysen.

I Del II -- «Resultater» -- blir det empiriske materialet analysert. Først vil jeg gjøre en komparativ analyse av Norges og Nederlands cyberstrategi. Videre inneholder kapittelet tre ulike spillteoretiske modelleringer av hvordan avskrekking gjennom nektelse, straff og aktivt

cyberforsvar kan anvendes av norske myndigheter. Formålet med dette er å undersøke hvilke handlingsalternativer Norge kan benytte, avhengig av hvilken avskrekkingsstrategi man velger.

Del III -- «Diskusjon» -- inneholder en drøfting av det som har kommet frem i oppgavens analyser opp mot oppgavens problemstilling. Denne delen inneholder tre kapitler hvor jeg først ser på om Norge har noe å lære av Nederlands strategi. Dernest ser jeg på hvilke fordeler og ulemper som er blitt identifisert i analysene ved dagens valgte avskrekkingsstrategi. Kapittelet avsluttes med et forsøk på å operasjonalisere et forslag til ny cyberstrategi for Norge. I denne er det hentet inn betydelig inspirasjon fra andre lands strategier, samt argumentasjon og funn som har blitt identifisert tidligere i oppgaven.

Oppgaven avsluttes med en konklusjon som oppsummerer oppgavens relevante hovedfunn.

1.4 Avgrensning og begrepsavklaringer

Behovet for å avgrense har vært betydelig i arbeidet med denne oppgaven. Årsaken til det er at cyberdomenet er stort og komplekst. I dette kapittelet vil jeg ta for meg de ulike avgrensningene som er gjort i arbeidet. Videre tar jeg for meg ulike sentrale begreper som oppgaven vil benytte seg av.

Selv om det innen cyberkrigføring eksisterer et bredt spekter av ulike operasjoner, vil denne oppgaven ta for seg de handlingene med konsekvenser som ligger under terskel for *væpnet angrep*, et begrepet jeg kommer nærmere tilbake til. Oppgaven vil heller ikke ta for seg virkemidler som ikke nødvendigvis er et folkerettslig brudd, men som kun er et demokratisk problem. Eksempler på dette er bruken av propaganda eller «fake news». Dette betyr ikke at slike virkemidler ikke kan ha en svært negativ effekt på et samfunn, men det vil falle utenfor oppgavens tematikk.

Selv om Etterretningstjenesten peker på flere typer aktører som fremover vil utgjøre en cybertrussel mot Norge (Etterretningstjenesten, 2023b), vil denne oppgaven fokusere på Russland som en statlig aktør. Årsaken til dette er blant annet Smeets beskrivelse av Russland som en «løs kanon», som besitter betydelige kapasiteter, men samtidig få egne begrensninger (2022, s. 51-53) Oppgaven vil således heller ikke ta for seg kriminelle aktører som opererer i det internasjonale systemet, hvor deres intensjoner ofte er profittbasert.

Oppgaven er ikke en juridisk oppgave, ei heller en teknisk oppgave. Derimot er det nødvendig å sette enkelte rammer for å kunne problematisere de aktuelle ukonvensjonelle metodene.

Innhold av juridiske betraktninger og teknisk forståelse vil derfor kun omtales på et overordnet nivå av de mest sentrale forhold. Det søker altså hovedsakelig å se dette i en sikkerhetspolitisk kontekst.

Der oppgaven benytter seg av spillteoretiske modelleringer i den hensikt å analysere potensielle handlingsalternativer i tre ulike scenarioer, er det viktig å påpeke at dette er en forenklet presentasjon av spillteori. Formålet med bruken av spillteori er muligheten for visualisering av aktørenes handlingsalternativer i de gitte scenarioene, samt illustrere de ulike handlingsalternativenes prioriteringer.

1.4.1 Cyberangrep, cyberoperasjon og cyberkrigføring

Sikkerhetstruende aktiviteter i det digitale domenet kan beskrives på en rekke ulike måter; cyberangrep, cyberoperasjoner, cyberkrigføring, digitale angrep, digital krigføring osv. I oppgaven vil det, for enkelhets skyld, kun bli benyttet cyberangrep for å beskrive disse virkemidlene. Generalisert kan cyberangrep deles i tre aktiviteter basert på intensjonen; spionasje, forstyrre eller ødelegge (Friis, 2020).

Spionasje er en aktivitet som har pågått i alle tider, i den hensikt å skaffe informasjon om hva motparten gjør for prøve å forutsi hva som skal skje. Spionasjeaktiviteten i seg selv er ikke brudd på folkeretten, og selv om det er vanlig at stater spionerer på hverandre har statene selv ofte strenge straffehjemler ovenfor de som bedriver spionasje (Schmitt, 2017, s. 174, Uthoff, 2021, s. 4; Wilner, 2017, s. 315). Dette vil derfor falle utenfor oppgavens rammebetingelser, og vil ikke bli videre omtalt.

Cyberangrep i den hensikt å forstyrre aktivitet kan innebære å lamme tjenester slik at de i en periode blir utilgjengelige. Eksempler på dette kan være tjenestenektangrep (DDoS-angrep). Slike angrep innebærer å gjøre en tjeneste utilgjengelig for legitime brukere fordi tjenesten i stedet blir oversvømt av annen datatrafikk (Dinnis, 2012, s. 294). Slike angrep ser ut til å øke i antall, og bli mer og mer potent. Som følge av dette løper stater en større risiko for at sentrale tjenester, i perioder, kan bli utilgjengelige. Eksempler på slike angrep er angrepet mot flere norske nettsider den 29. juni 2022 som ble utført av en pro-russisk gruppe. Angrepet lammet mange tjenester, blant annet Bank-ID, Arbeidstilsynet og politiet (Norum, Ulvin, Hestenes, Skei, Henriksen, Årtun, Kruse, Ekern, s.2022). Et annet kjent eksempel, er angrepet på Estland i 2007, hvor banktjenester, statlige tjenester og media ble lammet. Dette angrepet har vært toneangivende for hvordan NATO har utviklet seg for å møte slike angrep (Knudsen, 2023; NSM, 2022a; Dinnis, 2013, s. 38). En utfordring i det å håndtere cyberangrep, er at det kan

være vanskelig å forstå intensjonen bak angrepet. Dersom det foreligger et cyberangrep rettet mot kritisk infrastruktur, kan det ha til formål å ødelegge. Derimot kan det være en utilsiktet handling i form av en uintendert spillover-effekt, eller for eksempel rekognosering for senere angrep (Nye, 2017, s. 49). Spillover-effekt vil i denne oppgaven bli benyttet som et begrep på spredningseffekt. Det skal derfor ikke ses i sammenheng med det sentrale kjennetrekket innen Ny-funksjonalismen «spillover effekten» (Niemann, Lefkofridi & Schmitter, 2019, s. 45-49).

Tjenestenektangrepene kan skape meget store utfordringer for myndigheter, og samtidig skape usikkerhet hos befolkningen. For eksempel kan slike angrep lamme sykehus, som utilsiktet kan utgjøre en fare for liv og helse – et sentralt poeng jeg skal komme tilbake til.

I Norge er det Etterretningstjenesten som har mandat til å utføre offensive cyberoperasjoner (Forsvarsdepartementet, 2014). Selv om det eksisterer lite informasjon om kapasiteten, hvor betydelige deler av dette trolig er høyt gradert, eksisterer det noe informasjon. Forsvarsdepartementet publiserte cyberretningslinjer i 2014 (Forsvarsdepartementet, 2014). Disse retningslinjene statuerer at Norge skal besitte en kapasitet for offensive cyberoperasjoner, som blant annet skal kunne bidra til at Norge kan beskytte seg mot angrep utenfra. En slik tilnærming må sies å være offensivt og proaktivt rettet, da det pekes på at disse operasjonene skal bidra til beskyttelse mot et angrep. I tillegg til Friis (2020) sin tredelte generalisering av cyberangrep ovenfor, kan offensive cyberoperasjoner deles i to ulike aktiviteter; *Computer Network Exploitation* (CNE) og *Computer Network Attack* (CNA). Distinksjonen mellom disse går på at CNA benyttes i den hensikt å forstyrre, manipulere eller ødelegge som støtte til en militær operasjon. CNE, på den andre siden, benyttes for å oppnå tilgang til en aktørs datasystem i den hensikt å skaffe informasjon som skal nyttiggjøres som støtte til egne militære operasjoner. Informasjonen hentet i en CNE-operasjon gjennomføres uten at motstanderen er klar over dette. En sentral og viktig forskjell mellom de to ulike aktivitetene, er at beslutningsmyndigheten for utførelse av CNA ligger på strategisk nivå, mens aktiviteter definert som CNE er tillagt Etterretningstjenesten (Forsvarsdepartementet, 2014; Nye, 2017, s. 47).

1.4.2 NATOs tilnærming til cyberangrep

Som jeg kommer tilbake til, innebærer Norges cyberstrategi i stor grad å lene seg på internasjonale partnere (Departementene, 2019). Som følge av dette er det relevant å se litt nærmere på hvordan NATO har forholdt seg til cyberangrep de siste årene. Vi skal ikke lenger

tilbake i tid enn 10 år, hvor ingen av NATOs forsvarsministre ville klassifisere et cyberangrep som en militær handling (Dinniss, 2012, s. 39). Derimot er ikke fokuset på cybertrusler noe nytt fenomen i alliansen. Første sporet av slike trusler finner man i deklarasjonen etter NATO-møtet i Praha i 2002 da man anerkjente at man måtte styrke kapabilitetene til å motstå cyberangrep (Pruckova, 2022).

Under NATO-møtet i Wales i 2014 ser man det første sporet av alliansens aksept for at et cyberangrep kan utløse retten til kollektivt selvforsvar etter FN-paktens art 51, og NATOs artikkel 5. Samtidig finner man ingen føringer på dette tidspunktet for hva som skal til for at et cyberangrep skal utløse retten til kollektivt forsvar. Dette er noe man i 2014 skulle håndtere fra sak til sak hvis NATO eller et av medlemslandene ble utsatt for et cyberangrep. Tilsvarende ordlyd ble fremmet etter møtet i Warszawa i 2016 og Brussel i 2021 med unntak av at cyber i 2016 ble sidestilt som et operasjonelt domene, på lik linje med luft, sjø og land. En slik form for strategisk tvetydighet, i det å si at dette skal håndteres fra sak til sak, er en viktig prinsipiell avgjørelse i NATO. Alliansen ønsker ikke å svekke sin posisjon ved å vise hvor dens «røde linje» går i møte med cyberangrep. Derimot har NATO uttrykt at et cyberangrep tilsvarende det Estland opplevde i 2007, ville kunne ha utløst artikkel 5 i dag (Pruckova, 2022; Elspeth & Smith, 2018).

1.4.3 Folkerett i det digitale rom

Oppgaven tar for seg de aktiviteter som ligger under terskelen for maktbruk i FN-pakten og hva som er å regne som et væpnet angrep. Årsaken til dette, er at cyberangrep som ligger under, eller tett opp mot terskelen, fremstår utfordrende å håndtere, fordi stater i stor grad kan måtte håndtere disse alene. Som følge av dette er det naturlig å gjøre noen avklaringer om hva som ligger i FN-paktens artikkel 2 (4) og 51 og NATOs artikkel 5, slik at man setter rammen for hvilke cyberangrep som faller inn under de ulike tersklene som eksisterer.

Enhver maktbruk fra en stat ovenfor en annen blir regulert av FN-paktens artikkel 2 (4). Den pålegger stater et ansvar for «å avholde seg fra trusler om, eller bruk av væpnet makt mot noen stats territoriale integritet eller politiske uavhengigheten til en annen stat» (FN-pakten, 1945). Reglene er internasjonal sedvane og gjelder derfor alle stater, samt alle type pressmidler, herunder digitale angrep (Schmitt, 2017, s. 328-329; Hellestveit, 2022, s. 129).

Retten til selvforsvar kjenner vi igjen fra flere deler av vårt samfunn. FN-paktens artikkel 51 har blitt en av de viktigste, og danner blant annet grunnlaget for NATOs artikkel 5. PN-paktens

Artikkel 51 hjemler ikke bare individuelles rett til selvforsvar, men danner også grunnlaget for et kollektivt selvforsvar dersom en stat blir rammet av et væpnet angrep. Folkerettsjurister tar utgangspunkt i at terskelen for selvforsvar er høy, og at alvorligheten og skadeomfanget må være betydelig (FN-pakten, 1945; Hellestveit, 2022, s. 130-131).

NATOs artikkel 5 inneholder to sentrale prinsipper; et utsagn om samhold og besluttsomhet, samt et avskrekkende budskap. Dette i form av en tankegang rundt «én for alle – alle for én». I tillegg er ordlyden i artikkel 5 skrevet på en slik måte at en motstander ikke skal kunne forutse en potensiell respons, i den forstand at artikkelen bevisst er tvetydig rundt dette (NATO / Atlanterhavspakten, 1949). Artikkel 5 har kun blitt brukt en gang, av USA etter terrorangrepene 11. september 2001 (Tertrais, 2016). Selv da var det ubesluttsomhet å spore blant USAs allierte i NATO, spesielt knyttet til usikkerheten rundt hvorvidt angrepet stammet fra «utlandet». I den senere tid vurderte Frankrike å påberope Artikkel 5 under terrorangrepene 13. november 2015, da terrorgruppen IS drepte 130 personer. Franske myndigheter vegret seg på den tiden grunnet usikkerhet om hvor angrepet stammet fra (Tertrais, 2016).

Tertais peker på at NATOs artikkel 5 virker avskrekkende. Dette som følge av at ingen land noen gang har innledet en åpen storstilt militær operasjon mot et NATO-medlem (2016, s. 4) En relevant problemstilling er hvorvidt NATOs artikkel 5 er begrenset til å ha en avskrekkende effekt når det gjelder stor-skala militær aggresjon mot ett av medlemslandene, eller om den også fungerer avskrekkende ovenfor andre type trusler. Enkelte har hevdet at hverken Sovjetunionen eller Russland har vurdert å angripe NATO (Tertrais, 2016, s. 4). På den andre siden viser Kremls militære intervensjoner siden 1945 en mer nyansert historie. Et eksempel som blir trukket frem, er den væpnede konflikten mellom Russland og Georgia i 2008 (Tertrais, 2016, s. 4).

Tilbake til NATO-toppmøtet i Bucuresti i 2008, ble både Ukraina og Georgia den 3. april 2008 invitert inn som potensielle medlemmer av NATO – i starten av august samme år var krigen i Sør-Ossetia et faktum. Som belyst i senere tid, kan Russland ha oppfattet dette som en provokasjon rundt utvidelse av NATO, og et løftebrudd fra vestlig side, ettersom sentrale vestlige ledere tidligere hadde gitt uttrykk for at man ikke ville fortsette utvidelsen av NATO østover. Uansett vurderte nok de russiske myndighetene at et slikt angrep sannsynligvis ikke ville bli dekket av Artikkel 5, hvor Georgia og Ukraina ikke ville blitt forsvart av NATO. Ikke minst kan det tenkes at NATO aldri ville vurdert å fullstendig godta land som inneholder delvis okkuperte landområder (Tertrais, 2016, s. 4; Øverland, 2009).

Begrepene «bruk av makt» og «væpnet angrep» er sentrale i folkeretten. Hva ligger så i disse? Det er ingen konsensus om en offisiell definisjon når det gjelder begrepet «bruk av makt», ei heller innen cyber (Nye, 2017, s. 47). Derimot har Tallinn-manualen beskrevet «bruk av makt» innen det digitale domenet som «handlinger som skader eller dreper personer eller fysisk skader eller ødelegger gjenstander» (Schmitt, 2017, s.330-337). Tallinn-manualen er et juridisk oppslagsverk utviklet av en rekke internasjonale juridiske eksperter på oppdrag fra NATO, som har sett på anvendelse av folkeretten innen cyberdomenet (Schmitt, 2017). FNs artikkel 51 sier ikke noe om omfanget og intensiviteten til et angrep for at det skal være snakk om et «væpnet angrep». Ifølge Tallinn-manualen innebærer dette handlinger som forårsaker at mange mennesker dør eller blir alvorlig skadet, eller som forårsaker omfattende skader (Schmitt, 2017. s. 339-342) Derimot, enhver bruk av makt mot en stat, vil ikke umiddelbart anses som et væpnet angrep – det kreves altså bruk av makt av et visst omfang. Tallinn-manualen peker i begge tilfeller på to sentrale begreper, «*scale and effects*» (Schmitt, 2017, s. 330). I tillegg må handlingene ses i kontekst av begrepene «*circumstances and motivation*» (ICJ, 1986, s. 110).

Disse begrepene har sin bakgrunn fra den anerkjente «Nicaragua-dommen», fra Den Internasjonale domstolen i Haag tilbake i 1986 (ICJ, 1986, s. 93). Dommen fra Den internasjonale domstolen sier blant annet at rene grensetrefninger ikke vil falle inne under det som ligger i begrepet væpnet angrep. Selv om det ikke finnes noen klar definisjon, så skiller uansett dommen på bruk av makt, hvor kun de mest alvorlige formene kan defineres som et væpnet angrep (ICJ, 1986, s. 91, Hayward, 2017; Schmitt, 2017, s. 331-333). Begrepene finner man også igjen i Norges innspill til FN om anvendelse av folkeretten innen cyberdomenet. Der uttrykte Norge følgende i forbindelse med hva som skal til for at en cyberoperasjon skal kunne regnes som et væpnet angrep: *«Depending on its scale and effect, this may include a cyber operation that causes an aircraft crash"* (United Nations, 2021, s. 70).

Retten til selvforsvar etter FN paktens artikkel 51 blir utløst ved et væpnet angrep. Den internasjonale domstolen i Haag, fastslo i Atomvåpensaken i 1996 at artikkel 51 får anvendelse som følge av hvilken som helst bruk av makt, uavhengig av hvilke våpen som er benyttet (Schmitt, 2017, s. 328). Dette innebærer at et cyberangrep også når opp til terskelen for hva som vil bli definert som et væpnet angrep, omfattet av FNs artikkel 51. Når det er sagt, er det naturlig å tenke seg at utviklingen innen det digitale domenet går vesentlig raskere enn de førende juridiske vurderingene. Dette kan medføre juridiske utfordringer i vurderingen om når en digital operasjon utgjør et væpnet angrep. Tallinn-manualen har derimot pekt på enkelte tilfeller som åpenbart vil falle inn under begrepet, og hvilke som faller utenfor. Når det gjelder

digitale operasjoner/angrep som medfører tap av liv, alvorlig skade eller betydelige ødeleggelser, er dette ifølge Tallinn-manualen klare tilfeller som vil defineres som et væpnet angrep. På den andre siden mener ekspertene at tilfeller som klart faller utenfor definisjonen, er eksempler på subversjon, digitale innhentingsoperasjoner i etterretningsøyemed, samt mindre digitale operasjoner som medfører korte og periodiske forstyrrelser av ikke-kritiske digitale tjenester (Schmitt, 2017, s. 341).

Det eksisterer en rekke ulike lovlige svaralternativer i møte med cyberangrep. Disse bestemmes blant annet av hvorvidt et cyberangrep er å definere som ulovlig utført av en stat, og om offerets foreslåtte respons er lovlig. Retorsjon og mottiltak er eksempler på noen vanlige former for respons (Hellestveit, 2022, s. 126-128). Retorsjon er den vanligste reaksjonen mot en motstanders cyberoperasjoner. Dette er handlinger som i seg selv ikke bryter internasjonalt lovverk, men fremstår «uvennlige» sett fra motstanderens perspektiv. Eksempler på slike handlinger er økonomiske sanksjoner, utvisning av diplomater eller utsettelse eller kanselleringer av offisielle besøk. Samtlige er responser vi har sett de siste årene. Norge utviste nylig 15 russiske diplomater, og USA utviste diplomater, stengte russiske virksomheter og innførte sanksjoner etter den russiske påvirkningsoperasjonen mot valget i 2016. Fordelen med retorsjon som respons, er at en stat ikke trenger å juridisk attribuere en operasjon til en annen stat for å iverksette slike handlinger – retorsjon som virkemiddel trenger bare være basert på en enkel mistanke om involvering (Hellestveit, 2022, s. 127; Johnson & Schmitt, 2021, s. 22). Attribusjon er et begrep som vil bli omtalt senere i oppgaven.

I forlengelse av dette har blant annet Friis pekt på at «Responsibility of States of International Wrongful Acts»-lovverket, trolig vil være et av de mest relevante å forholde seg til med tanke på offensive cyberangrep under terskelen for væpnet konflikt (2020, s. 31). Lovverket, som i stor grad anses som sedvanerett (Crawford, 2019, sitert i Friis, 2020, s. 38), innebærer at en angrepet stat kan gjøre mottiltak, under terskelen for maktbruk, for å blant annet stanse et angrep (Friis, 2020, s. 38). Norge har selv uttalt seg rundt dette lovverket i sine innspill til FN når det gjaldt anvendelse av folkeretten innen cyberdomenet. Der uttrykte Norge blant annet at mottiltak kan iverksettes for å få en stat til å opphøre en urettmessig handling, (wrongful act) (United Nations, 2021, s. 72). Det er også interessant at Norge i samme innspill peker på at et slikt svar ikke trenger å være domenebundet. Altså – det er ikke krav om at mottiltaket skal være av samme karakter som de urettmessige handlingene man står ovenfor. Responser kan gis både innenfor og utenfor cyberdomenet (United Nations, 2021, s. 72). En slik norsk holdning kan bidra til å skape tvetydighet ovenfor en potensiell motstander.

Dersom en stat skulle trenge å iverksette mer robuste tiltak i form av nødvendige handlinger som ellers ville brutt med internasjonal lov, tillates det tiltak for å tvinge motstanderen til å stoppe, eventuelt begrense skade. Et eksempel på dette kan være at den rammede staten, selv kan iverksette en offensiv og ulovlig cyberoperasjon som ellers ville brutt Folkerettens prinsipper om staters suverenitet. Mottiltaket som iverksettes må være proporsjonelt i forhold til hva man ble utsatt for. Samtidig fremstår det som akseptert at mottiltak ikke kan innebære *bruk av makt*, altså handlinger som skader eller dreper personer eller fysisk skader eller ødelegger gjenstander (Schmitt, 2017, s.330-337). Naturlig nok er slike responser underlagt et strengt juridisk lovverk, hvor et sentralt vilkår er at den fiendtlige nettverksoperasjonen må være et brudd på Folkeretten, samt at operasjonen juridisk må kunne attribueres til en stat. Ved feilattribusjon vil mottiltaket bli sett på som ulovlig. Når det er sagt, er det ingen konsensus rundt hvorvidt en stat er forpliktet til å forsøke retorsjon eller andre mildere tiltak før man iverksetter mottiltak (Hellestveit, 2022, s. 127-128; Johnson & Schmitt, 2021, s. 21-25).

I ekstreme tilfeller kan en stat måtte svare ved bruk av makt for å håndtere cyberangrep. I disse tilfellene har staten tre alternativer. Samtykke fra staten responsen rettes mot, en resolusjon fra FNs sikkerhetsråd som gir fullmakt til handlingen, eller selvforsvar. Samtykke eller vedtak fra Sikkerhetsrådet fremstår per i dag usannsynlig når det er snakk om angrep utført fra russiske aktører. Da sitter man kun igjen med ett alternativ, og det er å benytte hjemlene om selvforsvar i FNs artikkel 51, eller NATOs artikkel 5.

1.5 Metode

Enhver forskningsmetode har sine fordeler og ulemper. Ett skille går mellom kvantitative og kvalitative forskningsmetoder innen samfunnsvitenskapelige metoder. Den fremtredende norske sosiologen Vilhelm Auberts (1972, s. 196) definerte metode som *«en fremgangsmåte, et middel til å løse problemer og komme frem til ny kunnskap»* (Furseth og Everett, 2020, s. 137).

Formålet med dette kapittelet er å gi et overblikk over fremgangsmåten og prosessen som ligger til grunn i arbeidet med oppgaven. Det vil bli redegjort for valg av metode, forskningsdesign med dertil tilhørende fordeler og begrensninger som følger av de metodologiske avgjørelsene som ble tatt. Metodekapittelet er sentralt i oppgaven, da det skal gi innblikk i min skriveprosess, valg som er tatt, søke å skape en transparent presentasjon av hvilke data som er funnet, samt hvordan disse presenteres. Avslutningsvis tar kapittelet for seg en kritisk refleksjon omkring

oppgavens validitet og reliabilitet, samt ikke minst se på hvilke eventuelle svakheter som er knyttet til min forskningsmetode.

1.5.1 Forskningsdesign

En av de største utfordringene, som tidlig ble identifisert i arbeidet med oppgaven, var hvordan jeg skulle angripe temaet og gjøre dette forskbart. Ettersom et sentralt prinsipp i dagens avskrekkingsstrategi innebærer tvetydighet og fordektbarhet i den forstand at man ikke ønsker å eksponere aktuelle responsopsjoner, ble det tidlig klart at det var svært lite å hente på å gjennomføre intervjuer. Med stor sannsynlighet ville disse intervjuene ikke tilført ny kunnskap utover det som allerede eksisterer i litteratur og offentlig dokumentasjon. I tillegg er en vesentlig andel av aktørenes strategier knyttet til oppgavens tematikk høyt gradert informasjon. Å skrive en klausulert oppgave har ikke vært ønskelig, både av hensyn til at et viktig prinsipp innen forskning er at den bør være offentlig tilgjengelig, men også fordi det av rent praktiske årsaker ville medført en svært komplisert og tidkrevende prosess.

På bakgrunn av dette vil oppgavens primære utgangspunkt være i form av en litteraturstudie med utgangspunkt i Norges avskrekkingsstrategier i møte med russiske cyberangrep. For å styrke metoden, har jeg valgte å komplettere dette på to måter: med et komparativt element, samt delvis benytte meg av spill (kjent fra spillteorien), med enkle modelleringer. (Johannessen et al., 2011, s. 89-91). Ved å sammenlikne Norges cyberstrategi med Nederlands, får deler av oppgaven et komparativt design (Bryman, 2016, s. 65). De to ulike casene er sammenliknet i et eget analyseskjema. Spill benyttes for illustrasjon av de tre casene som presenteres i oppgavens Del II. De nevnte casene innebærer en analyse av avskrekkingsstrategiene; *straff, nektelse* og *aktivt cyberforsvar*.

Som følge av dette endte min forskningsdesign opp med en kvalitativ og induktiv tilnærming, hvor målet er å komme frem til nye ideer og konseptutvikling basert på det jeg finner i mitt utvalgte datamateriale, samt de analysene som blir gjort (Johannessen et al., 2011, s. 51).

1.5.2 Datainnsamling

Kvalitativ litteraturstudie er en innholdsanalyse av eksisterende dokumenter. Formålet med innholdsanalysen er å tolke og filtrere informasjon fra litteratur for å kunne identifisere sammenhenger. Ikke minst kan litteraturstudiet bidra til å skaffe informasjon og data som ligger utenfor de nærmeste omgivelsene og eget sanseapparat (Bratberg, 2021, s. 11).

Fordelen med litteraturstudie er muligheten til å ta for seg et allerede eksisterende datamateriale, hvor min subjektive påvirkningskraft ikke vil påvirke datamaterialet. Derimot kan det være flere ulemper i form av at jeg ikke får anledning til å undersøke eventuelle fenomener eller å få svar på oppklarende spørsmål som ikke eksisterer i tilgjengelig datamateriale. Den komparative analysen bidrar til å se mønstre av likheter og ulikheter, som jeg videre kan benytte til å forklare elementer i Norges cyberstrategi.

Som teoretisk fundament til oppgaven foreligger det et betydelig utvalg av analysert litteratur, hvor den komparative delen konkret retter seg mot Norges og Nederlands siste cyberstrategier. Datainnsamlingen har foregått over tid, helt fra nysgjerrigheten rundt valgt tema dukket opp tidlig i prosessen rundt masteroppgaven, frem til godt ut i skriveprosessen til oppgaven. En av årsakene til denne lange innsamlingsperioden, er Russlands krigføring i Ukrainakrigen, som har bidratt til at min tematikk har vært høyst aktuell, spesielt innen akademiske miljøer. Dette har bidratt til å endre enkelte vurderinger rundt sannsynlige handlemåter knyttet til oppgavens analyserte scenarioer.

En naturlig avgrensning innen datainnsamlingen har vært de språklige barrierene det innebærer å innhente russisk litteratur som det kunne vært interessant å benytte seg av i forbindelse med de spillteorietiske modelleringene. En av utfordringene med dette, er at tilgjengelig litteratur fort kan havne i en gruppe som kan kategoriseres å ha et «vestlig bias». Dette medfører at man kan ha utfordringer med å se de aktuelle problemstillingene fra begge sider, men i stedet får et overdrevent vestlig syn. Min vurdering er imidlertid at dette ikke nødvendigvis svekker oppgavens intensjon og validitet, men er noe både jeg og lesere må være klar over når man leser oppgaven.

1.5.3 Utvalg av dokumenter

For å identifisere hvilke relevante dokumenter jeg skulle benytte meg av, var et godt og utfyllende litteratursøk nødvendig. Der hvor dokumentstudier ofte kan være utgangspunktet for videre empiriske undersøkelser, er det i denne oppgaven motsatt. For meg er selve gjennomgangen av dokumentene målet med studien. Dokumentene jeg har benyttet er derfor å regne som empirien som danner bakteppet til min oppgave (Tjora, 2020, s. 183).

Litteraturen jeg tar utgangspunkt i, består primært av samfunn- og statsvitenskapelig forskningslitteratur, hvor mange av disse baseres på empiriske studier. Mine undersøkelser kan i så måte ses på som «secondary research» metode (Curtis og Curtis, 2011). Dokumentutvalget

mitt har vært en løpende prosess gjennom hele studieperioden, helt fra da jeg begynte prosessen med å fundere på hvilket tema masteroppgaven skulle behandle. Allerede fra starten av begynte jeg å notere meg relevant litteratur som jeg skulle få anledning til å jobbe med videre i prosessen. Underveis har jeg dermed lest en rekke ulike dokumenter, som jeg fortløpende har forkastet, eller lagt til side for senere anvendelse. Ved å benytte meg av *NATO Cooperative Cyber Defence Centre of Excellence*, CCDCOE sitt bibliotek over nasjonal strategi og styring, fikk jeg raskt meget god oversikt. Det er videre to konkrete dokumenter jeg til slutt har valgt å benytte meg av, henholdsvis den siste utgaven av Norges og Nederlands offentlige cyberstrategi.

Nasjonal strategi for digital sikkerhet kom ut i 2019, hvor den norske regjeringen statuerte at digital sikkerhet er et av områdene man prioriterer høyt (Departementene, 2019). I 2018 kom den siste nederlandske utgaven av deres cyberstrategi ut, *Defensie Cyber Strategie 2018.* Der besluttet det nederlandske forsvarsdepartementet at de skulle øke sine offensive cyberkapasiteter og cyberresiliens. Resiliens innebærer å skape en robusthet slik at man både evner å redusere motstanderens potensielle fordeler av et angrep, samt sikre at egne kapasiteter og virkemidler til enhver tid er tilgjengelige for eventuelle mottiltak (Nye, 2017, s. 56).

Den norske cyberstrategien er først og fremst defensivt innrettet. Strategien bygger på et styrket samarbeid mellom offentlige-private aktører, sivilt-militært- og internasjonalt samarbeid. Strategien pålegger også norske virksomheter et betydelig ansvar, hvor man viser til ansvarsprinsippet som innebærer at virksomheter som har ansvaret i en normalsituasjon, også har ansvaret for nødvendige beredskapsmessige tiltak, samt håndteringen av ekstraordinære hendelser. Det er lite å spore av sentrale og nasjonale tiltak for å håndtere et cyberangrep. Selv når strategien redegjør for utvalgte relevante aktører, velger den kun å vise til Etterretningstjenestens mandat innen offensive cyberoperasjoner, noe som har vært kjent siden 2014. Det er for øvrig også relevant å peke på at det ikke en eneste gang i Norges strategi nevnes ordet *avskrekking.* På den andre siden peker strategien på at man skal styrke den nasjonale evnen til å attribuere og håndtere alvorlige digitale angrep, men kun innen rammen av videreutvikling av internasjonalt samarbeid (Departementene, 2019; Forsvarsdepartementet, 2014)

Den nederlandske strategien har på sin side et meget fremtredende fokus på offensive kapasiteter. Den nye strategien søker å offentlig konfrontere aktørene bak cyberangrep oftere, samt at de søker å investere ytterligere innen offensive kapasiteter. Innen nødvendige

kapasiteter nevner de konkret evnen til både å håndtere angrepet, samt attribuere. Et interessant virkemiddel strategien trekker frem, er at deres avskrekking ikke søker å være domenebundet. Med andre ord, angrep fra et annet domene, kan svares ut gjennom offensive cyberoperasjoner, og motsatt, tilsvarende Norges uttalelser til FN (United Nations, 2021, s. 72). For en trusselutøver kan dette oppleves som tvetydig, og utfordrende å forholde seg til. Avskrekkingen i den nederlandske strategien skal gjøre landet til et mindre attraktivt mål for cyberangrep, altså er viktig middel for konfliktforebygging. For å oppnå dette, krever avskrekkingen en troverdig offensiv evne (Ministerie van Defensie, 2018).

Dokumentstudier vil fort innebære at man analyser et dokument ut ifra den tiden man er i. Hvis litteraturen ikke oppdateres jevnlig, vil informasjonen fort kunne bli utdatert. Dette har vært et sentralt poeng i min oppgave, hvor jeg har tatt utgangspunkt i tradisjonelle avskrekkingsstrategier som har eksistert i mange ti-år.

1.5.4 Hermeneutikk og forforståelse

Det finnes en rekke ulike måter å tolke litteratur på, hvor mangfoldet av ulike teknikker innen tekstanalyse kan virke forvirrende. Det å tolke meningsbærende innhold byr på ulike utfordringer. Gir det man leser en fullstendig tilgang til meningsinnholdet? Er ideene først og fremst individuelle eller har de en kollektiv karakter? Samfunnsvitenskapelig metodelære gir få retningslinjer for slikt tolkningsarbeid, hvilket medfører at forutsetningen for å vurdere gyldigheten av ulike tolkninger er dårlig (Bratberg, 2021, s. 18-19). Hermeneutikk handler om nettopp dette, å skape meningsinnhold fra tekst – derfor er dette helt sentralt i studiet av tekst. Videre, mer inngående, handler dette om å avdekke underliggende mening og årsakssammenhenger (Asdal og Reinertsen, 2020, s. 243-244). I forlengelse av dette er det derfor essensielt å være bevisst egen forforståelse når man jobber med teksttolkning. Tross alt er det forlokkende aspektet ved tekstanalyse en mulighet, vel så mye som en begrensing (Bratberg, 2021, s. 23).

Hermeneutikk har et innslag av det man kan kalle for heuristikk. Dette er erfaringsbaserte antakelser man alltid har med seg. Disse antakelsene, eller forforståelsen om man vil, kan være hverdagslige, eller de kan opptre i møte med akademia. Heuristikker kan også komme i form av antakelser om ideer, i form av at jeg som student leser om relevante teorier og strategier, med en tanke om at strategien er utdatert (Bratberg, 2021, s. 20-24). Man kan derfor se på heuristikker som mentale snarveier som man som forsker må være klar over. Dette er noe hver

og en av oss har med seg og det er umulig å unngå. Det som derimot er mulig, er å være seg bevisst på hvilken forforståelse man tar med seg i arbeidet med ulike tekster.

Vår forforståelse kan lede oss på villspor. Bare se til politietaten, hvor man i mange år har vært opptatt av å unngå *confirmation bias* – altså det å søke etter bevis som støtter opp under egen antakelse (Rachlew, 2009, s. 23). Fra jeg startet denne prosessen, har arbeidet og prosessen blitt styrt av egen forforståelse. Forforståelsen min har fungert som en mental sprettball mellom ulik tematikk, men har til slutt havnet på nettopp dette temaet – dette er ikke tilfeldig. Forforståelsen min, som har ledet frem til mitt tema, preges av både min akademiske og profesjonelle karriere, samt ulike erfaringer og tanker jeg har gjort opp igjennom tiden. Når man leser dokumenter, handler det derfor om å være klar over at teksten man tolker, kan fortelle noe som ikke stemmer med egen forforståelse. Det er uansett viktig å være klar over at nøktern og objektiv observasjon må anses som relativt urealistisk.

Forskerens rolle vil derimot være å heller forstå hvordan aktører forstår seg selv og sin situasjon, og dermed indirekte hvorfor de handler som de gjør (Nilsen, 2012, s. 68-71; Bratberg, 2021, s. 26). I mitt arbeid med denne oppgaven, har dette vært særlig viktig, fordi dokumentene jeg tolker i stor grad preges av sikkerhetspolitisk fargelegging. Historien nasjonene bak dokumentene søker å fortelle, er i liten grad objektive. Derimot søker de trolig å underbygge eller forsterke egne kapasiteter og de forteller ikke om egne svakheter. Disse strategiske dokumentene søker altså å fortelle akkurat det myndighetene ønsker at leseren skal oppfatte. Dette innebærer at tekstene må analyseres slik Bratberg nevner, hvor man må søke å forstå aktørene og deres situasjon. Sånn sett handler altså dette mer om å analysere årsaksforhold i bredere forstand (2021, s. 26).

Dette har medført at jeg har forholdt meg til en induktiv tilnærming, selv om jeg har hatt enkelte teoribegreper jeg har forsøkt å lete etter i tekstene (Johannessen et al., 2011, s. 51). Teoribegrepene, i mitt tilfelle spesielt knyttet til avskrekking, kommer ofte til uttrykk gjennom handling, slik at jeg har vært nødt til å ikke ha forhåndsdefinerte kategorier som jeg har lett etter. Samtidig har jeg forsøkt å være bevisst egen forskerrefleksivitet, spesielt da en av mine analyserte aktører er staten Russland. Russlands brutale krigføring i Ukraina, gjør det utfordrende å tolke datamateriale objektivt (Nilsen, 2012, s. 65 og 139). Det sentrale poenget jeg har hatt et aktivt forhold til, er tilstedeværelsen av egen subjektivitet, og hvordan den eventuelt påvirker forskningen.

1.5.5 Analyse og presentasjon av data

Analysering av data innen de ulike kvalitative metodene trenger ikke nødvendigvis å være så ulik, til tross for at dokumenter og intervjuer har ulik opprinnelse. Walcott hevder at analyse er en sorteringsøvelse – «den kvantitative delen av kvalitativ forskning» (1994, s. 26, sitert i Johannessen et al., 2011, s. 186 og 197). Dette innebærer blant annet å vektlegge de dataene som er fremstilt, eller for eksempel å presentere funn i grafer eller diagrammer. Til dette har jeg benyttet meg av spillteoretiske modelleringer for å illustrere enkelte poenger. Sånn sett kan man si at analysen gjøres i den hensikt å sortere dataene, slik at man videre kan benytte disse for dypere analyser. Miles, Huberman og Saldana presiserer at slik analysering burde være en gjennomgående prosess underveis i løpet av hele datainnsamlingen (2020, s. 62). Dette har vært svært utfordrende å få til når studieprosessen har pågått samtidig med fulltidsjobb.

Min problemstilling handler blant annet om troverdigheten i Norges strategiske respons mot russiske cyberangrep. Det vil derfor være interessant å kartlegge hvordan Norge har respondert ved enkelte tidligere tilfeller. I tillegg er det aktuelt å se på Norges strategiske dokumenter mot andre lands, i mitt tilfelle Nederland, samt se etter mulige årsakssammenhenger mellom strategi og relevante hendelser.

Analysen startet med å samle inn data fra dokumentene. I det norske dokumentet startet jeg med gjentatte gjennomlesninger, der jeg uthevet relevante deler av teksten og kopierte inn interessante deler i ulike arbeidsdokumenter. I tillegg til dette benyttet jeg søkemekanisme for noen enkeltord der jeg hadde digitale dokumentkilder tilgjengelig.

I det nederlandske dokumentet var fremgangsmåten tilsvarende, bortsett fra at denne teksten måtte oversettes, da den ikke offisielt har blitt oversatt til engelsk. Til dette benyttet jeg en «plugin» i nettleseren som automatisk endret teksten til engelsk. Det er enkelte svakheter i en slik metode, da man kan risikere å miste, eller misforstå enkelte konkrete formuleringer. Dette er naturlig nok uheldig all den tid formuleringene er såpass viktig i politiske dokumenter. Dette er uansett noe jeg har tatt med i arbeidet jeg har gjort med det aktuelle dokumentet, og vært bevisst på i den videre analysen.

I prosessen har jeg forholdt meg til tre ulike arbeidsdokumenter. Det ene var et overordnet notat i OneNote, hvor samtlige notater ble kopiert inn. Videre hadde jeg et kodeark til den utvalgte litteraturen jeg satt igjen med etter en nøye utvelgelsesprosess, samt selve Word-dokumentet hvor tekst fortløpende ble skrevet. I kodearket ble dokumentasjonen tematisert, og påført koder for at jeg enkelt skulle kunne gå tilbake å se på dette senere.

Til den første syklusen av koding, benyttet jeg med av den anerkjente metoden «in Vivo-koding» (Miles et al., 2020, s. 60-65). Dette innebærer at man benytter kodeord som har sin bakgrunn direkte fra dokumentets eget språk, samt i noen tilfeller oversatt til norsk. Denne metoden er induktiv, før den deretter kan utvikle seg til koder av mer teoretisk format. I den andre kodesyklusen kalles dette for mønsterkoder. Dette er koder som i større grad er forklarende, hvor man går bort fra dokumentets ordbruk og over i analytiske kategorier (Miles et al., 2020, s. 60-65). I tillegg benyttet jeg meg av enkelte støttenotater «jottings», som benyttes for å huske en ide eller kommentar som dukket opp underveis. Under er et utsnitt av kodearket jeg benyttet meg av.

Forfatter	Tittel	Tematikk	In Vivo koding	Mønsterkode	Referanse i APA-stil	Jottings
Freedman	Deterrence: a reply	Avskrekking	Power-element Axis of evil Governance Economic practice Credibility		Freedman, L. (2005). Deterrence: a reply. Journal of Strategic Studies, 28(5), 789–801. https://doi.org/10.1080/01402390500393944	
Tor	Cumulative Deterrence as a new paradigm for Cyber Deterrence	Cybersavskrekking	Kumulativ avskrekking. Amerikansk avskrekkingsstrategi. Israel vs USA	Restriktivt konsept	Tor, U. (2017). 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence. Journal of Strategic Studies, 40(1-2), 92–117. https://doi.org/10.1080/01402390.2015.1115975	Nytt begrep – kumulativ avskrekking. Vises til av Muller
Adamsky	From Israel with Deterrence: Strategic Culture, Intra-war Coercion and Brute Force	Avskrekking Cybersavskrekking	Israelsk strandpunkt. Dynamisk strategisk effekt. Vestlige strategi klarer ikke tilpasse seg. Tre type aktører. ATP. Bottom-up. Mangler politisk konsistent. Red line definert i noen grad – her ref Tallinn. Panetta erkjenner	Ukonvensjonell avskrekking Kulminerende punkt for avskrekking	Adamsky, D. (2017). From Israel with Deterrence: Strategic Culture, Intra-war Coercion and Brute Force. Security Studies, 26(1), 157–184. https://doi.org/10.1080/09636412.2017.1243923	Libicki – sjekk ut om andre bruker denne. Kan utfylles med poenget om økt sikkerhet som boken peker på. Ref riksrevisjonens rapport om Forsvaret.

Ved gjennomgang av materialet ble det, i tillegg til de to definerte tekstene som ble analysert, identifisert fem ulike avskrekkingsstrategier som jeg definerte som interessante å følge opp. Avskrekking gjennom *nektelse, straff, aktivt cyberforsvar, forviklinger* (entanglement) og *restriktivt konsep*t (cumulativ) (Jasper, 2017, s. 9; Nye, 2017, s. 55-59; Tor, 2017) Selv om disse fem ble identifisert, valgte jeg kun å gå videre med tre; nektelse, straff og aktivt cyberforsvar. Årsaken til dette, har i stor grad vært en nødvendig avgrensning av oppgaven.

1.5.6 Validitet og reliabilitet

Det å arbeide med tekst byr på en rekke utfordringer. Ord kan tillegges mange meninger. Og kanskje den største utfordringer, de fleste ord er meningsløse med mindre man setter de i sammenheng med ordet som står foran og bak (Miles & Huberman, 1984, s. 54 sitert i

Johannessen et al., 2011, s. 164-165). Valget av litteratur til oppgaven er forankret med to ulike grunnleggende spørsmål; reliabiliteten til dataen, og validiteten den har. Oppgavens validitet bygger på en vurdering om hvorvidt jeg har lyktes i å gi en presis gjengivelse av mine tolkninger, og hvorvidt disse er forankret, samt forskningsresultatets gyldighet og relevans (Bratberg, 2021, s. 137-140). Med andre ord er spørsmålet hvorvidt jeg har klart å måle og gi en gjengivelse av det jeg ønsket å undersøke.

Reliabiliteten handler om oppgavens pålitelighet, og hvorvidt man kan stole på det resultatet som presenteres i oppgaven. I denne sammenheng peker Bratberg på at man i dette spørsmålet i stor grad ser på oppgavens repliserbarhet, altså oppgavens evne til å kunne reproduseres i detalj, hvor resultatet bør bli det samme (2021, s. 138). Dette innebærer at det er sentralt for oppgavens pålitelighet å dokumentere det man gjør, samt arbeide på en strukturert måte.

Utenom de to nasjonale cyberstrategiene til Norge og Nederland, har relevant litteratur i stor grad blitt hentet fra akademiske søkemotorer som JSTOR og Oria. Søkene ble gjort i tidsperioden mellom mai 2022 og september 2023. Søkestrategien etter søkeord og kombinasjoner har sin bakgrunn i min tematikk og problemstilling. Følgende søkeord ble i stor grad benyttet: *cyber* AND *deterrence, cyber* AND *operation* OR *attack* AND *strategy, cyber* AND *attribution, cyber* AND *Russia, cyber* AND *Norway, cyber* AND *game theory* og *deterrence* AND *attribution.* Søkestrategien etter initialsøkene mine, var i første omgang å gjennomføre en screening av tittel og årstall for utgivelse. Dette var nødvendig, da søkene mine ga alt for mange resultater til å gå igjennom samtidig. For eksempel ga søket *cyber* AND *deterrence* over 1500 treff på Oria, mens tilsvarende søk på JSTOR ga over 6000 resultater. Etter at screening av tittel ble gjort, fulgte jeg opp med et nytt screeningtrinn, hvor jeg leste igjennom sammendraget til artikkelen. De fleste artiklene ble ekskludert i dette trinnet. Avslutningsvis ble det gjennomført en screening av fullteksten, hvor jeg satt igjen med artikler som i større eller mindre grad er inkludert i denne oppgaven.

Det må også påpekes at enkelte deler av den valgte litteraturen ikke vil kunne bli ansett som empiri. Eksempler på dette er blant annet dataene fra CCDCOE, relevant lovverk, samt de utvalgte nasjonale strategiene. Dette til forskjell fra annen relevant litteratur som i stor grad har blitt fagfellevurdert. Disse eksemplene kan derimot kanskje bli regnet som data. Johannessen, Tufte og Christoffersen 2011, differensierer dette som at data er en registrert observasjon av virkeligheten, mens empiri er en forsøkt og utprøvd oppfatning. Empiri er derfor utsagn som baseres på erfaring i stedet for synsing (s. 32).

Et sentralt poeng spesielt knyttet til de to nasjonale cyberstrategiene, er at selv om validiteten til disse er høy, kan det stilles spørsmålstegn til litteraturens reliabilitet. Dette spesielt fordi disse konkrete dokumentene er skrevet i et nasjonalt sikkerhetspolitisk- og strategisk perspektiv. De forteller trolig ikke den fullstendige sannheten, de søker kanskje å avskrekke, eller de er skrevet for å være tvetydige. Dette innebærer at mye ansvar for tolkning tillegges meg selv.

Dette gjør at enkelte av mine tolkninger er sikrere enn andre. Dette er noe jeg søker å belyse spesifikt i løpet av oppgaven, spesielt i diskusjonskapittelet. Som et virkemiddel i å kvalifisere tolkningene mine, har jeg benyttet meg av sannsynlighetsord, etter inspirasjon fra det de norske EOS-tjenestene benytter seg av. Formålet med sannsynlighetsordene er å skape en bedre forståelse av mine tolkninger og deres validitet. Ordene som benyttes er *sannsynlig*, *mulig* og *lite sannsynlig*, hvor en tolkning som beskrives med sannsynlig kan tillegges mest verdi (PST, 2023, s. 2-3).

1.6 Teoretiske konsepter og tilnærminger

1.6.1 Avskrekkingsteori

Norges tradisjonelle strategiske tilnærming til eksterne trusler har gjennom tiden vært basert på en balanse mellom avskrekking og beroligelse (FFI, 2022b, s. 45), hvor det er det avskrekkende elementet som vil bli omtalt videre i denne oppgaven. Den tradisjonelle avskrekkingsteorien stammer fra amerikansk akademia under den kalde krigen, og har i stor grad, vært basert på avskrekking med fokus på kjernevåpen (Nye, 2017, s. 45-52). Prinsippet bak avskrekking med kjernevåpen innebærer at et angrep på en stat, ville resultere i et fullstendig destruerende motangrep – hvorpå en slik trussel skulle skape stabilitet. Et sentralt element innen avskrekking vil derfor være evnen til å påvirke en motstanders handlinger gjennom en implisitt trussel om å påføre betydelige skader. Hvordan andre aktører persiperer ens egen evne til motstand, er derfor et sentralt poeng innen avskrekkingsteorien (FFI, 2022b og Jervis 1979, s. 289-294; Nye, 2017, s. 52-53).

Det eksisterer ingen form for konsensusbasert definisjon på avskrekking. Dog, en tradisjonell beskrivelse som ofte benyttes er Schellings som beskriver avskrekking som en trussel som er ment for å hindre en motstander i å gjøre noe (Schelling 1966, sitert i Sperendei 2006, s. 166). Det amerikanske forsvarsdepartementet presiserer at avskrekking handler om å forebygge en motstanders uønskede handlinger. I tillegg søker den å påvirke beslutningskalkylen til en aktør

ved å true med å pålegge kostnader, eller nekte fordeler, samtidig som man oppmuntrer til tilbakeholdenhet (US Department of Defence 2011, sitert i Jasper, 2017, s. 3).

Glenn Harald Snyder er en annen anerkjent forsker innen avskrekkingsteori som, i sin definisjon av avskrekking, setter søkelyset på trusselen. Snyder peker på at man avskrekker en annen part fra å gjøre noe, ved den implisitte eller eksplisitte trusselen om å anvende en eller annen sanksjon, hvis den forbudte handlingen utføres, eller ved løfte om en belønning hvis handlingen ikke utføres (Snyder, 1961, s. 9). Et sentralt poeng ved avskrekkingsteorien er uansett at avskrekking som virkemiddel har mislyktes så fort missilene begynner å fly – eller i denne oppgavens tilfelle, så fort kodene begynner å knekkes.

Som sagt har den tradisjonelle avskrekkingsteorien ofte vært knyttet til terrorbalansen atomvåpen skaper mellom to eller flere stater. Dette fokuset er ikke en nødvendighet, noe flere forskere har pekt på. Blant annet nevner Jervis at *«although deterrence does not require nuclear weapons, their existence makes it easier to grasp the basic ideas"* (1979, s. 290). Innen akademia har det derimot vært uenighet knyttet til kjernevåpens rolle i avskrekkingsteorien, og hvorvidt kjernevåpen har en stabiliserende effekt. Sentrale realister som for eksempel Kenneth Waltz, har argumentert for at nukleær balanse kan skape stabilitet (Waltz, 2012). Statsviteren Patrick Morgan, på den andre siden, mener at dagens avskrekkingsstrategier trenger en justering da det foreligger mangelfullt empirisk grunnlag om kjernevåpens rolle i avskrekking, slik at konseptet ble behandlet som et abstrakt fenomen (2012, s. 85-87).

Avskrekking kan oppnås gjennom ulike strategier for hvordan man skal gjengjelde et angrep, og hvilke tiltak man kan iverksette for å nekte at motstanderens angrep lykkes. De tradisjonelle avskrekkingsteoriene har bygd på en forforståelse om at det vil komme en gjengjeldelse på et angrep, og at den mulige skaden vil overstige det potensielle utbytte. Tradisjonelt har man derfor, under den kalde krigen, snakket om to ulike strategier for avskrekking; *deterrence by punishment* og *deterrence by denial*, heretter omtalt som *straff* og *nektelse* (Nye, 2017, s. 54-57). I dette lå det en trussel om gjengjeldelse gjennom straff som innebærer at gevinsten man eventuelt kan oppnå ved angrepet er mindre enn kostnadene man kan påføres. I avskrekking gjennom nektelse derimot, er hensikten å gjøre det umulig eller usannsynlig at en motstander oppnår sine målsetninger med angrepet. I tillegg har man de siste ti-årene, som følge av økt globalisering introdusert begrepet *deterrence by entanglement*. Dette kan ses på som komplekse verdikjeder som følge av strategisk gjensidig avhengighet. Dette som følge av at gjensidige

interesser oppmuntrer til tilbakeholdenhet for å unngå utilsiktede følgevirkninger (Jasper, 2017, s. 9; Nye, 2017, s. 55-59). Sistnevnte strategi vil ikke bli videre omtalt i denne oppgaven.

For at avskrekkingsstrategien skal være effektiv, er man avhengig av at den må være basert på konkrete kapasiteter i form av å besitte *virkemidler* til å påvirke atferd, *kredibilitet* slik at motstanderen tror at mottiltak faktisk vil bli iverksatt, og *kommunikasjon* ment til å sende det riktige budskapet til rett publikum (Jasper, 2017, s. 10 og Strand, 2022, s. 46-47). Utfordringen med cyberdomenet er at effektive avskrekkingsstrategier kan være svært vanskelig å oppnå. For eksempel kan en angripers motivasjon være å oppnå politiske mål, nasjonal stolthet, egen tilfredshet eller økonomisk utbytte – hvorpå disse er svært vanskelig å avskrekke. Som følge av dette har Scott Jasper presentert en alternativ strategi; *aktivt cyberforsvar.* Poenget med aktivt cyberforsvar innebærer å skape resiliens, samt etablere offensive destruktive kapasiteter. Aktivt cyberforsvar søker å forsterke evnen til både straff og nektelse. Strategien kombinerer statens samlede motstandskraft til å stanse ondsinnet cyberaktivitet med skreddersydde destruktive kapasiteter for å hindre ondsinnede aktører å nå deres målsetninger (Jasper, 2017, s. 10).

Det kan dras paralleller mellom aktivt cyberforsvar som avskrekkingsstrategi og to nøkkelbegreper som har blitt presentert i de seneste amerikanske nasjonale cyberstrategiene «defending forward» og «persistent engagement» (Friis, 2020; U.S. President 2018). Persistent engagement innebærer en kontinuerlig engasjering av motstanderen i stedet for å sitte passivt å vente på å bli angrepet. Defending forward er et element i denne strategien som innebærer et proaktivt forsvar som vil forstyrre angripere i en tidlig fase slik at de i større grad må fokusere på forsvar enn angrep (Harknett, 2018; Kosseff, 2019 i Friis, 2020). Det fremstår som at denne strategien ikke i like stor grad spiller på samspillet mellom egen resiliens og utnyttelsen av offensive kapasiteter, noe Jaspers aktivt cyberforsvar er bygget på. Siden Norge i så stor grad spiller på viktigheten av å etablere en robust digital infrastruktur, er det naturlig at oppgavens videre diskusjon tar utgangspunkt i aktivt cyberforsvar som strategi, dog med inspirasjon fra amerikanske persistent engagement (Departementene, 2019).

Avskrekking innen cyberdomenet byr på flere utfordringer. En av årsakene til dette er ifølge Joseph S. Nye Jr. at man ofte er låst til å se avskrekking i lys av den kalde krigen med trusselen om massiv hevn på et nukleært angrep (Nye, 2017, s. 45). Cyberoperasjoner er fordekte av natur, kostnadseffektive, utfordrende å attribuere og de preges av opportunisme. Som følge av dette kan ikke alle involverte aktører garantere at deres defensive og offensive kapasiteter vil være tilstrekkelige (Moore, 2022, s. 104; Nye, 2017, s. 44-48). Det er også en viktig forskjell

mellom tradisjonell avskrekking og cyberavskrekking hvor sistnevnte krever en mer sammenhengende innsats fra både stat og samfunnet. Noe av årsaken til dette, er at cyberangrep ikke bare rettes mot staten, men også andre aktører som har implikasjoner for samfunnets sikkerhet (Kristiansen & Hoem, 2022, s. 21-22). Dette medfører at cyberoperasjoner er, og vil være en vedvarende og alvorlig trussel mot staters suverenitet, verdier og sikkerhetspolitiske interesser. Spesielt vil politiske beslutninger, militære strategier og teknologisk utvikling være særlige attraktive mål for andre statlige aktører, også i cyberdomenet. Sammenliknet med konvensjonelle trusler, er cyberangrep utfordrende å håndtere i den forstand at de til enhver tid må tilpasses for å utnytte de sårbarhetene som eksisterer. Som under den kalde krigen, foreligger det fortsatt en frykt for at en stat skal kunne utføre en «first (cyber) strike» som vil gjøre såpass stor skade at store deler av gjengjeldelseskapasitetene vil kunne bli ødelagt (Nye, 2017, s. 45; Morgan, 2012, s. 101). Morgan peker også på at cyberangrep trenger nøye oppmerksomhet av dagens avskrekkingsspesialister. Selv om utfordringene i dag er tilsvarende de man tidligere har analysert, er det to aspekter som burde veie tungt; attribusjonsutfordringene og uforholdsmessig gjengjeldelse (Morgan, 2012, s. 102).

Utfordringen med uforholdsmessig gjengjeldelse er at dette kan bidra til å eskalere en situasjon. Dette er spesielt relevant for cyberangrep, som fort har en tendens til å kunne spre seg vesentlig lenger enn de opprinnelige målene – en uintendert spillover-effekt. Dette medfører at en gjengjeldelse vil kunne tolkes som en eskalering i forhold til det opprinnelige målet, og dermed invitere til ytterligere respons (Morgan, 2012, s. 102). Det vil kunne medføre en svekkelse av avskrekkingsstrategiens kredibilitet, dersom responsen uteblir grunnet usikkerhet rundt svaralternativets proporsjonalitet (Kristiansen & Hoem, 2022, s. 24).

Det kan til tider være svært utfordrende å attribuere cyberangrep til konkrete stater, noe man har sett gjentatte eksempler på de siste årene, hvor mange cyberangrep forblir uløste i det offentlige. Dette har blitt pekt på som en av hovedårsakene til at avskrekking innen cyberdomenet er meget utfordrende (Nye, 2017, s. 49-50). I tillegg eksisterer det en rekke private grupper med en ikke ubetydelig knytning til statlig sektor, som utgjør en betydelig trussel i det digitale domenet. Dette gjør at stater fordekt kan gjennomføre cyberoperasjoner ved å benytte seg av private aktører. Dette er i stor kontrast til nukleær avskrekking hvor kun ni stater besitter nukleære våpen (Nye, 2017, s. 50).

1.6.2 Attribusjonsutfordringer

Som tidligere identifisert i forbindelse med anvendelse av folkeretten, er attribusjon et helt sentralt vilkår når det er snakk om selvforsvar, både i det fysiske konvensjonelle segmentet, men også innen cyber (Kristiansen & Hoem, 2022, s. 23). Offentlig attribusjon innebærer konkret å peke på hvem som har utført en handling – en offentlig anklage (Rid & Buchanan, 2014, s. 4). Attribusjon innen det digitale domenet byr på særskilte utfordringer. Gitt at trusselbildet overfor en stat strekker seg fra «gutteroms-hackeren» til statlige aktører, med et vidt spenn av intensjon, er det utfordrende å avgjøre med sikkerhet hvilken eller hvilke aktører som står bak (Rid & Buchanan, 2014, s. 5). Ikke minst har også attribusjonen en tendens til å være meget tidkrevende. Den kan ta flere måneder, hvis det i det hele tatt er mulig (Nye, 2017, s. 50). Flere stater har påpekt at det ikke foreligger noen juridisk forpliktelse om å offentliggjøre attribusjoner. På den andre siden nevner Tallinn Manual at flere stater mener man må legge frem bevis for hva attribusjonen bygger på for å kunne respondere mot cyberoperasjoner (Cyber Law Toolkit og Schmitt, 2017, s. 83). Det kan tenkes at årsaken til dette er for å unngå eskalering, samt at allierte trolig vil være avhengig av å se bevis før potensiell støtte blir gitt.

Gitt fordektbarhetens natur innen det digitale domenet, er det verdt å peke på utfordringen med at en part kan opptre på vegne av en annen, eller en privat aktør opptrer på vegne av en statlig aktør, såkalte proxyer (Nye, 2017, s. 50). Tallinn Manual peker på at begge disse eksemplene er operasjoner som kan tilskrives den statlige aktøren (Schmitt, 2017, s. 83). Det essensielle her er ikke nødvendigvis hvor man befinner seg geografisk, men hvorvidt man opptrer på instruksjon fra en stat. Dette illustreres godt i Canadas innspill til folkerettens anvendelse i cyberdomenet:

> *"A State can be responsible directly, or indirectly where a non-State actor has acted on the instructions of, or under the direction or control of, that State. In this respect, States cannot escape legal responsibility for internationally wrongful cyber acts by perpetrating them through non-state actors who act on a State's instruction or under its direction or control."*
>
> (Government of Canada, 2022).

Dersom vi relaterer dette til avskrekkingsstrategier, er det naturlig å peke på utfordringene man må håndtere knyttet til troverdighet rundt respons, spesielt når det gjelder strategien basert på

avskrekking gjennom straff. Dersom attribusjonsutfordringene blir for komplekse og utfordrende til at man velger å ikke attribuere angrep, vil avskrekkingsstrategien i praksis være mislykket.

Attribusjon differensiere mellom teknisk-, juridisk- og politisk attribusjon. Det er en distinkt forskjell mellom disse. Når man snakker om teknisk attribusjon, er det naturlig å tenke seg at dette er høyt graderte opplysninger, som går inn i kjernen til et lands eller en aktørs kapasiteter (Nye, 2017, s. 51). En slik form for attribusjon er derfor ikke noe en kan forvente. Britiske myndigheter uttalte i 2018 at de kan attribuere ondsinnet cyberaktivitet dersom det er i deres egen interesse, hvor slik attribusjon både kan gjøres offentlig, men også direkte gjennom diplomatiske forbindelser. I denne forbindelse er det naturlig å skille mellom juridisk- og politisk attribusjon. Det er i økende grad en oppfatning om at den tekniske delen av attribueringen i større grad er mulig. Attribusjonsproblemet som derfor tidligere har eksistert grunnet cyberangrepenes fordektbarhet, innebærer derfor nå i større grad et strategisk problem knyttet til hvorvidt man offentlig skal attribuere eller ikke (Egloff, 2020, s. 2).

Den juridiske attribusjonen er en integrert del av å karakterisere et angrep i et juridisk perspektiv, for eksempel relatert til FN-paktens artikkel 51 eller NATOs artikkel 5. Den politiske og i enkelte tilfeller den offentlige attribusjonen, er snarere en avgjørelse knyttet til strategiske vurderinger, og kan ofte bygge på staters privilegium og ikke nødvendigvis noe som er nødvendig i lys av folkeretten (Cyber Law Toolkit; Government of Canada, 2022).

I forlengelse av dette, er det interessant å se på Russlands innspill til FNs høringsnotat om anvendelse av folkeretten innen cyber. De sa følgende tilbake i 2021: *"any case, one should refrain from publicly imposing responsibility for an incident in information space on a particular State without supplying necessary technical evidence."* (United Nations, 2021, s. 80). Russlands offisielle uttalelse skaper intrikate utfordringer, da statene har ulikt syn på hva som kreves bevist. Russlands syn er naturlig nok ment for å støtte opp under egne hensyn, men samtidig utfordrer dette den vestlige handlemåte. Uten tekniske bevis knyttet til russiske beskyldninger, kommer sannsynligvis ikke Russland til å ta ansvar og erkjenne tilknytning til egne operasjoner.

1.6.3 Nasjonale cyberstrategier

Norges nasjonale militære strategi for bruk av cyberdomenet stammer fra 2014. Den gang kom Forsvarsdepartementet ut med «FDs cyberretningslinjer». Formålet med disse var å bidra til å

«sikre nødvendig handlefrihet i cyberdomenet, og å unngå eller redusere konsekvensene av alvorlige cyberangrep rettet mot egne systemer» (Forsvarsdepartementet, 2014, s. 4). Retningslinjene er avgrenset til forsvarssektoren. Den nyeste strategien Norge har, er en *nasjonal strategi for digital sikkerhet* som ble utgitt under daværende statsminister Erna Solberg i 2019.

Strategien er et samarbeid mellom Justis- og beredskapsdepartementet og Forsvarsdepartementet, og er den fjerde nasjonale digitale strategien. De tidligere ble utgitt i 2003, 2007 og 2012. Det er sentrale fellestrekk mellom strategiene fra 2012 og 2019, spesielt med hensyn til det underliggende risikobildet, de overordnede målene og strategiske prioriteringene, samt en rekke av de foreslåtte tiltakene (Riksrevisjonen, 2023, s. 95-96). Dette kan muligens ses på som en svakhet, i den forstand at strategien ikke har utviklet seg i tråd med den digitale utviklingen, der det mellom 2012 og 2019 åpenbart har skjedd mye. Strategien bygger på tre satsningsområder. Den fremhever viktigheten av sivil-militært, offentlig-privat og nasjonalt-internasjonalt samarbeid (Departementene, 2019; Riksrevisjonen, 2023, s. 93). Strategiens syn på kapasiteter til offensive cyberoperasjoner innebærer en sentralisert modell, hvor ansvaret ligger hos Etterretningstjenesten (Liebetrau, 2023, s. 138-139).

I forbindelse med CyCon23, NATO CCDCOE sin årlige cyberkonferanse, deltok Robin Bakke fra Justis- og beredskapsdepartementet i en paneldebatt om strategiutvikling. Der ble Norges gjeldende strategi presentert. I tillegg til de overnevnte satsningsområdene, trakk Bakke frem at strategien nå ikke bare retter seg mot myndighetene, men også i større grad sivile virksomheter (NATOCCDCOE, 2023, 31:19-43:58). I samme paneldebatt sa Bakke også at Norge, i forbindelse med utviklingen av dagens strategi, hadde tatt kontakt med Nederland og Storbritannia for å få innspill (NATOCCDCOE, 2023, 31:19-43:58).

Da strategien ikke inneholder informasjon om offensive kapasiteter, kan dokumentet sies å være defensivt innrettet (Wilhelmsen et al., s. 245). På dette området peker Simen Bakke i politiets IT-enhet på at Norges strategi skiller seg fra en rekke andre nasjoner. Han understreker at flere av Norges nærmeste allierte, herunder både USA og Storbritannia, i sine nasjonale cyberstrategier, fremhever at de fremover vil operere mer offensivt i cyberdomenet (Bakke, 2023).

Nederland har på den andre siden valgt en annen tilnærming i deres strategi. Der hvor Norges strategi ikke inneholder informasjon og budskap om offensive kapasiteter, er dette viet betydelige plass i den nederlandske strategien. Strategien kom ut i slutten av 2018, bare et par

måneder før Norges strategi. Nederlands cyberstrategi viser til noen helt sentrale kapasiteter og intensjoner de søker å styrke. De skal blant annet offentlig konfrontere og attribuere den angripende part. For å være i stand til å gjøre dette, skal de styrke den offensive cyberkapasiteten. Nederland skal samtidig styrke sine egne destruktive cyberkapasiteter slik at Nederland blir et mindre attraktivt mål (Ministerie van Defensie, 2018). I tillegg innebærer strategien et økt samarbeid mellom en egen cyberkommando og landets etterretningstjenester – det Liebetrau beskriver som en samarbeidende modell (2023, s. 135).

Nederlands nyeste strategi har fått offentlig anerkjennelse blant flere cybereksperter. Blant annet rangerte det amerikanske cyberfirmaet Humanize i 2023 Nederland som verdens sjette mektigste cybernasjon. Bakgrunnen for dette var blant annet deres dominerende cyberoffensive evne som kom i søkelyset etter et vellykket cyberangrepet fra en russisk hackergruppe i 2014. I forbindelse med dette angrepet kom det frem at den nederlandske etterretningstjenesten AIVD, hadde hatt tilgang til den russiske hackergruppen Cozy Bear sine tjenester i minst ett år (Humanize, 2023).

1.6.4 Spillteori

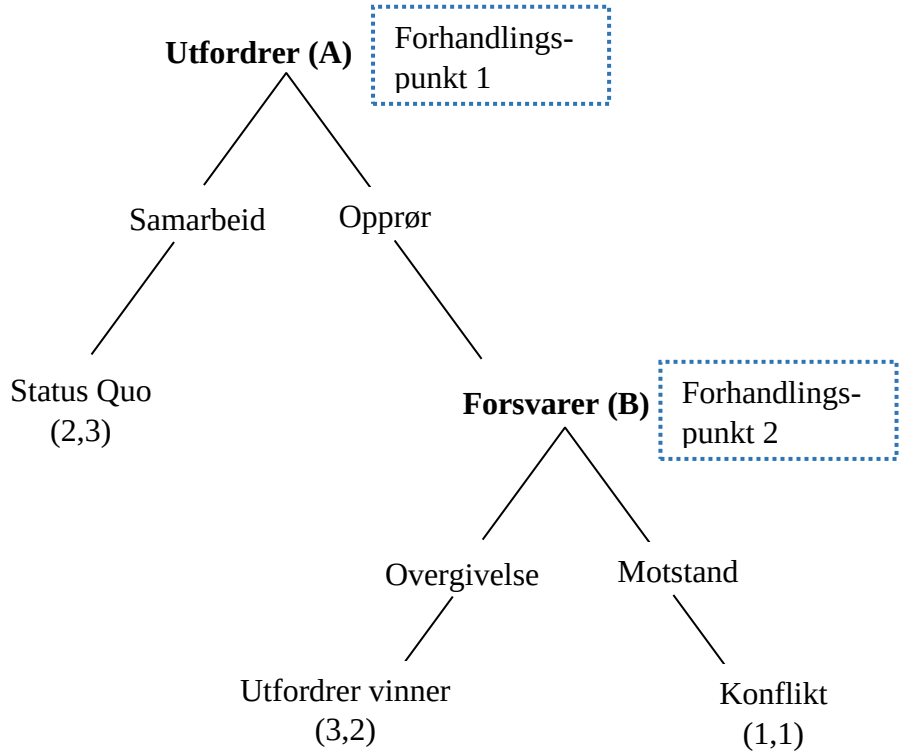
Den klassiske avskrekkingsteorien forutsetter og bygger på at de involverte partene foretar en rasjonell kost-nytte kalkulasjon der avskrekking oppnås gjennom en objektiv og rasjonell vurdering av motstanderens målsetninger, kostnader og styrkeforholdet dem imellom, samt at det forutsettes at partene i stort, deler det samme begrepsapparatet (Hovi, 2020, s. 17-20). For å forklare avskrekkingsstrategisk potensiale kan man benytte spillteori. Spillteori har sitt opphav tilbake til 1944 gjennom John Von Neumann og Oskar Morgenstern sin bok *Theory of Games and Economic Behaviour* (Midtgaard, 1967, s. 4). Teorien benyttes for å forklare interaksjonen mellom stater som en forhandling, og forklarer hvordan konflikter kan oppstå. Den kan også benyttes for å illustrere hvordan en konkret strategi, ut ifra det informasjonsgrunnlaget man sitter på, kan ha mulige alternative utfall. Spillteori beskriver aktørene som nyttemaksimerende, med et underliggende ønske om å minimere egne kostnader (Underdal, 2007, s. 233).

Et eksempel på hvordan man kan benytte spillteori som metode kan være å se til hvordan kommunikasjonen mellom USA og Nord-Korea var tilbake i 2006 da sistnevnte gjennomførte sine første kjernefysiske prøvesprengninger. I dette tilfelle ble de møtt med sanksjoner fra USA, hvorpå Nord-Korea reagerte med en form for motpress ved å svare at sanksjoner vil bli sett på

som en krigserklæring. En talsmann for regimet sa at *«jo større presset blir, jo sterkere blir vår respons»* (Aftenposten 11. oktober 2006 sitert i Hovi, 2020 s. 12). I senere tid har presset mellom de to statene vedvart. Et sentralt spørsmål er hvorvidt presset som utøves er *troverdig* eller om det kun er snakk om tomme trusler. Ved å se på presset som avskrekkingsstrategier kan man utarbeide hypoteser som man tester ved hjelp av spillteori og analyserer basert på hypotesenes sannsynlighet.

Den klassiske avskrekkingsteorien tar utgangspunkt i at en militær konflikt mellom to likeverdige stater, er det minst ønskelige utfallet for alle parter. Teorien kan deles inn i to pilarer; *Beslutningsteoretisk*- eller *strukturell avskrekkingsstrategi* (Gaddis, 1986, sitert i Quackenbush og Zagare, 2016, s. 2-3). Den strukturelle avskrekkingsstrategien forutsetter at sannsynligheten for en militær konflikt er direkte relatert til de kostnadene en slik konflikt vil ha. Her minker sjansene for militær konflikt dersom det antas at kostnadene ved krigføring vil være høye. Forholdet mellom statene antas å være stabil, for eksempel i form av et «spill» mellom to atomstater. Dersom maktforholdet er ujevnt fordelt, kan den overlegne parten dominere andre militært underlegne stater. I disse tilfellene vil ikke gjensidig avskrekking være til stede. Pilaren om strukturell avskrekking mangler derimot empirisk evidens, da både første- og andre verdenskrig er eksempler på krig og konflikter som brøt ut i et internasjonalt system som ifølge de teoretiske kriteriene var i maktbalanse og stabile (Quackenbush og Zagare, 2016, s. 2-4).

Den andre pilaren, beslutningsteorien, innebærer en antakelse om at en krig med forventede høye kostnader, er det minst ønskelige utfallet til samtlige parter. Også i dette tilfelle kan vi bruke eksempelet med at kjernefysisk avskrekking vil skape stabilitet, fordi det involverer en betydelig sannsynlighet og risiko for enorme kostnader. Teorien innebærer med andre ord at aktørenes persepsjon av potensielt svært høye kostnader, gjør at konflikten eller krigen vil være irrasjonell å delta i. Disse teoriene kan tradisjonelt eksemplifiseres i ulike spill (Quackenbush og Zagare, 2016, s. 5-8).



Figur 1: Asymmetrisk avskrekkingsspill hvor forsvarers trussel ikke er troverdig (Quackenbush & Zagare, 2016, s. 5).

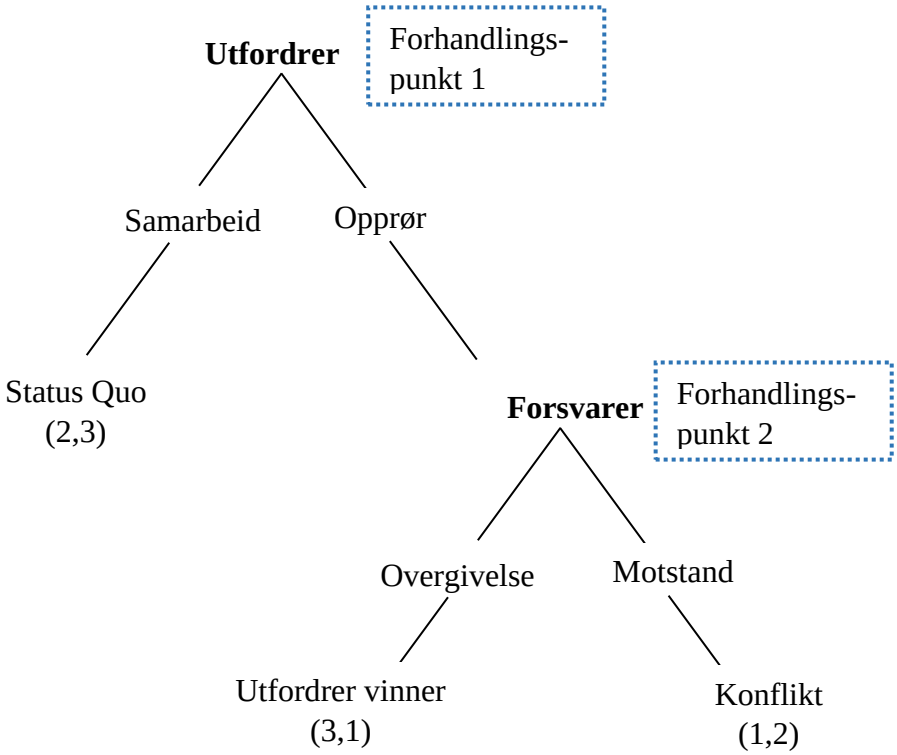
Figuren ovenfor tar utgangspunkt i et spill mellom to aktører, hvor stat A har rollen som utfordrer, og stat B innehar rollen som forsvarer. Modellen tar utgangspunkt i to scenarioer hvor utfallet av handlinger rangeres høyest til lavest, hvor spillernes mest foretrukne utfall rangeres med «3». Det minst foretrukne utfallet rangeres med «1». Dette eksemplifiseres ved at premisset om konflikt er det minst ønskelige utfallet for begge aktører – i tråd med den definerende forutsetningen til beslutningsteorien om at konflikt er minst ønskelig for alle parter.

Dersom vi forutsetter at stat A ikke er tilfreds med å opprettholde «status-quo», men derimot ønsker å utfordre sitt forhold til stat B, må begge statene kjenne til hvilke rasjonelle alternativer de har. Dette innebærer at stat B, under forhandlingspunkt 2, står ovenfor en utfordring fra stat A. Dersom stat B foretar rasjonelle valg, vil det være naturlig at de etterkommer utfordrerens krav om å endre «status quo», fordi dette handlingsalternativet gir et bedre utfall enn det motsatte, nemlig konflikt. Dette innebærer at utfordreren vinner. Modellen viser attpåtil at det vil være rasjonelt for stat A å utfordre B, fordi den forsvarende stat ikke rasjonelt kan gjengjelde utfordreren, da dette vil medføre konflikt. Dersom stat 2 derimot velger å overgi seg, oppnår de sitt nest beste utfall (*stat A vinner, 3,2*) (Quackenbush & Zagare, s. 2016, 6-8).

Spill- og avskrekkingsteoretiske akademikere har arbeidet lenge for å løse dette paradokset med avskrekking, hvor en av de mer kjente løsningene stammer fra Thomas Schelling. Hans løsning dreier seg om forsvarerens evne til å overbevise utfordreren om at trusselen ikke er rasjonell. Dette i den forstand at en trussel vil bli møtt med en totalt utslettende gjengjeldelse til tross for store kostnader (Quackenbush & Zagare, s. 2016, 6). Hvis forsvareren lykkes, vil utfordreren samarbeide på forhandlingspunkt 1, da alternativet er det minst ønskelige utfallet. Dette kan eksemplifiseres ved å true med kjernefysisk gjengjeldelse, hvor det eneste rasjonelle valget for utfordreren er å samarbeide, noe som oppnår nest høyest gevinst (*status quo, 2,3*).

Uansett vil en slik trussel om gjengjeldelse være irrasjonell, slik at forsvareren vil ha utfordringer med å få gjengjeldelsen til å fremstå troverdig, da dette er en sentral forutsetning innen avskrekkingsstrategien. En trussel fra en forsvarer som fremstår irrasjonell, vil med andre ord ikke være troverdig (Quackenbush & Zagare, 2016, s. 6-9).

I tillegg til den klassiske avskrekkingsstrategien, kom Zagare og Kilgours (2000) med et nytt bidrag til det teoretiske rammeverket med deres *Perfect deterrence theory*, heretter omtalt som PDT. I motsetning til den tradisjonelle beslutningsteorien, bygger PDT på en antakelse om at statene ikke kan vite motpartens vurdering av kostnader og nytte. Dette innebærer en informasjonsbrist og manglende forståelse for motpartens minst ønskelige utfall og antatte kostnader ved en militær konflikt. PDT behandler derfor motstanderens troverdighet som en variabel og ikke konstant. Spillernes kredibilitet avgjøres derfor ved sannsynligheten for at den avskrekkende trusselen vil bli utført (Zagare & Kilgours, 2020, s. 285-298). I tillegg bygger den på en forståelse av at gjensidig avskrekking fungerer best når begge spillerne har nødvendige kapasiteter og troverdige trusler. Kapabilitetene skal påføre smerte, og troverdigheten om truslene skal være rasjonelle (Zagare & Kilgours, 2020, s. 289).



Figur 2: Asymmetrisk avskrekkingsspill hvor forsvarers trussel er troverdig (Quackenbush & Zagare, 2016, s. 8).

Figur 2 tar utgangspunkt i eksakt det samme scenarioet som figur 1 – utfordreren ønsker å endre status quo, og utfordre sitt forhold til forsvareren der det er til forsvarerens fordel å opprettholde det eksisterende forholdet (*2,3*). Med utgangspunkt i realismens grunntanke om å sikre statens overlevelse, kan stater sørge for å følge sine egeninteresser, selv om dette er på bekostning av andre. Målet til den forsvarende parten vil derfor være å avskrekke maktbruk fra den andre staten, i den hensikt å sikre egen overlevelse. I følge PDT, kan dette utelukkende gjøres dersom man har en troverdig avskrekking – en forutsetning som ligger til grunn i figur 2, men ikke i figur 1. I motsetning til figur 1, vil ikke motstanderens trusler om gjengjeldelse nå være forsvarerens minst ønskelige utfall (*1,2*). I dette tilfellet foretrekker faktisk forsvareren konflikt fremfor å overgi seg til utfordreren (*3,1*). Igjen illustrerer dette viktigheten av persepsjon innen avskrekkingsteori, da hele modellen bygger på utfordrerens oppfatning av forsvarerens preferanser. I de tilfeller hvor avskrekkingen fremstår som troverdig vil utfordreren tape.

1.6.5 Spillteoretiske forutsetninger

Gjennom spill testes teorier om interaksjonen mellom rasjonelle aktører. I dette ligger blant annet forutsetningen om en rasjonell aktør som har konsistente preferanser og handler på en forutsigbar måte (Hovi, 2020, s. 17-18). Med andre ord kjenner man til hverandres intensjoner. Dette medfører også muligheten for spillteorietiske modelleringer, gitt at nødvendige forutsetninger legges til grunn. Sentralt for den videre analysen er hva som ligger i denne rasjonelle atferden. Harsanyi (1986) peker blant annet på at aktøren er nyttemaksimerende (s. 89, sitert i Hovi, 2020, s. 17). For å skape et felles bakteppe for den samlede videre analysen, legges det enkelte forutsetninger til grunn.

Forutsetningene har sin opprinnelse fra det teoretiske rammeverket, samt min subjektive opplevelse av hvordan statenes relasjoner og avhengigheter oppfattes i dag.

Forutsetninger:

- Norge (aktør A) er som småstat å regne. Samtidig er staten en sentral og viktig alliert i NATO, med landets strategisk viktige plassering i nordområdene. Norge er også en svært viktig produsent av naturressurser til det europeiske kraftmarkedet, og har en betydelig andel av kritisk undersjøisk infrastruktur, til bruk også for andre land.
- Russland (aktør B) har betydelige utfordringer med å oppnå overlegenhet i sin krig med Ukraina. Dette skaper blant annet utfordringer med legitimiteten til regimet i Kreml, med potensielt betydelig motstand i befolkningen. Russland har et betydelig avskrekkingspotensiale med sine kjernefysiske våpen. Det kan også fremstå som at myndighetene er i større grad uforutsigbare i sin villighet til å gjøre mer for å oppnå sine mål.
- De russiske cyberkapasitetene er bedre enn Norges isolerte kapasiteter, og man er kjent med hverandre kapasiteter.
- Den nye normaltilstanden innebærer lite samarbeid.
- Aktørene har tydelig definert enkelte grenser innen cyberkrigføring, men er tvetydig når det gjelder dens røde linjer.
- Samtlige aktører er å regne som rasjonelle i sine handlemåter.
- Cyberkrigføring favoriserer den offensive aktøren, spesielt knyttet til mulighetene for å overraske, utfordringer med å oppdage, samt at det til tider kan være svært utfordrende å attribuere.

- Aktørene er kjent med hverandres respektive kapasiteter og ambisjoner i det digitale domenet.
- Scenarioene vil ta utgangspunkt i Norge som aktør, men vil benytte handlingsalternativer fra både den norske og den nederlandske cyberstrategien.

Det er verdt å nevne at casene som benyttes som utgangspunkt for den videre analysen er oppdiktede, dog er det hentet inspirasjon fra reelle hendelser.

DEL II: RESULTATER

2.1 Introduksjon

Del II er todelt, og følger operasjonaliseringen slik den ble presentert i Del I. Først, i 2.2 *Komparativ analyse av Norge og Nederlands cyberstrategier*, sammenlignes Norges cyberstrategi med Nederlands. Analysen tar utgangspunkt i tre dimensjoner ved statenes cyberstrategier: *Suverenitet, institusjoner* og *innhold*. Dernest, i 2.3 *Norge, avskrekking og spill,* testes Norges strategi-alternativer i gitte situasjoner gjennom ulike spill med forenklede modelleringer. Disse tar utgangspunkt i avskrekkingsstrategiene, *straff, nektelse og aktivt cyberforsvar*.

2.2 Komparativ analyse av Norge og Nederlands cyberstrategier

Den komparative delen av oppgaven tar utgangspunkt i Norge og Nederlands siste utgaver av landenes cyberstrategier. Årsaken til at nettopp Nederlands strategi har blitt valgt ut for å sammenlikne med, er at landet i mange tilfeller kan sammenliknes med Norge som en småstat i for eksempel NATO-sammenheng. Landene besitter mange av de samme kapasitetene. Dette er illustrert i Global Firepower 2023 sin analytiske gjennomgang over nasjonenes potensielle militære kapabiliteter. I 2023 kom Norge på 35 plass, mens Nederland kom på 39 plass (Global Firepower, 2023). I tillegg har deres militære budsjetter i forhold til landenes BNP utviklet seg til å bli sammenliknbare slik SIPRI sin oversikt mellom 2017-2022 illustrerer.

		2017	**2018**	**2019**	**2020**	**2021**	**2022**
Nederland		1,16 %	1,22 %	1,32 %	1,44 %	1,38 %	1,58 %
Norge		1,71 %	1,72 %	1,84 %	1,97 %	1,72 %	1,64 %

Tabell 1: Militære utgifter i prosent av BNP, 2017-2022 (SIPRI, 2023)

Nederland har siden 2015 hatt en eksepsjonell økning i sine forsvarsbudsjetter, mens Norge i stor grad ligger på samme nivå. Der hvor det i 2015 var omtrent 26 milliarder norske kroner i differanse mellom landenes forsvarsbudsjetter i Nederlands favør (Institute for Strategic Studies, 2018, s. 130-135) var differansen i 2022 gått opp til nesten 55 milliarder – en økning på over 100% (Institute for Strategic Studies, 2023, s. 116-120).

Som analyseverktøy vil jeg benytte et komparativt analyseskjema hvor både Norges og Nederlands nasjonale cyberstrategier er oppsummert. I tillegg vil jeg benytte enkle spillteoretiske modelleringer for å analysere tre ulike spill hvor disse er relatert til tre ulike avskrekkingsstrategier. I disse spillene vil jeg trekke inn relevante synspunkter fra de to undersøkte nasjonale cyberstrategiene. Formålet med analysen er å forsøke å svare ut betydningen av Norges valgte avskrekkingsstrategi. Analyseskjemaet reflekterer en egen kvalifisert oppsummering etter de gitte variablene.

ANALYSESKJEMA			
Dimensjon	*Variabel*	**NORGE**	**NEDERLAND**
SUVERENITET	**Nasjonale interesser**	Digitale angrep -> trussel mot norsk suverenitet.	Rett til selvforsvar – Artikkel 51.
	Internasjonalt samarbeid	Styrke samarbeid og partnerskap. «Internasjonal cyberstrategi for Norge»	Kapasiteter til allierte oppdrag og operasjoner.
INSTITUSJONER	**Sivilmilitært samarbeid / Totalforsvaret**	Sivil støtte til Forsvaret. Norske virksomheter tar ansvar for håndtering av angrep i egen virksomhet. Ansvarsprinsippet NATO setter sivil-militært samarbeid på dagsorden.	Samarbeid med sivile partnere. Militær bistand og støtte til sivile myndigheter.
	Militært	Utvisking av ansvarsplassering mellom sivil og militær sektor. Virksomheter i forsvarssektoren skal samarbeide med sivil sektor for å identifisere, utveksle erfaringer og finne løsninger på digitale sikkerhetsutfordringer. Forsvarsdepartementet har	Militære kapabiliteter MIVD Kapasiteter for å oppnå og beholde dominans under militære operasjoner Økt informasjonsdeling Styrket destruktiv kapasitet

		ansvar for digital sikkerhet i forsvarssektoren.	
INNHOLD	**Tilnærming**	Defensiv – ikke definert	Offensiv
	Avskrekkings-mekanismer	Ikke definert En robust samfunnssikkerhet skal skape grunnlag for fungerende militært forsvar.	Avskrekking krever troverdige offensive evner. Avskrekking bidrar til å bli et mindre attraktivt mål. Aktiv attribusjonspolitikk
	Attribusjon	Gjennom videreutvikling av internasjonalt samarbeid	Eget kapittel Ønsker å offentlig konfrontere. Investere ytterligere i offensive kapasiteter for å kunne attribuere.

Tabell 2: Komparativ analyse av Norge og Nederlands cyberstrategi (Departementene, 2019; Ministerie van Defensie, 2018).

Overnevnte analyseskjema har sitt utgangspunkt i henholdsvis Norges og Nederlands nasjonale cyberstrategi. Gitt at de er utgitt med ca. tre måneders mellomrom, tas det utgangspunkt i at analysen bygger på relativt lik virkelighetsforståelse. Det er derimot verdt å peke på at Norges strategi, i stor grad tar utgangspunkt i den forståelsen man også hadde tilbake i 2012, da den forrige strategien ble gitt ut (Riksrevisjonen, 2023, s. 95-96). Analysen er delt inn i tre ulike dimensjoner og videre inndelt i variabler, i den hensikt at det skal kunne være mulig å dele dette inn i senere koder. Formålet er videre, sammen med den spillteoretiske analysen, at jeg skal nærme meg et steg i retningen å kunne operasjonalisere et alternativ til dagens foretrukne avskrekkingsstrategi i Norge. For enkelhets skyld vil det i den videre drøftelsen vises til hvilke innspill nasjonene har.

Suverenitets-dimensjonen bygger på en analyse om hva strategiene sier om cybertrusselens påvirkning av nasjonens suverenitet. Begge strategiene peker på at digitale angrep ses på som en betydelig trussel mot nasjonal sikkerhet. Det er derimot en distinkt forskjell. Der hvor Norge ser på digitale angrep som en trussel mot norsk suverenitet, viser Nederland konkret til at et cyberangrep i et slikt omfang klart kan sees på som et væpnet angrep. Nederland viser her til at staten har rett til å forsvarere seg i henhold til Artikkel 51 i FN-pakten.

Norge har et betydelig fokus når det gjelder internasjonalt partnersamarbeid hvor det blant annet vises til en egen strategi fra 2017, *«Internasjonal cyberstrategi for Norge»*. Strategien er snart er seks år gammel. En følge av dette kan være en utdatert strategi, da det har blitt gjennomført en rekke markante cyberangrep siden den tid, i tillegg til at seks år med digitalisering har bidratt til å skape ytterligere sårbarheter man ikke var klar over i 2017. Det fremstår videre som at Norge i dagens strategi, i stor grad ønsker å utnytte internasjonale kapasiteter i motsetning til Nederlands strategi. Den nederlandske strategien viser konkret til at man derimot burde søke å tilby nederlandske kapasiteter til allierte for oppdragsløsning eller til konkrete cyberoperasjoner. Nederland viser også til at den økende cybertrusselen krever en sterk internasjonal respons som er basert på internasjonale avtaler. De peker således også på at dagens status-quo fortsatt er utilstrekkelig. Dette fremstår som uvanlig konkrete og fremoverlente målsetninger når det gjelder internasjonalt partnersamarbeid (Departementene, 2019; Ministerie van Defensie, 2018).

I *den institusjonelle dimensjonen* viser begge strategiene til viktigheten av det sivil-militære samarbeidet, hvor Norge i stor grad spiller på totalforsvarstankegangen. Norges strategi er utgitt av både Forsvarsdepartementet og Justis- og beredskapsdepartementet i fellesskap, mens Nederlands strategi er utgitt av deres Forsvarsdepartement. Dette preger også denne dimensjonen. Norge viser til sivil støtte til forsvarssektoren, mens Nederland har snudd fokuset, og viser til den militære bistanden og støtten Forsvaret skal gi til sivile myndigheter. I tillegg viser Nederland til viktigheten av å samarbeide med sivile partnere. Norges strategi peker i stor grad på en forventning om at norske virksomheter tar ansvar for håndtering av angrep i egen virksomhet og viser i dette tilfelle til ansvarsprinsippet. En slik tankegang fremstår påfallende lik den regjeringen fikk knallhard kritikk for etter sprengingen av Nord Stream-rørene september 2022. Den gangen mente Olje- og energiministeren at det er selskapene selv som har ansvaret for sikkerheten på norsk sokkel (Melby, 2022). Mange sivile virksomheter understøtter det som norske myndigheter anser som kritisk infrastruktur. Derfor er det viktig at den norske strategien understreker nettopp dette. Derimot kan det være en uoppdaget svakhet ved at

ansvaret i stor grad legges til sivile virksomheter (Departementene, 2019; Ministerie van Defensie, 2018).

Når det gjelder det militære bidraget er ulikhetene store. Der Norge i stor grad viser til at totalforsvarskonseptet skal benyttes for å identifisere risikoer, utveksle erfaringer, samt finne løsninger på digitale utfordringer, har Nederland en mer pragmatisk tilnærming. Den understreker den nederlandske utenlandsetterretningstjenesten MIVD sin rolle innen cyber, hvor de selv kan aksjonere for å forstyrre akutte trusler. Videre vil Nederland søke å styrke de militære kapabilitetene hvor de fremover vil satse på å utvikle evnen til å oppnå og beholde dominans under militære operasjoner. De vil videre fokusere på økt informasjonsdeling, samt styrke sine destruktive kapasiteter. Norge derimot, nevner kun at Forsvarsdepartementet har ansvar for digital sikkerhet i forsvarssektoren. Nederlands militære strategi på dette punktet, fremstår relativt identisk med tankesettet til Jasper og hans avskrekkingsstrategi *aktivt cyberforsvar*. Tilsynelatende har norske myndigheter altså ikke en tydelig formidlet strategi for hvordan Forsvaret skal bidra, samt utnytte cyberdomenet for å nå statens overordnede strategiske målsetninger (Wilhelmsen et al., 2021, s. 245). Dette kan innebære en svakhet i Norges strategi, hvis vi tar utgangspunkt i den amerikanske akademikeren Robert Johnson, som viser til at enhver vellykket strategi krever en enhetlig aktør (2021, sitert i Wilhelmsen et al., 2021, s. 245).

Innholdsdimensjonen peker konkret på hva nasjonene presenterer, samt hvordan jeg tolker dette budskapet. Strategiene er svært ulike i sin tilnærming. Der Nederland har en meget fremoverlent og offensiv tilnærming, er ikke denne delen av cyberoperasjoner tilskrevet noe plass i Norges strategi. Årsakene til dette er uvisst, men det er vanskelig å se for seg at det er for å skjerme egne kapasiteter. Etterretningstjenestens mandat til å gjennomføre offensive cyberoperasjoner har vært kjent lenge før Norges strategi ble skrevet (Forsvarsdepartementet, 2014). Derimot fremstår en mulig årsak til tilnærmingen, at man har et mer defensivt standpunkt i bruken av slike virkemidler.

Videre er det naturlig å peke på strategienes avskrekkingsevne – evnen som tross alt må baseres på en kommunisert intensjon samt nødvendige og troverdige kapasiteter. I Norges strategi er ikke avskrekking nevnt konkret, så denne evnen må tolkes ut fra en større kontekst. Blant annet sier Norge at grunnlaget for et godt fungerende militært forsvar er robust samfunnssikkerhet. Igjen fokuset på sivilmilitært samarbeid (Departementene, 2019). Norges strategi kan dermed tolkes i den forstand at man søker å skape et motstandsdyktig samfunn, at dette skal bidra til å

avskrekke en motstander. Nederland har også i dette tilfellet valgt en annen strategi. Den poengterer avskrekkingsevnen konkret, samt hvilken effekt den skal ha, og viser til at dette oppnås gjennom troverdige offensive kapasiteter. Overordnet skal strategien bidra til å gjøre Nederland til et mindre attraktivt mål å angripe. Dette skal oppnås gjennom offensive kapasiteter sammen med en aktiv attribusjonspolitikk (Ministerie van Defensie, 2018).

Et konkret eksempel på dette, var deres avsløring og offentlige attribuering av en cyberoperasjon utført av russiske GRU mot Organisasjonen mot forbud mot kjemiske våpen (OPCW). Operasjonen ble utført av fire russiske personer med diplomatisk pass (Ministy of Defence, 2018). Disse ble pågrepet tre dager etter ankomst utenfor bygningene til OPCW. Bilen de ble pågrepet i, inneholdt datamaskiner og avlyttingsutstyr som var rettet mot kontorene til OPCW. OPCW undersøkte på dette tidspunktet nervegiften som ble benyttet til å forgifte Skripal, samt påståtte russiske kjemiske angrep i Syria. Russiske myndigheter kan derfor sies å ha et insentiv om å ramme OPCWs hovedkvarter. De fire russiske personene ble utvist samme dag (FFI, 2022b, s. 39). Operasjonen ble avslørt bare to måneder før Nederland presenterte den nye cyberstrategien. Det som var enestående i denne sammenheng, var at Nederland gikk til det skrittet å teknisk attribuere angrepet til Russland. Dette gjorde de i form av å offentlig publisere en 35 sider lang presentasjon med tekniske bevis som pekte i retning GRU (Ministry of Defence, 2018).

Ikke bare beviste Nederland at det var russiske aktører som stod bak cyberoperasjonen. De viste også at de både har kapasiteter, evne og vilje til både håndtere operasjonen, samt attribuere. Det viktigste budskapet Nederland sendte, var en tydelig politisk vilje til å vise et klart standpunkt, både når det gjelder strategisk kommunikasjon, men også bruk av kapasiteter. På fire dager rakk Nederland å avdekke, skaffe tilstrekkelig bevis, pågripe før angrepet var et faktum, offentlig, teknisk og politisk attribuere, samt utvise de fire russiske personene. Dette står i en interessant kontrast til Smeets, som vurderer Nederland som en aktør som både har lav kapasitet, samt selvpålagte høye begrensninger (Smeets, 2022, s. 65-69).

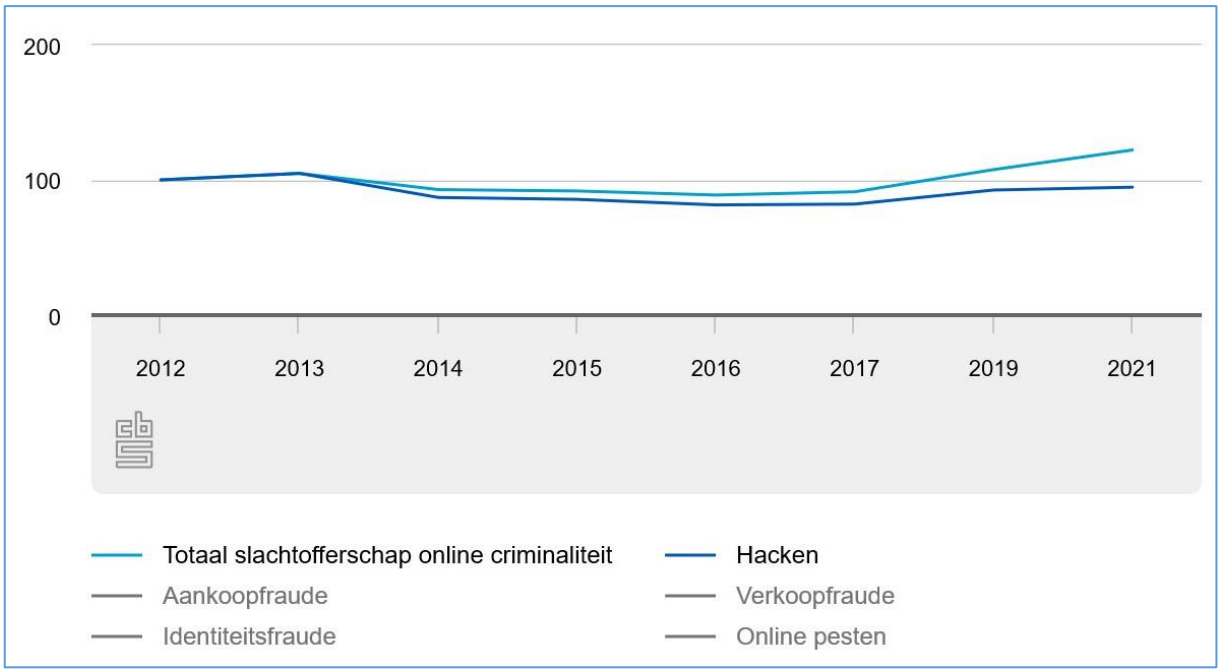
Når det gjelder attribusjon har ikke Norge berørt dette i sin strategi, utenom at det pekes på at de skal videreutvikle evnen til å attribuere gjennom internasjonalt samarbeid. Det at Norge søker å gjøre dette gjennom partnere, kan fort skape en uheldig avhengighet, hvor man i for stor grad lener seg mot andre lands beslutningstakere, som igjen må gjøre en kostnadsvurdering opp mot potensielt utbytte. I motsetning til Norge har Nederland et eget kapittel om dette. Nederland ønsker å offentlig konfrontere, samt investere ytterligere i offensive kapasiteter for å styrke

evnen til attribusjon. Dette budskapet, gjennom konkrete eksempler, kan skape en forutsigbar Nederlandsk respons. Dette skal igjen bidra til at en potensiell motstander heller velger å utføre angrepet mot et annet land.

Når det gjelder organiseringen av henholdsvis Nederlands og Norges cyberkapasiteter, er dette noe som har blitt undersøkt av Liebetrau. Hans vurdering er at landene har valgt to svært ulike retninger. Nederland har innrettet seg mot en samarbeidende modell som bygger på samspillet mellom tjenestene som besitter kapasiteter til henholdsvis bruk i krig eller konflikt, samt til etterretnings- og aktive forsvarsmål. Norge på den andre siden har innrettet seg etter en sentralisert modell hvor man ikke skiller mellom cyberkapasiteter til bruk for etterretningsmessige- eller militære formål (2022, s. 134-141).

Et annet sentralt spørsmål er hvorvidt Nederlands strategi faktisk har vært vellykket. Dersom det kan konkluderes med at den valgte strategien har betydelige svakheter, er dette naturlig nok noe som bør tas med i beregningen av hvorvidt en tilsvarende strategi skal implementeres i Norge. Strategiens måloppnåelse er naturlig nok svært vanskelig å fastslå, men gjennom å undersøke relevant nederlandsk statistikk over kjente cyberangrep, er det mulig å gjøre noen konkrete observasjoner.

Et naturlig sted å starte når man skal måle en slik effekt, er å se på utviklingen i antall cyberangrep Nederland har måttet håndtere de siste årene. Dette er tall som har vært utfordrende å finne. Det nederlandske statistiske sentralbyrået har publisert en oversikt over antallet offentlige kjente gjennomførte hackinger, samt oversikt over de totale ofrene for kriminalitet på nett. Som man ser av tabellen under er grafen ganske stabil når det gjelder hacking, mens for ofre generelt, har den steget noe de siste årene, spesielt siden 2017 (Central Bureau voor de Statistiek, 2022).



Tabell 3: Oversikt over digitale angrep i Nederland 2012-2021 (Central Bureau voor de Statistiek, 2022).

Til sammenligning har det i perioden 2019 til 2021 vært en tredobling i antall alvorlige digitale angrep mot offentlige og private virksomheter i Norge (Riksrevisjonen, 2023). Hvorvidt disse tallene er sammenliknbare, er høyst usikkert. Jeg skal derfor være forsiktig med å dra slutninger på bakgrunn av dette. Statistikken fra Nederland viser ikke tilsvarende økning. Hvorvidt dette er et resultat av deres strategi, mangelfull rapportering eller hvorvidt Nederland oppfattes som et lite attraktivt mål, er uklart. Dette kommer jeg nærmere tilbake til i diskusjonskapittelet.

Nederlands valgte cyberstrategi er avhengig av å fremstå som vellykket for at den skal oppnå den ønskede avskrekkende effekten. Dette innebærer at nederlandske myndigheter delvis vil ha et insentiv til å holde vellykkede cyberangrep skjult. Dette til tross for deres mål om offentlig attribusjon. I tillegg må statistikkens reliabilitet vurderes nøye, før man tillegger den betydelig verdi. Derimot ville trolig Nederland valgt en annen tilnærming når de i desember 2022 lanserte en ny cybersikkerhetsstrategi for 2022-2028 dersom deres strategi hadde vært mislykket. I denne har de valgt å opprettholde essensen av tiltakene i strategien fra 2018. Dette er en indikasjon på at den valgte strategien har hatt et ønsket måloppnåelse, som gjør at de ønsker å forlenge denne i neste strategiperiode frem til 2028 (Ministry of Justice and Security, 2022).

Analysen over bidrar til å kaste lys over Norges og Nederlands cyberstrategi, hvor hovedtrekkene innebærer to ulike tilnærminger mot det som oppleves som et felles mål – å sørge for å styrke evnen til å håndtere et cyberangrep.

2.3 Norge, avskrekking og spill

I denne delen analyseres tre ulike (men ikke gjensidig utelukkende) norske tilnærminger til avskrekking. Her brukes spill som metode for å identifisere aktørenes handlingsmuligheter og potensielle konsekvenser. Først gjennom *nektelse*, så gjennom *straff*, til slutt *aktivt cyberforsvar*. De ulike analysene vil ta utgangspunkt i et scenario som presenteres fortløpende.

Analyse av avskrekking gjennom nektelse

Avskrekking gjennom nektelse søker å overbevise motstanderen om at deres angrep vil mislykkes. Et sentralt poeng er at man reduserer risikoen ved å sørge for at det er vanskeligere og mer kostbart for motstanderen å initiere angrepet. Strategien er ikke utelukkende basert på egen motstandsdyktighet, men bygger i stor grad på motstanderens persepsjon - evnen til å få motstanderen til å tro at sannsynligheten for et vellykket angrep er redusert. Dette kan relateres til den norske strategien, som i dag i stor grad baserer seg på å styrke egen resiliens (Muller, 2019, s. 2). Cyberaktivitet utfordrer denne formen for avskrekking da den er fordekt av natur, samt kan ramme et bredt spekter av virksomheter i ulike deler av aktørens verdikjede (Nye, 2017, s. 56-57). Dette innebærer at motstandsdyktigheten må skapes i det som i Norge er kjent som totalforsvarsrammen – den gjensidige støtten mellom Forsvaret og det sivile samfunnet for å sikre tilstrekkelig beredskap (FFI, 2022a). Dette resulterer i at samtlige virksomheter i samfunnets til tider komplekse verdikjede, er avhengig av å bidra for å skape tyngde bak aktørens evne til å fremsette en overbevisende trussel mot en potensiell motstander.

Når vi videre skal se på denne analysen, må hovedtanken være at man skal søke å endre kost-nytte vurderingen til motstanden ved tydelig og troverdig å signalere at et digitalt angrep vil mislykkes (Jasper, 2017, s. 111-120). Norges cyberstrategi fremstår tydelig på dette punktet hvor man presiserer viktigheten av å ha et nært og tett samarbeid mellom Forsvaret og sivile virksomheter (Departementene, 2019). Dette er noe som også presiseres i Nederlands strategi hvor man skal søke samarbeid med det sivile for blant annet å sikre kritisk infrastruktur (Ministerie van Defensie, 2018).

Scenarioet den første analysen tar utgangspunktet i, bygger på et scenario hvor den sterke staten, Russland som statlig aktør, søker å påvirke den svakere staten, Norge. Russland har over tid fått svekket sin evne til å innhente informasjon som følge av at 15 russiske diplomater ble utvist i april 2023. Dette medfører at Russland må innhente informasjon med andre ukonvensjonelle

metoder, i dette tilfelle gjennom offensive cyberoperasjoner. Som et resultat av deres svekkede innflytelse i Norge, søker de derfor i stedet å få innsyn i graderte eller konfidensielle registre, i den hensikt å lettere identifisere potensielle kandidater de ønsker å benytte til innsamlingsformål. Norge søker å opprettholde status-quo, med unntak av at landet arbeider aktivt med egne sikringstiltak for å sørge for å redusere risikoen for infiltrasjon av kritisk infrastruktur.

Blant annet sier Norges internasjonale cyberstrategi at man skal skape robusthet gjennom ansvarliggjøring av sluttbrukere og virksomheter, samt avklare ansvar mellom myndigheter og privat sektor. Dette er utfordrende all den tid Norge ofte er svært tidlig ute med å implementere og benytte seg av ny teknologi (Utenriksdepartementet, 2021, s. 5-10). Overnevnte scenario er relativt identisk med hendelsen fra 2015 hvor et amerikansk personellregister ble infiltrert. Dette resulterte i at sensitiv informasjon til over 21 millioner personer ble stjålet, hvor informasjonen blant annet inneholdt oversikt over sikkerhetsklarering, fingeravtrykk, personalopplysninger samt oversikt over tidligere føderale ansatte (Jasper, 2017, s. 112 og CCDCOE, 2015).

Overnevnte scenario kan vi analysere gjennom å anvende spillteori. I det første trekket er det den sterke staten, i dette tilfelle Russland, som har initiativet, siden Norge først og fremst søker å opprettholde status-quo. I dette tilfelle må Russland gjøre en kost-nytte-vurdering for å kunne beslutte om man ønsker å utfordre den svakere staten gjennom destruktive cyberoperasjoner. Dersom Norge derimot har klart å etablere en russisk persepsjon om at kostnadene ved infiltrering vil bli større enn en potensiell gevinst, vil sannsynligvis Russland velge å opprettholde status-quo. I denne vurderingen må Russland også ta i betraktning hvilken støtte Norge potensielt vil få fra allierte. I henhold til relevant lovverk, vil et slikt angrep som beskrevet over, sannsynligvis falle under det som vil bli definert som et *væpnet angrep*, og således ikke utløse NATOs artikkel 5 og muligheten for å støtte seg på alliansen til å gjennomføre gjengjeldelse (Schmitt, 2017 s. 415).

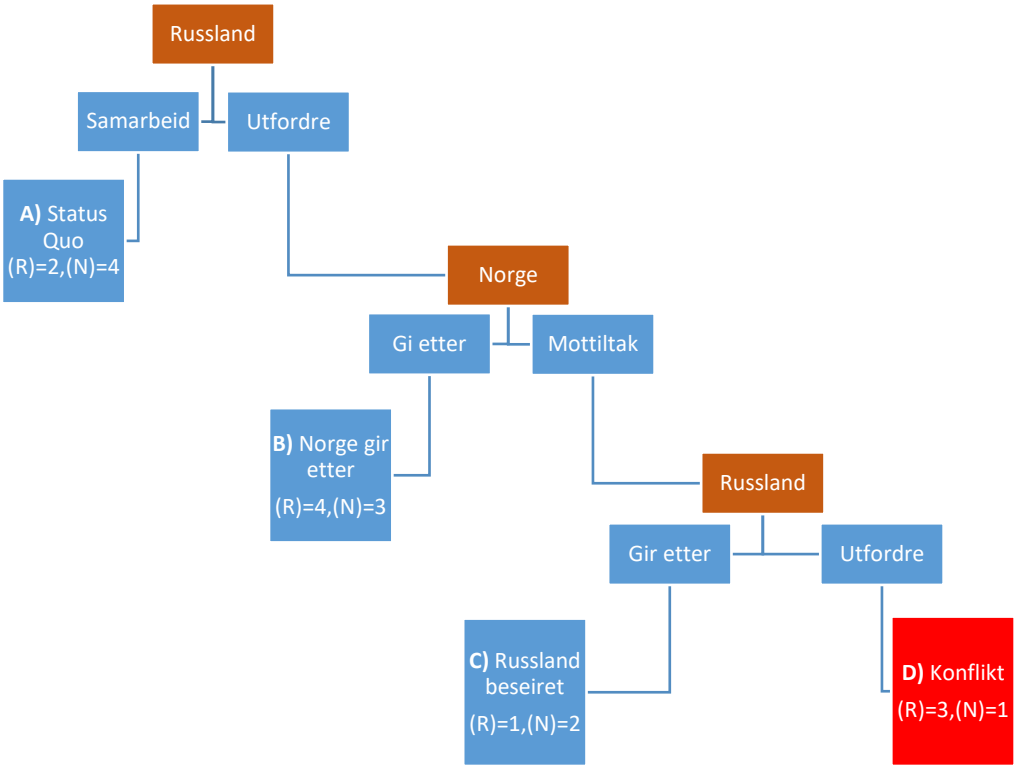
I det andre trekket må Norge gjøre et valg når det gjelder responsen på Russlands cyberoperasjon. Utfordringen i dette tilfelle, er at de norske myndighetene, eller den rammede virksomheten, i det hele tatt må være klar over det digitale angrepet. Dette vil sette søkelyset på evnen til å detektere angrep. Dette er trukket frem som et sentralt overordnet mål i Norges nasjonale strategi for digital sikkerhet (Departementene, 2019, s. 19). Tilsvarende statuerer Nederland at de har som mål å bedre og raskere oppdage digitale trusler (Ministerie van

Defensie, 2018, s. 7). Så fort angrepet er identifisert, står Norge ovenfor to valg: gi etter i form av at man begrenser seg til å gjenopprette kontroll på berørt infrastruktur, eller velge å utfordre den russiske motstanderen. Gitt at angrepet på slik infrastruktur er *under grensen* for hva Norge kunne forvente hjelp for ved allierte av NATO, er Norge begrenset til å håndtere saken bilateralt. Dette gjennom bruk av for eksempel diplomatiske eller økonomiske virkemidler. I dette tilfelle der man baserer avskrekkingsstrategien på nektelse, er det ikke et aktuelt virkemiddel å benytte seg av makt som gjengjeldelse.

De norske nasjonale retningslinjene legger ingen føringer på hvordan et slikt angrep skal bekjempes, annet enn at man skal bedre evnen til å håndtere angrepene. Norge opprettholder derfor en fordektbar holdning knyttet til en potensiell respons.

I det siste trekket er initiativet tilbake til utfordreren, Russland, i den forstand at Norge valgte å utfordre i form av diplomatiske eller økonomiske virkemidler. I dette tilfelle har Russland mulighet til å gi etter for Norges sanksjoner ved at man stopper det pågående angrepet eller de kan velge å se bort i fra dette. I og med at aktørene har mindre gjensidig avhengighet enn tidligere som følge av blant annet meget kraftige sanksjoner og dårlige diplomatiske forbindelser, er det sannsynlig at nye sanksjoner vil ha begrenset effekt.

I og med at det er fire alternativer, deles alternativene opp i en rangering som deles inn i 1-4, hvor 4 er den med høyest preferanse, og 1 er det minst ønskelige scenarioet, tilsvarende som vist i figur 2.



Figur 3. Avskrekking gjennom nektelse. R=Russland, N= Norge.

Tar vi utgangspunkt i Russland, er det nærliggende å tenke at scenarioet hvor Norge gir etter vil være mest ønskelig. Dette alternativet får derfor 4 (B). Det som åpenbart er det minst ønskelige scenarioet for Russland er å bli beseiret, ergo 1 (C). I vurderingen av hvilket scenario mellom status-quo og konflikt som er mest ønskelig for Russland, må det vurderes hvilke konsekvenser de ulike alternativene har. Dagens situasjon tilsier at det ikke er mange sanksjonerende tiltak som gjenstår ovenfor russiske myndigheter. I så måte er det nærliggende å tro at disse ikke vil påføre russiske myndigheter like store konsekvenser som «tapet» det er å opprettholde status-quo, et alternativ som jo er som lite ønskelig, all den tid man har ønsket å utfordre. Som følge av dette gis status-quo en score på 2 (A), mens konflikt får 3 (D).

For Russlands del blir derfor preferansene i dette spillet slik: A:2, B: 4, C: 1 og D: 3.

Når det gjelder Norges preferanser er det minst ønskelige utfallet en konflikt hvor man blir eksponert for en større og mer kompleks trussel. Dette alternativet får derfor 1 (D). Når det gjelder det mest ønskelige alternativet er den primære målsetningen for Norge som en småstat å opprettholde status-quo. Dette ville eventuelt betydd at man har oppnådd en tilfredsstillende

avskrekkende effekt gjennom nektelse. Når det skal vurderes hvordan Norge vurderer alternativ B og C, er det i seg selv bedre for Norge at man beseirer Russland. Alternativet er en situasjon der man må forholde seg til trusselen og heller forsøke å lære av den. På den andre siden, er det også aktuelt å se på hvilken situasjon Russland må håndtere i dag. Dersom det er lite sannsynlig at Russland vil gi etter for et økonomisk eller diplomatisk press, må man vurdere sannsynligheten for konflikt (D) opp imot det å gi etter (B). Vanligvis vil det kunne tenke seg at alternativ B ville være det nest minst foretrukne alternativet, men gitt at alternativ C er det minst ønskelige for Russland, i sammenheng med Russlands mulige persepsjon at de har lite å tape, vurderes det i denne oppgaven at alternativ B er nest best for Norges del med 3 (B), og 2 (C).

Norges preferanser blir følgende: A: 4, B: 3, C: 2 og D: 1.

Oppsummert kan man si at nektelse som avskrekkingsstrategi kun oppnås dersom den utfordrende staten vurderer det dithen at kostnadene overstiger den potensielle gevinsten. I dette tilfelle vil dette innebære at Russland må godta status-quo – et alternativ de regelmessig viser at de ikke forholder seg til. Dette i form av at man regelmessig ser cyberangrep utført av russiske aktører mot Norge, senest i januar 2023, hvor norske sykehusnettsider stod på angrepslisten (Fausko & Holmes, 2023). Som følge av dette ser vi at det vil være fordelaktig for Russland å fortsette sine operasjoner og angrep i det digitale domenet, så lenge de sørger for å ligge under det de tror er motstanderens terskler. Ikke minst er det utfordrende at angrepene ofte er godt fordekte, hvilket også gjør det vanskelig å attribuere. I den forbindelse kan man si at slike offensive cyberangrep i stor grad favoriserer den offensive parten, gitt at det er de som setter premissene, og i stor grad har mulighet til å opptre fordekte. Med andre ord har den svakere statens avskrekkingsstrategi med utgangspunkt i nektelse mislyktes, all den tid man enten bruker lang tid før man kan iverksette sanksjoner, eller at man ikke får gjort dette i det hele tatt. Dette understøttes av Aannø, som viser til at avskrekkingspotensiale innen nektelse mellom en småstat og er stormakt vil kunne innebære en eskalering og ikke oppnå målsetningen om å opprettholde status-quo (2018, s. 45-46).

Et sentralt poeng innen denne avskrekkingsstrategien er at den også potensielt kan bidra til å identifisere hvilke cyberkapasiteter og utfordringer aktørene må forholde seg til. Dette fremstår tidvis å være en underkommunisert utfordring innen attribusjonsproblemet. Der hvor mange peker på utfordringer med attribusjon i form av fordektbarhetens natur innen slike angrep, kan det på den andre siden være slik at statene faktisk ikke ønsker å attribuere eller legge frem bevis,

da dette gir et unikt innblikk i kapasiteter man ønsker å holde hemmelig. Dette kan også bidra til å sørge for at terskelen heves for når man offentlig går ut og attribuerer. Dette kan resultere i at det er langt flere cyberangrep som har blitt teknisk attribuert, men derimot ikke blitt offentlig attribuert.

For Nederlands del, fremstår denne avskrekkingsstrategien alene også utilstrekkelig. Selv om deres cyberkapasiteter i større grad og over tid har vært et satsningsområde, fremstår det uoppnåelig å skape en absolutt sikkerhetstilstand innen cyberdomenet. Selv om Nederland beskrives som en sentral aktør innen cybersikkerhet (Humanize, 2023), er de trolig ikke i nærheten av å kunne måle seg med for eksempel USA. Sommeren 2023 ser det ut til at amerikanske føderale byråer ble angrepet av russiske aktører (Lyngaas, 2023). I forlengelse av det, er det naturlig å understreke at dersom USA ikke evner å avskrekke Russland gjennom nektelse, er det lite sannsynlig at andre stater vil klare det.

Et annet eksempel går tilbake til august 2020 hvor Stortinget ble omfattet av et betydelig cyberangrep, hvor en rekke personlige opplysninger ble stjålet. Kun få måneder etter angrepet gikk den daværende regjeringen i oktober ut og attribuerte angrepet til Russland, men man valgte å ikke peke på en konkret aktør innen det russiske etterretning- og sikkerhetsmiljøet, ei heller legge frem hvilke bevis man satt på. Det er uansett verdt å merke seg at dette var første gang norske myndigheter offentlig har attribuert et land for et cyberangrep (Johansen, 2020). Som følge av utfordringene med nektelse som avskrekkingsstrategi innen cyberdomenet, spesielt når utfordreren opptrer som en sterkere stat, er det naturlig å se nærmere på en annen avskrekkingsstrategi; *straff*.

Analyse av avskrekking gjennom straff

Avskrekking gjennom straff innebærer evnen til å både kommunisere og potensielt utvise vilje til å gjengjelde angrep. Tradisjonelt har denne prinsipielle tilnærmingen vært tett knyttet til kjernevåpen og aktørenes evne til å motstå et første angrep, hvor flere akademikere har pekt på den stabiliserende effekten et balansert kjernefysisk arsenal har blant stormaktene. Dette vanskeliggjøres innen cyber, selv om prinsippene inne strategien er de samme – din motstander skal frykte konsekvensene av sine operasjoner (Nye, 2017, s. 55).

Et eksempel på hvordan dette kan gjøres, illustreres i Andy Greenberg sin bok, Sandworm, oppkalt etter den fryktede russiske hackergruppen Sandworm (GRU unit 74455). Gruppen er kjent for å blant annet slå ut ukrainsk elektrisk infrastruktur i 2015 og 2016, påvirke det

amerikanske valget i 2016, hacke det franske valget i 2017 og gjennomføre cyberangrepet NotPetya i 2017. Som følge av NotPetya skal Sandworm ha klart å tilegne seg over 10 milliarder dollar – hittil det mest kostbare cyberangrepet som er offentlig kjent. Et sentralt poeng Greenberg viser til, er at Sandworm enkelte ganger har installert ondsinnet programvare, utelukkende for å vise hva de er kapable til å gjøre (Greenberg, 2019). Dersom mottakeren oppfatter et slikt virkemiddel sterkt nok til å kunne skape totalt destruerende konsekvenser, vil dette kunne ha en avskrekkende effekt, selv innen cyber.

Den amerikanske statsviteren Richard Ned Lebow peker på at det er flere forhold som må ligge til grunn for at avskrekkingen skal ha effekt, som også er relevant for cyber; kredibilitet, kommunikasjon og repitisjon (Lebow, 1985, s. 205-211). Spesielt forholdet repetisjon kan relateres til straff som strategi. Norges respons mot et potensielt destruerende cyberangrep har gjentatte ganger blitt kommunisert. Selv om man nødvendigvis ikke har gått inn på hvordan, grunnet den bevisste tvetydigheten, kan man forutsette at Russland er klar over hvilke kapasiteter Norge besitter, samt NATOs kapasiteter i forlengelse av Norges posisjon i alliansen.

Som i analyse av avskrekking gjennom nektelse, benyttes tilsvarende scenario som utgangspunkt. Som en ekstra forutsetning for den videre analysen legges det til grunn at begge statene har en god og troverdig evne til å gjennomføre offensive cyberoperasjoner. Dette er en forutsetning som har sin bakgrunn i at jeg rent spillteknisk har tatt utgangspunkt i at Norge har valgt å følge den nederlandske strategien. Som utgangspunkt for casen i denne delen av analysen, benyttes Stuxnet-angrepet tilbake i 2010. Angrepet innebar å sabotere og ødelegge Irans nukleære infrastruktur, der flere av sentrifugene ble ødelagt. Det er ikke foretatt noen offentlig attribusjon til angrepet. Ei heller har det blitt bekreftet hvorvidt det er statlige- eller private aktører som sto bak. Der hvor ingen har definert konkret hvor den digitale grensen går for hva som er å anse som et væpna angrep innen cyberdomenet, har flere tatt utgangspunkt i at Stuxnet er noe av det nærmeste man har kommet denne grensen. Enkelte av ekspertene som bidro inn i arbeidet med Tallinn-manualen mente at angrepet på Iran er å definere som et væpnet angrep, med mindre angrepet skjedde som følge av selvforsvar. Som tidligere beskrevet i teori-kapittelet, er det sentrale spørsmålet her hvilke skader på sivile, og eventuelt hvilke materielle skader som ble påført (Schmitt, 2017, s. 342).

Casen som videre vil bli analysert, beskriver en situasjon hvor Russland har utført et vellykket cyberangrep mot norsk kritisk energiinfrastruktur på vinteren. Dette har medført materielle skader, samt store praktiske og økonomiske utfordringer, konkret relatert til manglende

energiforsyning til Europa. Angrepet er teknisk attribuert til en russisk statlig aktør, men Norge har enda ikke gått ut offentlig med dette. Det forutsettes at angrepet er i grenseland mellom hva Norge vil måtte håndtere alene, eller hvor man kan søke støtte fra allierte i NATO.

For å analysere dette, skal vi videre benytte tilsvarende spill som i den forrige analysen. I det første trekket har Russland allerede valgt at de ikke ønsker å opprettholde status-quo, da cyberangrepet allerede er et faktum. Det er mulig at en slik vurdering er begrunnet med cyberangrepets potensielle konsekvenser sett i lys av muligheten til å utføre dette fordekt. Norge står nå ved et veiskille hvor man må foreta et strategisk valg. Angrepet har skjedd, konsekvensene er klare, og den tekniske attribusjonen er utført. Norge har i analysen tre ulike valg. De kan gi etter i den hensikt å reetablere kontroll på egen infrastruktur, slik at man er i stand til å håndtere tilsvarende angrep senere på en bedre måte. I lys av Norges cyberstrategi fremstår dette som det mest sannsynlige scenarioet. Dette vil samtidig kunne bidra til å svekke egen troverdighet rundt valgt avskrekkingsstrategi, som igjen kan bidra til økt eksponering for tilsvarende angrep. Derimot har Norge i dette tenkte scenarioet betydelige offensive destruktive kapasiteter som de kan benytte seg av.

Det andre valget, retorsjon, innebærer at man gjør de interne tiltakene som nevnt i første alternativ, i tillegg velger man å komme med en form for sanksjon. Norge vil i dette tilfelle offentlig og politisk attribuere angrepet til Russland, og iverksette sanksjonerende tiltak, som utvisning av diplomater, samt relevante økonomiske sanksjoner. Motparten vil kunne tolke Norges respons på ulike måter, i den forstand at man viser handlekraft, men samtidig kanskje ikke nok til å opprettholde troverdig avskrekking. I det tredje tilfelle iverksetter Norge mottiltak i form av offensive operasjoner. Mottiltakene skal som tidligere nevnt være proporsjonale. I valget mellom en kinetisk eller digital operasjon, ville valget mest sannsynligvis falt ned på digital. Den offensive cyberoperasjonen vil sannsynligvis rette seg mot tilsvarende russisk infrastruktur i den hensikt å lamme eller ødelegge, alternativt angripe den konkrete cyberoperasjonen de er utsatt for, for å potensielt begrense ytterligere skader. Valget om å utføre mottiltak, må vurderes i lys av et mulig svar som kan bidra til å eskalere situasjonen ytterligere. Dersom Norges respons innebærer en uforholdsmessig gjengjeldelse, kan dette av russiske myndigheter oppfattes som en eskalering og igjen invitere til ytterligere respons (Morgen, 2012, s. 102).

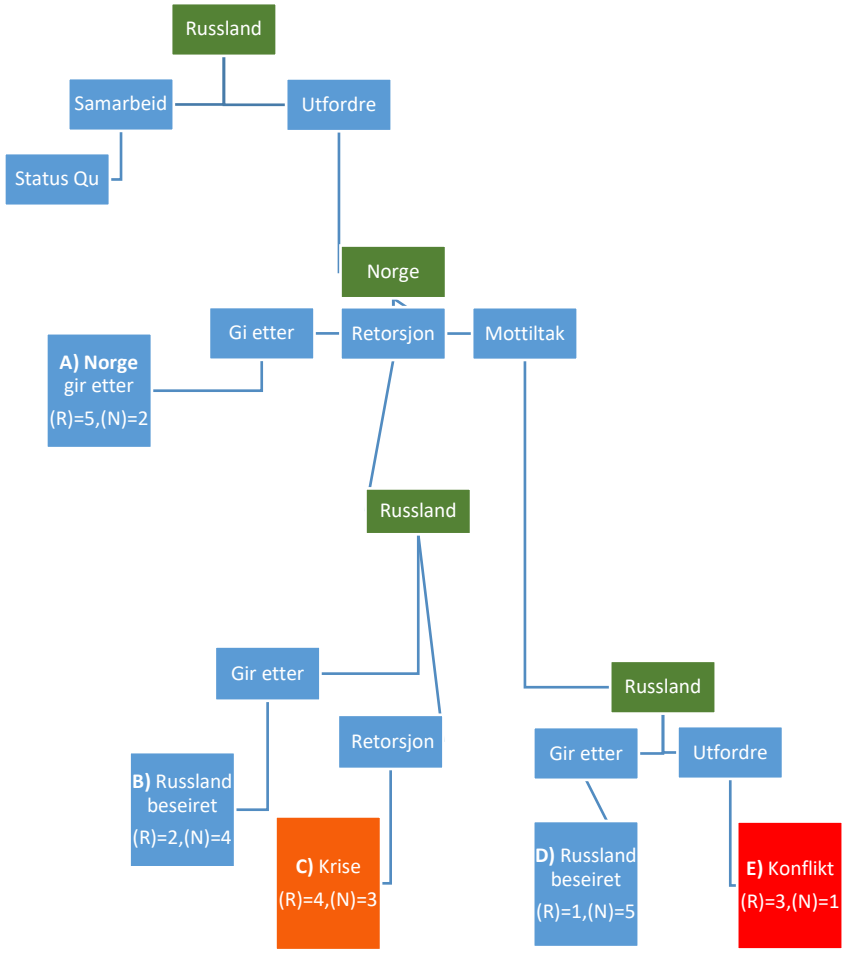
I det tredje og siste trekket, risikerer Russland å stå ovenfor to alternativer, enten at Norge har iverksatt sanksjonerende tiltak i form av brudd på diplomatiske relasjoner og økonomiske

sanksjoner, eller i form av en offensiv cyberoperasjon. I det første scenarioet har Russland mulighet for å gi etter for sanksjonene, ved at disse godtas uten at det innebærer ytterligere russiske responser. Dersom de russiske myndighetene vurderer det slik at resultatet fra deres egen operasjon veier tyngre enn de potensielle sanksjonene, kan et slikt utfall foretrekkes, selv om det innebærer å gi etter. Derimot kan dette ha implikasjoner for fremtidige operasjoner og annen etterretningsvirksomhet, slik at de potensielt må endre sin *modus operandi* – deres foretrukne handlemåte. I det andre tilfellet gjengjelder Russland sanksjonene, noe man ofte har sett tidligere eksempler på, der Russland utviser det samme antallet diplomater som de selv fikk utvist. Gjengjeldelse kan føre til en diplomatisk krise, men det er usikkert hvilken av partene som vil lide mest under dette.

Hvis vi ser nærmere på det andre alternativet, har Norge iverksatt en motoffensiv i form av en offensiv og destruktiv cyberoperasjon rettet mot russisk infrastruktur. En sannsynlig handlemåte vil være at Russland fordømmer operasjonen og ønsker å kalle inn FNs sikkerhetsråd. Der vil de kreve at det blir lagt frem tekniske bevis, noe de hverken har krav på, eller sannsynligvis er noe de vil få. Russland vil deretter kunne velge mellom to ulike alternativer. De kan enten gi seg, i den forstand at de ikke fortsetter egne operasjoner hvor de godtar operasjonen de blir utsatt for, men forsøker å begrense eget tap. Dette kan være tilfelle der de har oppnådd det de ønsket, samtidig som at de er i stand til å håndtere den trusselen de har blitt utsatt for.

På den andre siden, kan dette rent sikkerhetspolitisk fremstå som en svakhet i Kreml, hvor de har gitt etter for Vestens angrep. Et interessant spørsmål i denne sammenheng, vil derfor være om det kan være fordelaktig for Norge å gjennomføre klandestin-operasjoner eller operasjoner hvor kun russiske myndigheter får informasjon, slik at man gir Russland en mulighet til å ikke miste egen troverdighet blant befolkningen. Det siste alternativet vil være en fullskala cyberkrig, som kan skape uante konsekvenser all den tid man, per nå, ikke er fullstendig klar over egne sårbarheter. En slik situasjon vil kunne medføre en eskalering som kan føre til kinetiske virkemidler. Hvis responsen blir oppfattet som uproporsjonal, vil dette med stor sannsynlighet føre til en eskalering. Dette er spesielt risikabelt dersom det ikke foreligger en garanti om at en alliansepartner som for eksempel NATO vil kunne involvere seg (Aannø, 2020, s. 53-54). Uten videre vurdering av konsekvenser, vil derimot et slikt alternativ understøtte begge parters avskrekkingsstrategier, og i så måte gjøre disse mer troverdige i en potensiell senere konflikt.

Under er den overnevnte analysen satt inn som et spill. Det er totalt fem utfall i spillet, hvor disse rangeres fra 1-5, hvor 5 er det mest foretrukne alternativet. Spillet er laget for å illustrere alternativet som gir Norge mest ønsket utfall, men samtidig også vise til hvordan Russland kan oppfatte dette. Spillet kan derfor bidra til å illustrere at Norge burde søke å gå for et annet alternativ enn det beste, for å unngå potensielt uønskede videre konsekvenser.



Figur 4. Avskrekking gjennom straff. R=Russland, N= Norge

Spillet tar utgangspunkt i at Russland har valgt å ikke samarbeide, noe som ville opprettholdt dagens status-quo. Vi kan forutsette at Norge har diskutert angrepet i rammen av NATO, men NATO har valgt å ikke utløse artikkel 5 av flere årsaker. For det første, krever dette enstemmighet internt i alliansen, noe som tidligere har vist seg å kunne være utfordrende, gitt at artikkel 5 kun har blitt benyttet én gang tidligere. Derfor kan det være en rekke av NATOs medlemsland som vil vegre seg for potensielt å gå inn i en større konflikt med Russland, som for eksempel Russlands naboland og tidligere sovjetstater. I tillegg er det NATO-land som fortsatt har tette bånd til Russland, som for eksempel Ungarn og Tyrkia (Hem, 2023). Det å skulle samle NATO bak en offensiv mot Russland fremstår derfor utfordrende og lite

sannsynlig. Derimot har NATOs medlemsland selvstendig mulighet til å støtte Norge, da dette er hjemlet i FN-paktens artikkel 51.

Når det gjelder de konkrete alternativene, er disse vanskeligere å rangere i denne analysen, enn i den forrige, all den tid cyberangrepet nå har skjedd. Dette innebærer at avskrekkingsstrategien allerede har mislyktes. Det er uansett nærliggende å tenke, og et sentralt premiss, at en større konflikt er det minst ønskelige scenarioet, derfor får dette alternativ E=1 for Norges del. Ser vi nærmere på det mest ønskelige scenarioet, er det naturlig å tenke at alternativ B eller D er mest ønskelig. Dette innebærer at Russland beseires, enten i form av sanksjoner, eller i form av en større motoffensiv.

Selv om disse alternativene kan se like ut, er det en distinkt forskjell på dem. Alternativet der Russland beseires som følge av en motoffensiv (D), vil innebære at man i større grad opprettholder egen troverdighet rundt avskrekkingsstrategi, enn dersom man velger å svare ut angrepet på mildere måter gjennom alternativ B. I og med at troverdighet og motstanderens persepsjon om potensiell trussel er såpass viktig, er det naturlig at alternativ E favoriseres over C. Dette er også i tråd med Nederlands eksisterende strategi da den peker på at MIVD selv kan aksjonere for å bekjempe akutte digitale trusler (Ministerie van Defensie, 2018, s. 7). Rangeringen på disse to vil derfor bli slik: D=5 og B=4. Når det gjelder alternativ A som medfører at man ikke gjør stort annet enn å tette avslørte sikkerhetssvakheter, syns dette å være et dårlig alternativ. En slik respons vil medføre at troverdigheten rundt egen avskrekkingsstrategi svekkes sterkt, og vil kunne medføre nye angrep. Dette alternativet får dermed 2. Dette fører til at alternativ C som innebærer en krise, får en score på 3.

Oppsummert blir utfallet for Norge følgende: A: 2, B: 4, C: 3, D: 5 og E: 1

Ser vi på Russlands alternativer, starter vi med det mest foretrukne scenarioet. Det mest nærliggende å tenke seg, er at Russland vil foretrekke alternativ A. Dette vil innebære at deres cyberangrep har lyktes med svært få konsekvenser. Alternativ A får dermed score 5. For Russland er det essensielt ikke å gå på et nederlag. Dette gjør de i både alternativ B og D, hvor henholdsvis B innebærer at Russland velger å avslutte operasjonen og deres aggresjon som en følge av sanksjoner, mens alternativ D innebærer som sagt at de blir beseiret som følge av en motoffensiv. Siden sistnevnte vil bety at egen troverdighet svekkes, er det naturlig å tenke at dette alternativet det minst foretrukne. Alternativet får dermed 1, mens C får 2. Dette gjør at vi kun sitter igjen med C og E. På generelt grunnlag kan man forutsette at russiske myndigheter

ikke ønsker en større konflikt. Litt avhengig av hvor langt frem i tid dette aktuelle scenarioet utspiller seg, er det sannsynlig at Russland trenger betydelig tid på å rekondisjonere seg etter krigen i Ukraina. Dette understreker ytterligere at militærmakten trolig vil unngå større konflikter, selv om det kan være viktig for egen troverdighet og befolkningens støtte at deres håndtering ikke blir oppfattet som en svakhet i forhold til Norges. Som følge av dette får alternativ E=3. Dermed blir alternativ C 4.

Oppsummert blir utfallet for Russland følgende: A: 5, B: 2, C: 4, D: 1 og E: 3

Satt inn i et skjema blir fordelingen følgende:

	A	B	C	D	E
Russland	5	2	4	1	3
Norge	2	4	3	5	1
Totalt	7	6	7	6	4

Som man ser, er alternativ E med en større konflikt, totalt sett, det minst foretrukne alternativet. I motsatt ende har både alternativ A og C fått samme poengsum, og står frem som, totalt sett, de to beste alternativene. Det kan argumenteres for at alternativ C synes å være mest foretrukket av de to, siden dette scenarioet scorer relativt godt for begge spillerne. Norges score på alternativ A tilsier at denne løsningen ikke er ønskelig. Spørsmålet da blir i så fall hvorfor Norge allikevel skal unngå å svare?

Når vi snakker om betydelige sikkerhetspolitisk beslutninger, er det nærliggende å tenke at Norges respons ikke utelukkende baserer seg på en tolkning av eget handlingsalternativ. Det er derimot naturlig at man også ser på hvordan Russland som motstander potensielt vil respondere på ulike mottiltak. Derfor, slik man ser i eksempelet over, vil Norge i enkelte tilfeller måtte velge et mindre ønsket mottiltak for å unngå en uønsket respons. Selv om alternativ D fremstår som det beste valget for Norge, er det lite sannsynlig at Russland vil forholde seg nøytralt til dette.

Forutsetningen om at NATOs Artikkel 5 ikke er utløst, er lagt til grunn i analysen uten at dette er begrunnet utdypende. Selv om denne oppgaven i seg selv ikke har fokus på NATO, er det naturlig å rette noe søkelys på dette allikevel, fordi det trolig kan gi svar på hvorfor mange nasjoner kan oppleve seg relativt alene i møte med russiske cyberangrep. Hvordan kan det ha

seg at et cyberangrep utført av russiske statlige aktører, som i henhold til alle gitte offentlige uttalelser ikke bare møter, men går over de røde linjene innen cyberkrigføring, sannsynligvis ikke medfører at NATOs Artikkel 5 utløses?

For det første er NATO er en defensiv allianse. Hadde NATO ønsket en konflikt, ville trolig NATO eksempelvis vært involvert i Ukraina-krigen på en annen måte, selv om Ukraina ikke er medlem av NATO. Som følge av dette vil NATO være svært tilbakeholde når det gjelder å forplikte seg til konflikter. Dersom man ikke begrenser seg, kan dette medføre en eskalerende voldsspiral som kulminerer i en væpnet konflikt. Ikke minst har Russland i det siste fremstått som en uforutsigbar atommakt med en rekke uttalelser om utplassering og bruk av sine taktiske missiler (Hem, 2023). Det skal dermed svært mye til for at NATO skulle gå inn i en direkte konflikt med Russland.

For det andre vil utløsing av NATOs artikkel 5 være et politisk spørsmål (NATO / Atlanterhavspakten), snarere enn et operasjonelt eller strategisk spørsmål. Dette gir en helt annen dynamikk dersom man kaller inn NATO til å vurdere hvorvidt en hendelse skal utløse artikkelen om kollektivt forsvar – en avgjørelse som krever enstemmighet. Gitt den sentrale politiske dimensjonen, vil det trolig være flere land som vil vegre seg for å binde seg opp i en slik felles beslutning. Spesielt er det verdt å peke på enkelte land i NATO som fortsatt har eksisterende knytninger til russiske myndigheter utover de vanlige etablerte diplomatiske forbindelsene (Hem, 2023). Dersom disse landene også har sterke økonomiske forbindelser og avhengigheter til Russland, som vil kunne før til sanksjoner fra russisk side, vil dette bidra til deres avmålthet knyttet til artikkel 5.

For det tredje ser det ut som at det er intern uenighet i NATO om hva som kreves for at et cyberangrep skal kunne utløse artikkel 5. For utenforstående med innsyn i kun offentlig dokumentasjon, synes det å være uenighet knyttet til hva som kreves av bevis, og ikke minst hvorvidt dette må presenteres i attribusjonsprosessen. Dersom det ikke er klar enighet rundt de essensielle vilkårene, vil man heller ikke oppnå enighet. NUPI-forsker Karsten Friis har selv sagt at et cyberangrep alene sannsynligvis ikke vil utløse artikkel 5. Dette er ikke i tråd med det NATO, ei heller flere medlemsland har uttrykt de siste årene (Mauno, 2022).

Et konkret eksempel er Norges innspill til FN om hvordan Folkeretten gjelder innen cyber. Der uttrykte Norge følgende:

> *"A cyber operation that severely damages or disables a State's critical infrastructure or functions may furthermore be considered as amounting to an armed attack under international law. Depending on its scale and effect, this may include a cyber operation that causes an aircraft crash"* (United Nations, 2021, s. 70).

Det er interessant at Norge tar et slikt offisielt standpunkt. Dette vil åpenbart legge føringer for fremtidige politiske avgjørelser dersom det skulle dukke opp relevante problemstillinger. Hvis vi sammenlikner med eksempler på kinetiske angrep som NATO-land har blitt utsatt for etter 11. september 2001, uten at artikkel 5 har blitt utløst, kan man legge til grunn at det skal svært mye til for at artikkel 5 anvendes som følge av et cyberangrep. I så måte kan man forstå uttalelsene til Friis.

En sentral svakhet innen NATOs innretning mot cyberangrep synes å være deres operasjonelle planverk og deres strategi, som burde vært mer forutsigbar for de allierte. I forbindelse med NATO-toppmøtet i Brussel i 2021, ble følgende uttalt i møtets offentlige kommunikasjonsnotat: *«We reaffirm that a decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis»* (NATO, 2021). Dette er naturlig nok et fornuftig utgangspunkt på artikkel 5, gitt at man har lite å sammenlikne med.

Det eneste eksempelet, som det per i dag er naturlig å trekke paralleller til, er angrepet på Estland i 2007. Angrepet med dets omfang, har av NATO blitt definert som et type cyberangrep som kan lede til bruk av artikkel 5 (Pruckovà, 2022). For meg fremstår dette som noe uklart av flere årsaker. Angrepet er ikke attribuert til en konkret stat. Men beskyldninger mot russiske aktører er blitt fremsatt. I tillegg, og kanskje det mest sentrale argumentet, er at angrepet kom i form av et DDoS-angrep, altså et angrep som i hovedsak innebærer å lamme. Angrepet medførte minimalt med fysisk skade, og i så måte oppfylte ikke cyberangrepet vilkårene som må ligge til grunn for at angrepet skal være å anse som et væpnet angrepet (Cyber Law Toolkit B). Dette understøttes av Tallinn-manualen hvor det vises til at man ikke kan vise til at angrepet ble utført på vegne av en stat, ei heller nådde den gitte grensen (Schmitt, 2017, s. 376, 382 og 387). Med andre ord synes det merkelig at angrepet mot Estland i 2007 brukes som et eksempel av NATO, så lenge angrepet i dag ikke ville nådd grensen for et væpnet angrep (Pruckovà, 2022).

Tar vi utgangspunkt i analysen ovenfor, virker det som om potensielle cyberangrep vil være svært utfordrende å håndtere for småstater som Norge så vel som Nederland. Det ser ut til at det er et betydelig handlingsrom for trusselaktører som Russland å gjennomføre cyberangrep,

både mot småstater, og NATO som helhet. Dette innebærer at stater som Norge må sørge for å skape egen motstandsdyktighet for egne informasjonssystemer, slik at man sørger for at potensielle konsekvenser ved et cyberangrep begrenses så langt det lar seg gjøre. Dette bringer oss over til neste avskrekkingsstrategi, aktivt cyberforsvar.

Analyse av avskrekking gjennom aktivt cyberforsvar

Jasper argumenterer for at store deler av et lands kritiske infrastruktur, på en eller annen måte understøtter dets militære kapasiteter. Derfor vil et angrep på slik infrastruktur kunne være med å bidra til å forstyrre og ødelegge militære kapasiteter som er ment til å forsvare staten. For å illustrere dette bruker han et hypotetisk angrep som en «cyber Pearl Harbour» (Jasper, 2017, s. 4-5). Mike Rogers, medlem av representantenes hus siden 2003, uttalte følgende i 2014: *«the threat of a catastrophic and damaging cyberattack in the United States critical infrastructure like our power or financial networks is actually becoming less hypothetical every day"* (sitert i Jasper, 2017, s. 5). Et slikt scenario er like sannsynlig og relevant utenfor USA. Selv om angrepet på North Stream 2 enda ikke offentlig er attribuert til en stat, viser dette uansett en kapasitet og intensjon til å ramme europeisk kritisk infrastruktur. Nå er det på det rene at det ble benyttet kinetiske virkemidler til å oppnå eksplosjonen, men tilsvarende effekt kunne trolig blitt oppnådd som et digitalt angrep. Ikke minst hvis systemoperatørens sikkerhetsmekanismer og overvåkingssystemer ikke er i stand til å detektere angrepet før det får gjort stor nok skade.

Sikkerhetseksperter ser ut til å være enige om at den digitale trusselen mot kritisk infrastruktur er reell. Det er svært utfordrende å lage IT-systemer som ikke inneholder sårbarheter som kan utnyttes (Strand, 2022, s. 45). Det kan se ut som at staters fokus på å skape robuste informasjonssystemer for å senke risikoen for slike angrep, er underprioritert. Dette understøttes av NUPIs rapport fra 2018, hvor en av deres konklusjoner var at sikkerhetstiltakene som er iverksatt av offentlige og private aktører innen petroleumssektorene, ikke er i samsvar med den cybertrusselen man blir utsatt for (Muller, Gjesvik og Friis, 2018, s. 9).

Grunntanken bak de tradisjonelle avskrekkingsstrategiene, nektelse og straff, stammer fra motstanderens overbevisning om at trusselen om hevn eksisterer – kost/nytte vurderingen. En slik tilnærming mener Jasper at ikke er mulig innen cyber. Den tradisjonelle nukleære avskrekkingsstrategien der man var klar over skadepotensiale i et mulig motangrep, er ikke mulig innen cyber, der hemmelighold om kapasiteter er essensielt for å opprettholde deres effektivitet. Som følge av dette mener mange derfor at cyberavskrekking er uoppnåelig. Jasper

derimot, mener allikevel at det er mulig å komme dit. For å illustrere dette har han lansert en supplerende strategi, avskrekking gjennom *aktivt cyberforsvar* (Jasper, 2017).

Strategien om aktivt cyberforsvar innebærer en kombinasjon av sanntids-deteksjon, analyse og avbøtende tiltak mot egen infrastruktur i kombinasjon med bruk av offensive cyberkapasiteter. Tanken er at man skal kombinere tiltak som skaper motstandsdyktighet for å kunne motstå et angrep, samtidig som man har skreddersydde destruktive kapasiteter for å straffe angriperen. Dette er i tråd med Nederlands strategi, hvor de søker å styrke egen motstandsdyktighet samtidig som de spisser egne offensive kapasiteter (Jasper, 2017, s. 13-20 og 165; Ministerie van Defensie, 2018).

I 2015 advarte daværende sjef for det amerikanske etterretningsbyrået NSA, at det handler ikke om hvorvidt man kommer til å bli angrepet av cyberangrep. Det er snarere et spørsmål om når (Jasper, 2017, s. 165-170). Dette er like relevant i dag, illustrert av NSM i sin nylige utgitte rapport, Nasjonalt digitalt risikobilde 2023. Der peker de også på at cyberangrep er blitt hverdagskost, og at det et nå et spørsmål om når – ikke hvis (NSM, 2023, s. 10). Da dette fremstår som ny normaltilstand, viser Jasper til at man må sørge for at tiden mellom selve kompromitteringen frem til det faktiske tidspunktet man oppdager trusselen på, må minimeres. Det er derfor faretruende at oppdagelsestiden i gjennomsnitt ligger på rundt 146 dager (2017, s. 165-170). Med andre ord kan en trusselaktør i underkant av et halvt år, operere i en virksomhets nettverk uten å bli oppdaget.

Et eksempel som dukket opp nå underveis i skriveprosessen, er dataangrepet mot Departementenes sikkerhets- og serviceorganisasjon (DSS), som ble offentlig kjent 24. juli 2023. I etterkant av dette, kom det frem at hackere har hatt tilgang til en IKT-plattform brukt i regjeringsapparatet i minst to måneder (Støyva & Wikan, 2023). Den aktive cyberforsvarsstrategien har som formål å øke oppdagelsesrisikoen ved å benytte synkroniserte sanntids-kapasiteter, både for å oppdage, men også for å analysere og arbeide med sårbarheter, samt komme med en fornuftig respons. Jo tidligere man er ute med å identifisere sårbarheter, jo mer kan dette bidra positivt for attribusjonsproblematikken all den tid slikt kan ta noe tid (Jasper, 2017, s. 165-170).

På denne måten har man gjennom strategisk motstandskraft anledning til å nekte motstanderen fordeler og gevinster, samt pålegge kostnader gjennom skreddersydde forstyrrende mottiltak. Det strategiske alternativet aktivt cyberforsvar oppfyller derfor, ifølge Jasper, de tre nødvendige betingelsene for å oppnå avskrekking. Evnen til å levere et passende mottiltak, kommunikasjon

for å signalere intensjoner, som igjen vil bidra til å skape en trusselpersepsjon hos motstanderen, samt en kapasitet og troverdighet til å ikke tolerere ondsinnet aktivitet (2017, s. 166). Selv om Jasper sier at offensive kapasiteter er et sentralt virkemiddel for å oppnå avskrekking, er det andre akademikere som ikke er like overbevist. Max Smeets, peker på at det ser ut som at mange stater sliter med å utløse sitt fulle cyberpotensial, spesielt innen offensive cyberoperasjoner. Dette illustrerer han ved å peke på at selv om mange stater har beskrevne cyberkapasiteter, er det kun et fåtall som benytter seg av disse. Noe av årsaken til dette, er ifølge Smeets at statene er underlagt tunge strategiske, juridiske og operasjonelle begrensinger – den sparsommelige logikken (2022, s. 4, 32 og 40-49).

I Norge er det Etterretningstjenesten som har mandat til å utføre offensive cyberoperasjoner. Selv om området er omfattet av vesentlig hemmelighold, har Etterretningstjenesten, i rekrutteringsøyemed, etablert et talentprogram for cyberoperasjoner hvor de søker etter nye ansatte. I dette programmet lærer man, ifølge Etterretningstjenesten, blant annet å gjennomføre cyberoperasjoner mot nøye utvalgte mål, finne sårbarheter, programmering av trojanere, etablere infrastruktur for kommunikasjon og analyse av nettverkstrafikk (Etterretningstjenesten, 2023). I forlengelse av dette, er det naturlig å anta at Etterretningstjenesten både har kapasitet til å finne sårbarheter hos potensielle motstandere, skaffe aksess, samt innhente informasjon, og benytte seg av destruktive virkemidler. Spørsmålet i så måte er hvordan man kan benytte seg av en slik kapasitet, i lys av Jaspers strategi.

Et eksempel er New York Times, som i 2019 beskrev hvordan USA utførte offensive cyberangrep for å ta ned nettverk og datasystemer i Iran i den hensikt å hindre sabotasje mot skipstrafikk. En annen offensiv cyberoperasjon USA skal ha utført, skal ha hatt som formål å ta ut infrastrukturen som styrer Irans missil-kapasiteter (Barnes & Gibbons-Neff, 2019). Selv om Iran i dette tilfelle nektet for at de hadde blitt utsatt for et slikt angrep, er det naturlig å tenke seg at Norges kapasiteter kan benyttes i tilsvarende grad – å bryte seg inn i motstanderens datasystemer i den hensikt å lamme og begrense egne kostnader. Nederland har allerede vist at de besitter slike kapasiteter. Blant annet klarte nederlandske etterretningstjenester å bryte seg inn i datasystemene til den meget kjente russiske hackergruppen «Cozy Bear» (Smeets, 2022, s. 66).

I den videre analysen tas det utgangspunkt i et scenario hvor Norge har blitt utsatt for et cyberangrep, som har slått ut kritisk infrastruktur knyttet til norsk gass og petroleums-

virksomhet. Angrepet har medført at Equinors prosessanlegg på Kårstø, som spiller en sentral rolle innen transport og behandling av gass fra viktige området på norsk kontinentalsokkel, har måttet stenge ned for at infrastruktur eller råvarer ikke skal bli ødelagt (Equinor, 2023).

I det første trekket har allerede Russland definert at det er ønskelig å utfordre Norge. Russland kunne i stedet valgt å fortsette samarbeidet, noe som ikke ville medført endringer i status quo. Dette resulterer i at Norge står ovenfor, i dette scenarioet, tre ulike valg. Man kan for det første gi etter. Dette innebærer at man velger å ikke møte angrepet på noe annen måte enn at man iverksetter tiltak for å begrense skadepotensiale og sørge for at man så raskt som mulig kommer tilbake i normalt drift. Jasper argumenterer for at dette kan resultere i svekket troverdighet rundt valgt avskrekkingsstrategi (2017). Dette kan igjen medføre en økt risiko for flere tilsvarende angrep. Det andre valget innebærer at man offentlig går ut og attribuerer angrepet til Russland. Formålet med dette kan være mange. All den tid man med stor sannsynlighet søker å unngå teknisk attribusjon, vil man trolig møte sterke motreaksjoner fra russiske myndigheter rundt manglende bevis. Attribusjonen kan derimot være et ledd i å gjengjelde angrepet for eksempel med sanksjonerende tiltak. Historien har derimot vist at slike sanksjonerende tiltak kan ha begrenset effekt. Derfor kan det være naturlig å vurdere mottiltak som en mulig respons. Det er uansett naturlig å peke på at vi i et slikt scenario først må ha gjennomført attribusjon.

I forlengelse av dette, er det interessant å se tilbake til Russlands offisielle uttalelse (United Nations, 2021, s. 80) som skaper intrikate utfordringer, da statene har ulikt syn på hva som kreves bevist. Russlands syn er naturlig nok ment for å ivareta egne hensyn, men samtidig utfordrer dette vestlige handlemåter. Uten tekniske bevis knyttet til russiske beskyldninger, kommer sannsynligvis ikke Russland til å ta ansvar og erkjenne tilknytning til egne operasjoner.

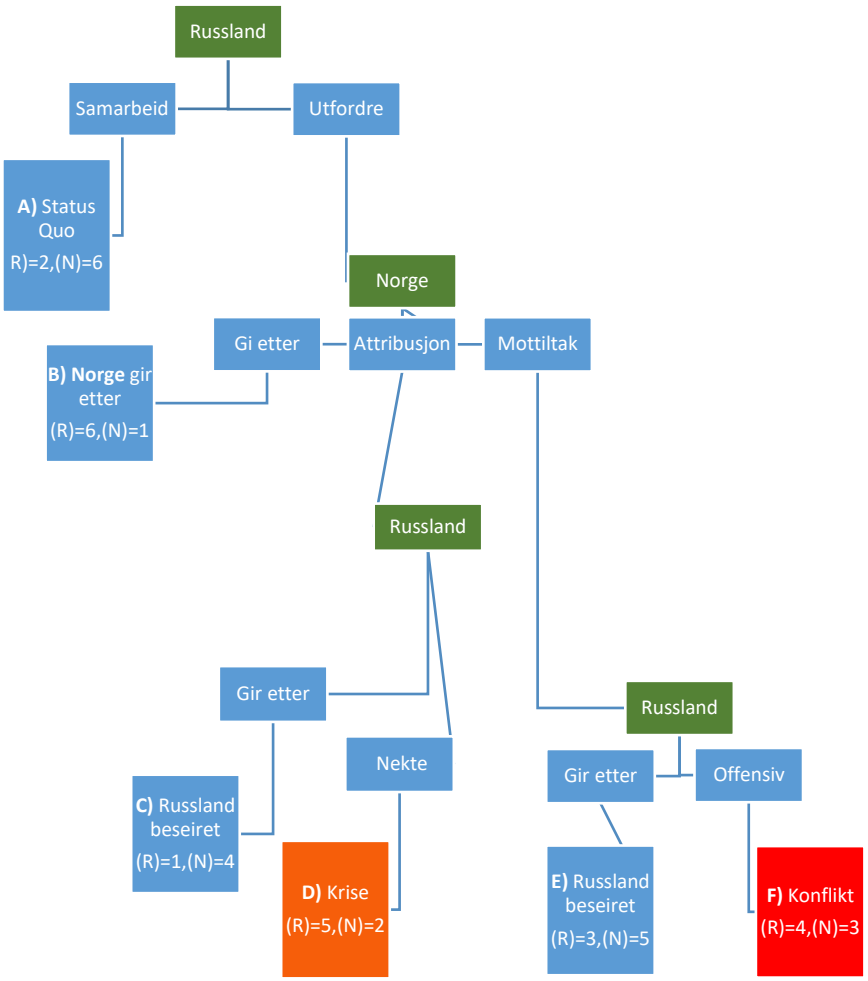
Det tredje alternativet Norge kan velge, er å iverksette offensive cyberoperasjoner mot motstanderens aktør. I dette tilfelle er det naturlig å se på CNA-operasjonen i den hensikt å redusere og hindre aktørens evne til fortsatt å benytte cyberangrepet til egne operasjoner. Dette kan være i form av å skaffe seg aksess til aktørens digitale infrastruktur, i den hensikt å stoppe, ødelegge og fjerne kompromittert informasjon, eller å lamme aktørens evne i den hensikt å kunne gjenetablere kontroll over egne systemer. En slik operasjon gjøres i stor grad fordekt, men norske myndigheter kan legge igjen spor i egne operasjoner for at motstanderens aktør skal forstå at mottiltaket kommer fra Norge. Sistnevnte kan muligens også ha en fremtidig preventiv effekt i den forstand at man statuerer en kapasitet og en intensjon om hevnangrep der dette er nødvendig.

Gitt at Norge, i scenarioet, kan velge mellom å utføre enten attribuerende, eller offensive tiltak, vil det tredje trekket innebære to alternativer, avhengig av norsk respons. I det første har norske myndigheter valgt å attribuere angrepet. Russland kan i dette tilfellet velge å gi etter for de tiltak som er iverksatt, og avslutte cyberangrepet. Dette vil kunne medføre ulike problemstillinger, blant annet i Kreml, spesielt knyttet til i hvor stor grad den russiske staten oppfattes som «svak» hvis man gir etter for press. Et slikt alternativ fremstår lite sannsynlig. På den andre siden er det naturlig, og sannsynlig, at Russland vil søke å nekte for sin involvering i saken. Dette spesielt sett i lys av deres uttalte utgangspunkt når det er snakk om å attribuere cyberangrep – en slik anklagelse skal understøttes av tekniske bevis (United Nations, 2021, s. 80). Noe slikt bevis vil derimot neppe legges frem, til det er konsekvensene for store. Russiske myndigheter vil trolig fordømme det de vil peke på er en alvorlig og uakseptabel provokasjon, lik det man så etter at norske myndigheter beskyldte Russland for dataangrepet mot Stortinget i 2020 (Fausko & Holmes, 2020). Resultatet av en slik respons fra russisk side, vil trolig føre relasjonen inn i en enda dypere sikkerhetspolitisk- og diplomatisk krise.

I den andre alternative responsen, har Norge valgt å iverksette en offensiv og destruktiv cyberoperasjon, CNA. Dette i den hensikt å lamme motstanderens evne til i å skaffe seg et handlingsrom til å iverksette avbøtende tiltak. Cyberoperasjonen har også til hensikt å svekke motstanderens evne til å gjennomføre tilsvarende operasjoner, slik at det må forventes at operasjonen vil ha en destruerende effekt på motstanderens infrastruktur. Russland kan i dette tilfellet svare på to ulike måter, de kan gi etter og avslutte angrepet, eller de kan fortsette sin operasjon, eventuelt eskalere.

Hvis vi tar for oss det første handlingsalternativet, overgivelse, vil dette på samme måte som overgivelse etter attribusjonsalternativet, kunne innebære negative innenrikspolitiske konsekvenser. Dog, en sentral distinksjon i dette alternativet, er at Norges respons med stor sannsynlighet vil være fordekt. Russland står dermed i en posisjon der de fortsatt kan opprettholde et eget narrativ som ikke innebærer at deres posisjon svekkes, selv om dette i realiteten innebærer at de gir etter for norsk press. Det andre handlingsalternativet er at Russland velger å intensivere sin egen operasjon, i forsøk på å hindre den norske motresponsen i å lykkes. Dette vil kunne ha en eskalerende effekt, som til slutt kan innebære en «tit-for-tat» utveksling av ulike angrep og operasjoner (Hovi, 2020, s. 94-95). Dette er et resultat som mange forskere tidligere har pekt på som konsekvens i cyberkonflikter hvor attribusjon og manglende strategiske gevinster fremstår som utfordrende (Whyte, 2019).

Videre følger den overnevnte analysen satt inn i et spill. Det er totalt seks utfall i spillet, hvor disse rangeres fra 1-6, hvor 6 er det mest foretrukne alternativet. Spillet er laget for å illustrere alternativet som gir Norge potensielt størst utbytte, men samtidig se Norges handlingsalternativer i relasjon til sannsynlig russisk respons.



Figur 5. Avskrekking gjennom aktivt cyberforsvar. R= Russland, N= Norge.

Spillet innledes med at russerne har valgt å ikke samarbeide, men iverksatt cyberangrep. Alternativt ville russerne opprettholdt status quo, en lite ønskelig situasjon. Det betyr ikke nødvendigvis at status-quo er det minst ønskelige alternativet. Alternativ C, hvor Russland har overgitt seg som følge av en norsk attribusjon, vil anses som et verre tap. Det vil bryte med deres standardiserte respons om fordømmelse av beskyldningene og krav om bevis. En slik endring i respons fra russisk side, vil trolig kunne påføre russiske myndigheter større problemer, enn om de skulle opprettholdt status-quo. Alternativ C får dermed den laveste scoren, 1. Det er ganske enkelt å peke på hvilken norsk respons som ville vært den mest foretrukne for russerne. Alternativ B som resulterer i norsk overgivelse, ville trolig blitt oppfattet som en stor seier, med

god måloppnåelse, der sannsynligheten for motreaksjoner er små. Dette ville trolig også kunne skape en forståelse for at slike tilsvarende operasjoner sjelden blir møtt med sterkere motreaksjoner, og skape et utvidet handlingsrom for Russland. Dette alternativet får dermed høyeste score, 6.

Igjen er det utfordrende å skille mellom flere av alternativene. Opprettholdelse av status-quo fremstår uinteressant for russisk side. På den andre siden, dersom normaltilstanden tilsier at russiske aktører, både statlige og statlig tilknyttet, kan utføre cyberoperasjoner mot Norge uten å løpe den store risikoen, kan et slikt normalbilde være ønskelig å opprettholde. Utgangspunktet for spillet er at Russland ønsker en mer aggressiv strategi samt en endring i dagens liberale verdensorden. Dette innebærer at alternativ A får nest dårligst score, 2. Det er naturlig at alternativ E får score, 3, dersom den settes opp mot alternativ D og F, da det kun er alternativ E som innebærer en form for tap for Russland. Det er uansett verdt å merke seg at de kan holde tapet internt i Kreml gitt fordektbarheten rundt Norges respons. Dette alternativet fremstår derfor ikke som et like stort nederlag som alternativ C.

Hvis vi derimot ser på alternativ D og F, vil D innebære en forverret sikkerhetspolitisk- og diplomatisk situasjon, mens F vil kunne medføre en potensiell eskalering av situasjonen. Gitt at Russland ved sin operasjon har nådd sitt mål, og Norges respons fremstår som forholdsmessig, er det naturlig å tenke seg at det er mer ønskelig å gå inn i en krise, enn å havne i en større konflikt. Dette understøttes av at Russland, i denne situasjonen, har valgt å utføre angrepet i en allerede eksisterende vanskelig situasjon med betydelige sanksjoner og dårlig forhold til vesten. Det kan tenkes at Russland vurderer at de ikke lenger har så mye å tape, rent diplomatisk. Samtidig fremstår det lite sannsynlig at Russland ønsker å binde seg opp i en ny og potensielt større konflikt. Som følge av dette gis alternativ D score 5, mens alternativ F får score 4.

Oppsummert blir utfallet for Russland følgende: A: 2, B: 6, C: 1, D: 5, E: 3 og F: 4

Ser vi på Norges alternativer, kan vi starte med hva som er minst ønskelig. Det åpenbare svaret på dette er alternativ B som fremstiller Norge som handlingslammet. Dette vil kunne skape splid i egen befolkning rundt motstandsdyktigheten mot slike angrep. Ikke minst vil dette, som vist ovenfor, kunne skape et nytt handlingsrom for ytterligere angrep. Alternativ B får dermed score 1. Herfra er det naturlig å se på hva som er mest ønskelig. I mange tilfeller, hvor Norge som småstat, har svært lite å vinne på å binde seg opp i kriser eller konflikter, er det naturlig å søke å opprettholde dagens status-quo. Dette alternativet får derfor score, 6. Det virker som at

Norge i større grad enn tidligere offentlig attribuerer cyberangrep, eller at angriperne selv annonserer dette. Det kan tross alt fra motstandernes perspektiv, ligge litt prestisje i dette. Som følge av at Norges foretrukne respons synes å være i form av attribusjon, kan det tenkes at alternativ C fremstår som et bedre resultat, enn en sikkerhetspolitisk krise. Derimot strider dette litt mot Jaspers strategi om å regelmessig påføre motstanderen kostnader. Derfor er det naturlig at alternativ E får nest høyest score, 5. I valget mellom krise og konflikt, kommer alternativ C best ut, tilsvarende resultatet av analysen av de russiske responsene. Alternativ C får dermed score, 4. Vi står da igjen med alternativ D og F.

Skal man legge Jaspers tanke til grunn, bør en søke å påføre kostnader for å skape ny presedens. Dette taler for at alternativet med konflikt bør vurderes høyere enn krise. En slik tanke fremstår likevel litt underlig – hvorfor skal man ønske en konflikt, i stedet for en diplomatisk krise? Til det må man se på intensjonen bak Jaspers tanke. Man har hittil ikke sett en distinkt endring i Russlands cyberaktiviteter ut fra tidligere responser, snarere tvert imot. Det fremstår som at cybertrusselen man står ovenfor, er økende. Dette understøttes av Etterretningstjenestens årlige trusselvurdering, Fokus. I 2023 skrev Etterretningstjenesten at Russland forventes i økende grad å prioritere fremstilling av avanserte systemer for elektronisk krigføring og cyberkapasiteter (Etterretningstjenesten, 2023).

I følge Jasper handler avskrekking gjennom aktivt cyberforsvar å kommunisere en kapasitet, evne og vilje til å komme med en troverdig respons. Hvis dette i tillegg kombineres med en automatisk kapasitet i å detektere og hindre nye angrep, vil denne strategien kunne oppnå en avskrekkende effekt (Jasper, 2017, s. 185). Oppsummert velger jeg derfor å foretrekke alternativ F fremfor alternativ D. Dette innebærer at alternativ F får score, 3, mens D får score, 2.

Oppsummert blir utfallet for Norge følgende: A: 6, B: 1, C: 4, D: 2, E: 5 og F: 3

Satt inn i et skjema blir fordelingen følgende:

	A	B	C	D	E	F
Russland	2	6	1	5	3	4
Norge	6	1	4	2	5	3
Totalt	8	7	5	7	8	7

Som man ser av de overnevnte resultatene, ser det ut til at flere av handlingsalternativene havner på relativt likt resultat. Det er derimot et alternativ som kommer vesentlig dårligere ut enn de andre, alternativ C. Dette alternativet bygger i stor grad på hvordan norsk respons mot russisk cyberoperasjoner oppleves å være i dag, hvor man enten velger å attribuere eller ikke, hvor dette blir møtt med russisk nektelse. Et slikt scenario har ikke vist seg å ha en nevneverdig avskrekkende effekt, snarere tvert imot. Både alternativ A, status-quo og E, russisk tap som følge av norsk motoffensiv, oppnår analysens høyeste resultat. For å identifisere hvilket av disse to alternativene som til slutt fremstår best, kan man se på resultatet til begge aktørene. Alternativ A er tross alt Russlands nest minst ønskelige scenario. Dette argumenterer for at alternativ E bør foretrekkes.

Videre understøttes dette av at alternativ E innebærer et resultat som begge parter kan sies å være godt fornøyd med. For Russlands del innebærer dette et alternativ som er helt «midt på treet» i forhold til de andre alternativene, mens for Norge sin del, gitt valgt avskrekkingsstrategi, fremstår som det nest mest ønskelige. Som et resultat av dette, rangeres alternativ E som det scenarioet som begge parter har mest å tjene på totalt sett. Resultatet påfører Russland riktignok et tap, men kanskje ikke i form av tap av omdømme og intern legitimitet.

Det er uansett verdt å merke seg at cyberaktivitet i større grad enn kinetiske virkemidler er dynamiske. Dette betyr at begge aktørene i analysen fortløpende kan vurdere handlingsalternativets måloppnåelse ut fra ønsket effekt, og eventuelt endre egen strategi. Det illustrerte spillet viser dermed hvordan partene dynamisk kan endre egne strategier slik at man oppnår maksimalt utbytte.

Oppsummert kan analysen indikere at Norge potensielt kan ha noe å vinne på å endre avskrekkingsstrategi, fra de tradisjonelle om nektelse og straff, til i større grad å satse på troverdige robuste tiltak i kombinasjon med offentlige destruktive kapasiteter. Dette illustrerer også mulighetsrommet for Norge i å implementere hele eller deler av den nederlandske strategien i egen cyberstrategi. Det er uansett verdt å peke på at sentrale norske akademikere er usikre på hvorvidt en egen militær strategi er den riktige veien å gå. Det pekes derimot på at cyberkapasiteter er verktøy i verktøykassen, som fint kan tillegger de allerede eksisterende strategiene (Wilhelmsen et al., 2021, s. 259-260).

DEL III: DISKUSJON

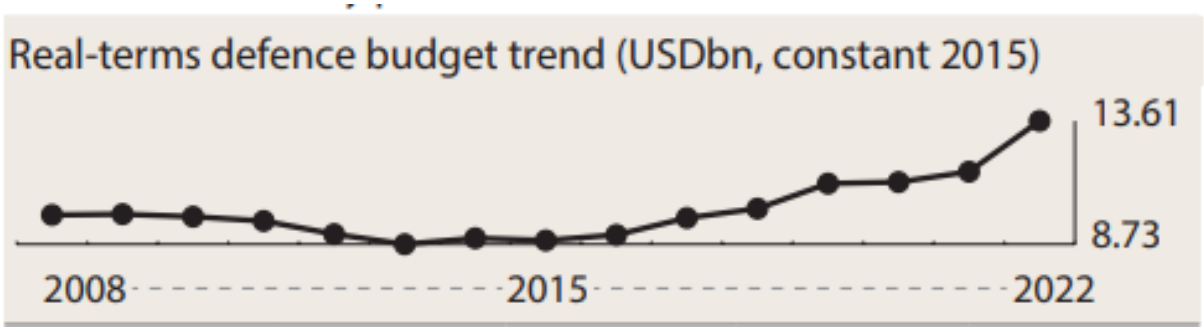
3.1 Introduksjon

Formålet med denne oppgaven er å undersøke om Norge har noe å lære av den nederlandske cyberstrategien i møte med russiske cyberangrep. Del I klargjorde oppgavens premisser, metode og relevante teorier og konsepter. I Del II ble Norges cyberstrategi sammenlignet med Nederlands. Dessuten ble ulike avskrekkingsstrategier analysert og testet gjennom enkle spill. I Del III skal den overordnede problemstillingen besvares gjennom tre oppsummerende diskusjoner rundt funnene i Del II. Den første diskusjonen handler om hvorvidt Norge har noe å lære av Nederland. Den andre diskusjonen ser på de tradisjonelle avskrekkingsteoriene og undersøker hvorvidt det ligger et nytt potensiale i strategien *aktivt cyberforsvar*. Den tredje diskusjonen forsøker å operasjonalisere en ny cyberstrategi for Norge. Del III avrundes med en konklusjon som søker å oppsummere oppgavens sentrale funn.

3.2 Har Norge noe å lære av Nederland?

«Nederland er i cyberkrig med Russland». Sitatet kommer fra den daværende nederlandske forsvarsministeren Ank Bijleveld i forbindelse med utvisningen av de fire russiske etterretningsagentene som ble avslørt i forbindelse med det tidligere omtalte cyberangrepet på OPCW i 2018 (Aftenposten, 2018). Budskapet til forsvarsministeren, sammen med den tekniske attribusjonen og de raske og tydelige retorsjonelle tiltakene kan ha bidratt til å skape legitimitet bak Nederlands benyttede strategi. Et relevant spørsmål er derfor. Har Norge noe å lære av Nederlands tilnærming til disse dynamiske utfordringene?

Først er det naturlig å se på hvilke konsekvenser dette har hatt for Nederland. De opprettet en egen cyberkommando som omfavner både defensive, offensive og etterretningsmessige kapabiliteter (Smeets, 2022, s. 67 og Wilhelmsen et al., 2021, s. 245). Formålet med etableringen var å styrke deres defensive og offensive evner i cyberdomenet (Liebetrau, 2023, s. 134-135). Som tidligere forklart, vil en slik styrking av kapasiteter innebære betydelige økonomiske utgifter. Dette er derfor en sentral utfordring ved den Nederlandske strategien. Over tid, vil den være krevende å opprettholde som følge av betydelige økonomiske utgifter til videreutvikling av egne kapasiteter. Dette understøttes av en økning i budsjettet til den nederlandske cyberkommendoen fra ca. 23 millioner NOK i 2012 til ca. 230 millioner NOK i 2018 ut ifra dagens kronekurs (Smeets, 2022, s. 71). Dette illustreres også i utviklingen av Nederlands forsvarsbudsjett.



Tabell 4: Nederlands forsvarsbudsjett i USD (Institute for Strategic Studies, 2023, s. 116).

Derimot viser oppgavens komparative analyse at utviklingen i Nederland har hatt sine positive effekter også. Antallet alvorlige cyberangrep ser ikke ut til å ha hatt tilsvarende økning som det vi blant annet har identifisert i Norge (Central Bureau voor de Statistiek, 2022 og Riksrevisjonen, 2023). Ikke minst har den også hatt en meget positiv utvikling i hvordan enkelte miljøer anerkjenner Nederlands cyberkapasiteter (Humanize, 2023).

Liebetrau peker på at Norge har valgt en annen tilnærming til dette. Norge har, i likhet med flere av sine allierte, ikke opprettet en egen cyberkommando. Derimot har Norge som kjent valgt å gi mandatet for offensive cyberoperasjoner til Etterretningstjenesten. Dette har de gjort, blant annet for å redusere kostnader ved å utvikle egne cyberkapasiteter (2020, s. 138-139).

Den komparative undersøkelsen av Norge og Nederlands cyberstrategier ble delt inn i tre ulike analytiske dimensjoner; *organisatorisk, institusjonelle og innhold.* I den organisatoriske dimensjonen ble det identifisert en svært ulik tilnærming til hvordan landene har beskrevet utfordringene med cyberangrep. Der Norge peker på at et digitalt angrep innebærer et angrep på norsk suverenitet, mener Nederland at det kan ses på som et væpnet angrep. Med andre ord viser landene til ulike former for folkerettslige terskelbrudd. Enhver stat har suveren myndighet over egen digital infrastruktur, men det er kun de mest alvorlige cyberangrepene som forårsaker at en rekke mennesker dør, eller fører til alvorlig materielle skader som vil kunne bli regnet som et væpnet angrep (Hellestveit, 2022, s. 125-127 og Schmitt, 2017. s. 339-342). Dette innebærer at Nederland klart har statuert sine folkerettslige vurderinger knyttet til cyberangrep i egen strategi. Norge har ikke gjort det i egen cyberstrategi, men dette er noe man har gjort i etterkant (United Nations, 2021, s. 70).

Videre har landene ulike synspunkter på internasjonalt samarbeid. Der Norge i sin strategi i større grad søker å utnytte et slikt samarbeid, understreker Nederland viktigheten av å tilby egne

kapasiteter. Nederland var blant annet et av de første landene som annonserte at de ville tilby egne cyberkapasiteter til NATO-oppdrag og operasjoner (Smeets, 2022, s. 68). Et slikt tilbud kan fremme ulike formål. Dels kan dette innebære et ønske om å kommunisere at man har styrket egne kapasiteter. Ikke minst er det mye som tyder på at en mer fremoverlent kommunikasjon om nasjonale cyberkapasiteter kan benyttes for å markere ambisjoner om å være en aktiv og kompetent aktør, samt at det kan ha en avskrekkende effekt (Strand, 2022, s. 52-53). For Norges del, kan organiseringen og begrensede kapasiteter være en naturlig forklaring på den valgte tilnærmingen. Gitt at man ikke har egen cyberkommando ville et større internasjonalt bidrag medført at kapasiteter måtte hentes fra Etterretningstjenesten, som igjen kan svekke muligheten for å drifte egne operasjoner og aktiviteter.

I den institusjonelle dimensjonen viser analysen at Norge og Nederland har svært ulik tilnærming til det sivil-militære samspillet. Dette er interessant da Norge blant annet etterspurte innspill fra Nederland i forbindelse med utviklingen av dagens strategi (NATOCCDCOE, 2023, 31:19-43:58). Der Nederland søker samarbeid med sivile aktører samt en intensjon om å gi militær bistand og støtte til sivile myndigheter, peker Norge på at det sivile skal støtte Forsvaret. Den norske strategien understreker også viktigheten av ansvarsprinsippet, og at norske virksomheter har et selvstendig ansvar for håndteringen av angrep i egen virksomhet. Skillet mellom samfunnssikkerhet og statssikkerhet blir utydelig i cyberdomenet (Wilhelmsen et al., 2021, s. 245-246). Dette innebærer at ansvaret for håndteringen av cyberangrep også vil bli utydelig mellom sivile og militære myndigheter. Dette kan svekke den norske strategien i noe grad. Hadde strategien konkretisert ansvaret mellom sivile og militære myndigheter, ville dette mulig kunne bidratt til å understøtte tanken bak ansvarsprinsippet.

Den nederlandske strategien har et betydelig fokus på å styrke egne offensive og destruktive kapasiteter, samt kapasiteter for å oppnå og beholde dominans. Dette bringer oss over på innholdsdimensjonen som i stor grad illustrerer et fremoverlent og offensivt Nederland i motsetning til den mer defensive norske tilnærmingen. Ikke bare det, men slike kapasiteter er ikke en gang nevnt i den norske strategien. Analysen peker på ulike tilnærminger for hvilken avskrekkende effekt egne kapasiteter og strategier skal ha. I Nederlands strategi er dette nevnt konkret, mens i Norges må det tolkes ut ifra ordlyd. Der hvor Nederland understreker at man skal skape avskrekking gjennom offensive kapasiteter og aktiv attribusjonspolitikk, der målet er at landet skal oppfattes som et mindre attraktivt mål å angripe, er Norge knappere i egen ordlyd. Den norske strategien understreker viktigheten av å skape et resilient og robust samfunn, og kan dermed tolkes dithen at man ønsker å avskrekke gjennom nektelse. Dette er

dog noe egne og andres analyser (Aannø, 2018, s. 44-46) har pekt på som utfordrende, om ikke svært vanskelig for en småstat som Norge.

I forlengelse av dette er det interessant å se at sjef for Etterretningstjenesten, Nils Andreas Stensønes, har sagt at offentlig attribusjon ikke har bidratt til å stoppe russiske cyberangrep selv om Norge ved flere anledninger har pekt på Russland og Kina som sentrale trusselaktører mot egen digital infrastruktur (Skei & Tønset, 2021 og Pedersen, 2023). Nederland på den andre siden synes å ha tatt ett skritt videre når det gjelder attribusjon i kombinasjon med andre mottiltak. Deres operasjon i 2018 som avslørte fire russiske diplomater som var i ferd med å utføre en cyberoperasjon mot Organisasjonen mot forbud mot kjemiske våpen, OPCW, er et godt eksempel på dette (Ministy of Defence, 2018). Her ble en kombinasjon av offentlig attribusjon med retorsjonelle tiltak i form av umiddelbare utvisninger av de fire diplomatene benyttet svært effektivt. Ikke bare sendte dette et tydelig signal til russiske myndigheter, men det kan også virke avskrekkende ovenfor andre trusselaktører.

3.3 Dagens avskrekkingsstrategier sammenliknet med aktivt cyberforsvar

Noe denne studien søker å finne ut, er hvorvidt dagens avskrekkingsstrategier i møte med russiske cyberoperasjoner har lyktes, og at man dermed har oppnådd en avskrekkende effekt. Et resultat, eller snarere kanskje et symptom på det motsatte er at dagens avskrekkingsstrategi ikke kan sies å ha endret Russlands atferd. Vi står fortsatt regelmessig overfor russiske cyberangrep. Riksrevisjonen oppsummerer blant annet at flere av de sentrale tverrsektorielle tiltakene for å håndtere digitale angrep knyttet til Norges cyberstrategi er forsinket, hvor forsinkelsen medfører økt risiko for at digitale hendelser ikke håndteres effektivt (Riksrevisjonen, 2023 s, 25-26). Dette vil naturligvis kunne ha implikasjoner på Norges avskrekkingspotensiale, da det kan sås tvil om troverdigheten til Norges robusthet mot cyberangrep, samt ikke minst den politiske styringen, når en slik konklusjon også peker på i hvor liten grad et slikt arbeid er prioritert av myndighetene.

Oppgavens analyser har pekt på flere utfordringer ved dagens strategi. Det kan se ut som om Russlands avgjørelser de siste årene har bidratt til å gjøre dagens strategi utdatert. Der hvor man tidligere har hatt, et om ikke velfungerende samarbeid, så har man tross alt hatt dialog og en gjensidig avhengighet landene imellom. Spesielt i Nord-Norge har det vært tidvis et godt samarbeid, spesielt innen søk- og redningstjenesten, og om den historiske delelinjeavtalen i

2010. Strategidokumentet *«Nordområdene»* beskrev attpåtil at man skulle satse på styrking av forholdet til Russland, hvor kontakten og samarbeid over grensen har en klar sikkerhetspolitisk dimensjon (Meld. St. 7, 2012, s. 61 og 69).

Tidene har forandret seg. Sanksjoner kan ha fått begrenset effekt siden Russland allerede er påført en rekke kraftige økonomiske og diplomatiske sanksjoner. Med økte sanksjoner kan det fremstå som at Russland i større grad har mindre å tape. De må tross alt få dekket sitt informasjonsbehov på andre måter når deres påståtte etterretningsagenter blir utvist fra land som Norge. Dette kan medføre økt bruk av fordekte metoder, herunder bruk av digitale aktiviteter. Dette må hensyntas når man analyserer avskrekkelse gjennom nektelse. Analysen sannsynliggjør at Russland ikke har så mye å tape på en konflikt, hvilket innebærer at avskrekkingspotensialet er betydelig svekket. Scenarioet hvor Russland blir beseiret gjennom at de gir opp angrepet som følge av norske sanksjoner, fremstår lite sannsynlig.

Det er også interessant at Norges nest mest ønskelige scenario, etter å opprettholde status-quo, er å gi etter gjennom å lukke identifiserte sikkerhetshull, snarere enn å iverksette mottiltak. En slik defensiv holdning, minner kanskje litt om dagens cyberstrategi, men vil mest sannsynlig innebære at man konkluderer med at avskrekking gjennom nektelse har mislyktes. I tillegg innebærer strategien en utfordring. Det vil være vanskelig å overbevise en potensiell angriper om at deres angrep uansett vil mislykkes. Motstanderen er høyst sannsynlig klar over at det er svært vanskelig å lage digitale systemer som ikke inneholder sårbarheter som kan utnyttes. De digitale tiltakene som skal skape motstandsdyktighet består av koder, koder er skrevet av mennesker, og mennesker gjør feil (Strand, 2022, s. 45).

Fordelen med en defensiv tilnærming kan tross alt være at man opprettholder en framferd som ikke fremstår eskalerende. Derfor var det noe overraskende at Norge gikk til det skritt å utvise 15 diplomater i 2023. Tidligere har det virket som at norske diplomatiske sanksjoner har blitt gjort i tett samarbeid med andre allierte, slik at Norges handlinger ikke ble isolerte. I 2023 stod Norge relativt alene i sanksjonene som kom over ett år etter at for eksempel Danmark utviste 15 diplomater (Westersø, 2022). I så måte viste Norge en uvanlig handlekraftig respons overfor Russland, men det spørs om det var strategisk klokt eller egnet til å bygge opp under egen avskrekkingsstrategi. Det er også et interessant funn at dersom Norge velger å iverksette mottiltak mot Russlands utfordring, vil Russland favorisere det å havne i en konflikt fremfor å gi etter for de norske tiltakene. Dette innebærer at Norges handlingsrom svekkes av potensiell fare for eskalering av en konflikt.

Hvis vi ser nærmere på scenarioet der avskrekking gjennom straff er analysert, viser dette tre mulige norske responser på et russisk cyberangrep, henholdsvis gjennom å gi etter, retorsjon eller offensive mottiltak. Det er to scenarioer som oppsummert fremstår som mest foretrukne, men hvor en sikkerhetspolitisk krise favoriseres som følge av dette alternativet foretrekkes i større grad av begge aktører. Dette innebærer i praksis at man ikke har iverksatt straffen som ligger i avskrekkingsstrategien, da en slik respons medfører utfall som er mindre ønskelige totalt sett. Scenarioet hvor Russland gir etter for en norsk straffereaksjon fremstår som usannsynlig, gitt at Russiske cyberkapasiteter trolig er overlegne de norske, samt at analysen viser at Russland sannsynligvis vil foretrekke en konflikt. De har potensielt ikke så mye å tape på det. Samtidig eksisterer det en mulighet for at Norge ikke ønsker å forlenge konflikten ytterligere, gitt at dette er Norges minst ønskelige utfall. Hvis Russland sørger for å holde seg godt innenfor det som oppfattes som Norges røde linje, vil de trolig kunne opererer som de vil, uten alt for store konsekvenser.

Dette er en utfordring ved begge avskrekkingsstrategiene, hvor manglende responser på konkrete cyberangrep skaper større og større handlingsrom for ikke bare Russland, men også andre relevante cybertrusselaktører. I tillegg spiller attribusjonsproblemet inn, som gir den offensive parten anledning til å operere fordekt, samt benekte innblanding dersom de senere offentlig skulle bli beskyldt for angrepet. Aannø konkluderte i sin masteroppgave at det for en småstat vil være en irrasjonell strategi å avskrekke en stormakt gjennom å true dens kritiske infrastruktur. Dette bygget blant annet på risikoen for at en slik handling vil medføre en eskalerende situasjon, noe min analyse også peker på (Aannø, 2018, s. 53-54)

Dette understøttes av Pedersen, 2023, som analyserte et tilsvarende scenario, hvor han så på potensialet som ligger i avskrekking ved bruk av straff for en småstat som Norge. Pedersens konklusjon var at enhver utvikling av en effektiv cyberavskrekking ved straff ser ut til å ville mislykkes. Noe av årsaken til dette var at utviklingen av offensive cyberkapabiliteter disfavoriserer småstater, som følge av utfordringen med å etablere nødvendige kapasiteter. I tillegg, hvis en småstat skulle hatt relevante offensive kapasiteter, vil disse være svært utfordrende å kommunisere (Pedersen, 2023). Dette innebærer at også i dette scenarioet står Norge ovenfor et dilemma hvor en potensiell straff vil kunne medføre eskalering av situasjonen. Pedersens analyse understøttes også av den tyske forskeren Matthias Schulze som kom frem til samme konklusjon for Tyskland sin del. Hans synspunkt på denne formen for avskrekking, er at den innen cyber er dømt til å mislykkes. Noe av årsaken til dette er at intensjoner og politisk vilje ofte er uklare fordi store deler av nasjonens cyberaktivitet utføres av landets

etterretningstjenester (Schulze, 2018). I forlengelse av dette, er det verdt å peke på beslutningsmyndigheten til de offensive cyberoperasjonene i Norge, hvor CNA ligger på strategisk, politisk nivå, mens aktiviteter definert som CNE er tillagt sjef for Etterretningstjenesten (Forsvarsdepartementet, 2014). Dette kan forsterke utfordringen som også Liebetrau peker på, nemlig at Norges organisering skaper en risiko for at mange av utfordringene for samarbeid forblir i Etterretningstjenesten (2023, s. 140). Dette igjen, understøttes av Nye, som viser til at cyberangrep i stor grad kan bli benyttet til politiske budskap, så vel som kun å ødelegge eller forstyrre (2017, s. 49).

Årsaken til at Scott Jasper introduserte strategien om aktivt cyberforsvar var at de tradisjonelle strategiene ikke fremstod som å være tilstrekkelige innen cyber. Dette blir understøttet av mine analyser. Spørsmålet i forlengelse av dette, er hvorvidt aktivt cyberforvar kan skape det avskrekkingspotensialet innen cyber som man tidligere har manglet?

Et umiddelbart, og godt argument for å implementere denne strategien, er at toneangivende cybernasjoner ser ut til å bruke sentrale prinsipper innen aktivt cyberforsvar i egne cyberstrategier. Både USA, Storbritannia og Nederland, som Humanize kåret til første, fjerde og sjette plass over de mest mektige cybernasjonene i verden i 2022, har nylig i mer eller mindre grad endret sine cyberstrategier (Humanize, 2023). Dog, som illustrert ovenfor, risikerer Norge som småstat, uten tilsvarende kapasiteter, å eskalere en situasjon dersom de velger å straffe Russland.

Det er fortsatt verdt å merke seg at landene fortsatt ønsker å opprettholde status-quo. Aktivt cyberforsvar søker ikke å utfordre dette, men snarere bygge videre på et ønske om å iverksette tiltak for å opprettholde status-quo. En distinkt forskjell fra de tidligere analysene, er at Norge i dette tilfelle ikke trenger å være tilsvarende bekymret for eskalering av situasjonen. Noe av årsaken til dette, er at Norge, i dette tenkte scenarioet, gjennom aktivt cyberforsvar har etablert et konsept med offensive kapasiteter som har blitt presentert som en ny strategi. Dette medfører at Norges respons, selv om den er i form av offensive destruktive mottiltak, er forutsigbar. Denne forutsigbarheten kan sannsynligvis bidra til at terskelen for hvor avskrekkingsstrategien kommer til anvendelse, heves. Analysen gir også uttrykk for dette, da en norsk motoffensiv ikke fremstår som det dårligste alternativet for Russland, uavhengig av om de velger å gi etter, eller om de velger å fortsette egen offensiv.

Aktivt cyberforsvar som strategi, har sine likheter med avskrekking gjennom nektelse og straff. Grunntanken om at man skal overbevise en motstander om at egne systemer og forsvarsevne er

så robust at et angrep uansett vil mislykkes. Dette innebærer at en strategiendring trolig ikke vil måtte endre grunntanken til norske myndigheter. Dette er en stor fordel, gitt den politisk viktige dimensjonen i strategisk respons. For å oppnå tilstrekkelig avskrekking er man avhengig av kontinuitet, uavhengig av hvem som styrer landet. Det fremstår, uten at oppgaven har gått nærmere inn på dette, at norsk utenrikspolitisk budskap i stort har vært ganske konsekvent. Dette er en fordel, kanskje også en forutsetning, dersom man skal implementere en ny strategi som inneholder trekk fra dagens strategi. Noe annet ville kunne skapt en utydelig kommunikasjon, som igjen kunne skapt et handlingsrom for en motstander. Dette understøttes av FFI, som peker på at Norges største handlingsrom er å styrke egen motstandsdyktighet ved for eksempel å lukke sårbarheter i kritiske samfunnsfunksjoner og infrastruktur (FFI, 2022b, s. 53).

Da USA, Storbritannia og Nederland regner for å være digitale stormakter, er kanskje ikke sammenlikningsgrunnlaget med norsk tilnærming til stede. Derimot er det verdt å nevne at der hvor Nederland i 2020 ble kåret til verdens femte mektigste cybernasjon, var dette et betydelig hopp fra en 12-plass de fikk i 2018 (Belfer Center, 2020). Sånn sett illustrerer dette at Nederlands strategiske retningsvalg i 2018 muligens kan ha hatt en betydelig effekt. Det er samtidig verdt å merke seg at Norge i 2018 kom på 9. plass, mens de i 2020 ikke ble nevnt i rangeringen, dette etter at Norges cyberstrategi ble utgitt. En av årsakene er at Belfer Center mener at Nederland har styrket sin posisjon gjennom å signalere etableringen av offensive kapasiteter i sin nyeste cyberstrategi (ITU Publications 2018). Selv om Norge ikke ble nevnt i analysen, er det naturlig å tolke det dithen at de har falt nedover på rangeringslisten. Sannsynligvis ville uansett Norge vært ansett som et land med lav intensjon og begrensede kapasiteter, hvilket trolig ville plassert oss lenger ned på listen. Nederlands utvikling kan derimot argumentere for at det ligger et potensiale for Norges del i å tilpasse egen strategi. Dette må holdes opp mot argumentet om at det ikke finnes noe rasjonale for Norge, som småstat, å styrke egne kapasiteter i den hensikt på sikt å kunne gi Russland motstand.

Det finnes derimot motstandere av Nederlands tilnærming, som mener at en trussel om offensive cyberoperasjoner ikke nødvendigvis vil ha en avskrekkende effekt, og kaller dette en overfladisk forståelse av avskrekking. Schulze sier at dersom cyberkapasitetene ikke er troverdig kommunisert, og spesielt hvis det ikke er vilje til å bruke dem, vil dette skape en rekke fallgruver. Ikke minst kan egne cyberoffensiver lide under samme utfordring man selv står ovenfor når det gjelder potensielle utilsiktede effekter (Schulze, 2019). Dette innebærer at man ikke nødvendigvis kan være i stand til å forsikre seg om at egne mottiltak utelukkende rammer

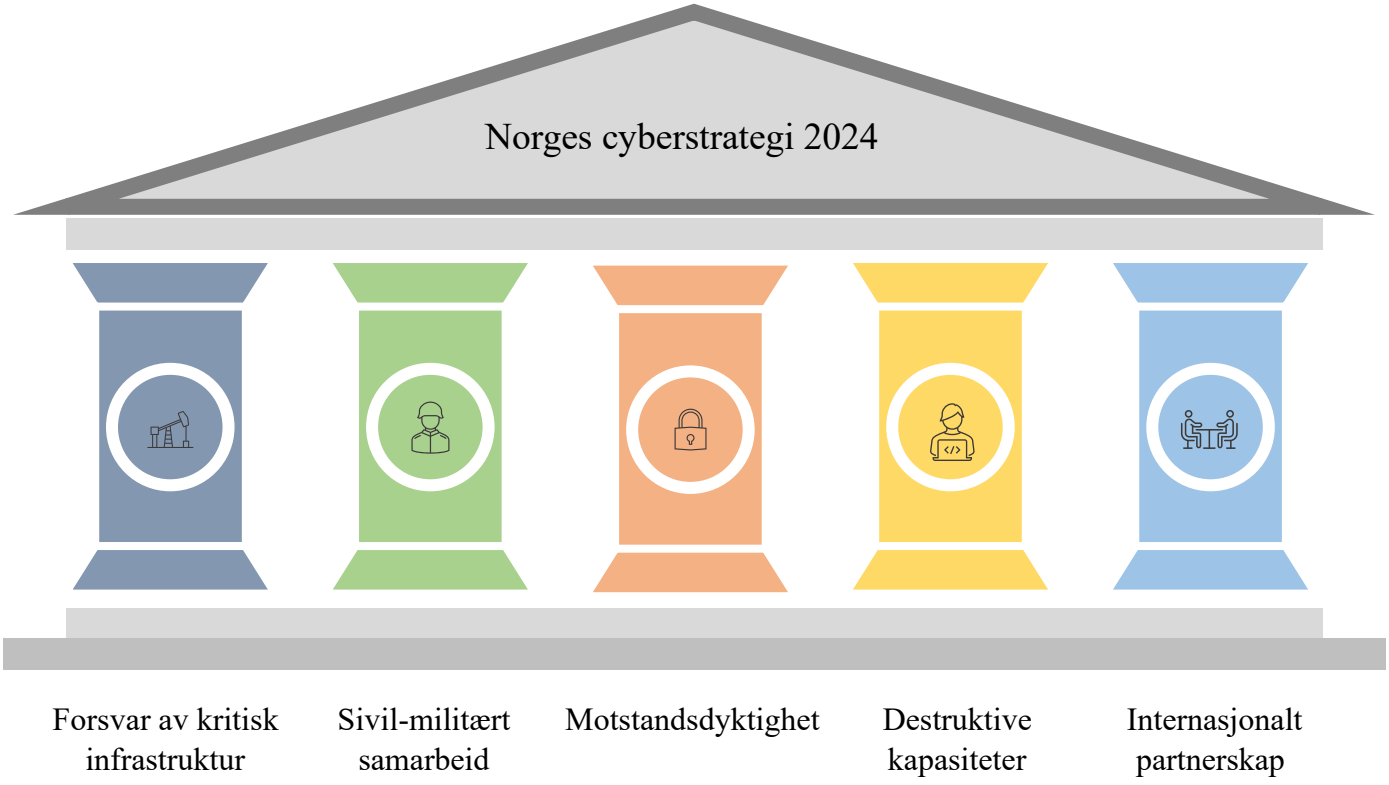
det ene målet man har sett for seg. Utfordringen med potensiell eskalering, kan derfor innebære en vegring mot å iverksette egne offensiver.

3.4 Operasjonalisering av ny cyberstrategi for Norge

Samtidig som jeg sitter i min skriveprosess, jobber Regjeringen med det som skal bli Norges nye digitaliseringsstrategi. Strategien skal legges frem i 2024, der sikkerhet kommer til å bli et viktig punkt. Dette presenterte Statsminister Jonas Gahr Støre i august 2023 i forbindelse med det tidligere omtalte datainnbruddet i DSS. Kanskje det mest oppsiktsvekkende er at Støre i samme intervju sa *«jeg leder nå en regjering som egentlig er under angrep»* (Aftenposten, 2023). Dette fremstår som en ytterligere eskalering av den beskrevne ordbruken, da man tidligere i stor grad har hatt fokus på angrepenes tekniske og operasjonelle konsekvenser. Støre peker konkret på at angrepet er et angrep på regjeringen, med andre ord begynner vi å nærme oss et angrep som rammer norsk suverenitet.

Der hvor Nederlands forsvarsminister i 2018 mente de var i cyberkrig med Russland, mener altså nå Norge at deres regjering er under et digitalt angrep. Dette illustrerer behovet for en ny strategi, som i større grad innretter seg etter det andre toneangivende aktører har presentert i sine strategier.

Formålet med dette avsluttende kapittelet er å sammenstille oppgavens funn, og operasjonalisere eventuelle anbefalinger i form av et forslag til ny cyberstrategi for Norge. Etter inspirasjon fra USA, Storbritannia og Nederlands siste cyberstrategier foreslår denne oppgaven at Norges nye strategi baseres på fem pilarer; *forsvar av kritisk infrastruktur, sivil-militært samarbeid, skape en motstandsdyktig fremtid, styrke egne destruktive kapasiteter, internasjonalt partnerskap* (The White House, 2023, Department of Defence, 2018, HM Government, 2022 og Ministerie van Defensie 2018). Disse er valgt for å etablere et overordnet strategisk mål i tillegg til å være retningsgivende for nødvendige prioriteringer. Dette vil sørge for kontinuitet innen det overordnede arbeidet med strategisk respons i møte med russiske cyberangrep.



Figur 6. Norges nye cyberstrategi – delt inn i fem pilarer.

Da russiske statlige aktører sannsynligvis vil fortsette med cyberangrep som ligger under terskelen for militær eskalering, vil ikke ansvaret for respons være tydelig plassert hos henholdsvis de militære eller sivile myndighetene. Dette innebærer at ansvaret for håndteringen kan bli fragmentert (Wilhelmsen et al., 20212, s. 246), spesielt siden et cyberangrep ofte vil ramme samfunn- og ikke statssikkerheten. Som følge av dette må norske myndigheter ta et tydeligere selvstendig ansvar. Det fremstår ikke tilstrekkelig at norske myndigheter retter et betydelig ansvar til virksomhetene selv, slik dagens strategi legger til grunn. Dette var et av de sentrale hovedfunnene fra Riksrevisjonen da de undersøkte myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor. Riksrevisjonen konkluderte med at Justis- og beredskapsdepartementet ikke har sørget for god nok oppfølgning av Norges cyberstrategi (Riksrevisjonen, 2023).

Norge må også ta ansvar på vegne av europeiske og andre internasjonale partnere (Departementene, 2019). Dette innebærer at Norge, som en sentral energileverandør til det europeiske kraftmarkedet, må ta et eget ansvar for å sikre slik kritisk infrastruktur. Hovedlærer ved Forsvarets Høgskole Geir Hågen Karlsen, utpekte så sent som i slutten av august 2023 at norsk olje- og gassektor sannsynligvis er det mest utsatte målet i Europa for et terrorangrep fra

Russland, hvor et slikt angrep like gjerne kan komme i form av et cyberangrep (Lillegård, 2023). Et slikt angrep er noe som vil gi størst strategisk effekt, samtidig som det involverer cyberdomenets mulighetsrom for fordektbarhet. En annen viktig årsak til at man burde ha særlig fokus på dette punktet, er at et angrep på slik infrastruktur i stor grad kan skape farlige spillover-effekter til andre deler av samfunnet.

Ikke bare må myndighetene ha oversikt over nasjonal kritisk infrastruktur, men kanskje burde også flere sentrale virksomheter underlegges Sikkerhetsloven og defineres som en grunnleggende nasjonal funksjon. For eksempel ble Norges gassrør til Europa definert som en GNF først sommeren 2022, tre og et halvt år etter at muligheten for dette ble tilgjengeliggjort. Dette er viktig fordi virksomheter som er definert som en GNF, blant annet har mulighet til å motta høyt gradert informasjon om trusler (Strand, 2022). Dette bringer oss over til den andre pilaren.

Den andre pilaren handler om at Norge burde sørge for et styrket sivil-militært samarbeid. I dette ligger det en videreutvikling av dagens strategi, som tross alt i stor grad bygger på denne type samarbeid. Samtidig har analysen vist at norske myndigheter i større grad må erkjenne og ta det overordnede ansvar for håndtering av cyberangrep som rammer sivile virksomheter. De norske myndighetene kan ikke på den ene siden si at et cyberangrep på finansiell sektor kan være såpass alvorlige at de kan utløse NATOs artikkel 5, og samtidig overlate ansvaret for håndteringen over på virksomheten (United Nations, 2021, s. 70). Dette understøttes også av en fersk kronikk fra tidligere assisterende sjef for Politiets Sikkerhetstjeneste Hedvig Moe. Hennes vurdering er at rammene for norsk næringsliv er for uklare, der norske virksomheter i for liten grad sitter på viktig informasjon om trusselbildet. Dette medfører at virksomhetene har for dårlige forutsetninger til å kunne ta gode beslutninger. Dette totalbildet er det som Moe sier, kun myndighetene som per i dag har (Moe, 2023).

Sivile virksomheter må gis nødvendige informasjon som myndighetene sitter på, slik at de blir mer robuste til å håndtere de til enhver tid mest fremtredende truslene. I denne sammenheng bør myndighetene og EOS-tjenestene bli dyktigere til regelmessig å distribuere tilstrekkelig med informasjon uten at dette går på kompromiss med operasjonelt nødvendig hemmelighold. En slik varslingsfunksjon bør sentraliseres i større grad, i stedet for gjennom de ulike cybersikkerhetssentrene i Norge. Disse er fordelt mellom ulike sektorer eller store virksomheter. I 2016 eksisterte det 11 slike sentre i Norge, hvor antallet i dag trolig er større (Thorsheim, 2016). Det er derfor et sentralt spørsmål hvorvidt ansvarsprinsippet i Norges

eksisterende cyberstrategi har medført et for desentralisert ansvar for å håndtere cyberangrep. Et ansvar som også pålegger virksomhetene betydelige økonomiske forpliktelser. Kanskje dette er noe av årsaken til at Totalberedskapskommisjonens rapport viser at kun 29% av undersøkte virksomheter i 2021 hadde planverk for cyberangrep (NOU 2023:17, s 415).

I desember 2022 varslet regjeringen at den vil forsterke samarbeidet mellom Politiets sikkerhetstjeneste, politiet, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet i bekjempelse av sammensatte trusler. Samarbeidet skulle være i form av et Nasjonalt etterretnings- og sikkerhetssenter, NESS (Regjeringen, 2022). I ettertid finnes det lite spor av denne satsningen, slik at det er knyttet usikkerhet til hvorvidt senteret er operativt. Totalberedskapskommisjonen har identifisert tilsvarende. Den sier blant annet at det i NESS mangler en innretning der sikkerhetspolitisk risiko knyttet til nasjonale sikkerhetsinteresser, blir helhetlig vurdert. Et ansvar de norske myndighetene bør ta i forbindelse med endring av dagens cyberstrategi, er å utvikle et system og en funksjon for nasjonalt og rettidig situasjonsbilde innen cyberdomenet som sikrer tilstrekkelig håndtering, analysering og rapportering til både myndigheter og sivile virksomheter. Totalberedskapskommisjonen peker på videreutvikling av NESS i et slikt perspektiv (NOU, 2023:17, s. 96 og 117). Dette understøttes også av at det har blitt foreslått at Norge ikke har en enhetlig cyberstrategi, der forståelsen om trusselbildet, og forholdet mellom det sivile og militære fremstår uklare (Wilhelmsen et al., 2021, s. 257-258). Dog, det er verdt å merke seg Liebetrau sin vurdering av den Nederlands tilnærming, hvor han mener det eksisterer juridiske utfordringer samt uklare mandater i slike samarbeidende modeller (2023, s. 135). Dette er i så fall noe man må være seg bevisst i mandatsutformingen til et slikt nasjonalt etterretning- og sikkerhetssenter.

For det tredje burde det være et mål at den nye strategien skal skape et tilstrekkelig motstandsnivå, proporsjonalt med den til enhver tid eksisterende trusselen og risikoen man står ovenfor. Det er uansett verdt å understreke at en målsetning om å skape en absolutt resiliens ikke er realistisk, da de mest sofistikerte trusselaktørene vil være i stand til å overvinne selv de mest robuste cybersikkerhetstiltakene. Dette handler derimot om å påføre motstanderen så store investeringer og kapasitetsbruk for å komme igjennom eget system, at de heller velger rette angrepet mot noen andre, mer sårbare systemer. Det handler med andre ord ikke om å gjøre Norge til den mektigste cybernasjonen i verden, men snarere å sørge for at vi ikke blir ansett av våre motstandere som en av de mest sårbare og kostnadseffektive å angripe.

Ikke bare spiller Norges posisjon som kraftleverandør inn når man diskuterer viktigheten av å skape robuste informasjonssystemer. Norge er, og har de siste årene vært, blant de ledende landene i Europa når det gjelder digitalisering. Som følge av avhengighetene den økte digitaliseringen skaper, bidrar dette også til et mer sårbart samfunn (Nye, 2017, s. 45). DESI-indeksen til EU-kommisjonen måler landenes digitale kompetanse, samt blant annet utbredelse og bruk av digitale tjenester. I 2022 havnet Norge på femte plass bak Finland, Danmark, Nederland og Sverige (European Commission, 2022). Det at Norge er såpass langt fremme når det gjelder digitale tjenester, innebærer ikke bare fordeler – det skaper også sårbarheter.

Spørsmålet i så måte, er hvorvidt digitaliseringen har gått for langt, uten at man samtidig har investert nok i et robust forsvar. Som følge av både høy grad av digitalisering, sammen med en digital globalisert verden, skaper dette en rekke avhengigheter og sårbarheter. Derfor fremstår det essensielt at prinsippet om å skape en robust digital infrastruktur også ses i sammenheng med det sivil-militære samarbeidet. En vanlig oppfatning er at industrialiserte og digitaliserte samfunn er de mest sårbare. Attribusjon kan i noen grad motvirke dette. Digitaliserte samfunn besitter gjerne en høy teknisk kompetanse som slikt sett kan gjøre landet mindre attraktivt å angripe fordi faren for attribusjon øker (Rid & Buchanan, 2014, s. 31).

Det nederlandske forsvarsdepartementet har som mål at de selv skal være eiere og ansvarlige for egne IT og våpensystemer (Ministerie van Defensie 2018). Dette er noe Norge også kanskje i større grad burde implementere. Formålet med dette er å ikke gjøre seg avhengige av andre lands aktører. Et nylig eksempel er hvordan det nylige DSS-angrepet benyttet en sårbarhet som motstanderen fant i et utenlandsk datasystem (Støyva & Wikan, 2023).

For det fjerde burde Norge investere ytterligere i egne offensive cyberkapasiteter, og ikke minst være tydelige på en slik investering i ny strategi. I tillegg bør det kommunisere at kapasitetene vil bli benyttet med full styrke for å respondere på de mest sofistikerte truslene. Man bør dog være bevisst på hvilke utfordringer dette kan innebære. Smeets hevder det er en rekke organisatoriske utfordringer med en slik utvikling. Konkret har han utviklet et rammeverk for å vurdere statens evne – PETIO, oversatt til MUVIO. Dette innebærer behov for *mennesker* som ligger til grunn for en vellykket operasjon, *utnyttelser* og *verktøy* er nødvendige for at mennesker skal kunne gjøre jobben sin. I tillegg innebærer dette *infrastruktur* som er ryggraden i en operasjon, samt *organisasjonsstruktur* som kan hjelpe til med å integrere ressurser og kunnskap (2022, s. 73-92). Norge ville av Smeets trolig blitt beskrevet som en stat med få kapasiteter, og store begrensinger. Følgelig ville han nok ment at det vil være vanskelig å

utvikle egne cyberkapasiteter. Smeets beskriver hvordan man utvikler en organisasjon og hvordan man får den til å fungere, samt hvordan man effektiviserer cyberoperasjoner, men han retter i mindre grad fokus på cyberkapasitetenes avskrekkende evner. Hans bekymring for at en stats utvikling av egne cyberkapasiteter vil kunne føre til en uheldig syklus hvor hver stat forsøker å opprettholde overlegenhet, fremstår som mindre relevant sett i lys av det norske perspektivet. Spørsmålet her er ikke nødvendigvis hvorvidt Russland vil oppfatte de norske cyberkapasitetene som en eksistensiell trussel, men snarere hvorvidt de oppfatter Norge som en vanskeligere mål å ramme enn andre relevante stater. Dersom man går tilbake og ser dette i lys av avskrekking, kan transparens rundt egne offensive cyberkapasiteter styrke cyberavskrekkingsevnen. Dette er i tråd med eksempler fra andre verdenskrig hvor Tyskland valgte å ikke benytte kjemiske våpen mot Storbritannia og USA fordi de hadde vært tydelige på hvilken respons det ville få (Nye, 2017, s. 53).

Det norske Forsvaret har som sin hovedoppgave å forsvare Norges interesser i alle domener. Derfor bør det heller ikke være tvil om dette i en ny strategi. Oppgavens analyser knyttet til strategien rundt aktivt cyberforsvar tilsier at det kan være nødvendig å gjøre nye vurderinger knyttet til hvilken avskrekkingsstrategi Norge bør benytte seg av. Der hvor de tradisjonelle i stor grad kan være, ja nettopp tradisjonelle og statiske, skaper cyberangrepenes ustanselige utvikling og andre komplikasjoner en situasjon hvor man i større grad er avhengig av dynamiske virkemidler. Her vil cyberkapasiteter være en nøkkel for å kunne løse disse utfordringene. I forlengelse av dette, må kapasitetene understøttes av strategisk kommunikasjon. Dette kan fremstå motstridende all den tid både offensive og defensive cyberkapasiteter har best forutsetning for å være effektive dersom de holdes hemmelig ovenfor en potensiell motstander (Strand, 2022, s. 43-45). Allikevel er dette nødvendig for å oppnå ønsket avskrekkingseffekt. Når det er sagt, er uansett det å faktisk utføre reelle operasjoner mot en motstander den mest troverdige måten å kommunisere egen evne på. Dette innebærer også at motstanderen må gjøres kjent med hvor angrepet kommer fra.

Analysen har sett på to ulike løsninger, enten å gjøre dette fordekt, eller offentlig – begge deler har sine fordeler og ulemper. Fordelen med å gjøre dette offentlig er at dette understøtter egne intensjoner. Utfordringene kan derimot være at dette kan bidra til å eskalere situasjonen. Fordelene med å gjøre dette fordekt, er at samme budskap sendes bare til motstanderen, hvor dette muligens ikke vil medføre samme behov for respons. Det innebærer derimot at budskapet ikke sendes til andre aktuelle trusselutøvere. Dette kan resultere i at den avskrekkende effekten kun rettes mot én aktør, hvor den derimot svekkes ovenfor alle andre. Et siste alternativ, som

regelmessig blir brukt, er å ikke aktivt ta avstand til eller bestride beskyldninger om egne operasjoner. Dette fordrer at operasjonen har vært både sofistikert og vellykket. Et eksempel på dette, er hvordan USA har brukt overraskende lite energi på å tilbakevise påstandene om at de stod bak det tidligere omtalte Stuxnet-angrepet mot Iran (Strand, 2022, s. 51).

Både USA, Storbritannia og Nederland går i en retning hvor de i større grad søker å vise frem sine intensjoner om bruken av egne offensive virkemidler. For eksempel skriver engelske myndigheter at de vil benytte seg av hele sitt spekter av kapasiteter til å svare ut cyberangrep. Dette inkluderer målrettet bruk av offensive cyberkapasiteter for å forstyrre og avskrekke slike trusler (HM Government, 2022, s. 49). Nederland peker tilsvarende på at de har en ambisiøst målsetning om å skape en digital slagkraft. I tillegg til å skape en bedre evne til å attribuere, krever avskrekkingen troverdige offensive evner (Ministerie van Defensie, 2018, s. 4-8). For at avskrekkingen skal være troverdig, er det et poeng at den er synlig. Dette kan skapes gjennom å offentlig forplikte seg til dette i en strategi, men også konkret gjennom handling.

Dersom man velger å gå for en slik tilnærming i ny cyberstrategi, er det sentralt at dette følges opp, tilsvarende det Nederland og USA har gjort. Som amerikanerne tydelig gir uttrykk for, skulle egen evne til avskrekking mislykkes, står et samlet forsvar klar til å iverksette samtlige av militærets kapasiteter som respons (Department of Defence, 2018, s. 4). Dersom Norge velger å implementere en tilsvarende tilnærming, innebærer dette en forventning om at norske myndigheter i større grad må respondere på angrep. Aktivt cyberforsvar skal bidra til å forhindre, avdekke og håndtere cyberangrep, slik at motstanderen ikke får operere konsekvensfritt.

I forlengelse av dette burde strategien inneholde et punkt om domenespesifikk avskrekking tilsvarende det Nederland har påpekt. Med andre ord, avskrekkingen trenger ikke være domenebundet. Norge har allerede ytret dette tidligere, men da ikke i form av et nasjonalt strategisk dokument (United Nations, 2021, s. 72). Dette understøttes også av Nye. Selv om avskrekking gjennom straff er benyttet, trenger ikke den avskrekkende trusselen å være avgrenset til en digital respons (Nye, 2017, s. 45). Som en konsekvens av dette står Norge fritt til å svare ut en trussel fra et annet domene ved bruk av offensive cyberkapasiteter. Fordelene med dette kan potensielt være store. Trusselen kan fremstå tvetydig ovenfor en motstander, og kan være utfordrende å forholde seg. Ulempene derimot er at en slik strategi trolig vil være både tidkrevende og forbundet med høye kostnader. I tillegg vil dette kunne bidra til å

eksponere egen teknisk kompetanse, som igjen kan skape en påfølgende sårbarhet. Dette er som vi har sett, et stadig tilbakevendende dilemma.

Det er uansett verdt å merke seg at de strategiene denne oppgaven sammenlikner, i stor grad har blitt utgitt av de respektive landenes forsvarsdepartement. Et spørsmål, som denne oppgaven ikke kommer til å gå nærmere inn på, er hvorvidt en beskrivelse av Norges offensive kapasiteter og intensjoner burde beskrives i en nasjonal cybersikkerhetsstrategi slik den Støre viser til skal komme neste år. Alternativt kunne en slik strategi utarbeides av Forsvarsdepartementet. Det er tross alt en distinkt forskjell mellom safety og security, hvor et naturlig spørsmål for myndighetene vil være hvorvidt man burde blande tiltakene til disse respektive områdene, eller om de skal splittes opp i to ulike strategier.

For det femte og siste bør Norge i en ny cyberstrategi beskrive og forplikte seg til internasjonalt partnerskap for å forfølge felles mål. Et slikt samarbeid er allerede beskrevet i dagens cyberstrategi, hvor man blant annet søker å styrke internasjonalt samarbeid for å være i bedre stand til å attribuere cyberangrep. Allikevel bør man i større grad forplikte seg til å etablere strategiske partnerskap med for eksempel privat sektor, akademia, og internasjonale partnere. Spesielt innen akademia kan man ha en del å hente, gitt at fokus på videreutvikling av teknologi og kunnskap trolig vil være sentrale for og både skape en motstandsdyktig nasjon, samt evne til å være dynamiske i en eventuell respons. Et eksempel er Nederlands opprettelse av *«Cyber Innovation Hub",* et sivil-militært samarbeidsprogram. Målet med dette er å legge til rette for innovasjon og bygge et økosystem av partnere for å redusere cybertrusler (Ministerie van Defensie 2018).

Mange av Norges partnere og allierte har trolig avanserte cyberkapasiteter som utfyller våre egne. Mulighetsrommet som ligger i å etablere et samarbeid for å kunne utnytte alliertes ressurser vil være et positivt supplement, som Norge trolig vil være avhengig av. Dette vil også kunne skape et nødvendig og alternativt kollektivt cyberansvar, all den tid oppgavens analyser har identifisert enkelte utfordringer cyberangrep har i lys av NATOs artikkel 5. Dette kan sammenlignes med hvordan støtte i dag blir gitt til Ukraina. De vestlige landene har i stor grad en egeninteresse i at Russlands krigføring i Ukraina ikke flytter seg lenger vest. Selv om NATO ikke er involvert direkte i krigføringen som en allianse, har de fleste medlemslandene gått positivt inn med ulike former for støtte.

En mulig retning kan være å følge Nederlands tilnærming hvor de ønsker å tilby sine offensive cyberkapasiteter til andre allierte for oppdragsløsning eller til konkrete cyberoperasjoner. Et

eksempel på dette kan for eksempel være at de nordiske landene etablerer et cybersikkerhetsfelleskap hvor nasjonenes tjenester regelmessig deltar på felles øvelser og raskere deling av kritisk informasjon. Fordelen med å ha dette internt i Norden er flere. Ikke bare har vi mye av den samme kulturforståelsen, men Norden består av små land som har en relativt lik tilnærming og utfordring stilt overfor eksempelvis russiske trusler.

3.5 Konklusjon

Norge er i dag kanskje ikke i stand til å avskrekke Russlands bruk av cyberangrep – til det er Støres beskrivelse av cyberangrepet mot DSS sommeren 2023 beskrivende.

Det var tross alt et angrep på hans regjering.

Hensikten med denne oppgaven har vært å forsøke å svare på om Norges avskrekkingsevne er tilstrekkelig for å håndtere russiske cyberangrep. Det synes fortsatt som at tematikken rundt avskrekking innen cyberdomenet mangler tilstrekkelig med empiri til at det er mulig å gi klare råd til norske myndigheter på hvordan man burde gå frem. Mangelen forsterkes også av den raske utviklingen cyberdomenet står ovenfor. Oppgaven har tatt utgangspunkt i en komparativ analyse mellom Norge og Nederlands cyberstrategi, hvor landene i betydelig grad har valgt to ulike tilnærminger. Dernest har relevante avskrekkingsteorier blitt testet gjennom spillteoretiske modelleringer. Denne oppgaven er spesielt relevant i disse dager, da norske myndigheter er i en prosess hvor de skal utarbeide nye cyberstrategier for Norge.

Nederland har i motsetning til Norge over tid offentlig endret sin ambisjon når det gjelder landets cyberstrategi. Den søker i større grad å videreutvikle egen resiliens mot cyberangrep, samt styrke egne offensive og destruktive cyberkapasiteter, i tråd med både strategien rundt aktivt cyberforsvar og «defending forward». Dette synes å ha påført Nederland betydelig kostnader, ettersom deres budsjetter, spesielt knyttet til cyberforsvar, har vært økende i mange år. Det kan tyde på at strategien har hatt en positiv effekt, da Nederland nå i flere tilfeller blir pekt på som en cyberstormakt. Dette kan sannsynligvis ha bidratt til å understøtte deres uttalte ambisjon om at deres satsning skal ha en avskrekkende effekt. Deres uttalte mål er å få Nederland til å fremstå som et mindre attraktivt mål å angripe. Ikke minst underbygges dette av at det Nederlandske statistiske sentralbyrået peker på en mer positiv utvikling innen opplevde cyberangrep enn det andre land rapporterer. En slik utvikling vil kunne bidra til å styrke Nederlands suverenitet og sikkerhetspolitiske interesser.

Hvorvidt cyberangrepene skjer som følge av feil anvendelse av avskrekkingsstrategier eller ikke, er uklart. Det som derimot fremstår tydelig, er at manglende respons mot cyberangrep skaper handlingsrom for relevante trusselaktører. Flere av oppgavens analyser viser at dette allikevel er Norges foretrukne alternativ i flere scenarioer.

Selv om det er utfordrende å komme med en absolutt konklusjon, peker oppgaven på at Norge kan ha noe å vinne på å endre dagens avskrekkingsstrategi som i stor grad baseres på nektelse. Dersom Norge hadde satset ytterligere på troverdige motstandsdyktige tiltak i kombinasjon med destruktive kapasiteter, i tråd med avskrekking gjennom *aktivt cyberforsvar*, kunne man oppnådd flere positive resultater. Både som følge av at en slik tilnærming, så fremt den er understøttet av nødvendige troverdighet og egeninnsats, ser ut til å ha hatt en positiv effekt for Nederland. I tillegg ser tilnærmingen ut til å redusere sannsynligheten for å havne i en eskalerende situasjon.

Norge vil ha utfordringer med egen kredibilitet når det gjelder å benytte en strategi som innebærer avskrekking gjennom straff. Velger man derimot en slik tilnærming, skal man være forberedt på at Russland vil teste ut hvorvidt Norge er politisk og operasjonelt forberedt på bruk av offensive kapasiteter, og ikke minst om Norge er villige til å håndtere de konsekvensene dette eventuelt vil ha. Alternativt kan Norge innta en posisjon hvor de benytter seg av avskrekking gjennom nektelse – litt i tråd med den man i dag forholder seg til. Oppgavens analyse har derimot identifisert at dette alene sannsynligvis ikke er tilstrekkelig for å avskrekke fremtidige russiske cyberangrep. Til det er ikke Norges motstandskraft tilstrekkelig. Strategien mislykkes fordi motstanderens kost-nytte vurdering ikke går i Norges favør.

Avskrekking innen cyberdomenet skaper store utfordringer, men det er ikke umulig. Det å forholde seg statisk til de tradisjonelle strategiene ser ut til å medføre at forsvarlig avskrekking mislykkes. De tradisjonelle teoriene kan, så lenge de opptrer dynamiske i møtet med de til enhver tid største truslene gi allsidig avskrekking. En viktig suksessfaktor vil uansett være strategisk og politisk styring preget av kontinuitet og forutsigbarhet. Hvis ikke vil effektene ikke være kontrollerbare. Bruken av aktivt cyberforsvar som avskrekkingsstrategi, vil for Norges del fremover kunne skape et motstridende ønske mellom å holde egne kapasiteter skjult, samtidig som de i noen grad må demonstreres for å oppnå en avskrekkende effekt. Ved å ikke tillate motstandere å operere konsekvensfritt i eget nettverk, og med en mer offensiv tilnærming, i kombinasjon med defensive tiltak, kan dette ved å bruke strategien aktivt cyberforsvar, bidra til å forhindre, avdekke og håndtere cyberangrep.

Norge vil sannsynligvis også i fremtiden stå ovenfor et opportunistisk Russland som søker å utføre sine cyberangrep på en fordekt måte. Norge vil måtte håndtere alle utfordringene dette medfører. Problemet med attribusjon, proporsjonalitet og kontrollerbarhet av en eventuell respons vil fortsatt være like aktuelt. I et kort tidsperspektiv vil Norge trolig ikke være tjent med å gå inn i en situasjon med eskalerende cyberangrep med Russland. Til det fremstår ikke Norge i dag å inneha nødvendige kapasiteter. Norge bør også være forberedt på en ytterligere eskalering i bruken av sammensatte trusler. Oppgavens analyse har vist at Russland i mindre og mindre grad har noe å tape på for eksempel økonomiske eller diplomatiske sanksjoner. Norges tidligere diplomatiske sanksjoner har skapt nye utfordringer for Russland, hvor de trolig vil søke å opprettholde sitt informasjonstilfang. Dette må derimot gjøres på andre, kanskje mer fordekte måter enn tidligere, hvilket kan innebære en intensivering av cyberangrep mot Norge.

Norge burde videreutvikle NESS slik at man etablerer en overordnet funksjon som ivaretar vurderingen av sikkerhetspolitisk risiko knyttet til egne nasjonale sikkerhetsinteresser. Norge bør i større grad søke å underlegge samtlige sentrale virksomheter eller tjenester som støtter kritisk infrastruktur sikkerhetsloven, slik at de settes bedre i stand til å håndtere cyberangrep mot egen virksomhet. Man burde samtidig sørge for at hemmelighold ikke går på kompromiss med informasjonsdeling. Dersom de som står i førstelinjen i håndteringen av cyberangrep sitter på rettidig informasjon om det til enhver tid aktuelle trusselbilde, vil dette styrke totalforsvarets motstandsdyktighet. I forbindelse med organisering av kapasiteter, er det sentralt at man sørger for at håndtering- og responsmulighetene ikke hemmes av utfordringer med strukturelle og juridiske mandater. Videreutvikling av et etterretning- og sikkerhetssenter kan bidra til å håndtere det som i dag fremstår som et utfordrende ansvarsskille i håndteringen av cyberhendelser, der cyberangrep utfordrer skillelinjene mellom statssikkerhet og samfunnssikkerhet. Det avgjørende er at man klarer å bygge og vedlikeholde et sivilt tverrsektorielt situasjonsbilde for å kunne samordne både vertikalt og horisontalt.

Et av oppgavens funn peker på at norske myndigheter i større grad burde ta et sentralt ansvar. Det er uheldig at ansvaret i for stor grad desentraliseres ned til hver enkelt virksomhet. Dette er et funn som også understøttes av Riksrevisjonens konklusjoner i deres rapport om blant annet Norges cyberstrategi. Kompleksiteten i det å opprettholde en troverdig avskrekkingskapasitet understreker viktigheten av sentral oppfølgning, prioriteringer og vurderinger.

Uttalelsene som statsminister Jonas Gahr Støre kom med sommeren 2023 om at hans regjering er under angrep, bør av norske myndigheter ses på som et vendepunkt i innsatsen med å sikre

norske interesser mot cyberangrep. Det stadig mer digitaliserte norske samfunnet skaper nye handlingsrom, men også nye sårbarheter og trusler. Sikkerhet og robusthet skapes best sammen – for Norges del i Totalforsvarsrammen. Ved å benytte oss av samfunnets samlede innsats, sammen med våre allierte, kan vi bygge et mer robust og sterkere cyberforsvar og dermed sikre en tryggere fremtid for alle.

Oppsummert fremstår Norge i dag ikke i stand til å avskrekke Russlands bruk av cyberangrep. Landet forholder seg i for stor grad til utilstrekkelige avskrekkingsstrategier. Norges strategiske respons har skapt et farlig handlingsrom for russiske trusselaktører. Manglende responsmuligheter knyttet til attribusjonsproblematikk, kan på sikt medføre utfordringer for norske sikkerhetspolitiske interesser. Til slutt vil den akkumulerte mengden av cyberrelaterte hendelser kreve en reaksjon for å unngå en innforstått aksept for at Russland får definisjonsmakten til å bestemme hva som skal være akseptert atferd innen cyberdomenet.

Dette må vi for all del unngå.

REFERANSER

Aannø, S., T. (2018). *Strategisk avskrekking i det digitale rom: Finnes det rasjonelle strategier for små stater?* [Masteroppgave]. Forsvarets Høgskole

Aftenposten (2018, 14. oktober). Nederlandsk minister mener landet er i cyberkrig med Russland. https://www.aftenposten.no/verden/i/BJ93L7/Nederlandsk-minister-mener-landet-er-i-cyberkrig-med-Russland

Aftenposten (2023, 7. august). Støre om cybertrusler: – Regjeringen står under angrep. https://www.aftenposten.no/norge/politikk/i/VPBkbV/stoere-om- cybertrusler-regjeringen-staar-under-angrep

Asdal, K., Reiertsen, H. (2020). *Hvordan gjøre dokumentanalyse. En praksisorientert metode*. Oslo: Cappelen Damm Akademisk.

Bakke, S. (2023, 12. juni). Trenger Norge en ny nasjonal cyberstrategi? *DN*. https://www.dn.no/innlegg/etterretningstjenesten/nils-andreas-stensones/cybersikkerhet/trenger-norge-en-ny-nasjonal-cyberstrategi/2-1-1464982

Barnes, J., E., Gibbons-Neff, T. (2019, 22. juni). U.S. Carried Out Cyberattacks on Iran. *The New York Times.* https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html

Belfer Center (2020). *National Cyber Power Index 2020* https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

Bratberg, Ø. (2021). *Tekstanalyse for samfunnsvitere* (3. utg) Cappelen Damm akademisk.

Bryman, A. (2016). *Social research methods* (5. utg). Oxford University Press.

CCDCOE (2015). *Office of Personell Management data breach (2015)* https://cyberlaw.ccdcoe.org/wiki/Office_of_Personnel_Management_data_breach_(2015)

Central Bureau voor de Statistiek (2022). *Cybersecuritymonitor 2021*. https://www.cbs.nl/nl-nl/longread/rapportages/2022/cybersecuritymonitor-2021/4-cybercrime

Cyber Law Toolkit A (2023). *Attribution*. https://cyberlaw.ccdcoe.org/wiki/Attribution

Cyber Law Toolkit B (2023). *Cyber-attacks against Estonia (2007).* https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007)

Departementene (2019). *Nasjonal strategi for digital sikkerhet.* https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

Department of Defence (2018). *Summary – Cyber Strategy* https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Dinniss, H., H. (2012). *Cyber Warfare and the Laws of War.* Cambridge University Press

Egloff, F. J. (2020). *Public attribution of cyber intrusions.* Journal of Cybersecurity. https://doi.org/10.1093/cybsec/tyaa012

Elspeth D., B., Smith, H., A. (2018). *North Atlantic Treaty Organization: Challenges to Collective Defense in Cyberspace.* American Intelligence Journal. Vol. 35, No. 2, Counterintelligence and the Insider Threat (2018)

Etterretningstjenesten (2023a). *Talentprogram cyberoperasjoner.* https://www.etterretningstjenesten.no/jobb-og-karriere/cybertalent

Etterretningstjenesten (2023b). *Fokus 2023.* https://www.etterretningstjenesten.no/publikasjoner/fokus/innhold

Equinor (2023). *Landanlegg.* https://www.equinor.com/no/energi/landanlegg

European Commission (2022). *The Digital Economy and Society Index — Countries' performance in digitization.* https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

Fausko, L., Holmes, M., C., S. (2020, 14. oktober). Russisk ambassade: - En alvorlig provokasjon. *VG.* https://www.vg.no/nyheter/innenriks/i/x3Pb7R/russisk-ambassade-en-alvorlig-provokasjon

FFI (2022a). *Kort forklart. Hva er totalforsvaret?* https://www.ffi.no/aktuelt/podkaster/kort-forklart-hva-er-totalforsvaret

FFI (2022b). *Hva kan Norge lære av andre lands tilnærming til sammensatte trusler – rapport til Forsvarskommisjonen. 22/02310*.

https://ffipublikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/3088/22-02310.pdf

FN-pakten. (1945). *De Forente Nasjoners Pakt (26-06-1945 nr 1 Multilateral).* Lovdata. https://lovdata.no/dokument/TRAKTAT/traktat/1945-06-26-1

FN (2021). *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution*. https://ccdcoe.org/uploads/2018/10/UN_-Official-compendium-of-national-contributions-on-how-international-law-applies-to-use-of-ICT-by-States_A-76-136-EN.pdf

Forsvarsdepartementet (2014) Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner I forsvarssektoren "FDs cyberretningslinjer". Hentet 8. august 2023 fra: https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf

Fridman, O. (2018). *Russian Hybrid Warfare – Resurgence and politicization*. C. Hurst & Co.

Friis, K. (2020). *Offensive cyberoperasjoner: Den nye normalen?* Økonomi & politik. 2020, 93 (3), 30-44. https://nupi.brage.unit.no/nupi-xmlui/handle/11250/2684974

Furseth, I., Everett, E., L. (2020). *Masteroppgaven – Hvordan begynne- og fullføre.* (3. utgave). Universitetsforlaget

Gibson, J. S. (1957). *ARTICLE 51 OF THE CHARTER OF THE UNITED NATIONS. India Quarterly, 13*(2), 121–138. http://www.jstor.org/stable/45067909

Global Firepower (2023). *2023 Military Strength Ranking.* https://www.globalfirepower.com/countries-listing.php

Government of Canada (2022). *International Law applicable in cyberspace*. https://www.international.gc.ca/world-monde/issues_development enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng

Greenberg, A. (2019). Sandworm - *A new era of cyberwar and the hunt for the Kremli's most dangerous hackers.* Anchor Books

Hayward, R. J. (2017). *EVALUATING THE "IMMINENCE" OF A CYBER ATTACK FOR PURPOSES OF ANTICIPATORY SELF-DEFENSE*. Columbia Law Review, 117(2), 399–434. http://www.jstor.org/stable/44159464

Hellestveit, C. (2022). Folkerett i det digitale rom. I Bergsjø, H., & Friis, K. (red). *Digitalisering og internasjonal politikk.* (s. 121-147) Universitetsforlaget

Hem, M. (2023 11. juli) Freden innad i Nato er truet. *Forsvarets forum.* https://www.forsvaretsforum.no/analyse-nato-utenriks/freden-innad-i-nato-er-truet/335370

HM Government (2022). *Government Cyber Security Strategy – Building a cyber resilient public sector.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf

Hovi, J. (2020). *Spillteori – En innføring* (2. utg). Universitetsforlaget

Humanize (2023). *The 10 Most Powerful Cyber Nations in the World.* https://www.humanize.security/blog/cyber-awareness/the-10-most-powerful-cyber-nations-in-the-world#TheNetherlands

ICJ (1986). *Case concerning military and paramilitary acitivites in and against Nicaragua.* https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

Institute for Strategic Studies (2023). *The military balance.* Institute for Strategic Studies.

Institute for Strategic Studies (2019). *The military balance.* Institute for Strategic Studies.

ITU Publications (2018). *Global Cybersecurity Index (GCI) 2018.* https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Jasper, S. (2017). *Strategic Cyber Deterrence – The active cyber defense option.* Rowman & Littlefield

Jervis, R. (1979). *Deterrence Theory Revisited*. World Politics, 31(2), 289–324. https://doi.org/10.2307/2009945

Johannessen, A., Christoffersen, L., Tufte, P.A. (2011*). Forskningsmetode for økonomiskadministrative fag* (3. utgave). Abstrakt Forlag

Johansen. P., A. (2020). Regjeringen: Russland sto bak dataangrep på Stortinget. *Aftenposten.* https://www.aftenposten.no/norge/i/39JXme/regjeringen-russland-sto-bak-dataangrep-paa-stortinget

Johnson, D. E., Schmitt, M. N. (2021). *Responding to Proxy Cyber Operations Under International Law.* The Cyber Defense Review, 6(4), 15–34. https://www.jstor.org/stable/48631304

Knudsen, E. (2023, 15. februar). Knuser alle rekorder: Dette er det kraftigste tjenestenektangrepet noensinne. *DIGI.* https://www.digi.no/artikler/knuser-alle-rekorder-dette-er-det-kraftigste-tjenestenektangrepet-noensinne/526365

Kristiansen, M., Hoem, N. (2022). *Small players in a limitless domain: Cyber deterrence as small state strategy.* Comparative Strategy, 41(1), 19–31. https://doi.org/10.1080/01495933.2021.2017740

Lebow, R., N. (1985). *Conclusions. I psychology & deterrence.* Johns Hopkins University Press.

Lebow, R. N. (2007). *Thucydides and Deterrence.* Security Studies, 16(2), 163–188. https://doi.org/10.1080/09636410701399440

Liebetrau, T. (2022). *Organizing cyber capability across military and intelligence entities: Collaboration, separation, or centralization*. Policy Design and Practice. https://doi.org/10.1080/25741292.2022.2127551

Lillegård, H. (2023, 28. august) – Det aller største angrepsmålet. *Dagbladet.* https://www.dagbladet.no/nyheter/det-aller-storste-angrepsmalet/80060345

Lyngaas, S. (2023, 15. juni). Exclusive: US government agencies hit in global cyberattack. *CNN.* https://edition.cnn.com/2023/06/15/politics/us-government-hit-cybeattack/index.html

Mastekaasa, A. (2010). *Sosial bakgrunn og suksess i yrkeslivet.* Universitetsforlaget.

Mauno, H. (2022, 17. mars). Det er mye man kan gjøre uten å starte en full krig. *Dagsavisen.* https://www.dagsavisen.no/nyheter/2022/03/17/det-er-mye-man-kan-gjore-uten-a-starte-en-full-krig/

Melby, G. (2022, 28. September). Heldigvis fant regjeringen ut at de hadde det øverste ansvaret for Norges sikkerhet. *TV2.* https://www.tv2.no/mening_og_analyse/heldigvis-fant-regjeringen-ut-av-de-hadde-det-overste-ansvaret-for-norges-sikkerhet/15143711/

Meld. St. 7 (2012). *Nordområdene – Visjon og virkemidler*. Det kongelige utenriksdepartementet

Midtgaard, K. (1967). *Strategisk tenkning – Noen spillteoretiske emner med særlig tanke på internasjonal politikk.* Norsk utenrikspolitisk institutt

Miles, B. M., Huberman, A. M. & Saldana, J. (2020). *Qualitative Data Analysis – A Methods Sourcebook* (4 utgave). Sage Publications

Ministerie van Defensie (2018). *Defensie Cyuber Strategie 2018 – Invensteren in degitale slagkracht voor Nederland*. https://www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018

Ministy of Defence (2018). *GRU close access cyber operation against OPCW*. https://english.defensie.nl/topics/cyber-security/russian-cyber-coperation

Ministry of Justice and Security (2022). *The Netherlands Cybersecurity Strategy 2022-2028.* https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands- cybersecurity-strategy-2022-2028

Moe, H. (2023). Ikke bedriftenes ansvar å utforme sikkerhetspolitikken. *DN.* https://www.dn.no/innlegg/jus/politikk/sikkerhetsloven/ikke-bedriftenes-ansvar-a-utforme-sikkerhetspolitikken/2-1-1535499

Moore, D. (2022). *Offensive Cyber Operations*. Hurst Publishers.

Morgan, P. (2012). *The State of Deterrence in International Politics Today*. Contemporary Security Policy, 33(1), 85-107. https://www.tandfonline.com/doi/full/10.1080/13523260.2012.659589

Muller, L., P., Gjesvik, L., Friis, K. (2018). *Cyber-weapons in International Politics: Possible sabotage against the Norwegian petroleum sector.* https://www.nupi.no/en/publications/cristin-pub/cyber-weapons-in-international-politics-possible-sabotage-against-the-norwegian-petroleum-sector

Muller, L., P (2019). *Military Offensive Cyuber-Capabilities: Small-State Perspectives.* NUPI: Policy Brief (1/2019).

NATO (2023). *NATO Strategic Concept 2023.* https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO (2021). Brussels Summit Communiquè. Hentet 6. Jul 2023 fra: https://www.nato.int/cps/en/natohq/news_185000.htm

NATO / Atlanterhavspakten. (1949). *Traktat for det nordatlantiske området (04-04-1949 nr 1 Multilateral).* Lovdata. https://lovdata.no/dokument/TRAKTAT/traktat/1949-04-04-1

NATOCCDCOE (2023, 19. jun). Evolution of Strategy: Can Policy Makers Keep Up? [Video] Youtube. https://www.youtube.com/watch?v=EF7T0NjeVSQ

Niemann, A., Lefkofridi, Z. & Schmitter, P., C. (2019). Liberal Intergovernmentalism. 64-87 i Wiener, A., Börsel, T., A. & Risse, T. (2019). European Integration Theory. (3. utg). Oxford University Press

Nilsen, V. (2012). *Analyse i kvalitative studier – Den skrivende forskeren*. Universitetsforlaget.

Norum, H., Ulvin, P., B., Hestenes, S., G., Skei, L., Henriksen, T., K., Årtun, A., B., Kruse, J., E., Ekern, S. (2022, 29. juni). Russisk hackergruppe skal ha startet angrep mot Norge. *NRK.* https://www.nrk.no/norge/russisk-hackergruppe-skal-ha-startet-angrep-mot-norge-1.16020947

NOU 2023:17 (2023). *Nå er det alvor – Rustet for en usikker fremtid.* Departementenes sikkerhets- og serviceorganisasjon. https://www.regjeringen.no/contentassets/4b9ba57bebae44d2bebfc845ff6cd5f5/no/pdfs/nou202320230017000dddpdfs.pdf

NOU 2015:13 (2015). *Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden.* Justis- og beredskapsdepartementet https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

NSM (2022a). *Målrettede tjenestenektangrep mot norske nettsteder.* https://nsm.no/aktuelt/malrettede-tjenestenektangrep-mot-norske-nettsteder

NSM (2022b). *Cyberangrep har blitt hverdagskost*.https://nsm.no/aktuelt/digitalt-risikobilde-2022-cyberangrep-har-blitt-hverdagskost

NSM (2023). *Nasjonalt digitalt risikobilde 2023.* https://nsm.no/getfile.php/1313382-1697777843/NSM/Filer/Dokumenter/Rapporter/Nasjonalt%20digitalt%20risikobilde%202023.pdf

Nye, J. S., Jr. (2017). *Deterrence and Dissuasion in Cyberspace.* International Security, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Pedersen, T. (2023). *A Small State's Cyber Posture: Deterrence by Punishment and Beyond.* https://www.researchgate.net/publication/371350319_A_Small_State's_Cyber_Posture_Deterrence_by_Punishment_and_Beyond

Pruckovà, M. (2022). *Cyber-attacks and Article 5 – a note on a blurry but consistent position of NATO.* https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/

PST (2023). *Nasjonal trusselvurdering 2023*. https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2023/

Quackenbush, S., L., Zagare, F., C. (2015). *Modern Deterrence Theory: Research Trends, Policy Debates, and Methodological Controversies.* Oxford Handbook Topics in Politics. https://doi.org/10.1093/oxfordhb/9780199935307.013.39

Rachlew, A. (2009). *Justisfeil ved politiets etterforskning – noen eksempler og forskningsbaserte mottiltak.* [Ph.d. avhandling]. Den juridiske fakultetet, UiO.

Regjeringen (2022). *Forsterket innsats mot sammensatte trusler.* https://www.regjeringen.no/no/aktuelt/forsterket-innsats-mot-sammensatte-trusler/id2949146/

Rid, T., Buchanan, B. (2014). *Attributing Cyber Attacks*. Journal of Strategic Studies, 38, 1–2, 4–37. https://doi.org/10.1080/01402390.2014.977382

Riksrevisjonen (2023). *Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor.* Dokument 3:7 (2022–2023) https://www.riksrevisjonen.no/globalassets/rapporter/NO-2022-2023/myndighetenes-samordning-av-arbeidet-med-digital-sikkerhet-i-sivil-sektor.pdf

Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare* (2. Utg), Cambridge University Press

Schulze, M (2019). *Cyber Deterrence is Overrated*. https://www.swp-berlin.org/publications/products/comments/2019C34_she.pdf

Skei, L., Tønset, T., S. (2021, 26. desember). E-sjefen: Russland fortsetter de digitale angrepene. *NRK.* https://www.nrk.no/norge/den-norske-etterretningssjefen_-russland-fortsetter-de-digitale-angrepene-1.15782971

Smeets, M. (2022). *No Shortcuts – why states struggle to develop a military cyber-force.* C. Hurst & Co

Snyder, G. H. (1961). *Deterrence and defense: toward a theory of national security*. Princeton University Press.

SIPRI (2023). *SIPRI Military Expenditure Database.* https://milex.sipri.org/sipri

Sperandei, M. (2006). *Bridging Deterrence and Compellence: An Alternative Approach to the Study of Coercive Diplomacy*. International Studies Review, 8(2), 253–280. http://www.jstor.org/stable/3880225

Strand, S. (2022). Strategisk kommunikasjon av cyberkapasiteter. I Bergsjø, H. & Friis, K. (red). *Digitalisering og internasjonal politikk.* (s. 43-61). Universitetsforlaget.

Strand. T. (2022). Sikkerhetslovens «far»: – Svært uheldig at vi har tapt så mye tid. *Aftenposten.* https://www.nrk.no/norge/sikkerhetslovens-far_-_-oljebransjen-er-ikke-godt-nok-forberedt-1.16129483

Støyva., A., B., Wikan. V., S. (2023). Nasjonal sikkerhetsmyndighet: Hackere hadde tilgang til plattform brukt av departementene i over to måneder. *Aftenposten.* https://www.aftenposten.no/norge/i/gEOEL1/nasjonal-sikkerhetsmyndighet-hackere-hadde-tilgang-til-plattform-brukt-av-departementene-i-over-to-maaneder

Svenungsen, B. (2022). Digitalisering av det militære: militære cyberkapabiliteteter. I Bergsjø, H., Friis, K. (red). *Digitalisering og internasjonal politikk.* (s. 25-43). Universitetsforlaget

Tertrais, B. (2016). *Article 5 of the Washington Treaty: Its Origins, Meaning and Future*. NATO Defense College. http://www.jstor.org/stab_le/resrep10238

The White House (2023). *National Cybersecurity Strategy.* https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Thorsheim, P. (2016, 29. mars). Uheldig at Norge skal ha så mange CERT. *DIGI.no* https://www.digi.no/artikler/uheldig-at-norge-skal-ha-sa-mange-cert/348176

Tjora, Aksel (2020*). Kvalitative forskningsmetoder i praksis*. (3. utgave). Gyldendal Norsk Forlag

Tor, U. (2017). *Cumulative Deterrence as a New Paradigm for Cyber Deterrence.* Journal of Strategic Studies, 40(1-2), 92-117. https://doi.org/10.1080/01401290.2015.1115975

Underdal, A. (2007). Internasjonale forhandlinger, i Hovi, J. og Malnes, R. (red.) *Anarki, makt og normer: innføring i internasjonal politikk.* Abstrakt Forlag

United Nations (2021). *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/26.* https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

U.S. President (2018). *National Cyber Strategy 2018.* White House: Washington DC. https://trumpwhitehouse.archives.gov/wp- content/uploads/2018/09/National-Cyber-Strategy.pdf

Utenriksdepartementet (2017). *Internasjonal cyberstrategi for Norge.* https://www.regjeringen.no/no/dokumenter/cyberstrategi/id2569056/

Uthoff, C. S. (2021). *Cyber intelligence: Actors, policies, practices*. Lynne Rienner Publishers.

Waltz, K. N. (2012). *Why Iran Should Get the Bomb: Nuclear Balancing Would Mean Stability*. Foreign Affairs, 91(4), 2–5. http://www.jstor.org/stable/23218033

Westersø, R., S. (2022, 5. April). Danmark udviser 15 russiske diplomater for sponage. *TV2. https://nyheder.tv2.dk/politik/2022-04-05-danmark-udviser-15-russiske-diplomater-for-spionage*

Whyte, C. (2020). *Beyond tit-for-tat in cyberspace: Political warfare and lateral sources of escalation online.* European Journal of International Security, 5(2), 195–214. https://doi.org/10.1017/eis.2020.2

Wilhelmsen, V., R., Larsen, T., Soldal Lund, M., Svenungsen, B., Aannø, S., T. (2021). Jakten på Norges militære cyberstrategi. I Heier. T. (red) *Militærmakt i Nord.* (s. 242-263). Universitetsforlaget.

Zagare, F., C., Kilgour, D., M. (2000). *Perfect deterrence theory*. Cambridge University Press

Øverland, I. (2009). *Georgia og Russland.* https://www.nupi.no/skole/hhd-artikler/2009/georgia-og-russland