FFI Forsvarets forskningsinstitutt

24/01194

FFI-RAPPORT

Statsvitenskapelige perspektiver på cyberoperasjoner

– en gjennomgang av sentral litteratur

Mathilde Israelsen

Statsvitenskapelige perspektiver på cyberoperasjoner
– en gjennomgang av sentral litteratur

Mathilde Israelsen

Forsvarets forskningsinstitutt (FFI) 17. september 2024

Emneord
Cyberoperasjoner
Cybermakt
Statsvitenskap

FFI-rapport
24/01194

Prosjektnummer
1715

Elektronisk ISBN
978-82-464-3552-7

Engelsk tittel
Perspectives in Political Science on Cyber Operations: A Review of Key Literature

Godkjennere
Tormod K. Sivertsen, *forskningsleder*
Ronny Windvik, *forskningssjef*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Opphavsrett
© Forsvarets forskningsinstitutt (FFI). Publikasjonen kan siteres fritt med kildehenvisning.

Sammendrag

Denne rapporten beskriver og diskuterer sentrale bidrag i den statsvitenskapelige litteraturen om staters bruk av cyberoperasjoner som et maktmiddel i internasjonal politikk. Rapporten er delt inn etter litteratur som diskuterer endring av maktbalansen, cyberoperasjoner som et middel for signalering av intensjoner til andre stater, og mulighetene for tilsiktet og utilsiktet eskalering som en følge av cyberoperasjoner mellom stater.

De sentrale perspektivene i bidrag som dekker disse aspektene kan oppsummeres på følgende måte:

- Cyberdomenet utgjør et unikt strategisk miljø. Dette er kjennetegnet av aktiviteten vedvarende innsats, som gjennom effekter mot motstanderes systemer kan endre maktbalansen og etablere rammer for akseptabel atferd i cyberdomenet.

- En rekke eller serier, omtalt som kampanjer, av cyberoperasjoner kan bidra til å endre maktbalansen mellom stater. Derfor bør de overordnede effektene av cyberoperasjoner analyseres i et kampanjeperspektiv.

- Cyberoperasjoner kan være strategisk nyttige, men operasjonelle avveininger legger begrensninger på den reelle effekten. Aktøren må balansere mellom styrken og omfanget av effektene, tidsbruk mellom starten på operasjonen og øyeblikket ønsket effekt er oppnådd, og kontroll over egen operasjon. Denne balansegangen innebærer blant annet at en kortere tidsramme på operasjonen, vil føre til redusert effekt og kontroll

- Problematikk knyttet til attribusjon av en cyberhendelse til en aktør begrenser mulighetene for å benytte dette virkemiddelet for å oppnå avskrekking og tvang av en annen stat. Dette innebærer at cyberoperasjoner benyttes for å hindre at en annen stat handler på en bestemt måte, eller for å få den andre staten til å endre handlemønster. I tillegg svekkes potensialet for disse effektene som følge av problematikk knyttet til å oppnå en tilstrekkelig sterk effekt som en følge av cyberoperasjoner.

- Hvorvidt cyberoperasjoner er aktivitet som påvirker stabiliteten mellom stater avhenger av hvordan beslutningstagere oppfatter situasjonen og hvorvidt relasjonen mellom to stater er preget av generell stabilitet eller ustabilitet. Oppfatninger og kontekst må dermed tas med i betraktning når mulige følger av cyberoperasjoner skal vurderes.

Summary

This report describes and discusses key contributions in the political science literature on the use of cyber operations as a tool of power and influence in international politics. The report is divided into literature that analyses the potential for a change in the balance of power as a result of cyber operations, cyber operations as a means of signalling intentions to other states, and the possibilities of intentional and unintentional escalation resulting from the use of cyber operations between states.

Key perspectives in contributions to the literature covering these aspects can be summarised as follows:

- The cyber domain constitutes a unique strategic environment. It is characterised by persistent engagement, which, by applying effects to important digital systems of the opponent, may change the balance of power and establish norms for acceptable behaviour in the domain.

- A sequence or series of cyber operations, described as campaigns, may contribute to altering the balance of power between states. This means that cyber operations can accumulatively alter the balance of power. Thus, the argument goes that cyber operations should be analysed in a campaign perspective.

- Cyber operations can be strategically useful, but operational trade-offs limit their actual impact. The actor must balance the intensity and scope of the effects, the time from the start of the operation to the moment the desired effect is achieved, and control over their own operation. This trade-off involves, among other things, that a shorter timeframe of the operation will result in reduced control over and effects of the operation.

- The difficulty of attributing a cyber operation limits the possibilities of using this as an instrument for deterrence or coercion against another state. Additionally, the potential for coercive effects or deterrent effects is weakened by the difficulty of achieving a sufficiently strong impact using cyber operations.

- Whether cyber operations affect the stability between states depends on how decision-makers perceive the situation and whether the relationship between two states is characterised by stability or instability. Perceptions and context must therefore be considered when assessing the possible consequences of cyber operations.

Innhold

1 Innledning

Denne rapporten kartlegger og diskuterer det jeg anser som sentrale bidrag i den statsvitenskapelige litteraturen om cyberoperasjoner som et statlig maktmiddel. Gjennomgangen vektlegger perspektiver knyttet til den strategiske nytten ved cyberoperasjoner for å oppnå politiske målsettinger. Disse perspektivene er delt inn i hvordan cyberoperasjoner kan oppnå endringer i maktforholdet mellom stater, og hvordan de kan benyttes for signalering av intensjoner og vilje til bruk av makt, blant annet i form av tvang og avskrekking. Videre omhandler noen av bidragene hvordan cyberoperasjoner kan inngå i militære operasjon, og dermed hvordan de kan ha operasjonell nytte. Til sist beskriver og diskuterer jeg perspektiver i litteraturen knyttet til hvordan cyberoperasjoner kan resultere i tilsiktet eller utilsiktet eskalering mellom stater.

En gjennomgang av sentral litteratur er nyttig for å legge et grunnlag for å videreutvikle forståelsen av cyberoperasjoner som et statlig maktmiddel. Den statsvitenskapelige litteraturen om cyberoperasjoner er relativt ung. De fleste bidragene som fortsatt henvises til er utgitt etter 2010. Dette betyr at den konseptuelle utviklingen er i en tidlig fase, som medfører at majoriteten av de sentrale bidragene fokuserer teoretisk utvikling. Dette innebærer at litteraturen er rettet mot hvordan statsvitenskapen kan forstå cyberoperasjoner som et fenomen, og utvikling av rammeverk for å kunne analysere dette fenomenet. For å utvikle rammeverk blir ofte noen perspektiver utelatt. Å fremheve hvilken type nyanser som kan bli utelatt i utviklingen av rammeverk kan bidra til å danne et grunnlag for å utvikle forståelsen av cyberoperasjoner. Videre vil konseptuell utvikling gjerne sette konseptet implisitt inn i en kontekst. Det kan være nyttig å være klar over denne konteksten, da det gjerne inkluderer bestemte antagelser. Denne litteraturgjennomgangen vil gjennomgå konteksten, og hva det kan ha å si for forståelsen av cyberoperasjoner som et statlig maktmiddel.

I beskrivelser av staters bruk av cyberoperasjoner blir det ofte gjort et skille mellom cyberoperajoner for effekt og cyberoperasjoner for etterretning. Den førstnevnte typen har som mål å skape en direkte effekt i motstanderens systemer, mens den andre typen søker å hente ut informasjon fra eller overvåke systemer. Den statsvitenskapelige litteraturen fokuserer hovedsakelig på cyberoperasjoner for effekt (se eks. Borghard og Lonergan, 2017, 2023; Buchanan og Cunningham, 2020; Libicki og Tkacheva, 2020). Noen bidrag de seneste årene har imidlertid undersøkt cyberoperasjoner for etterretning (se eks. Chesney & Smeets, 2023). I andre tilfeller omtaler forfatterne cyberoperasjoner som et overordnet fenomen – de skiller ikke mellom effekt og etterretning (se eks. Harknett og Smeets, 2022). Jeg vil i denne litteraturgjennomgangen inkludere bidrag som beskriver nytten av både cyberoperasjoner for effekt og etterretning.

Rapporten gjennomgår det jeg anser som sentrale deler av de statsvitenskapelige bidragene. Dette gir et smalere utvalg, men det muliggjør en dypere gjennomgang av hvert enkelt bidrag, samt en kritisk diskusjon av disse bidragene. De sentrale bidragene har bidratt til å forme forståelsen av staters nytte av cyberoperasjoner. Derfor er en grundig gjennomgang av disse bidragene nødvendig for å forstå hvilke perspektiver som har formet oppfatningen av staters

bruk av cyberoperasjoner, samt legge et grunnlag for videre utvikling eller endring av denne forståelsen.

Jeg deler litteraturen inn i fem hovedområder:

I. Hvordan cyberoperasjoner kan endre maktforholdet mellom stater, samt aspekter som legger begrensninger på dette potensialet

II. Operasjonelle og institusjonelle begrensninger ved å oppnå strategisk nytte gjennom cyberoperasjoner

III. Hvordan cyberoperasjoner kan fungere som et operasjonelt og taktisk virkemiddel

IV. Hvordan og hvorvidt cyberoperasjoner kan benyttes for å påvirke andres staters handlemåte ved å fungere som et virkemiddel for signalering

V. Hvordan og hvorvidt cyberoperasjoner kan resultere i tilsiktet eller utilsiktet eskalering mellom stater

2 Metode

Utvalget av litteratur for denne gjennomgangen ble gjennomført i to steg. Første steg innebar søk i databasen Web of Science etter «cyber», «cyber attack», «cyber operations» og «offensive cyber operations». Søket ble avgrenset til kategoriene «political science» og «international relations», treff i titler, abstrakter og selve teksten.

Databasen Web of Science inneholder hovedsakelig fagfellevurderte artikler fra tidsskrifter. Den inneholder ikke rapporter fra forskningsinstitutter som ikke er fagfellevurderte eller doktorgradsavhandlinger l. Dette begrenser utvalget. For å få et innblikk i omfanget av det som mulig blir utelatt gjennom det første søket, utførte jeg samme søk i Google Scholar. Det var imidlertid i stor grad overlapp i hvilke publikasjoner som kom opp i de to søkene. Etter å ha fått et overblikk over litteraturen, valgte jeg å tidsmessig avgrense utvalget til publikasjoner utgitt mellom 2017 og 2024. Dette valget ble gjort for å begrense omfanget for å gjøre det mulig å kritisk diskutere bidragene. I tillegg har jeg vurdert det som viktig å fokusere på den litteraturen som har formet den nåværende forståelsen av staters bruk av cyberoperasjoner. Litteraturen er i stor grad teoribasert, og dermed har forståelsen endret seg i møte med ny empiri. Dette gjør at forståelsen av nytten ved cyberoperasjoner som et statlig maktmiddel har gått gjennom store endringer. Derfor ble det gjort et valg om å ikke ta med eldre litteratur.

Det andre steget besto av å vurdere hva som er de sentrale bidragene i den statsvitenskapelige litteraturen om cyberoperasjoner. Jeg har valgt å legge til en kvalitativ vurdering til grunn for utvalget av litteratur. Dette betyr at publikasjoner som har blitt løftet frem og diskutert i ulike anerkjente fora, blir lagt ekstra vekt på. Vurderingen av hva som er anerkjente fora stammer fra erfaring etter å ha fulgt tematikken over lengre tid. Eksempler på toneangivende fora er Lawfare, Texas National Security Review og Royal United Services Institute (RUSI). Valget om å ta utgangspunkt i en kvalitativ vurdering for utvalget av litteratur er gjort for å kunne diskutere og klargjøre bidrag som har vært toneangivende for den rådende forståelsen av staters bruk av cyberoperasjoner.

3 Endring av maktforholdet mellom stater

I litteraturen som analyserer nytte av cyberoperasjoner er et mye diskutert spørsmål om, og i så fall hvordan, cyberoperasjoner kan endre maktforholdet mellom stater. Jeg tar her for meg publikasjoner som argumenterer for at cyberoperasjoner kumulativt kan erodere vekk eller tære på styrken i andre staters maktmidler. Disse bidragene løfter også frem påstander om at cyberoperasjoner kan oppnå strategiske effekter som staten ellers må gå til krig for å oppnå. For å diskutere disse påstandene gjennomgår jeg bidrag som anlegger alternative forståelser av nytten ved cyberoperasjoner, og jeg benytter andre deler av den statsvitenskapelige litteraturen på hva som påvirker relasjoner mellom stater for å ytterligere nyansere de sentrale påstandene. Deretter fremhever jeg bidrag som diskuterer institusjonelle og operasjonelle begrensninger ved å oppnå strategisk nytte av cyberoperasjoner. Til sist beskriver jeg bidrag som analyserer cyberoperasjoner som et taktisk og operasjonelt virkemiddel.

3.1 Vedvarende innsats for å endre maktbalansen mellom stater

I *Cyber Persistence Theory* (2022) presenterer Fischerkeller, Goldman og Harknett et teoretisk rammeverk for å forstå hvordan cyberoperasjoner påvirker relasjoner mellom stater. Teorien bygger på en antagelse om at cyberoperasjoner oppstår i et distinkt strategisk miljø. Forfatterne forstår et strategisk miljø som kjennetegnene ved en teknologi eller sammensetninger av teknologi som på egen hånd (*independently*) har evnen til å opprettholde eller endre fordelingen av makt i det internasjonale systemet. Det distinkte strategiske miljøet skaper bestemte systemiske forhold og bestemte sikkerhetslogikker, og påvirker dermed hele spekteret av mellomstatlig strategisk konkurranse.

Utgangspunktet for denne vurderingen er at teknologien knyttet til konvensjonelle og kjernefysiske våpen skapte strategiske miljø der trusselen om straff og ødeleggelse kunne endre motstanderens handlemønster, såkalt tvang og avskrekking. De strukturelle forholdene i det konvensjonelle strategiske miljøet på et samspill mellom en angreps- eller forsvarsfordel, mens det kjernefysiske strategiske miljøet er basert på å besitte en offensiv dominans. *Cyber Persistence Theory* hevder det cyber-strategiske miljøet kjennetegnes av sammenkobling og konstant kontakt, heller enn tvang og avskrekking. Dette skaper et strategisk miljø der logikken «vedvarende initiativ»[1] råder. Forfatterne legger til grunn at et miljø preget av vedvarende initiativ innebærer at du kun kan forsvare deg i øyeblikket. Dette betyr at det ikke er mulig å etablere et forsvar som vil være effektivt over lengre tid. I stedet må forsvaret opprettholdes og gjenopprettes kontinuerlig. Dette perspektivet omtales her i form av «vedvarende innsats» og «vedvarende initiativ».

Fischerkeller et al. legger til grunn at et strategisk miljø kjennetegnet av «vedvarende initiativ», gir overtaket til aktører som kan forutse utnyttelse av sårbarheter i digitale systemer, og som kan finne og utnytte sårbarheter i andre aktørers digitale systemer. Denne evnen legger et

[1] Min oversettelse av begrepet «*persistent initative*» i *Cyber Persistence Theory.*

grunnlag for å etablere en «vedvarende innsats»[2] i cyberdomenet. Derfor er et sentralt poeng i *Cyber Persistence Theory* at den dominerende strategiske oppførelsen i cyberdomenet er å utnytte andre aktørers sårbarheter for å oppnå en strategisk fordel.

Ut fra disse forutsetningene følger to ulike atferder i cyberdomenet: *cyber fait accomplis*[3] og direkte cyber-innsats.[4] *Cyber fait accomplis* refererer til en begrenset, ensidig fordel oppnådd gjennom en cyberoperasjon som motstanderen ikke er klar over eller ikke har mulighet til å svare på. Fischerkeller et al. omtaler dette som å utføre en effekt med umiddelbar virkning mot systemer, eller å posisjonere seg for å skape en effekt på et fremtidig tidspunkt uten at motstanderen har kjennskap til det. Målet med denne atferden er å fremme en stats interesser ved å påføre effekter på andre staters systemer. Forfatterne fremhever Kinas cyberoperasjoner for å stjele intellektuell eiendom og Nord-Koreas *ransomware*-operasjoner som empiriske eksempler på *cyber fait accomplis* (Ficherkeller, et al., 2022, s. 65–74).

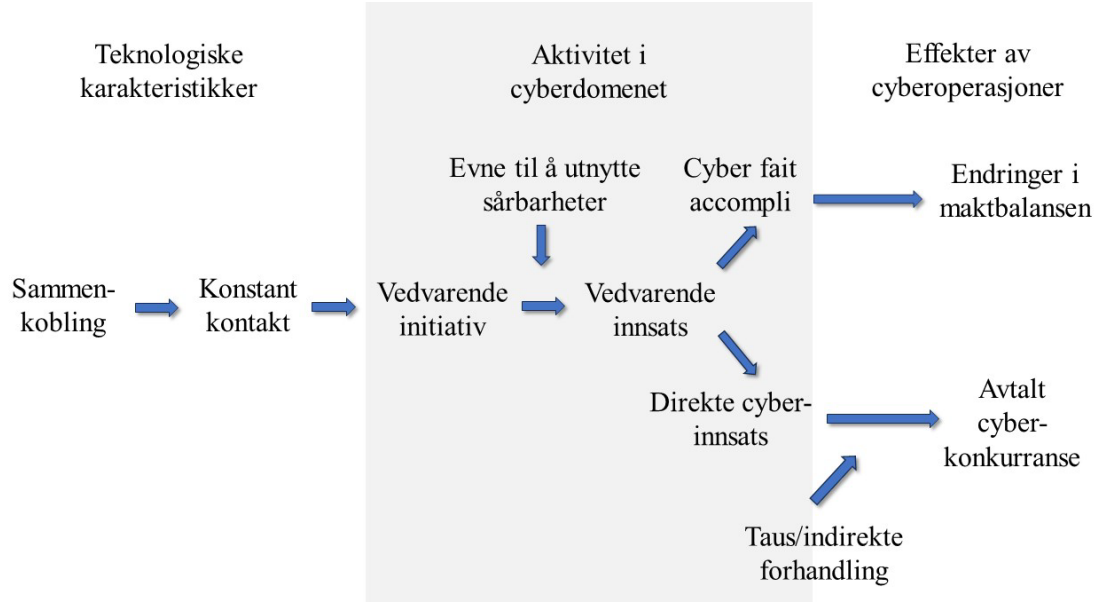
Gjennom cyber fait accompli søker stater å opprettholde eller endre den internasjonale maktbalansen. Ifølge *Cyber Persistence Theory* er det mulig å oppnå denne effekten på grunn av de grunnleggende karakteristikkene ved det strategiske miljøet i cyberdomenet: konstant kontakt og sammenkobling. Dette miljøet gjør at nasjonale kilder til makt er kontinuerlig tilgjengelig for utnyttelse gjennom cyberoperasjoner. Disse forutsetningene gjør det mulig å endre maktbalansen mellom stater direkte gjennom cyberdomenet.

Direkte cyber-innsats referer til å ta kontroll over det forfatterne omtaler som «*key cyberspace terrain*». Fischerkeller et al. (2022) henviser til to former for aktivitet som eksempler på direkte cyberinnsats. Den første er å ta kontroll over motstanderens infrastruktur for utvikling av skadevare, og den andre er å påvirke strategisk viktige systemer, som kommando og kontroll tilknyttet kjernefysiske kapabiliteter (Fischerkeller, et al., 2022, s. 44–45). Hva «kontroll» innebærer i denne sammenhengen definerer ikke forfatterne. *Key terrain* blir i andre taktiske og operasjonelle sammenhenger omtalt som områder som kan gi en tydelig fordel for den som enten angriper eller forsvarer det gitte området (Headquarters, Department of the Army, 2013, s. 25). Ut fra dette kan vi forstå kontroll over *key terrain* som alle former for handlinger som kan gi en fordel overfor motstanderen. Dette kan innebære å nekte eller forstyrre aktørens tilgang til sine systemer og servere, eller selv skaffe tilgang til slik infrastruktur for deretter å deaktivere nettverkene eller korrumpere dataen deres. Følgene av denne atferden beskriver Fischerkeller et al. som indirekte eller taus forhandling.[5] Forhandlingen skjer ved at en stat kommuniserer direkte eller indirekte hva som er akseptabel oppførsel gjennom egen atferd i cyberdomenet, heller enn å kommunisere gjennom formelle eller uformelle diplomatiske kanaler. Ved å kommunisere akseptabel oppførsel gjennom egen atferd, forutser Fischerkeller et al. i *Cyber Persistence Theory* at et akseptabelt konfliktnivå i cyberdomenet vil etableres over tid (2022, s. 45, s. 110–111).

[2] Min oversettelse av begrepet «*persistent engagement*» i *Cyber Persistence Theory.*
[3] Det samme begrepet som Fischerkeller et al. benytter. Kan oversettes til «fullført handling» og referer til noe som allerede har skjedd, og som dermed ikke kan endres, forhindres eller reverseres.
[4] Min oversettelse av begrepet «*direct cyber engagement*» i *Cyber Persistence Theory.*
[5] Min oversettelse av begrepet «*tacit barganing*» i *Cyber Persistence Theory.*

De sentrale argumentene i Fischerkeller et al. (2022) kan oppsummeres på følgende måte: Eksisterende teoretiske rammeverk for å forstå hvordan stater samhandler er ikke direkte overførbare til cyberdomenet. Derfor utviklet de et teoretisk rammeverk som legger teknologiske egenskaper ved cyberdomenet til grunn: sammenkobling og konstant kontakt. Fischerkeller et al. antar at sammenkobling og konstant kontakt spiller en sentral rolle i å forme staters atferd i cyberdomenet. De argumenterer for at de teknologiske karakteristikkene skaper et insentiv til å oppnå vedvarende initiativ. En stat vil kunne følge dette insentivet gjennom vedvarende innsats, dersom stater har en evne til å utnytte sårbarheter.

Figur 3.1 viser logikken i Fischerkeller, Goldman og Harknetts (2022) argument[6].



Figur 3.1 Vedvarene innsats av Fischkeller, Goldman & Harknett (2022).

I det følgende vil jeg diskutere noen av antagelsene som ligger til grunn for *Cyber Persistence Theory*, og hvordan disse antagelsene danner grunnlaget for deres konklusjoner om hvilke effekter stater kan oppnå gjennom cyberoperasjoner.

Sammenkobling og konstant kontakt er de grunnleggende premissene i *Cyber Persistent Theory*. Premissene er basert på det Fischerkeller et al. (2022) mener er sentrale karakteristikker ved cyberdomenet. Oppkobling av digitale systemer til internett gjør det mulig å oppnå tilgang til systemer uten å være fysisk nær systemet. Dette muliggjør nye former for tilgang, sammenlignet med konvensjonelle domener. Internett blir dermed driveren i denne strukturen (Fischerkeller et al., 2022, s. 27–28). Det er positivt at forfatterne baserer sine grunnleggende premisser på det de anser som grunnleggende teknologiske karakteristikker ved cyberdomenet, og ikke abstrakte teoretiske premisser som ble utarbeidet for å beskrive andre

[6] Alle illustrasjoner av argumentasjon i ulike publikasjoner er laget av forfatteren av denne rapporten.

statlige virkemidler. Dette er positivt fordi et utgangspunkt i teknologiske egenskaper kan bidra til å gjøre teorien mer relevant og anvendelig i praksis.

De grunnleggende teoretiske premissene kan imidlertid nyanseres. Selv om antagelsen om sammenkobling fremstår som riktig, er det ikke nødvendigvis slik at alle systemer er koblet sammen på samme måte. Systemer med sensitiv eller gradert informasjon vil trolig tildeles et høyere sikkerhetsnivå enn andre systemer, og noen av disse systemene vil ikke være direkte tilkoblet internett. Det viktigste her er at det stater anser som mest betydningsfullt, inkludert kilder til nasjonal makt, ikke nødvendigvis er koblet sammen på samme måte som elementer som betraktes som mindre viktige. Dette vil forme mulighetsrommet for å endre maktbalansen gjennom såkalte *cyber fait accomplis,* blant annet ved at det stiller betydelige krav til utformingen av cyberoperasjoner, med et økt behov for tid og ressurser for å oppnå effekter mot systemer med et høyere nivå av sikkerhet.

Fischerkeller et al. (2022) legger videre til grunn at konstant kontakt vil gjøre det utfordrende å etablere et effektivt forsvar mot cyberoperasjoner. De beskriver forsvar av systemer mot cyberoperasjoner som noe du «bare kan forsvare i øyeblikket»[7] (Fischerkeller et al., 2022, s. 32). Dette fremstår som den viktigste forklaringen for hvorfor det er behov for å beskrive cyberdomenet som et helt nytt strategisk miljø, og hvorfor dette miljøet krever vedvarende innsats i møte med andre aktører. Fischerkeller et al. (2022, s. 9–24) tar utgangspunkt i det konvensjonelle og kjernefysiske domenet for å etablere en forståelse av hva som er et effektivt forsvar. I disse domenene kan et statisk forsvar bestående av fastlagte regler og forhåndsdefinerte svar på handlinger være effektivt over tid. En utfordring med denne påstanden er at det ikke nødvendigvis er korrekt å anta et strategisk miljø preget av hyppig kontakt ikke kan forsvares over tid. Et slikt miljø vil kreve en annen fremgangsmåte, som vi kan omtale som et dynamisk forsvar. Et slikt forsvar vil kjennetegnes av et behov for å svare på og tilpasse seg til trusler idet de oppstår, for eksempel nye metoder for å oppnå tilgang til systemer (Zheng et al., 2022). Dersom forsvaret av digitale systemer evner kontinuerlig å tilpasse seg nye trusler, kan det bidra til sikkerhet over tid. Dette betyr at vi må endre forståelse av at det er fastlagte rammer eller regler for hvordan man skal reagere på en trussel eller hva som utgjør en trussel som er grunnleggende for et effektivt forsvar. I stedet må vi evne å skape fleksibilitet i forsvarsmekanismer, samt å predikere hvilke endringer som er nødvendig for å opprettholde et effektivt forsvar over tid. Totalen av dette kan forstås som kontinuerlig forsvar, ikke forsvar i øyeblikket. Hvis vi vrir litt på oppfatningen på hva som utgjør et effektivt forsvar, er det dermed ikke gitt at et miljø preget av hyppig kontakt ikke kan forsvares.

Vi kan se til Ukraina som eksempel. I kontekst av krigen i Ukraina, løfter ukrainske politiske ledere frem digital motstandsdyktighet (*resilience*) som en strategi for å stå imot effekten av cyberoperasjoner fra Russland (Fedorov, 2023).

[7] Fischerkeller et al. (2022, s. 32) skriver: «*At the tactical level, you can indeed defend in cyberspace, but you can only defend in the moment – in the configuration of software, hardware, and processing that existed at the time you deployed a configuration you thought was secure*».

De løfter frem tre prinsipper for å oppnå digital motstandsdyktighet:

1. Nasjonal hendelseshåndtering, reaksjon og gjenopprettelse av systemer.
2. Å øke motstandsdyktigheten ved å øke beredskapen for enhver mulig hendelse.
3. Å styrke samhandlingen mellom ulike organisasjoner ansvarlig for den statlige cybersikkerheten i Ukraina.

Dersom vi ser nærmere på muligheten for å forsvare cyberdomenet – og tar hensyn til at dette er en reell mulighet – vil det påvirke antagelsen til Fischerkeller et al. (2022) om at konstant kontakt nødvendiggjør vedvarende innsats. Når vi justerer de grunnleggende antagelsene i det teoretiske rammeverket, fører dette til behovet for en justering av antagelsen om at vedvarende innsats er en uunngåelig følge av strukturen. Tar vi utgangspunkt i dette blir vedvarende innsats et bevisst valg for staten, snarere enn noe som blir pålagt som følge av strukturelle forhold.

Fischerkeller et al. (2022) argumenterer for at vedvarende innsats (*persistent engagement*) kan føre til økt stabilitet gjennom taus forhandling. Healy (2019) har presentert en rekke argumenter mot denne fremgangsmåten. For det første mener han at denne tilnærmingen kan føre til økt ustabilitet og forsterke konflikt, heller enn å skape stabilitet. For det andre argumenterer han for at vedvarende innsats som den styrende aktiviteten i cyberdomenet kan føre til et økt behov for ressurser. Healy viser til at en sentral logikk i vedvarende innsats er å tvinge motstanderen til å bruke ressurser på å opprettholde sentrale funksjoner i egne systemer, heller enn å skaffe tilgang og påvirke funksjoner i egne systemer. Han løfter imidlertid frem at dette kan ha en utilsiktet konsekvens; dersom det er relativt billig for motstanderen å bygge opp infrastruktur igjen eller den kan skaffe seg ny infrastruktur, kan vedvarende innsats kreve store ressurser for å redusere motstanderens evne til å angripe deg ved å påvirke funksjonaliteten i deres egne systemer (Healy, 2019, s. 7).

Når et mål er vanskelig å forsvare, og lettere å angripe, er det vanlig å anta at angriperen har en fordel i den relative balansen mellom forsvar og angrep. Det er en utbredt oppfatning i den statsvitenskapelige litteraturen om cyberoperasjoner at teknologien gir angriperen en fordel, inkludert *Cyber Persistence Theory*. Jeg velger å beholde konseptet om en forsvar-angrepsbalanse, men ønsker å utforske hvordan den spiller inn i cyberdomenet. Fischerkeller et al. (2022) ser ut til å anta at balansen mellom forsvar og angrep primært avhenger av teknologiske egenskaper: Det er lettere å trenge seg inn i et system enn å holde noen ute fra det. Vi kan imidlertid forstå balansen mellom forsvar og angrep som betinget av andre karakteristikker. Slayton (2016) argumenterer for at balansen mellom forsvar og angrep ikke bestemmes av teknologi alene, men av de organisatoriske prosessene som styrer interaksjonen mellom teknologi og teknologisk avanserte aktører. Dette innebærer at man må vurdere aktørens evne til å organisere avansert teknologi når man vurderer forsvar–angrepsbalansen. Hun påpeker også at målene for cyberoperasjoner spiller en rolle. Disse målene er varierte, og noen kan være vanskeligere å oppnå tilgang til enn andre. Til sist argumenterer hun for at balansen ikke er systemisk, men dyadisk. For å vurdere balansen må man vurdere evnen den ene aktøren har til å organisere og benytte teknologi, relativt til en annen aktør.

Andre bidrag til litteraturen på forsvar–angrepsbalanse argumenterer også for at balansen ikke er betinget av teknologiske karakteristikker alene. Glaser og Kaufman (1998) definerer forsvar–angreps balansen som kostnaden som kreves for å etablere styrker som er i stand til å ta et gitt territorium, relativt til kostnaden som kreves for å etablere styrker som kan forsvare tilsvarende territorium. Offensive operasjoner som har som mål å ta kontroll over et større territorium vil være vanskeligere enn mindre ambisiøse operasjoner. Kost-nytte-raten øker med ambisjonsnivået på operasjonen. Dette flytter forsvars-angreps balansen mot forsvaret når ambisjonsnivået på angrepet er høyere.

Fischerkeller, Goldman og Harknett (2022, s. 120) legger til grunn at det er lave kostnader for å delta i aktivitet i cyberdomenet, og dette skaper et insentiv til å delta i vedvarende innsats i cyberdomenet. Beskrivelsen av lave kostnader ved gjennomføring tar utgangspunkt i en teknologisk karakteristikk ved cyberdomenet – sikkerhetsarkitekturen har svakheter, og en sentral antagelse er at selv aktører med mindre avansert kjennskap til mulighetsrommet for teknologien kan delta i aktivitet. Trekker vi inn Slayton (2016) og Glaser og Kaufmans (1998) perspektiver, må vi imidlertid nyansere denne påstanden. Dersom sikkerhetsnivået hos målet er høyt og ambisjonen for operasjonen er høy, vil også terskelen for å delta være høy. For å komme rundt et høyt sikkerhetsnivå kreves mer enn evne til å finne og utnytte sårbarheter i programvare. Man må ha dyp kunnskap om hvordan teknologien fungerer, hvordan den brukes, og hvordan den er satt opp og konfigurert i det aktuelle målet. Dette innebærer også en evne til å gjøre risikovurderinger av egne handlinger, da feil kan føre til store konsekvenser. I tillegg kan det være nødvendig anskaffe og gjøre egen analyse av spesialsystemer, som for eksempel proprietære[8] IKT-systemer for kommando og kontroll. Aktøren må også gjennomføre interne vurderinger av verdien på operasjonen opp mot verdien av økt sikkerhet i egne systemer. Sårbarheten som benyttes kan også være til stede i aktørens egne systemer. Denne vurderingen består av hvorvidt operasjonen skal gjennomføres, eller om oppdagelsen av sårbarheten skal brukes til å sikre egne systemer.

Videre legger Fischerkeller et al. (2022) til grunn at vedvarende initiativ skaper atferden vedvarende innsats, gjennom staters evne til å finne og unytte sårbarheter. *Cyber Persistence Theory* antar at enhver stat vil utnytte andre staters sårbarheter dersom de har muligheten, og karakteriserer slik alle stater i denne teoretiske strukturen som grunnleggende antagonistiske (*belligerent*). Teorien antar dermed at internasjonal politikk er et miljø preget av sterk konkurranse der staten hele tiden må arbeide for å beholde initiativet over andre stater. Implisitt er denne beskrivelsen bygget på at aktørene i strukturen som Fischerkeller et al. (2022) beskriver er USA mot stater som Iran, Nord Korea, Russland og Kina. Dynamikken mellom disse statene kan beskrives som antagonistisk. Når teorien imidlertid setter seg som mål å beskrive strukturen for hele cyberdomenet burde dette premisset nyanseres.

I et mer praktisk perspektiv vil atferden til noen stater være antagonistiske, men andre stater vil være sikkerhetssøkende. Stater som hovedsakelig søker egen sikkerhet er mest opptatt av å utforme aktivitet som forsterker statens sikkerhet, uten at det utfordrer andre staters sikkerhet

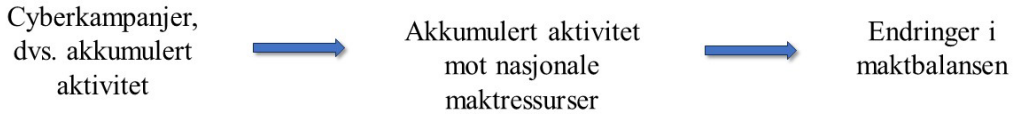
[8] Systemer som er omfattet av eiendomsrett, til forskjell fra åpen kildekode.

unødvendig mye (se Glaser, 2010, s. 4). Introduksjon av stater i teorien som er litt mer tilbakeholden i sin fremferd i cyberdomenet, ville bragt flere nyanser inn *Cyber Persistence Theory*. I sin nåværende form begrenses overførbarheten til analyser av land og regioner som er mer offensiv i sin fremferd i cyberdomenet, og den klarer ikke å fange variasjonene som eksisterer mellom hvor frempå eller tilbakeholdne stater er i cyberdomenet. Det eksisterer insentiver til å utnytte sårbarheter i digitale systemer og nettverk. Samtidig vil det være en viktig oppgave å forstå enkeltstaters valg og regionale dynamikker for å utvikle forståelsen av aktivitet i cyberdomenet. *Cyber Persistence Theory* legger opp til et strategisk miljø preget av sterk konkurranse. Dette gjør det vanskelig å forklare stater som har evnen til å utnytte sårbarheter, men ikke velger en like fremoverlent strategi i cyberdomenet.

3.2 Cyberkampanjer for å endre maktbalansen

Oppfatningen om at cyberoperasjoner kan endre maktbalansen mellom stater blir også fremmet av Harknett og Smeets i «Cyber Campaigns and Strategic Outcomes» (2022). Forfatterne argumenterer ut fra observasjoner av aktiviteten i cyberdomenet de siste årene. De påpeker at denne aktiviteten består av kampanjer som involverer koblede og koordinerte cyberoperasjoner. Disse kampanjene strekker seg over tid og har en spesifikk målsetting om å oppnå gunstige strategiske utfall, uten å måtte ty til angrep med tradisjonelle militære virkemidler. Cyberoperasjoner forstås dermed som et strategisk alternativ til krigføring (Harknett & Smeets, 2022, s. 541). Disse kampanjene er, ifølge forfatterne, svar på de samme strukturelle imperativene som ligger til grunn for *Cyber Persistence Theory* – sammenkobling og konstant kontakt. Så lenge de sentrale strukturene i cyberdomenet opprettholdes, kan vi forvente at kampanjer vil være de sentrale mekanismene i statlig strategisk konkurranse gjennom cyberdomenet.

Harknett og Smeets hevder Kinas tyveri av intellektuell eiendom gjennom cyberoperasjoner understøtter argumentet om at kampanjer benyttes for å påvirke kilder til nasjonal makt, og dermed endre maktbalansen i internasjonal politikk. Logikken i Harknett og Smeets argument kan oppsummeres i den følgende figuren.



Figur 3.2 Harknett og Smeets: Cyberkampanjer og strategiske utfall (2022).

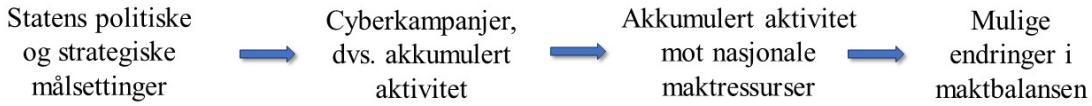
Harknett og Smeets går fra et empirisk argument om at cyberoperasjoner bør forstås som kampanjer, og slutter direkte ut fra dette argumentet om at hensikten med disse kampanjene er å oppnå strategiske målsettinger uten å gå til angrep på motstanderen med tradisjonelle militære virkemidler. At hensikten ved disse kampanjene er å endre maktbalansen, kan imidlertid trekkes i tvil. Effekten på sikt kan være at maktbalansen endres, men dette betyr ikke at det

nødvendigvis er et tydelig mål bak en rekke av koordinerte cyberhendelser. Å konkludere med at hensikten bak handlingen er å endre maktbalansen, kontra å konkludere med at handlingen kan føre til en endring i maktbalansen, er to forskjellige konklusjoner, og bør skilles mellom. Årsaken er enkel: intensjon er ikke det samme som faktisk konsekvens, og for å forstå hvordan cyberoperasjoner påvirker internasjonal politikk bør vi skille tydelig mellom disse to. Et skille mellom hensikt og konsekvens åpner også opp for tydeligere å utarbeide en forståelse av hvordan maktbalansen kan endres på sikt.

Jeg mener at den største svakheten i dette argumentet til Harknett og Smeets er at de ikke utmeisler mekanismer mellom leddene «påvirker nasjonale maktressurser» og «endringer i maktbalansen». Forfatterne besvarer hva som skjer, men ikke hvordan det skjer. Hvordan cyberoperasjoner endrer eller påvirker relasjoner mellom stater anser jeg som et sentralt spørsmål for å videreutvikle forståelse av cyberoperasjoners potensielle strategiske nytteverdi.

Jeg kommer i det følgende til å legge Harknett og Smeets empiriske grunnlag – kinesiske cyber-kampanjer – til grunn og utlede eksempler på mekanismer som kunne vært en del av årsaksrekken. Formålet med dette er å illustrere hvordan alternative mekanismer kan virke inn mellom aktiviteten cyberoperasjoner og mulige formålstjenlige effekter og dermed fange en større andel av kompleksiteten knyttet til cyberoperasjoners potensial for å være strategisk nyttige. Med utgangspunkt i Harknett og Smeets (2022) står det «endringer i maktbalansen» som en effekt av cyberoperasjoner på relasjoner mellom stater. Mer overordnet kan dette også forstås som statens politiske målsettinger, da strategisk nytteverdi også kan forstås på denne måten. For å forstå hvordan cyberoperasjoner har en innvirkning på relasjoner mellom stater, må slike mekanismer utarbeides.

Harkenett og Smeets (2022, s. 558) gir tydelig uttrykk for at cyberoperasjoner kan endre maktforholdet mellom stater: «*the empirical record supports an argument that cyber campaigns and operations can be pivotal in world affairs by independently* (…) *supporting the maintenance or alteration of the balance of power*» (2022, s. 558). Dette uttrykker en forståelse av cyberoperasjoner som et selvstendig virkemiddel i internasjonal politikk, som på egen hånd kan bidra til å endre maktforholdet mellom stater. Talmadge (2019) argumenterer for at teknologi ikke er en uavhengig variabel, men heller en mellomliggende variabel. For eksempel er det ikke slik at teknologi tvinger statsledere til å eskalere en situasjon, men at de heller synes å aktivt benytte teknologi for å øke eskaleringsfaren eller benytter teknologien opportunistisk i en konflikt. Dermed kan teknologi være nødvendig for at eskalering skal oppstå i noen tilfeller, men den er ikke alene tilstrekkelig for at denne effekten skal oppstå, og i noen tilfeller er teknologien heller ikke nødvendig. De sterkeste driverne for eskalering finner vi i politikk eller i strategi. Hvis vi benytter dette som en analogi for å forstå cyberoperasjoner, leder det til en forståelse av at cyberoperasjoner er et middel for å oppnå en målsetting i internasjonal politikk, heller enn en mekanisme som selvstendig kan endre relasjoner mellom stater, slik Harknett og Smeets hevder.



Figur 3.3 Cyberoperasjoner som mellomliggende variabel, basert på Talmadge (2019).

Perspektivet om at cyberoperasjoner bør forstås som en bestanddel av statens overordnede aktivitet for å fremme målsettinger har blitt fremmet i litteraturen. I «Offensive Cyber Capabilities and State Violence» skiller Egloff og Shires (2021) mellom en offensiv cyberkapabilitet og offensive cyberoperasjoner. En offensiv cyberkapabilitet er kombinasjonen av mennesker, teknologier og organisatoriske kjennetegn som sammen muliggjør offensive cyberoperasjoner, som de definerer som manipulering av digitale tjenester eller nettverk. Videre forstås offensive cyberoperasjoner i et kampanjeperspektiv, som innebærer gjentatte forsøk på inntrengninger i nettverk, samt forsøk på å etablere vedvarende tilgang til systemer. Artikkelen forstår denne aktiviteten som en del av et større sett av beslutninger staten tar for å oppnå bestemte målsettinger. Implikasjonen av dette perspektivet er at det ikke finnes rene «cyberkampanjer», men bare handlinger som er innlemmet i andre handlinger (f.eks. etterretning, teknisk innsamling, militære styrker, osv.).

Gilli og Gilli (2019) fremhever hvordan utbyttet fra cyberoperasjoner kan omgjøres til nytte for staten, med utgangpunkt i kinesiske cyberoperasjoner for intellektuell eiendom. De argumenterer for at det ikke bare er å stjele intellektuell eiendom; man må også besitte den institusjonelle kunnskapen for å dra nytte av dette i utvikling og innovasjon. Deres analyse kretser rundt militær teknologi, og de utfordrer påstanden om at industrispionasje gjennom cyberoperasjoner kan bidra til å erodere USAs militær-teknologiske overlegenhet.[9] Hovedargumentet til Gilli og Gilli er at dette argumentet ignorere kompleksiteten i moderne militærteknologi. På bakgrunn av dette, er imitasjon og replikasjon av militære systemer en svært vanskelig oppgave. For å kopiere andre staters militære teknologi, må stater ha avanserte teknologiske, industrielle og vitenskapelige kapasiteter innen våpenproduksjon.

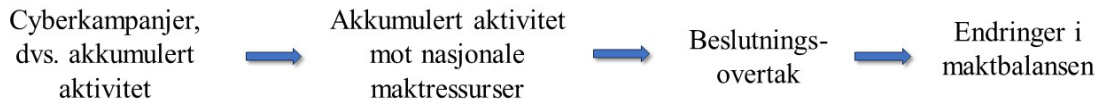
Tar vi utgangspunkt i kinesiske cyberoperasjoner er implikasjonen at akkumulert aktivitet for å oppnå intellektuell eiendom ikke er nok for å endre maktbalansen. Kinesiske myndigheter og selskaper må også ha en evne å omsette denne kunnskapen til fungerende systemer. Med utgangspunkt i Gilli og Gilli (2019) er hovedpoenget at det ikke er den akkumulerte aktiviteten som potensielt endrer maktbalansen – det er hvordan staten drar nytte og omformer det til et fortrinn gjennom sine egne interne prosesser. Dette kan forstås som et samspill mellom aktiviteten i cyberdomenet – uthenting av informasjon gjennom industrispionasje – og institusjonell kunnskap. Tar vi utgangspunkt i dette argumentet, kan vi utlede årsaksrekken som illustrert i Figur 3.4.

[9] Argumentet om at teknologi er enkelt å kopiere går igjen i flere publikasjon, se Goldman (2004, s. 4) i «The Information Revolution and Military Affairs in Asia» og Horowitz (2010, s. 27–28) i *The Diffusion of Military Power.*

Figur 3.4 Cyberoperasjoner og institusjonell kunnskap, basert på Gilli og Gilli (2019).

Et annet perspektiv handler om hvordan stater benytter informasjon til sin fordel. Etterretningsinnsamling kan skape en situasjon der en stat besitter mer informasjon enn motstanderen. Dette betyr at staten vet mer om motstanderen beslutningstagning enn motstanderen vet om statens egen beslutningstagning. Denne situasjonen har blitt beskrevet som et beslutningsovertak.[10] Hovedargumentet er at et relativt høyere nivå av tilgang til informasjon reduserer statens usikkerhet om andre staters intensjoner (Sims, 2022). Intensjoner har blitt forstått som viljen til å bruke makt. Stater har insentiver til å gi et feilaktig bilde av denne viljen for å oppnå bedre forutsetninger for seg selv (Fearon, 1994, s. 586). Tilgang til privat informasjon gir dermed andre stater en fordel i beslutningstaking. Totalt kan denne dynamikken bidra til å stille beslutningstagere i en bedre posisjon til å ta beslutninger som kan bidra til å fremme statens politiske målsettinger relativt til andre stater.

Med bakgrunn i dette, er det ikke den akkumulerte cyberaktiviteten med formål om å hente ut informasjon som endrer maktbalansen, det er hvordan beslutningstagere evner å dra nytte av denne informasjonen til statens fordel. Med utgangspunkt i samme empiriske eksempel som Harknett og Smeets, kan kinesiske cyberkampanjer forstås som et forsøk på å skaffe et beslutningsovertak overfor andre stater, og bruke dette overtaket til sin fordel. Tar vi utgangspunkt i dette argumentet, kan vi utlede årsaksrekken som illustrert i *Figur 3.5*.



Figur 3.5 Strategiske effekter som følge av beslutningsovertak, basert på Sims (2022).

En implikasjon av disse to alternative årsaksrekkene er at cyberoperasjoner kan være et virkemiddel som skaper forutsetninger eller grunnlaget for videre handling. Fordelene som cyberoperasjoner skaper må aktivt omformes til kilder til makt som kan benyttes til å oppnå en strategisk målsetting; de kan ikke selvstendig oppnå dette.

[10] Min oversettelse av begrepet «*decision advantage*».

3.3 Institusjonelle begrensninger ved å oppnå strategisk nytte

For å oppnå strategisk effekt av cyberoperasjoner må stater utvikle en cyberkapabilitet som kan utføre cyberoperasjoner. Smeets (2022) studerer i boken *No Shortcuts – Why States Struggle to Build a Military Cyber-Force* forutsetningene som må ligge til grunn for at stater skal utvikle en effektiv cyberkapabilitet. Et sentralt argument er at ressursene som kreves for å utføre operasjoner er langt høyere enn oppfatningen som råder i litteraturen. På bakgrunn av dette utvikler Smeets (2022) et rammeverk for ressursene som kreves for å etablere en cyberkapabilitet. Disse ressursene består av mennesker, sårbarheter, verktøy, infrastruktur og organisasjon.

Hovedpoenget under «mennesker» er at det kreves ansatte med varierte fagbakgrunner for å utvikle en effektiv cyberkapabilitet. I tillegg til teknologer er det blant annet nødvendig med lingvister, analytikere, strateger og jurister. «Verktøy» og «sårbarheter» innebærer både utvikling av nulldagsårbarheter[11], men også evnen til å dra nytte av kjente sårbarheter og skadevare. Forutsetninger her er god kjennskap til systemet eller nettverket som skal rammes og en forståelse av hvordan utnyttelse av sårbarhetene vil kunne påvirke påvirker systemet direkte og indirekte. Investeringer i infrastruktur er også sentralt. Dette innebærer målutvelgelse, utvikling, utprøving og trening.

Ressursen «organisasjon» involverer samspillet mellom ulike organisasjoner i statsapparatet, og internt i organisasjoner som har fullmakt til å utføre cyberoperasjoner. Mellom organisasjoner er integrering av en stats militære innsats og etterretningsoperasjoner viktig for å øke effektiviteten til cyberoperasjoner, sikre overføringen av kunnskap og redusere overlapp mellom operasjoner. Internt i organisasjoner er det en spenning mellom å etablere standard operasjonsprosedyrer for å utføre komplekse rutineoperasjoner og å opprettholde individuell fleksibilitet, ifølge Smeets.

Et av de mest sentrale poengene til Smeets i *No Shortcuts* er at stater ikke kan kjøpe en komplett cyberkapabilitet; den må bygges opp internt ved at organisasjonen som har ansvar for å utføre cyberoperasjoner har evne til å tiltrekke seg tilgjengelig kompetanse og utvikle infrastruktur som er nødvendig for å gjennomføre cyberoperasjoner. Dette er ikke en fullstendig ny problemstilling. F-35 kapasiteten ble anskaffet, men det kreves fortsatt et bredt spekter av kompetanse for å drifte og vedlikeholde kampflyene og opprettholde de svært avanserte systemene som er nødvendig for å holde flyene på vingende. Rapporter har beskrevet at Forsvaret sliter med å beholde nødvendig personell for å vedlikeholde denne kapasiteten, og at den tilgjengelige kompetansen ikke finnes, den må utdannes (Påsche & Sørbø, 2024).

I tillegg til perspektiver knyttet til ressurser som er nødvendig for å utvikle en cyberkapabilitet, presenterer Smeets (2022) en typologi for cyberaktører. Denne typologien består av fire ulike aktører, og deles inn etter to dimensjoner: tilgjengelige organisatoriske og økonomiske

[11] Disse sårbarhetene utgjør sårbarheter i programvare eller maskinvare som ikke er oppdaget av andre, og dermed ikke er rettet.

ressurser og i hvor stor grad aktøren har begrensinger pålagt for utførelse av cyberoperasjoner. Smeets (2022) deler begrensinger inn i tre deler: strategisk, juridisk/normativ og organisatorisk. Strategiske begrensninger referer til hvordan cyberoperasjoner kan benyttes for å oppnå en politisk målsetting. Juridiske og normative begrensninger referer til hvordan regler i folkeretten og nasjonale rettsregler legger begrensinger på mulighetsrommet for stater. Organisatoriske begrensninger referer til avveininger som må gjøres mellom behov i ulike organer intern i staten. For eksempel balansegangen mellom å utføre en cyberoperasjon for effekt opp mot å miste en potensielt verdifull kilde til etterretningsinnsamling. Sammen former begrensingene hvordan og når stater kan utføre cyberoperasjoner. Den første typen aktør er aktører som har få begrensninger og store ressurser tilgjengelig. Den andre typen aktør har få begrensinger på hvordan de kan utføre cyberoperasjoner, men heller ikke store ressurser tilgjengelig. Den tredje typen aktør har store begrensninger i hvordan de kan utføre cyberoperasjoner, men har samtidig ressurser tilgjengelig for å utvikle og utføre disse. Den siste typen aktør er pålagt store begrensninger for utførelse av operasjoner, og har også begrensede ressurser for å utvikle og utføre operasjoner.

Smeets har tidligere argumentert for at cyberoperasjoner kan endre maktbalansen mellom stater (Harknett & Smeets, 2022), men dette, eller nytten av cyberoperasjoner mer generelt, diskuterer han ikke ytterligere i boken. I *No shortcuts* fremstiller han imidlertid en rekke påstander om nytten av cyberoperasjoner:

> «*There is growing recognition that cyber effect operations are versatile and can be deployed in a wide range of situations. They can be undertaken in times of both peace and war, in conflicts with different intensity, and with and without kinetic force. They can influence the activities of all other domains of warfare and lead to escalation of de-escalation*» (Smeets, 2022, s. 36).

Dette er påstander om nytten ved cyberoperasjoner, det er ikke beskrivelser av den reelle nytten. Mangel på tilgjengelig empiri og problematikk tilknyttet hvordan å måle effekter av cyberoperasjoner, gjør at det ikke er tydelig etablert hva den reelle nytten av dette virkemiddelet er. Studiene som blir omtalt i denne gjennomgangen, er i stor grad teoretisk fundert og basert på enkelthendelser eller et lite utvalg av hendelser. Til tross for at Smeets (2022) hevder at det er økt forståelse for nytten av cyberoperasjoner, er ikke dette en helt ukontroversiell påstand. Slik denne gjennomgangen har vist, og vil vise, er det fortsatt mange spørsmål som må tas tak i før en moden forståelse av nytten av cyberoperasjoner er etablert.

Basert på poenget over mener jeg at det er ett steg som ligger forut for utvikling av infrastruktur og innhenting av kompetanse. Dette steget består av å utvikle en mer moden og egnet forståelse av hvordan kapabiliteten kan være nyttig for å nå bestemte målsettinger som staten har i sin egen utenriks- og sikkerhetspolitikk. Stater kan slite med å utvikle en cyberkapabilitet fordi det ikke er helt tydelig hva denne kapabiliteten skal brukes til og hvilken konkret nytte den kan ha innen sine egne rammer for tilgjengelig ressursbruk. Dette utelukker imidlertid ikke relevansen av Smeets (2022) poeng om tilgjengelig personell. Dette gir muligheten til å balansere mellom å forstå hvordan cyberoperasjoner kan brukes som et verktøy i en stats utenriks- og

sikkerhetspolitikk, og samtidig ha tilstrekkelig personell til å utvikle forståelsen av mulighetsrommet for utvikling og gjennomføring av cyberoperasjoner.

3.4 Operasjonelle begrensninger ved cyberoperasjoner

Maschmeyer (2021, 2023, 2024) argumenterer for at cyberoperasjoner har potensial for å være formålstjenlig for å oppnå strategiske målsettinger, men at praktisk utførelse av operasjoner involverer avveininger som reduserer den reelle strategiske nytten. Strategisk nytte forstås som kapasitet til å målbart bidra til å oppnå politiske målsettinger og/eller endre maktbalansen i internasjonal politikk (Maschmeyer, 2024, s. 6). Maschmeyer (2021, 2024) tar utgangspunkt i at *hvordan* aktører utformer operasjoner på operasjonelt nivå er et bedre utgangspunkt for å predikere hvor vellykket operasjonen vil være heller enn selve teknologien som blir brukt.

Gjennom å trekke på teoretiske konsepter om subversjon, forstår Maschmeyer (2021, 2023, 2024) cyberoperasjoner som subversiv aktivitet. Denne forståelse stammer fra at både tradisjonell subversjon og cyberoperasjoner unytter og manipulerer systemer for å oppnå målsettinger. Cyberoperasjoner har datasystemer integrert i moderne samfunn, organisasjoner og institusjoner som sentrale mål. Tradisjonell subversjon unytter sosiale systemer. I likhet med tradisjonell subversjon utnytter cyberoperasjoner sårbarheter i sosiale systemer, men også sårbarheter i digitale systemer for å få systemet til å opptre på en måte som ikke var den opprinnelige intensjonen (Maschmeyer, 2024, s. 11).

Subversiv aktivitet er av natur hemmelig og fordekt (Maschmeyer, 2021, s. 55). Dermed forstår Maschmeyer subversive cyberoperasjoner som en underkategori av fordekt aktivitet (*covert action*). Dette kjennetegnet legger grunnlaget for en rekke fordeler som kan bidra til å fremme politiske målsettinger. For det første innebærer det lavere risiko og kostnader sammenlignet med åpenlyse metoder for intervenering i andre staters interne anliggender. For det andre vil det å holde sin egen identitet skjult redusere faren for eskalering ved å unngå at motstanderen får press på seg for å gjengjelde handlingen. For det tredje vil det å holde sin egen identitet skjult redusere faren for å tape ansikt når staten trosser prinsippet om å ikke gripe inn i andre staters interne anliggender. Den siste fordelen er knyttet til at subversjon utnytter motstanderens systemer. Dette reduserer ressursbruken knyttet til å oppnå effekter. Samlet skaper disse fordelene et potensial for at cyberoperasjoner kan være strategisk nyttige.

Den strategiske nytten ved cyberoperasjoner er imidlertid begrenset av det Maschmeyer omtaler som et subversivt trilemma (2021, 2024). Trilemmaet oppstår fordi det er krevende å holde en operasjon skjult. Fordi en skjult operasjon vil legge grunnlaget for strategisk nytte, vil en aktør likevel streve for å oppnå dette. Dette ønsket påvirker den operasjonelle effektiviteten ved subversiv aktivitet langs tre variabler:

I. Effekters intensitet, forstått som styrken eller omfanget av effektene.
II. Hastighet på operasjonen, forstått som tidsrommet fra operasjonsstart til effekten mot det digitale systemet inntreffer.

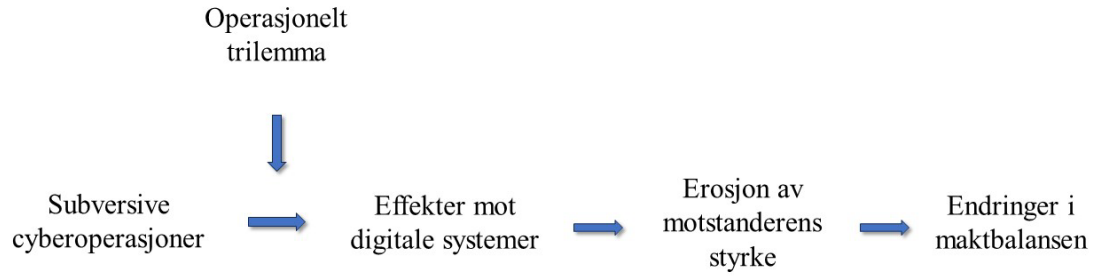
III. Kontroll over egen operasjon. Høy grad av kontroll er forbundet med å unngå å bli oppdaget i systemet, kontroll over hvilke effekter som inntreffer, samt å unngå utilsiktede effekter.

Trilemmaet skaper en avveining som aktøren som utfører subversiv aktivitet må ta stilling til. For eksempel vil trilemmaet innebære at en høyere hastighet på en operasjon vil tendere til å redusere styrken på effektene og kontrollen over egen operasjon. På grunn av avveiningen mellom disse tre variablene er subversive cyberoperasjoner enten for treg eller svak, eller for ustabil for å skape reell strategisk nytte, ifølge Maschmeyer (2021, 2024). Stuxnet, som var en hendelse mot et anlegg for urananriking i Natanz i Iran, illustrerer Maschmeyers poeng. Hendelsen førte til at sentrifugene i anlegget begynte å spinne raskere enn de skulle, og hindret dermed anrikningsprosessen. Hendelsen hadde høy grad av intensitet og kontroll. Hastigheten var imidlertid lav; det skal ha tatt fem år å utvikle operasjonen (McDonald et al., 2013).

I A new and better Quiet option? argumenterer Maschmeyer (2023) for at cyberoperasjoner som subversjon egner seg til å oppnå erosjon av motstanderens styrke. Styrken svekkes gradvis ved å sabotere infrastruktur eller institusjoner knyttet til økonomisk og industriell kapasitet, svekke offentlighetens tillit til myndighetene eller forsterke sosiale spenninger. I noen tilfeller kan dette også innebære å svekke militære kapabiliteter (Maschmeyer, 2023, s. 3, 8). Suksess i denne sammenheng vil involvere en målbar endring i maktbalansen, eller en endring i den offentlige opinionen hos motstanderen (Maschmeyer, 2023, s. 15). Dermed, argumenterer Maschmeyer, utgjør cyberoperasjoner et strategisk alternativ til diplomati som gir de samme gevinstene ved krigføring, bare ved en lavere risiko og kostnad. Maschmeyer trekker frem at cyberoperasjoner som erosjon er mest relevant i en strategisk konkurranse mellom stormakter. Dette er fordi ressursbehovet for å gjennomføre cyberoperasjoner som kan balansere det operasjonelle trilemmaet er stort. Mindre ressurssterke aktører vil trolig ikke klare å oppnå endringer i maktbalansen mellom stater da operasjonelle begrensinger vil være for sterke (Maschmeyer, 2023, s. 18–19).

Maschmeyer omtaler cyberoperasjoner i bred forstand i sitt teoretiske rammeverk, men har analysert den mulige strategiske nytten av subversive cyberoperasjoner i lys av russisk aggresjon mot Ukraina. Konteksten for rammeverket er dermed hovedsakelig militær aktivitet og konflikt både under og over terskelen for krigføring. Forståelsen av cyberoperasjoner som subversive handlinger bør forstås ut fra denne konteksten. Overføringsverdien til andre kontekster er ikke nødvendigvis stor. Dette er fordi statens målsettinger ved å benytte seg av cyberoperasjoner bør samsvare med målsettingene for subversjon som fremheves i rammeverket. Dette forstår Machmeyer som infiltrering, utnyttelse og manipulasjon og grupper, institusjoner og samfunn med formål om å oppnå tre bestemte målsettinger: manipulere politikk og offentlig opinion, sabotere infrastruktur og andre fasiliteter og å skape regimeskifte fra innsiden (Maschmeyer, 2024, s. 8).

Hovedargumentet til Maschmeyer (2021, 2023, 2024) oppsummeres i *Figur 3.6*



Figur 3.6 Maschmeyer (2021, 2023, 2024): Subversive cyberoperasjoner.

Maschmeyers påpeker at for å oppnå tilstrekkelig virkningsfulle og treffsikre effekter av cyber-operasjoner, er det nødvendig med en lang planleggingsprosess. Han påpeker flere begrensninger ved denne prosessen som påvirker effektiviteten av slike operasjoner.

Jeg vil løfte frem to hensyn som må balanseres for å omgå begrensingene ved cyberoperasjoner. For det første vil det innebære en evne til å utføre flere parallelle avanserte cyberoperasjoner, og skape effekter som inntreffer så tett opptil hverandre at motstanderen ikke har mulighet til å rette opp skadene før en ny effekt inntreffer. Hvis aktøren ikke har denne evnen, kan det bety at motstanderen har hatt nok tid til å rette opp eventuelle negative effekter av cyberhendelser før neste effekt slår inn. Dersom motstanderen lærer seg å motstå effektene, enten gjennom sikkerhetstiltak i og rundt digitale systemer, eller politisk og sosiale motstandsdyktighet mot effekter, vil vanskelighetsgraden for å oppnå virkningsfulle effekter trolig øke. I tillegg vil ressurspådraget økes ettersom motstandsdyktigheten hos motstanderen øker.

For det andre krever det en evne til å koordinere og forutse effekter over tid. Dette gjelder koordinering av effekter fra ulike cyberhendelser, men også effekter av cyberhendelser opp mot politiske og sosiale systemer. Digitale systemer er komplekse, og det er derfor vanskelig å vurdere hvilken effekt som vil inntreffe, til tross for lang planleggingstid. Dette kommer blant annet av at komplekse systemer ofte har mange avhengigheter og interaksjoner som ikke alltid er forstått i detalj. Dette kan føre til uventede effekter av en cyberhendelse. I tillegg vil kompleksiteten øke med størrelsen på systemet; jo større systemet er, desto flere variabler er det å ta hensyn til. Videre vil digitale systemer endres og oppdateres kontinuerlig. Sårbarheter kan rettes eller nye introduseres med oppdateringer, og endringer i konfigurasjoner kan påvirke systemers sikkerhet og funksjonalitet. Denne dynamikken gjøre det utfordrende å forutse effektene av en cyberoperasjon på et gitt tidspunkt. Skal en aktør oppnå en strategisk effekt som erosjon av motstanderens styrke, er det ikke nok å vurdere effekter av cyberoperasjoner – det må også vurderes opp mot effektene på politiske og sosiale systemer. Sosiale og politiske systemer er også komplekse, og å vurdere hvilken innvirkning cyberoperasjoner vil ha over tid mot disse systemene, vil derfor være en svært vanskelig oppgave. Dette legger begrensninger på staters mulighet til å oppnå strategiske effekter gjennom erosjon over tid.

Kombinerer vi disse to hensynene, kan det bety at en aktør må være villig til å investere store ressurser i en kapabilitet som det er usikkert om vil føre til ønskelige effekter. I tillegg er det vanskelig å måle hvorvidt slike effekter faktisk er oppnådd. Dette gjør det utfordrende for stater

å oppnå strategisk erosjon gjennom cyberoperasjoner, da usikkerheten og kompleksiteten i digitale og sosiale systemer krever en betydelig ressursinnsats for å oppnå og opprettholde ønskede effekter.

3.5 Cyberoperasjoner som et operasjonelt og taktisk virkemiddel

I boken *Offensive Cyber Operations* setter Moore (2022) spørsmålstegn ved flere av de sentrale antagelsene som legges til grunn i Maschmeyers analyse samt i andre deler av litteraturen. Disse antagelsene er at operasjonene er fordekte, at de krever en lang planleggingsprosess, og at virkemiddelet ikke har verdi hvis det blir oppdaget. Moore argumenterer i stedet for at cyber-kapabiliteten kan være nyttig selv om den har blitt oppdaget.

Dette argumentet løfter han frem gjennom det han omtaler som «*event based operations*», som vi kan oversette til hendelsesbaserte operasjoner.[12] Dette er offensive cyberoperasjoner som utføres med kort forberedelsestid mot systemer. Disse hendelsene benytter som regel kjente sårbarheter. Hendelsesbaserte operasjoner kan enklere benyttes i en militær konflikt, der det er nødvendig å oppnå en effekt over et mål uten langsiktig planlegging, som en analogi til kapabiliteter som kan deployeres i felt. Moore løfter frem at tjenestenekt av motstanderens kommando og kontroll i felt kan forstås som en parallell til elektronisk krigføring. I kontrast til denne kategorien av offensive cyberoperasjoner, løfter Moore frem «*presence-based operations*», eller tilstedeværende operasjoner. Dette er offensive cyberoperasjoner med en lengre tidshorisont, som består av langsiktige inntrengninger som skal lede frem mot en effekt på sikt. Disse hendelsene utnytter oftere egenutviklede sårbarheter.

Moores rammeverk beskriver et mulighetsrom for hvordan vi kan tenke om offensive cyber-operasjoner i krigføring. Han legger til grunn at vi bør forstå offensive cyberoperasjoner som immateriell krigføring. Dette innebærer at vi bør forstå denne aktiviteten som en parallell til elektromagnetisk krigføring og signaletterretning, ikke subversjon eller vedvarende innsats (*persistent engagement*). Jeg mener imidlertid at skal dette være nyttig er det noen problem-stillinger som må klargjøres. For det første må man etablere hva målsettingen for offensive cyberoperasjoner skal være i en krigskontekst. Skal det på den ene siden være et opportunistisk virkemiddel som favner bredt, uten å diskriminere på mål, på linje med Moores hendelsesbaserte operasjoner. Eller skal offensive cyberoperasjoner på den andre siden ha som målsetting å utføre en nøyaktig og kontrollert effekt mot et system på et bestemt tidspunkt. Hvis cyberoperasjoner blir vurdert som best egnet til den andre kategorien, vil Maschmeyers subversive trilemma fortsatt være en problemstilling som må tas med i beregningen av begrensningene for hva cyberoperasjoner kan oppnå som et statlig virkemiddel for maktbruk.

Flere av bidragene jeg har gjennomgått så langt legger til grunn at cyberoperasjoner kan oppnå strategiske målsettinger og gevinster tilsvarende det en krig ville oppnådd, uten at staten må bøte med kostnadene ved krigføring. Schulze (2020) problematiserer denne påstanden. I «Cyber in War – Assessing the strategic, tactical and operations utility of military cyber

[12] Jeg bruker oversettelser etablert i Bakke (2023)

operations» er det sentrale spørsmålet hvilken nytte cyberoperasjoner for effekt kan ha i en konfliktsituasjon. For å undersøke dette deler han inn cyberoperasjoner på strategisk, operasjonelt og taktisk nivå. Utgangspunktet til Schulze er en påstand om at den strategiske nytte ved cyberoperasjoner er begrenset. Det samme behøver imidlertid ikke å være tilfellet på operasjonelt og taktisk nivå, og denne nytten bør undersøkes nærmere, ifølge Schulze (2020).

Cyberoperasjoner i en krigskontekst utføres ofte av militære organisasjoner, og har ofte militær infrastruktur som hovedkvarter, våpensystemer og kommando og kontroll, som de viktigste målene for operasjonene (Schulze, 2020). Dette gjør at de utfører en militær hensikt heller enn en etterretningshensikt. Schulze (2020) argumenterer for at to variabler påvirker nytten av cyberoperasjoner i krig: timing og operasjonens kompleksitet. Timing innebærer spørsmål om når og hvor lenge en cyberoperasjon skal være aktiv for å maksimere effekter. Kompleksitet henviser til hvor vanskelig det er å oppnå ønskelig effekt. Kompleksitet skapes av antallet mål (ett system eller hundrevis av systemer), forsvarsnivået på systemet (åpne eller lukkede systemer) og tilgangen til ressurser for å utføre operasjonen (etterretning og skadevare), i tillegg til størrelse, organisering og koordinering av gruppen som utfører operasjonen (Schulze, 2020, s. 193).

Dette utgangspunktet leder til de følgende hypotesene for Schulze (2020):

I. Det er enklere å oppnå suksess tidlig i en konflikt. Dette er fordi cyberoperasjoner har størst sjanse for å lykkes når motstanderen ikke forventer operasjonen.
II. Jo lenger forberedelsestid det er foran en operasjon, desto større er sjansen for at operasjonen vil være en suksess.
III. Høy operasjonell kompleksitet øker risikoen for at operasjonen mislykkes. Kompleksitet økes blant annet ved at flere militære komponenter eller organisasjoner inkluderes. Dette er fordi koordineringen mellom disse blir vanskeligere.
IV. Dersom militære ledere har alternative fremgangsmåter til cyberoperasjoner med høy kompleksitet og dermed usikker grad av pålitelighet, vil de tendere til å velge et tryggere alternativ.

4 Signalering

Signalering handler om å kommunisere informasjon om intensjon, besluttsomhet eller kapabiliteter til andre stater (Gartzke et al., 2017). Målsettingen med dette kan være å avskrekke en annen stat fra å utføre en bestemt handling gjennom trusselen om straff, tvinge staten til å endre handlingsmønster gjennom trusselen om gjengjeldelse, eller å kommunisere en vilje til å eskalere en allerede anspent situasjon mellom to stater. De følgende bidragene beskriver hvorvidt og/eller hvordan cyberoperasjoner kan benyttes for å oppnå disse strategiske målsettingene. Når det gjelder avskrekking og tvang er det to posisjoner i litteraturen. Den ene tar utgangspunkt i at avskrekking og tvang ikke er mulig, mens den andre tar utgangspunkt i at tvang vil være mulig under bestemte forutsettinger.

4.1 Tvang gjennom cyberoperasjoner

Borghard og Lonergan (2017) løfter frem attribusjonsproblemet i deres diskusjon om hvorvidt det er mulig å oppnå effektiv tvang av motstanderen gjennom signalering av egen beslutsomhet i cyberdomenet. Argumentet baserer seg på det sentrale premisset i tvangsteori (*coercion-theory*) om at kommunikasjon er grunnleggende for å oppnå strategiske målsettinger om å endre motstanderens handlemåte (se Schelling, 1966). Borghard og Lonergan argumenterer for at stater ikke nødvendigvis vet hvem som står bak en cyberhendelse. Dermed er det problematisk for andre stater å kommunisere besluttsomhet gjennom cyberoperasjoner. Bakgrunnen for dette er en forståelse av at kommunikasjon skjer gjennom selve hendelsen. Likevel løfter Borghard og Lonergan (2017) frem at attribusjon er mulig på tre ulike måter. For det første kan aktøren som utfører hendelsen selv gå offentlig ut med informasjon. For det andre kan staten som er mål for hendelsen attribuere ved å ha tilgang til motstanderens systemer og følge med på hendelsen i sanntid. Til sist er attribusjon mulig ved å vise til bestemte karakteristikker ved hendelsen. Det er imidlertid forbundet stor usikkerhet ved disse fremgangsmåtene. Derfor er en sentral konklusjon hos Borghard og Lonergan (2017) at tvang er vanskelig å oppnå gjennom cyberoperasjoner.

I *Cyber Strategy* ønsker Valeriano, Jensen og Maness (2018) å teste hvordan cyberoperasjoner kan fungere som tvang overfor en annen stat. Forfatterne inntar en bred posisjon knyttet til potensialet for tvang mellom stater. I tradisjonell tvangs-teori (eks. Schelling, 1966) ligger hovedfokuset på kommunikasjon av mulig straff dersom motstanderen krysser en linje. *Cyber Strategy* legger imidlertid til grunn at stater bruker cyberoperasjoner for et fortrinn ovenfor en motstander. Dette inkluderer tvang gjennom trusselen om straff, til signalering som en form for eskaleringskontroll, propaganda og manipulering av den langsiktige informasjonsbalansen (Valeriano et al., 2018).

Cyber Strategy deler cyberoperasjoner inn i *disruption* (forstyrrelse), *espionage* (spionasje) og *degradation* (nedbryting). Valeriano et al. (2018) forstår «forstyrrelse» som hendelser som er forbundet med en lav kostnad og lavt utbytte. Dette innebærer at aktøren må bruke relativt lite

ressurser for å gjennomføre hendelsen, og selve effekten når hendelsen vil være begrenset. Forfatterne anser det som usannsynlig at disse hendelsen vil endre oppførelsen til målet. «Spionasje» forstås som innsats for å endre en informasjonsbalanse eller manipulere oppfatninger gjennom digitale midler på en måte som skaper fordeler i forhandlinger for aktøren som utfører disse cyberoperasjonene. Disse fordelene kan være intellektuell eiendom eller informasjon om materielle komponenter i militære kapasiteter. «Nedbryting» innebærer handlinger forbundet med høye kostnader for gjennomføring som påfører høy grad av smerte hos motstanderen. Slike hendelser søker å bryte ned eller ødelegge kritiske kapabiliteter gjennom cyberoperasjoner.

Hovedfunnet i boka er at cyberoperasjoner bare kan skape begrensede innrømmelser fra motparten. Ved å undersøke 192 hendelser av cyberoperasjoner mellom rivaler finner Valeriano et al. (2018) at bare 5,7 % av tilfellene fører til observerbar endring i handlingsmønster. De fremhever at kategorien nedbryting er den som i størst grad vil skape endringer. Innenfor denne kategorien var det bare hendelser som var tilstrekkelig kostbar som skapte en tvangseffekt. Dette er fordi det bare er nedbryting som vil kommunisere en tydelig intensjon om straff dersom motstanderen ikke kommer med innrømmelser eller endrer sitt eget handlemønster.

4.2 Avskrekking gjennom cyberoperasjoner

I «Deterrence and Dissuasion» løfter Nye (2017) frem attribusjonsproblemet som et viktig hinder for å oppnå effektiv avskrekking i cyberdomenet. Et sentralt poeng er at attribusjonsproblemet trolig vil være alvorlig nok til å hindre effektiv avskrekking gjennom straff. Nye legger til grunn at identiteten til aktøren som har utført handlingen er usikker, i tillegg til at det til enhver tid vil være flere ukjente motstandere. På bakgrunn av dette konkluderer Nye med at avskrekking gjennom straff ikke vil være en relevant fremgangsmåte for å forhindre angrep i cyberdomenet. Attribusjonsproblemet vil imidlertid ikke være alvorlig nok til å hindre avskrekking gjennom nektelse. Dette innebærer at et forbedret forsvar vil øke kostnaden ved angrep, og dermed redusere insentivene til å forsøke å påvirke systemer og nettverk. En konsekvens av denne fremgangsmåten er at det frigjør ressurser til å fokusere på avanserte aktører.

I «Deterrence by Denial» diskuterer Borghard og Lonergan (2023) mulighetene for å oppnå effektiv avskrekking i cyberdomenet. En løsning for å oppnå avskrekking er å straffeforfølge enkeltindivider, hevder forfatterne. De løfter imidlertid frem attribusjonsproblemet som et hinder for effektiv avskrekking i cyberdomenet. Før straffeforfølgning av enkeltindivider skal være mulig, er det nødvendig å attribuere hendelsen til disse individene. Å attribuere aktivitet eller hendelser til enkeltpersoner er en praksis USA har utført i flere år (se eks. Office of Public Affairs, 2024). Dette er imidlertid en tidkrevende prosess, og det tar dermed lang tid før straffeforfølgning er et mulig alternativ. Dette tidsrommet gjør pålitelig avskrekking i cyberdomenet vanskelig å oppnå (Borghard & Lonergan, 2023).

Attribusjon står i sentrum for Borghard og Lonergan (2017, 2023) og Nye (2017) i deres analyser av signalering gjennom cyberoperasjoner. Attribusjon er ikke umulig, men i mange tilfeller vil det ta noe tid å gjennomføre. I stedet for å anse attribusjon som problematisk, bør aktører som utfører cyberoperasjoner ta utgangspunkt i at en fremtidig attribusjon er en mulighet. Fremtidig er stikkordet – det introduserer en tidsvariabel. Dette tidselementet mangler i Borghard og Lonergan (2017; 2023) og Nye (2017) sin gjennomgang av potensialet for tvang og avskrekking gjennom cyberoperasjoner. Hvis det går lang tid mellom en hendelse og attribusjonen av hendelsen vil potensialet for å oppnå disse effektene trolig svekkes. For det første, når det gjelder hendelser med intensjon om å påføre tvang bør det være en bestemt tidslinje som kommuniseres sammen med hendelsen. Uten en bestemt tidslinje vil ikke aktøren som mottar trusselen gjennom en cyberhendelse ha et insentiv til å endre handlemåte (Biddle, 2020, s. 102). Et annet perspektiv er at presset som den opprinnelige handlingen la på målet trolig vil reduseres over tid. Dette er fordi opplevelsen av å stå overfor en umiddelbar trussel vil avta over tid. Kjernen i tvangsteori er at aktøren skal oppleve at straff vil bli påført dersom handlingsmønsteret ikke endres. Opplevelsen av umiddelbarhet er derfor en komponent i denne effekten. Når det tar lang tid mellom utførelse av hendelse og attribusjon av hendelse, kan opplevelsen av umiddelbarhet svekkes.

Teori om tvang har forstått selve handlingen som bærende for kommunikasjon av beslutsomhet. Dette legges også til grunn i analyse til Borghard og Lonergan (2017, 2023) og Nye (2017). Tvang må imidlertid ikke oppnås ved en isolert handling, men kan skapes gjennom en kombinasjon av handlinger. George (1991, s. 9) har argumentert for at tvang ikke bare inkluderer rene handlinger, men også verbal kommunikasjon. Mer konkret har Poznansky og Perkoski (2018) argumentert for at en stat vil kunne ta på seg ansvaret for en cyberhendelse, og gjøre dette i hemmelighet, dersom målet er å legge press på eller tvinge målet for hendelsen. En cyberoperasjon for effekt og signal av hvem som står bak kan kommuniseres direkte til målet gjennom diplomatiske kanaler eller uformelle kanaler. Dette innebærer at dersom intensjonen er å oppnå en tvangseffekt, kan kommunikasjonen følge denne intensjonen. Dette oppfyller det sentrale premisset om at tydelig kommunikasjon må til for å oppnå en troverdig trussel om fremtidig straff dersom staten ikke endrer sin handlemåte. I litteratur om tvang i cyberdomenet legges det til grunn at det er et mål om å holde aktiviteten skjult. Denne skjulte aktiviteten gjør at krav ikke kan fremsettes (Lindsay & Gartzke, 2018, s. 17). Men dersom intensjonen er å tvinge den andre staten til å endre handlemønster ved å kommunisere en vilje til å bruke makt, er det mulig å kommunisere dette gjennom andre kanaler.

4.3 Muligheter for kommunikasjon gjennom fordekt aktivitet

Selv om handlingen ikke følges opp med direkte kommunikasjon, kan motstanderen i noen tilfeller likevel forstå intensjonen bak handlingen. Carson og Yarhi-Milo (2017) har utviklet et rammeverk for å forstå signalering i en fordekt sfære (*covert sphere*). Rammeverket bidrar til en forståelse av hvordan stater oppfatter den intenderte meldingen bak fordekt kommunikasjon av besluttsomhet. Forfatterne legger til grunn at fordekte handlinger ofte vil bli oppfattet av strategiske rivaler på grunn av moderne etterretningsinnsamling. Basert på dette identifiserer

Carson og Yarhi-Milo (2017) mekanismer som gir troverdighet til fordekte signaler. Den første mekanismen er knyttet til irreversible kostnader, som er aktivitet som utnytter ressurser som ikke er mulig å få tilbake. Dette kommuniserer at staten mener alvor. Den andre mekanismen omhandler hvordan fordekte handlinger som skal kommunisere besluttsomhet kan fremstå som pålitelige fordi de innebærer en risiko for eskalering. Andre stater reagerer gjerne på fordekte handlinger på måter som kan føre til en oppskalering av konflikten, som kan medføre at situasjonen eskalerer ut av kontroll. Hemmelighold forsterker denne dynamikken, da det tar bort noe av begrensninger som press som legges på statslederen fra interesser både innenriks og utenriks. Hvis vi tar dette i betraktning, kan det være mulig å kommunisere tvang til andre stater, fordi staten oppfatter denne handlingen i en bestemt kontekst.

Trusler om tvang kan deles inn i to kategorier. Ren kommunikasjon om fremtidig bruk av makt og en begrenset handling som viser vilje til bruk av makt (Schelling, 1966). Den første fremgangsmåten er vanskelig å oppnå ved bruk av cyberoperasjoner for effekt. Dette er fordi det bør involvere en spesifikk trussel for å virke troverdig. Spesifikke trusler kan bli avverget ved å sikre systemer. Videre er evnen til å utvikle aksesser til nettverk og systemer hemmelig informasjon. Dette gjør at det er knyttet usikkerhet til hvor stor skade en stat kan gjøre mot en annen stat. Usikkerheten kan forsterke troverdigheten til trusselen om fremtidig skade, men det kan også føre til at den andre staten tror trusselen er en bløff. Stater som har renommé for å ha en velutviklet cyberkapabilitet kan teoretisk sett kommunisere trusler om straff gjennom denne fremgangsmåten. Stater som ikke har et slikt rennommé, vil trolig slite med å oppnå effektiv tvang mot andre stater gjennom cyberoperasjoner.

Når det gjelder den andre fremgangsmåten, er det i teorien mulig å signalisere besluttsomhet ved å påvirke motstanderens kritiske systemer. Denne handlingen kommuniserer en vilje til bruk av makt, og antyder at ytterligere tiltak kan følge dersom den andre staten ikke endrer sin atferd. Problemet er imidlertid at kommunikasjon av beslutsomhet krever tilstrekkelig skadelige virkninger, og dette er vanskelig å oppnå gjennom cyberoperasjoner (Siedler, 2016, s. 33–34). Grensen for hvor store effekter en cyberoperasjon må kunne skape for å kommunisere besluttsomhet er ikke etablert. Valeriano et al. (2018) løfter frem cyberoperasjoner som tilsvarer Stuxnet i effekt som et referansepunkt for hvilke typer hendelser som kan oppnå en tvangseffekt overfor en annen stat. Dette er svært ressurskrevende aktivitet og vil kreve at en aktør utvikler tilganger til kritiske nettverk og systemer i fredstid. Terskelen for å kunne oppnå slike effekter er dermed svært høy. Derfor er det nærliggende å konkludere med at cyberoperasjoner for effekt er lite egnet for å oppnå tvangseffekter. Teoretisk er det mulig å gjennomføre ved å kombinere cyberoperasjonen mot kritiske systemer med en dimensjon av klar kommunikasjon. Rent praktisk er det et stort hinder at nedre grense for hvor omfattende effekten må være for å skape en tvangseffekt ikke er tydelig etablert. Trolig vil det uansett kreve et høyt ressursnivå for å etablere aksesser som er i stand til å skape en tilstrekkelig sterk effekt for å kommunisere beslutsomhet.

4.4 Eskalering som signalering

I *Escalation Dynamics in Cyberspace* tar Lonergan og Lonergan (2023) utgangspunkt i fraværet av eskalering mellom stater som følge av cyberhendelser. De legger til grunn at teknologien settes grensene for muligheter og begrensninger for eskalering. Derfor fokuserer Lonergan og Lonergan på de tekniske aspektene ved cyberoperasjoner og mulighetene og begrensningene disse aspektene legger på statsledere. Forfatterne løfter frem fem kjennetegn ved cyberdomenet som former eskaleringsdynamikker: (i) hemmelighold, (ii) troverdig benektelse, (iii) kravene for å planlegge og gjennomføre offensive cyberoperasjoner, (iv) usikkerhet knyttet til cyberoperasjonens kostnad for motstanderen, og (v) rollen som etterretning spiller, knyttet til avveiningen mellom å beholde tilgang til systemer for etterretning mot å utføre en effekt på systemet gjennom en offensiv cyberoperasjon (Lonergan og Lonergan, 2023, s. 34–56).

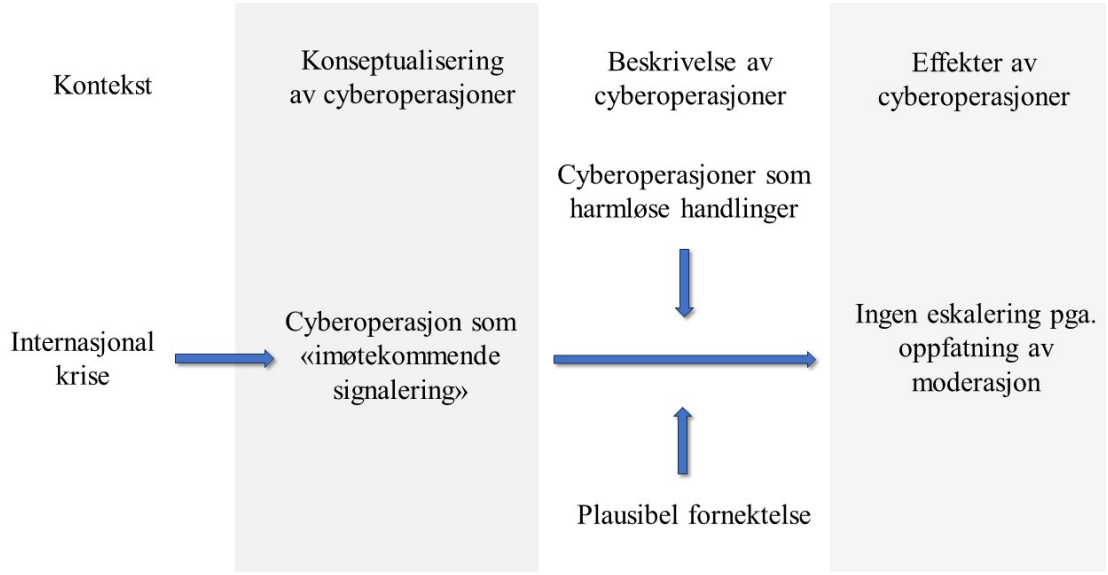
Disse karakteristikkene påvirker hvordan stater bruker cyberoperasjoner for strategiske hensikter. Karakteristikkene legger grunnlaget for et mulighetsrom som formes av tre sentrale mekanismer:

I. De fleste offensive cyberoperasjoner av strategisk betydning er kostbar, kompleks, uforutsigbar, vanskelig å opprettholde over tid og begrenset i deres evne til å skape store kostnader hos målet. Implikasjonen av dette er at den angripende part ikke har overtaket i cyberdomenet (Lonergan og Lonergan, 2023, s. 38–46).
II. Karakteristikker som hemmelighold og plausibel fornektbarhet skaper et pusterom som kan gi beslutningstagere litt mer tid til å handle (Lonergan og Lonergan, 2023, s. 34–38).
III. Mulighetene som cyberdomenet skaper for innhenting av etterretning skaper avveininger som beslutningstagere må ta hensyn til (Lonergan og Lonergan, 2023, s. 54–56).

Implikasjonene av disse mekanismene er et strategisk miljø der interaksjonen mellom motstandere trolig vil være karakterisert av relativ stabilitet og begrensede eskaleringsdynamikker (Lonergan og Lonergan, 2023, s. 84–85).

Lonergan og Lonergan følger opp dette perspektivet med en gjennomgang av hvordan cyberoperasjoner kan bidra til å dempe konfliktsituasjoner. Den sentrale mekanismen i denne sammenhengen er at offensive cyberoperasjoner gir beslutningstagere muligheten til å handle i en situasjon som ellers er kjennetegnet av et begrenset handlingsrom for å benytte militære virkemidler. Dette omtaler Lonergan og Lonergan som imøtekommende signalering. Beslutningstageren velger i denne situasjonen aktivt å ikke benytte seg av militære virkemidler, men heller et mindre skadelig virkemiddel. Valget om å avstå fra mer skadelige virkemidler kan bidra til å kommunisere et ønske om å ikke eskalere situasjonen til motstanderen. Denne effekten oppstår ved å kommunisere at aktøren holder igjen tilgjengelige virkemidler, som igjen kommuniserer moderasjon og vilje til å inngå kompromiss. Handlingen er også synlig, men kan ikke direkte kobles til avsenderen. Dette skaper troverdig benektelse. Implikasjonen

av dette er at offensive cyberoperasjoner som imøtekommende signalering kan bidra til å redusere spenningsnivået i konflikten (Lonergan og Lonergan, 2023, s. 86-107). Utvalget til Lonergan og Lonergan i deres studie består hovedsakelig av hendelse som involverte distribuert tjenestenekt (DDoS) og *defacement* av nettsider. Disse typene operasjoner utgjør 15 av 18 hendelser i utvalget. Én hendelse omtaler forsøk på phishing, en annen om skadevare mot myndighetsnettverk og en tredje om forsøk på å få tilgang til e-postkontoer (se Lonergan g Lonergan, 2023, s. 159–162). Lonergan og Lonergan konkluderer med at cyberoperasjoner for «imøtekommende signalering» er kjennetegnet av lave kostnader for gjennomføring og synlige effekter (Lonergan, 2023, s. 195). Basert på denne beskrivelsen kan vi forstå det som at de henviser til DDoS og *defacement.*[13] Cyberoperasjoner skal altså kunne fungere som imøtekommende signalering og legge grunnlaget for en fredelig løsning av en konflikt som følge av de samme mekanismene som gjør at offensive cyberoperasjoner ikke skaper eskalering. Den sentrale argumentasjonen til Lonergan og Lonergan oppsummeres i den følgende illustrasjonen.



Figur 4.1 Lonergan og Lonergan: Eskaleringsdynamikker i cyberspace (2023).

Hovedargumentet til Lonergan og Lonergan er at cyberoperasjoner kan fungere som et signal om vilje til å de-eskalere en spent situasjon mellom to stater. Dette konseptet omtales gjerne som beroligelse (*reassurance*) i andre deler av den statsvitenskapelige litteraturen om relasjoner mellom stater. Lonergan og Lonergan henviser også til dette begrepet i sin omtale av hvordan cyberoperasjoner kan benyttes til signalering (se eks. Lonergan og Lonergan, 2023, s. 104, 107). De henviser også til begrepet *restraint*, som kan oversettes til tilbakeholdenhet,

[13] Her må vi ta hensyn til en skjevhet i det tilgjengelige datamaterialet: DDoS er svært synlige hendelser, og det er dermed en overvekt av rapporter om disse hendelsene i åpne kilder. Det samme er ikke nødvendigvis tilfellet for andre typer cyberhendelser. Påstanden om at DDoS kan fungere godt som «imøttekommende signalering» kan dermed være et resultat av skjevhet i datamaterialet. Lonergan og Lonergan påpeker selv skjevheten i datamaterialet (2023, s. 108), men reflekterer ikke rundt hvordan dette kan ha påvirket deres sentrale konklusjoner.

for å beskrive hvordan cyberoperasjoner kan virke inn på konfliktsituasjoner (Lonergan og Lonergan, 2023, s. 96). Dette blir gjerne omtalt for å beskrive kjennetegn med mer overordnede strategiske fremgangsmåter i litteraturen, og ikke en metode for å signalere intensjon til andre stater i krisesituasjoner (se eks. Posen, 2014). Jeg velger derfor å fokusere på begrepet beroligelse i denne gjennomgangen.

En sentral mekanisme i beroligelse er kostbare signaler[14] (se f.eks. Fearon, 1997; Kydd, 2000; Montgomery, 2006). Kostbare signaler sendes for å overtale en motstander om at de kan ha tillit til at statens handlinger er troverdige. Troverdigheten stammer fra at signalet er så kostbart eller risikabelt at det ikke ville blitt sendt dersom avsenderen ikke mente alvor. Dette betyr at for å berolige den andre staten må signalet være tilstrekkelig kostbart (Fearon, 1997; Kydd, 2000; Montgomery, 2006). Et illustrerende eksempel er å trekke militære styrker tilbake fra grenseområder, mens den andre staten fortsatt har sine styrker utplassert på andre siden av grensen. Handlinger som ikke innebærer en tilstrekkelig stor risiko, kan bli oppfatt som et forsøk på å lure motstanderen og dermed ikke bidra til å endre oppfatning om statens intensjoner (Fearon, 1997). Troverdig signalering av beroligelse innebærer dermed å relativt svekke sin egen makt for å berolige den andre parten om velvillige intensjoner.

Hvis vi setter argumentet til Lonergan og Lonergan opp mot sentral litteratur på å signalisere beroligelse til andre stater, støter det sentrale argumentet i *Escalation Dynamics* på et problem: cyberhendelse kan bli oppfattet som det Fearon (1997) beskriver som *cheap talk*[15]. Dette er handlinger som vil oppfattes av den andre parten som halvhjertede tiltak som utføres mest for syns skyld, og ikke for å reelt sett endre den andre partens oppfatning av egen intensjon. Handlingen innebærer ikke tilstrekkelig stor risiko for avsenderen til å bli tatt på alvor av mottakeren. Hvis vi legger dette til grunn, kan lavskala cyberoperasjoner som «imøtekommende signalering» stå i fare for å ikke bli forstått som et forsøk på å berolige, men heller blir oppfattet av den andre staten som et forsøk på å lure motstanderen.

Et problem med argumentet er imidlertid at selv lavskala cyberoperasjoner gjerne blir omtalt som en aggressiv handling. Hendelsene blir gjerne beskrevet som et «angrep», på like linje med mer alvorlige cyberoperasjoner. Siden det synes å være en mangel på nyanser i offentlig omtale av cyberoperasjoner og dermed hvordan handlingen blir oppfattet og mottatt, kan det være risikabelt å anta at en lavskala cyberoperasjon i alle tilfeller vil bli oppfattet som en intensjon til å de-eskalere en internasjonal konflikt. Lonergan og Lonergan løfter frem at lavskala cyber-operasjoner er relativt harmløse handlinger. Denne påstanden er riktig. Det er imidlertid en forskjell mellom den reelle effekten en handling kan oppnå og oppfatningen av hva denne

[14] Min oversettelse av begrepet «*costly signals*».

[15] Lonergan og Lonergan referer selv til Fearon (1997) i utviklingen av sin teori. De tar imidlertid ikke høyde at deres beskrivelser at cyberoperasjoner som de-eskalerende handlinger også kan omfattes av hans konsept om «cheap talk». De henviser hovedsakelig til det Fearon skriver om besluttsomhet («resolve»): «*States can convey how resolved they are by engageing in different forms of costly signaling, allowing resolute states to distinguish themselves form irresolute ones*» (Lonergan & Lonergan, 2023, s. 88).

handlingen kan oppnå. Dette gjelder særlig for cyberoperasjoner. I en anspent konfliktsituasjon kan motstanderen blir usikker på om handlingen er opptakten til et mer alvorlig angrep, slik vi så var tilfelle i januar 2022 i forkant av den russiske invasjonen av Ukraina. En usikkerhet knyttet til mottagerens oppfatning av handlingen vil dermed være til stede. Basert på dette bør vi inkludere misoppfatninger som en del av potensielle eskaleringsdynamikker som kan utspille seg etter en offensiv cyberoperasjon. Faren for misoppfatninger av intensjoner vil imidlertid variere mellom ulike stater. Dersom statene har gode kanaler for kommunikasjon under kriser (f.eks. diplomatiske kanaler eller bak-kanaler), er det rimelig å anta at en cyberoperasjon ikke vil blir oppfattet som en stor trussel om ytterligere eskalering av situasjonen. Dersom kanaler for kommunikasjon ikke er til stede, er det rimelig å anta at misoppfatningen kan føre til en fare for ytterligere destabilisering av situasjonen.

5 Tilsiktet og utilsiktet eskalering

Diskusjoner om mulig eskalering som følge av cyberoperasjoner er relevant i tilknytning til strategisk nytte. Dette er fordi det diskuterer følgene av å benytte cyberoperasjoner for strategisk effekt, samt at det belyser en ekstra dimensjon av mulige begrensninger ved å bruke cyberoperasjoner for strategisk effekt. Lonergan og Lonergan (2023) diskuterer hvordan cyberoperasjoner kan virke de-eskalerende på en anspent situasjon mellom to stater. Hvorvidt cyberoperasjoner kan føre til eskalering, forblir imidlertid et bestridt moment. Det følgende vil presenterere to ulike posisjoner knyttet mulige effekter cyberoperasjoner kan ha på eskalering mellom stater.

I «Preparing the Battlefield» diskuterer Buchanan og Cunningham (2023) potensialet for eskalering som følge av problemet med å skille mellom cyberoperasjoner for etterretning og operasjoner som forbereder en fremtidig effekt mot systemet. Hovedargumentet til Buchanan og Cunningham er at dette problemet skaper et mulig forløp for utilsiktet eskalering. Potensialet for utilsiktet eskalering oppstår når den ene parten utfører en cyberoperasjon for etterretning, mens målet for operasjonen oppfatter dette som en forberedelse for fremtidig effekt. En forutsetning for at eskalering skal oppstå er at den blir oppdaget i kontekst av en krise. Et sentralt premiss i Buchanan og Cunninghams teori er at cyberoperasjoner er hemmelig informasjon. Dette legger grunnlaget for usikkerheten om reelle intensjoner bak en hendelse.

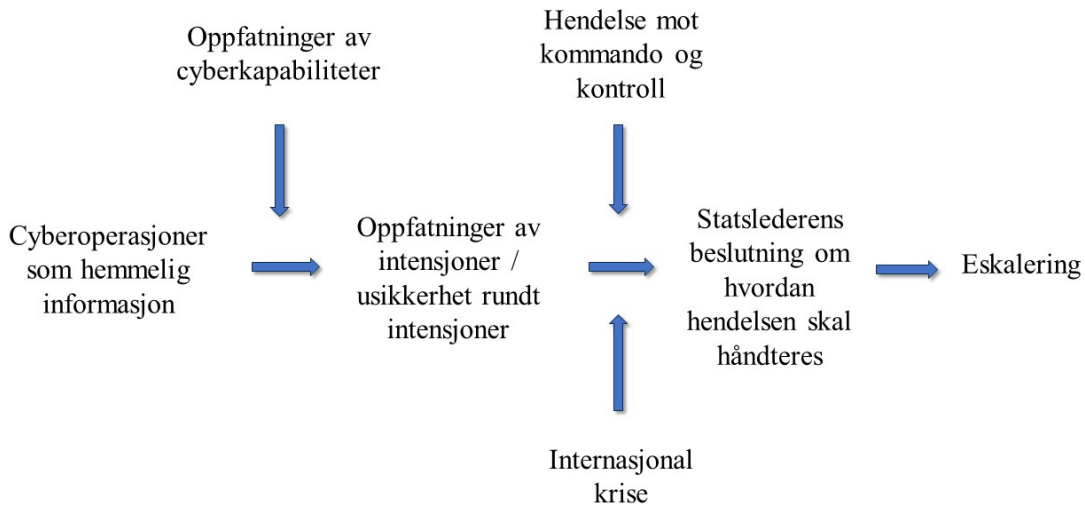
En forutsetning for å utføre en cyberoperasjon som har potensialet for å oppnå en strategisk effekt er forberedelse og overvåkning av systemet. Evnen til å oppnå en målrettet effekt krever god forståelse av målsystemet. Dette kan skape frykt for et nært forestående cyberangrep med omfattende konsekvenser. Dette kan resultere i at målet velger å svare ved å bruke makt først,

enten gjennom et cyberangrep eller gjennom kinetiske midler, ifølge Buchanan og Cunningham (2023). En stat som oppdager at en motstander har kommet seg inn i kommando og kontroll knyttet til kjernefysiske våpen, eller kommunikasjonsnettverk under en krise er et særlig alvorlig scenario. At en motstander klarer å skaffe tilgang til kommando og kontroll til kjernefysiske våpen er et usannsynlig scenario. Disse systemene har et svært høyt sikkerhetsnivå. Dersom en aktør skulle oppnå tilgang til denne typen systemer, vil det være tydelig at aktøren mener alvor. Det er nok nettopp på grunn av dette at Buchanan og Cunningham (2023) løfter det frem som et særlig alvorlig scenario.

Basert på dette presenterer Buchanan og Cunningham (2023) to forløp for eskalering. Den første er tilsiktet eskalering. Stater kan vurdere at cyberhendelser utført en alvorlig, men akseptabel trussel og fortsatt velge å eskalere situasjonen fordi de har strategiske eller politiske insentiver til å velge det handlingsforløpet. Slike strategiske eller politiske insentiver kan være å oppnå et militært overtak, signalere beslutsomhet eller å komme motstanderens forsøk på å signalere beslutsomhet i forkjøpet.

Det andre forløpet går ut på at beslutningstagere velger å ikke bruke makt etter å ha oppdaget en cyberhendelse under en krisesituasjon – selv om de er sikre på at hendelsen var en forberedelse på en cyberoperasjon for effekt. Årsaken til dette er at de vurderer at cyberoperasjonen ikke utgjør en alvorlig trussel. Dette handlingsforløpet baserer seg på at beslutningstagere vurderer at cyberoperasjoner ikke har potensialet for å skape effekter som er alvorlige nok til å rettferdiggjøre et motsvar gjennom maktbruk.

Hovedargumentet til Buchanan og Cunningham kan illustreres på følgende måte.



Figur 5.1 Buchanan og Cunningham: Et mulig eskaleringsforløp (2023).

Selve antagelsen om at cyberoperasjoner er hemmelig informasjon har blitt problematisert. Baram (2023) skriver at ulike aktører som utfører cyberoperasjoner selv har valgt å gå ut med

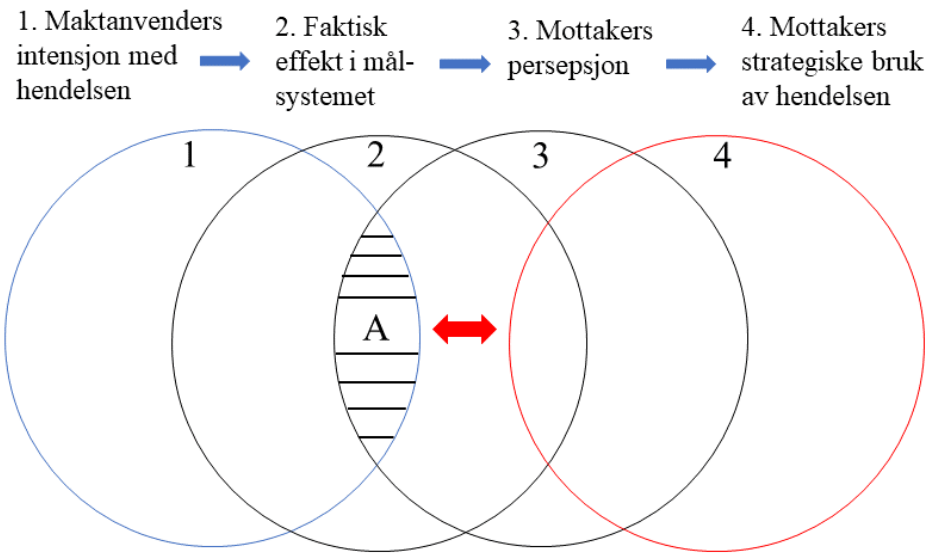
denne informasjonen, til tross for fordelene ved å holde aktiviteten hemmelig. Situasjonen bør ikke beskrives som hemmelighold/ikke hemmelighold, men heller at aktørene har en rekke valg de kan ta for hvordan de vil håndtere situasjonen. Å benekte at en står bak hendelsen er ikke det samme som å forbli stille. Nytten av disse to handlingene vil dermed være ulik. Videre kan målet for operasjonen velge å ikke gå offentlig ut med informasjonen, for å gi begge parter større spillerom til å håndtere situasjonen.

Et annet poeng gjelder vilje til å eskalere situasjonen. Hvis beslutningstagere ikke har en direkte interesse av å eskalere situasjonen, vil tilfeller som denne trolig tas gjennom offentlig fordømmelse av hendelsen eller reaksjoner gjennom diplomatiske kanaler. Trusselen ble oppdaget før den inntraff, og dersom statene har god bilateral krisekommunikasjon kan det resultere i at spenningen reduseres før den øker ut av kontroll. Det er også tiltak staten kan ta i sine egne systemer for å håndtere hendelsen før den velger å svare ved bruk av makt.

Et alternativt perspektiv til det i avsnittet over følger av at viktig kjennetegn ved cyberhendelser er at koblingen mellom angripers intensjon, faktisk virkning og hvordan den som rammes forstår og kommuniserer virkning og effekt av operasjonen er løs. Virkningen av en cyberoperasjoner er lite synlig, og dette gir derfor den som rammes en sterk definisjonsmakt over hva som skjedde.

Dette perspektivet er illustrert i Figur 5.2[16] som viser at det kan være lite sammenfall (område A) mellom angripers intensjon, faktisk virkning for mottagerens systemer og mottagers oppfatning av effekt. Denne situasjonen skaper en mulighet for forsvareren til å bruke og fremstille hendelsen på en måte som avviker fra avsenders intensjon. En mulig konsekvens av dette er at den som blir rammet av en hendelser ønsker å overdrive effekten av denne for å kunne dra strategisk nytte av cyberhendelsen. En tenkt situasjon der den som rammes kan oppnå slik nytte, er dersom den har et ønske om å eskalere situasjonen til de fysiske domene. Da er det tenkelig at effekten av en cyberhendelse kan overdrives for å legitimere en eskalerende utvikling av konflikten.

[16] Figuren er basert på tidligere arbeider ved FFI.



Figur 5.2 Sammenfall mellom angripers intensjon, faktisk effekt og mottakers oppfatning av effekt.

Et sentralt poeng hos Buchanan og Cunningham (2023) er at innbrudd i systemer har potensial for eskalering fordi det kan benyttes for å oppnå en destruktiv effekt på et senere tidspunkt. Aktøren som beskytter systemet, vet ikke hva den reelle hensikten med tilgangen er. Dermed er det viktig å ta beslutningstageres vurdering av situasjonen inn i beregningen. Ulike studier presenterer motstridende funn rundt hva beslutningstageres vurdering kan bestå av. Schneider (2017) har vist gjennom en serie av krigsspill at sivile og militære beslutningstagere i USA er mindre villig til å benytte cyberoperasjoner for effekt tidlig i en konfrontasjon fordi de ble ansett som for provoserende. Beslutningstagerne i studien var også mindre villig til å benytte dem senere i en konflikt, da de ble ansett for å være mindre effektive for å oppnå strategiske målsettinger relativt til kinetiske virkemidler. En studie av Jensen, Valeriano og Whitt (2024) presenterer et annet perspektiv. Gjennom krigsspill fant de at deltagerne foretrakk å benytte ikke-eskalerende cyberoperasjoner fremfor tradisjonelle militære handlinger. Cyberoperasjoner ble ansett som et positivt element fordi det skapte et utvidet forhandlingsrom og utgjorde et alternativ til militærmakt. Jensen et al. fant dermed at muligheten for å benytte cyberoperasjoner reduserer sannsynligheten for at situasjonen eskalerer ved å tilby et alternativ til konvensjonelle militære handlinger.

Krigsspillstudiene til Schneider (2017) og Valeriano et al. (2024) er utgitt med flere års mellomrom. De kan bidra til å illustrere hvordan oppfatningen av nytten ved cyberoperasjoner blant beslutningstagere endres over tid. USA valgte i 2019 å utføre en cyberoperasjon mot iranske våpensystemer, heller enn å benytte luftangrep mot tilsvarende mål. En iransk etterretningsgruppe var også mål for en cyberoperasjon. Dette skal ha vært et angrep mot en oljetanker, som den iranske etterretningsgruppen deltok i planleggingen av (Barnes & Gibbons-Neff, 2019). En mulig forklaring kan dermed være at amerikansk praksis gjennom

cyberoperasjoner har bidratt til å forme oppfatningen av mulighetsrommet for bruk av dette virkemiddelet. Det forutsetter imidlertid tilgang til mål som er av strategisk betydning for motstanderen. USA er regnet som staten med den fremste cyberkapabiliteten etter en indeks (Voo et al., 2022). En stat uten tilsvarende ressurser vil ikke nødvendigvis ha evnen til å oppnå tilgang til slike systemer. Dette kan påvirke vurderingen som beslutningstagere gjør, da dette vil formes av det de oppfatter som det reelle mulighetsrommet for å benytte cyberkapabiliteter.

Et annet bidrag som tar for seg eskalering som følge av cyberoperasjoner er Healey og Jervis' (2023) artikkel «The Escalation Inversion». Utgangspunktet for Healey og Jervis er at de anser det som usannsynlig at cyberoperasjoners innvirkning på stabilitet ikke avhenger av kontekst, som eksisterende litteratur antar. Trusselen mot stabilitet vil endres basert på det gjeldende forholdet mellom statene, ikke som følge av de kjennetegn på aktiviteten som gjennomføres.

Healey og Jervis (2023) analyserer disse forholdene gjennom et rammeverk som de omtaler som «situasjonsbetinget cyberstabilitet» og løfter frem fire mekanismer som påvirker situasjonen. Den første mekanismen går ut på at cyberoperasjoner kan legge en demper på konfliktnivået når konteksten er kjennetegnet av fred og stabilitet. I denne konteksten har stater ikke ønsket å besvare cyberhendelser med kinetiske virkemidler. Healey og Jervis (2023) løfter frem at dette er situasjonsbetinget – det kan endre seg dersom kontekster er kjennetegnet av et høyere konfliktnivå.

Den andre mekanismen går ut på at cyberhendelser kan føre til eskalering uten at det krever en direkte gjengjeldelse på en konkret hendelse. I stedet kan eskaleringsprosessen være kjennetegnet av en trend over tid. I denne prosessen er det ikke mulig å etablere et konkret kausalt forløp, men heller en intensifiering av konfliktnivået over tid. Healey og Jervis fremhever at et økt geopolitisk spenningsnivå i årene fremover kan føre til at stater vil være mindre tilbakeholdne i cyberdomenet.

Den siste mekanismen knyttes opp mot at bruken av (eller frykten for) cyberoperasjoner kan eskalere akutte geopolitiske kriser. Når sentrale nasjonale ressurser står på spill, vil en annen dynamikk i cyberdomenet fremtre. Healey og Jervis fremhever at det ikke er direkte relevant om cyberkapabiliteter kan oppnå strategiske effekter. Beslutningstagere synes å tro at de kan det, og denne (feil)oppfatningen er drivkraften bak denne mekanismen, hevder de. Årsaken til dette er at oppfatningen av hvilke effekter cyberhendelser kan skape kan føre til feilvurderinger og feilsteg, som kan bidra til å forsterke en eksisterende konfliktsituasjon. Denne effekten forsterkes ved at stater oppfatter og fortolker risiko og usikkerhet i cyberdomenet på ulike måter (Brantly, 2021). Det er dermed vanskelig å etablere en forståelse av betydningen av (feil)oppfatninger, da dette synes å variere mellom stater. På bakgrunn av dette vil andre stater mulige (feil)oppfatninger være en kilde til usikkerhet når stater skal vurdere muligheter og begrensninger ved å benytte cyberoperasjoner for å påvirke relasjonen til en annen stat.

6 Konklusjon

Om cyberoperasjoner kan være strategisk nyttige, er et omtvistet punkt i litteraturen. Gjennomgangen viser at dette har vært et sentralt spørsmål, men at konklusjonene spriker rundt den reelle nytten av cyberoperasjoner for å oppnå strategiske målsettinger. De sentrale perspektivene i litteraturen kan oppsummeres på følgende måte:

- Cyberdomenet utgjør et unikt strategisk miljø. Dette er kjennetegnet av aktiviteten vedvarende innsats, som gjennom effekter mot motstanderes systemer kan endre maktbalansen og etablere rammer for akseptabel atferd i cyberdomenet.
- En rekke eller serier, omtalt som kampanjer, av cyberoperasjoner kan bidra til å endre maktbalansen mellom stater. Derfor bør de overordnede effektene av cyberoperasjoner analyseres i et kampanjeperspektiv.
- Cyberoperasjoner kan være strategisk nyttige, men operasjonelle avveininger legger begrensninger på den reelle effekten. Aktøren må balansere mellom styrken og omfanget av effektene, tidsbruk mellom starten på operasjonen og øyeblikket ønsket effekt er oppnådd, og kontroll over egen operasjon. Denne balansegangen innebærer blant annet at en kortere tidsramme på operasjonen, vil føre til redusert effekt og kontroll.
- Problematikk knyttet til attribusjon av en cyberhendelse til en aktør begrenser mulighetene for å benytte dette virkemiddelet for å oppnå avskrekking og tvang av en annen stat. Dette innebærer at cyberoperasjoner benyttes for å hindre at en annen stat handler på en bestemt måte, eller for å få den andre staten til å endre handlemønster. I tillegg svekkes potensialet for disse effektene som følge av problematikk knyttet til å oppnå en tilstrekkelig sterk effekt som en følge av cyberoperasjoner.
- Hvorvidt cyberoperasjoner er aktivitet som påvirker stabiliteten mellom stater avhenger av hvordan beslutningstagere oppfatter situasjonen og hvorvidt relasjonen mellom to stater er preget av generell stabilitet eller ustabilitet. Oppfatninger og kontekst må dermed tas med i betraktning når mulige følger av cyberoperasjoner skal vurderes.

Gjennomgangen har vist at den statsvitenskapelige litteraturen om cyberoperasjoner består av å diskutere fenomenet opp mot eksisterende teoretiske rammeverk, samt å utvikle nye rammeverk for å forstå staters bruk av cyberoperasjoner som et maktmiddel. Denne fremgangsmåten har tre følger. For det første tar flere av bidragene tar utgangspunkt i abstrakt teori heller enn praksis. En styrke ved Maschmeyer (2021, 2024) er en kombinasjon av teori med praktiske tilnærminger til cyberoperasjoner. Resultatet er en mer nøyaktig beskrivelse av mulighetsrom og begrensinger ved staters bruk av cyberoperasjoner for å påvirke relasjoner til andre stater. Denne fremgangsmåten anbefaler jeg blir mer utbredt.

For det andre, ved å ta utgangspunkt i ulike teorier beskriver den statsvitenskapelige litteraturen cyberoperasjoner som ulike fenomener. For eksempel er «imøtekommende signalering» og «subversjon» to ulike fenomener. Dette er nyttig for å beskrive en del av aktiviteten som fore-

kommer i empirisk materiale, men ikke all aktivitet. Problemet er imidlertid at flere bidrag i litteraturen omtaler «cyberoperasjoner» i en bred forstand. Dette bidrar til en forenklet fremstilling av cyberoperasjoners innvirkning på internasjonal politikk. Cyberoperasjoner blir benyttet for å oppnå flere ulike målsettinger. Dette må vi ta med oss inn i en forståelse av cyberoperasjoner, og dermed forstå bidragene som forsøk på å beskrive mulige bruksområder for og nytte av cyberoperasjoner i internasjonal politikk. Virkemiddelet blir ikke benyttet for å oppnå en enkelt målsetting, som å endre maktbalansen i internasjonal politikk, og dette bør gjenspeiles i teoretiske rammeverk.

Fremtidig forskning kan være tjent med å legge vekt på to ulike aktiviteter. Den første aktiviteten er å utvikle eller forbedre forståelsen av hvilke mekanismer som kan bidra til å beskrive sammenhengen mellom cyberaktivitet og potensiell strategisk nytte. Deler av den eksisterende litteraturen tenker for enkelt når det gjelder cyberoperasjoner. Det er derfor vi må åpne for å inkludere mer avanserte årsakskjeder og å studere kjente cyberoperasjoner i sin kontekst, og ikke abstrahere bort relevante detaljer som blant annet teknologisk utvikling innen cybersikkerhet. Dette vil bare føre til en forenkling, og ikke til forbedrede forutsetninger for å forstå de sentrale mekanismene i stater bruk av cyberoperasjoner som et maktmiddel i internasjonal politikk. Den andre aktiviteten er å stykke opp cyberaktivitet i ulike kategorier for aktiviteten. For eksempel etterretningsaktivitet i fredstid, (industri)spionasje, statsdrevet økonomisk kriminalitet, annen økonomisk kriminalitet, taktiske cyberoperasjoner i kontekst av væpnet konflikt, sabotasje/*brute force* (mot kritisk infrastruktur).

Referanser

Ashraf, C. (2021). Defining cyberwar: Towards a definitional framework. *Defense & Security Analysis*, *37*(3), 274–294. https://doi.org/10.1080/14751798.2021.1959141

Bakke, S. (2023, april 25). *Offensive Cyber Operations, av Daniel Moore*. Stratagem. https://www.stratagem.no/offensive-cyber-operations-av-daniel-moore/

Baram, G. (2023). Public Secrets: The Dynamics of Publicity and Secrecy in Offensive Cyber Operations. *Journal of Global Security Studies*, *8*(3), https://doi.org/10.1093/jogss/ogad013

Barnes, J. E., & Gibbons-Neff, T. (2019, juni 22). 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

Biddle, T. D. (2020). Coercion Theory: A Basic Introduction for Practitioners. *Texas National Security Review*, *3*(2).

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

Borghard, E. D., & Lonergan, S. W. (2023). Deterrence by denial in cyberspace. *Journal of Strategic Studies*, *46*(3), 534–569. https://doi.org/10.1080/01402390.2021.1944856

Brantly, A. F. (2021). Risk and uncertainty can be analyzed in cyberspace. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab001

Buchanan, B., & Cunningham, F. S. (2023). Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-A- merican Crisis. I R. Chesney, J. Shires, & M. Smeets (Red.), *Cyberspace and Instability*. Edinburgh University Press. https://www.jstor.org/stable/10.3366/jj.7358680.7

Carson, A., & Yarhi-Milo, K. (2017). Covert Communication: The Intelligibility and Credibility of Signaling in Secret. *Security Studies*, *26*(1), 124–156. https://doi.org/10.1080/09636412.2017.1243921

Chesney, R., & Smeets, M. (Red.). (2023). *Deter, Disrupt, or Decieve: Assessing Cyber Conflict as an Intelligence Contest*. Georgetown University Press.

Delerue, F. (2020). *Cyber Operations and International Law*. Cambridge University Press; Cambridge Core. https://doi.org/10.1017/9781108780605

Egloff, F. J., & Shires, J. (2021). Offensive Cyber Capabilities and State Violence: Three Logics of Integration. *Journal of Global Security Studies*, *7*(1). https://doi.org/10.1093/jogss/ogab028

Fearon, J. (1997). Signaling Foreign Policy Interests: Tying Hands Versus Sinking Costs. *Journal of Conflict Resolution*, *41*(1), 68–90.

Fearon, J. D. (1994). Domestic Political Audiences and the Escalation of International Disputes. *American Political Science Review*, *88*(3), 577–592. Cambridge Core. https://doi.org/10.2307/2944796

Fedorov, M. (2023). *The Face of Modern Hybrid Warfare*. Digital Front Lines. Hentet 17. april 2024, fra https://digitalfrontlines.io/2023/05/31/lessons-from-ukraine-in-the-heat-of-an-ongoing-hybrid-war/

Fischerkeller, M. P., Goldman, E. O., Harknett, R. J., & Nakasone, P. M. (2022). *Cyber Persistence Theory: Redefining National Security in Cyberspace* (1. utg.). Oxford University Press. https://doi.org/10.1093/oso/9780197638255.001.0001

Gartzke, E. A., Carcelli, S., Gannon, J. A., & Zhang, J. J. (2017). Signaling in Foreign Policy. I E. A. Gartzke, S. Carcelli, J. A. Gannon, & J. J. Zhang, *Oxford Research Encyclopedia of Politics*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.481

George, A. L. (1991). *Forceful Persuasion: Coercive Diplomacy as an Alternative to War*. United States Institute for Peace Press.
Gilli, A., & Gilli, M. (2019). Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage. *International Security*, *43*(3), 141–189. https://doi.org/10.1162/isec_a_00337
Glaser, C. L. (2010). *Rational Theory of International Politics: The Logic of Competition and Cooperation*. Princeton University Press; JSTOR. https://doi.org/10.2307/j.ctt7t1j1
Glaser, C. L., & Kaufmann, C. (1998). What is the Offense-Defense Balance and Can We Measure it? *International Security*, *22*(4), 44. https://doi.org/10.2307/2539240
Goldman, E. O. (2004). Introduction: Military Diffusion and Transformation. I E. O. Goldman & T. G. Mahnken (Red.), *The Information Revolution in Military Affairs in Asia*
(s. 1–21). Palgrave Macmillan US. https://doi.org/10.1057/9781403980441_1
Harknett, R. J., & Smeets, M. (2022). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, *45*(4), 534–567. https://doi.org/10.1080/01402390.2020.1732354
Headquarters, Department of the Army. (2013). *Field Manual 3-90-1 Offense and Defense Volume 1*. Department of the Army.
Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity*, *5*(1), tyz008. https://doi.org/10.1093/cybsec/tyz008
Healey, J., & Jervis, R. (2023). The Escalation Inversion and Other Oddities of Situational Cyber Stability. I R. Chesney (Red.), *Cyberspace and Instability* (s. 21–59). Edinburgh University Press. https://doi.org/10.1515/9781399512510-004
Horowitz, M. C. (2010). *The Diffusion of Military Power: Causes and Consequences for International Politics*. Princeton University Press; JSTOR. https://doi.org/10.2307/j.ctt7sqwd
Jensen, B., Valeriano, B., & Whitt, S. (2024). How cyber operations can reduce escalation pressures: Evidence from an experimental wargame study. *Journal of Peace Research*, *61*(1), 119–133. https://doi.org/10.1177/00223433231219440
Kydd, A. (2000). Trust, Reassurance, and Cooperation. *International Organization*, *54*(2), 325–357. https://doi.org/10.1162/002081800551190
Lindsay, J., & Gartzke, E. (2018). Coercion through Cyberspace: The Stability-Instability Paradox Revisited. I K. M. Greenhill & P. Krause (Red.), *Coercion: The Power to Hurt in International Politics*. Oxford University Press.
Lonergan, E. D., & Lonergan, S. W. (2023). *Escalation Dynamics in Cyberspace* (1. utg.). Oxford University Press.
Maschmeyer, L. (2021). The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. *International Security*, *46*(2), 51–90. https://doi.org/10.1162/isec_a_00418
Maschmeyer, L. (2023). A new and better quiet option? Strategies of subversion and cyber conflict. *Journal of Strategic Studies*, *46*(3), 570–594. https://doi.org/10.1080/01402390.2022.2104253
Maschmeyer, L. (2024). *Subversion: From Covert Conflict to Cyber Conflict*. Oxford University Press.
McDonald, G., Murchu, L. O., Doherty, S., & Chien, E. (2013). *Stuxnet 0.5: The Missing Link*. Symantec Security Response. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-088.pdf
Montgomery, E. B. (2006). Breaking Out of the Security Dilemma: Realism, Reassurance, and the Problem of Uncertainty. *International Security*, *31*(2), 151–185. https://doi.org/10.1162/isec.2006.31.2.151

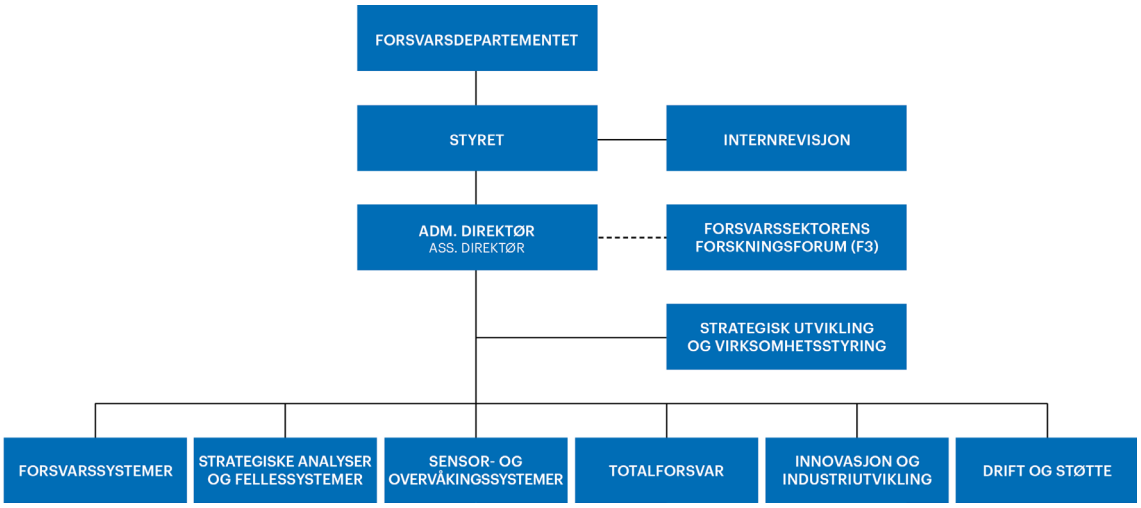
Moore, D. (2022). *Offensive Cyber Operations: Understanding Intangible Warfare* (1. utg.). Oxford University Press. https://doi.org/10.1093/oso/9780197657553.001.0001
Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), 44–71. https://doi.org/10.1162/ISEC_a_00266
Office of Public Affairs. (2024, mai 29). *911 S5 Botnet Dismantled and Its Administrator Arrested in Coordinated International Operation | United States Department of Justice*. Office of Public Affairs - U.S. Department of Justice. https://www.justice.gov/opa/pr/911-s5-botnet-dismantled-and-its-administrator-arrested-coordinated-international-operation
Posen, B. R. (2014). *Restraint: A New Foundation for U.S. Grand Strategy*. Cornell University Press; JSTOR. http://www.jstor.org/stable/10.7591/j.ctt5hh0db
Poznansky, M., & Perkoski, E. (2018). Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution. *Journal of Global Security Studies*, *3*(4), 402–416. https://doi.org/10.1093/jogss/ogy022
Påsche, E. S., & Sørbø, K. (2024, februar 14). *Teknikermangel på F-35: – Vi er halvparten av det vi skulle vært*. Forsvarets Forum. https://www.forsvaretsforum.no/f-35-flytekniker-kjevik/teknikermangel-pa-f-35-vi-er-halvparten-av-det-vi-skulle-vaert/363070
Raymond, D., Cross, T., Conti, G., & Nowatkowski, M. (2014). Key terrain in cyberspace: Seeking the high ground. *2014 6th International Conference On Cyber Conflict (CyCon 2014)*, 287–300. https://doi.org/10.1109/CYCON.2014.6916409
Schelling, T. C. (1966). *Arms and Influence*. Yale University Press; JSTOR. https://doi.org/10.2307/j.ctt5vm52s
Schneider, J. (2017, juli 26). *Cyber Attacks on Critical Infrastructure: Insights from War Gaming*. War on the Rocks. https://warontherocks.com/2017/07/cyber-attacks-on-critical-infrastructure-insights-from-war-gaming/
Schulze, M. (2020). Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. *2020 12th International Conference on Cyber Conflict (CyCon)*, 183–197. https://doi.org/10.23919/CyCon49761.2020.9131733
Siedler, R. E. (2016). Hard power in cyberspace: CNA as a political means. *2016 8th International Conference on Cyber Conflict (CyCon)*, 23–36. https://doi.org/10.1109/CYCON.2016.7529424
Sims, J. E. (2022). *Decision Advantage: Intelligence in International Politics from the Spanish Armada to Cyberwar*. Oxford University Press.
Smeets, M. (2022). *No Shortcuts: Why States Struggle to Develop a MIlitary Cyber-Force* (1. utg.). Oxford University Press.
Talmadge, C. (2019). Emerging technology and intra-war escalation risks: Evidence from the Cold War, implications for today. *Journal of Strategic Studies*, *42*(6), 864–887. https://doi.org/10.1080/01402390.2019.1631811
Valeriano, B., Jensen, B., & Maness, R. C. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press. https://doi.org/10.1093/oso/9780190618094.001.0001
Voo, J., Hemani, I., & Cassidy, D. (2022). *National Cyber Power Index 2022* (Cyber Project). Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/national-cyber-power-index-2022
Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. *Digital Communications and Networks*, *8*(4), 422–435. https://doi.org/10.1016/j.dcan.2021.07.006

Om FFI
Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan, med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs formål
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

FFIs visjon
FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs verdier
Skapende, drivende, vidsynt og ansvarlig.



Forsvarets forskningsinstitutt (FFI)
Postboks 25
2027 Kjeller

Besøksadresse:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telefon: 91 50 30 03
E-post: post@ffi.no
ffi.no

Norwegian Defence Research Establishment (FFI)
PO box 25
NO-2027 Kjeller
NORWAY

Visitor address:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telephone: +47 91 50 30 03
E-mail: post@ffi.no
ffi.no/en