Fagfellevurdert

Internasjonal POLITIKK
Skandinavisk tidsskrift for Internasjonale Studier

Årgang 77, Nummer 3, side 252-265, 2019, ISSN 1891-1757, www.tidsskriftet-ip.no, Publisert september 2019

Fokus: Cybersikkerhet

Avskrekking som element i cybersikkerhetsstrategi fra et småstatsperspektiv

Marius Kristiansen* og Njål Hoem
Forsvaret

Sammendrag

Artikkelen ser på mulighetene og utfordringene med avskrekking som strategisk tilnærming til det stadig viktigere cyberdomenet, fra et småstatsperspektiv. Forfatterne argumenterer for at det er essensielt å opprette og ansvarliggjøre en multinasjonal og multidepartemental/-sektoriell cyberorganisasjon for at reell *cyberavskrekking* skal være mulig å generere.

Innledningsvis beskriver artikkelen den klassiske og utvidete oppfatningen av *avskrekking*, og hvilke kriterier som må ligge til grunn for å kunne oppnå avskrekkende effekt: *kapasitet, kredibilitet* og evnen til å *kommunisere* effektivt. Sett fra et globalt sikkerhetsperspektiv har muligheten til å generere avskrekkende effekt vært med på å forme verden, spesielt i perioden 1945 til 1990. Kompleksiteten i sikkerhetssektoren har imidlertid økt signifikant siden da, mye grunnet økt global konnektivitet og fremveksten av cyberdomenet.

Artikkelen diskuterer hvordan kriteriene for avskrekking utfordres når strategien skal appliseres i cyberdomenet, med fokus på problemene knyttet til *antallet aktører/vektorer*, *ulike motiver* for handlinger, manglende *felles grunnlag* som utgangspunkt for å adressere utfordringene, og forskjellig oppfatning omkring *attribusjon og proporsjonalitetsprinsippet*. Forfatterne fremholder at disse utfordringene gjør det vanskeligere, men desto viktigere å identifisere hvordan man kan generere avskrekking i cyberdomenet – spesielt for høyteknologiske småstater, som Norge. Å håndtere dette på en god måte forutsetter at man ser på bredden av avskrekkingsteori i sammenheng over tid, og småstater må erkjenne sine svakheter og spille på sine styrker. Anbefalingene som

*Kontaktinformasjon: Marius Kristiansen, e-post: malarius@oslo.mil.no

Citation: Marius Kristiansen og Njål Hoem (2019). Avskrekking som element i cybersikkerhetsstrategi fra et småstatsperspektiv. Internasjonal Politikk, 77(3): 252–265. http://dx.doi.org/10.23865/intpol.v77.1385

fremlegges, er åpningstrekk som gjør nettopp dette, og som samtidig bereder grunnen for å dra veksler på komplementære effekter av ulike dimensjoner ved avskrekkingststrategi på lengre sikt.

Nøkkelord: kollektiv sikkerhet · folkerett · avskrekking · småstat · cyber

«… differently from the great battles of the past, which opened with a barrage of artillery or aerial bombardment, the next war will begin with a massive cyber attack …»
– António Guterres, FNs generalsekretær

Innledning: Et nytt domene – på godt og vondt

Den globale konnektiviteten øker kontinuerlig (Kilcullen, 2013, s. 107), og på det personlige og sosiale plan blir vi stadig mer avhengig av mulighetene dette medfører (Grøtan, 2018). Samtidig har vi for lengst passert punktet hvor moderne samfunn er avhengig av elektroniske kommunikasjonstjenester (EKOM-tjenester) for å fungere normalt. I Norge er *EKOM-tjenester* øverst på listen over «kritiske almenne innsatsfaktorer» – nødvendig for å opprettholde «kritiske samfunnsfunksjoner» (DSB, 2012, s. 24). Interstatlig gir cyberdomenet (Forsvarsdepartementet, 2014, s. 4) nye muligheter for interaksjon og samhandling og nye verktøy for å realisere strategiske målsettinger. Baksiden av medaljen er at den gjennomgående avhengigheten av cyberdomenet på alle nivå i stat og samfunn også skaper nye utfordringer og sårbarheter (Etterretningstjenesten, 2018, s. 31).

Cyberdomenet er i ferd med å bli militarisert (NATO, 2018). Cyberdimensjonen av krigføring (Forsvarsstaben, 2014, pkt. 05077) er den raskest voksende og samtidig den dimensjonen med størst usikkerhet. Norges undertegning av NATO sitt såkalte Cyber Defence Pledge (NATO, 2016) er én av flere markører for den gryende politiske og militærstrategiske erkjennelsen av at cyberdomenet kanskje representerer et av de største gapene i eksisterende sikkerhetsteori og -strategi.

Domenet er i praksis uregulert (The Guardian, 2017; Beaver, 2016) og derfor svært uforutsigbart. FNs generalsekretær har tatt til orde for å regulere krigføring i cyberdomenet (Reuters, 2018), og FN har gjentatte ganger understreket behovet for felles retningslinjer i domenet (f.eks. UN Doc. A/RES/57/239; UN Doc. A/RES/58/199; UN Doc. A/RES/64/211; UN Doc. A/RES/71/28; UN Doc. A/RES/70/174). På tross av at man siden millenniumskiftet gradvis har beveget seg mot en aksept for at internasjonal lov (og FN-pakten) skal ha bæring også for staters handlinger i cyberdomenet, er man fremdeles langt unna konsensus om hva som skal reguleres, og hvordan (The Guardian, 2017).

Å holde tritt med utviklingen i et «lovløst» domene krever enorme ressurser, noe som gjør cyber – i statlig anvendelse – til først og fremst et stormaktsdomene. Dette gjør at enkelte hevder at dagens situasjon tilsvarer «… the same stage of intellectual development as we were in the 1950s in relation to possible nuclear

war» (The Guardian, 2010). I fortsettelsen av den samme logikken har flere tatt til orde for at avskrekking er en farbar vei for å håndtere cyberdimensjonen (Nye, 2017). I et globalt sikkerhetsperspektiv har kjernefysisk avskrekking spilt en avgjørende rolle i å forme staters atferd på den internasjonale arena siden 1945. Dersom det samme tankegodset kan nyttes målrettet for å forme atferd også i det digitale rom, vil det ha stor global betydning. Å identifisere hvordan dette kan gjøres, og generelt hvordan cyberdomenet skal reguleres, er et arbeid som påvirker oss alle. Viktigst er dette kanskje for høyteknologiske småstater som Norge, hvor teknologien har blitt premissleverandør for alle sider av statens og samfunnets virksomhet.[1]

Hensikten med denne artikkelen er å gi et bilde av mulighetene og utfordringene med avskrekking som del av cybersikkerhetsstrategi. Forfatterne argumenterer for at det er essensielt å opprette og ansvarliggjøre en multinasjonal og multidepartemental/-sektoriell cyberorganisasjon for at reell *cyberavskrekking* skal være mulig å generere. Som det fremkommer av det påfølgende, er effekten av både klassisk og utvidet oppfatning av avskrekking betinget av spesifikke kriterier som utfordres når strategien skal appliseres i cyberdomenet. Dette gjør det vanskeligere, men desto viktigere å identifisere hvordan man kan generere avskrekking også her. Å håndtere dette på en god måte forutsetter at man ser på bredden av avskrekkingsteori i sammenheng over tid, og småstater må erkjenne sine svakheter og spille på sine styrker. Anbefalingene som fremlegges, er åpningstrekk som gjør nettopp dette, og som samtidig bereder grunnen for å dra veksler på komplementære effekter av ulike dimensjoner ved avskrekkingststrategi på lengre sikt.

Konseptet avskrekking

Konseptuelt går avskrekking ut på å «[…] use the threat of punishment, or increasing expected costs of an activity, to prevent an actor from taking an action they might otherwise take» (Blanken, 2011). En klassisk oppfatning av *avskrekking* som element i en sikkerhetsstrategi er at det innebefatter *påvirkning* av én eller flere aktører sine intensjoner (Schelling, 2008, s. 35). Tre forutsetninger må ligge til grunn for effektiv avskrekking. For det første må det finnes reell ***kapabilitet*** – altså evne til å påvirke en aktør. Det andre er ***kredibilitet*** – opplevd vilje til å bruke virkemidlene. Det tredje er ***kommunikasjon*** – som innebærer at det må være mulig å kommunisere budskapet tydelig til relevante aktører (Jasper, 2015, s. 65).

Når dette operasjonaliseres, er det i hovedsak fire typer avskrekkingstrategier. De to første refereres gjerne til som «classical deterrence», mens de to siste er en del

[1] Det eksisterer mange definisjoner av småstater (jf. Matthias Maass, «The elusive definition of the small state», *International Politics, 2009*.), men i grove trekk kan småstater defineres som «enhver stat i det internasjonale system som ikke er en stormakt» (jf. Handel, sitert i Kjølberg og Nyhamar [FFI-rapport 2011/01698], s. 6).

av det som beskrives som «broad deterrence» (Nye, 2017). Den første er avskrekking gjennom straff – ***deterrence by punishment***. Den andre er avskrekking gjennom nektelse – ***deterrence by denial*** (Mearsheimer, 1983, s. 14–15). Den tredje er avskrekking gjennom gjensidig avhengighet – ***deterrence by entanglement*** (Keohane & Nye, s. 1977). Den fjerde er avskrekking gjennom felles normer – ***deterrence by norms*** (Nye, 2017). Den ønskede avskrekkende effekten oppnås når det er etablert en oppfatning av at det finnes en reell risiko for (i et kost–nytte-perspektiv) ikke-proporsjonale konsekvenser for handlinger som bryter med normative og/eller anerkjente oppfatninger. Sikkerhetsstrategi basert på avskrekking forutsetter derfor at oppfatningen omkring konsekvenser, og evnen til å effektuere disse, opprettholdes til enhver tid.

Avskrekking er typisk stormaktsatferd. Det betyr ikke at avskrekking er utelukket for småstater (som Norge), men innenfor klassisk avskrekking er det nærmest umulig for småstater alene å generere nødvendig *kapabilitet* og *kredibilitet*. Man er avhengig av sikkerhetssamarbeid for å oppnå dette. Innenfor «broad deterrence» er det mulig å skape en grad av avskrekking også for småstater, men man er avhengig av at det eksisterer et felles normativt utgangspunkt som er allment kjent og *kommunisert*. Dermed er småstater uansett prisgitt andre aktører for å oppnå avskrekkende effekt.

Det er i hovedsak tre hovedgrunner til at avskrekkingsstrategi ikke lykkes. Den første er at *kommuniserte konsekvenser ikke er reelle*. Den andre er *at det faktisk er mulig å unngå/omgå konsekvensene* ved at en aktør benytter seg av et smutthull som den andre parten ikke har tenkt på (Schelling, 2008, s. 35–49). Den tredje er *at det er utfordrende, eller umulig, å kommunisere et klart budskap til en aktø*r. Disse forholdene kan virke enkle nok, men troverdig avskrekking har vist seg å være en kompleks eksersis med «kun» fire dimensjoner. Å generere reell avskrekking i den femte dimensjonen kan vise seg å være svært krevende – av flere årsaker.[2]

Utfordringer med avskrekking i cyberdomenet

Avskrekking i cyberdomenet er definert som:

> *[…] a strategy by which a defending state seeks to maintain the status quo by signaling its intentions to deter hostile cyber activity by targeting and influencing an adversary's decision making apparatus to avoid engaging in destructive cyber activity for fear of a greater reprisal by the initial aggressor.* (Iasiello, 2014, s. 55)

Logisk sett vil alle klasser av avskrekkingsstrategi være domeneuavhengig og avhengig av de samme tre forutsetningene. En viktig forskjell mellom tradisjonell avskrekking

[2] NATO har tradisjonelt operert med fire dimensjoner for krigføring (air, land, sea and space), men har inkorporert cyberspace som den femte dimensjonen. Se f.eks. Pierluigi Paganini (2016), *NATO officially recognizes cyberspace a warfare domain*, https://www.securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html

og avskrekking i cyberdomenet synes imidlertid å være behovet for enhetlig statlig og samfunnsmessig innsats. Trusselen knyttet til cyberdomenet er ikke bare rettet mot staten, men også mot andre aktører hvis sikkerhet likevel er avgjørende for den samfunnsmessige sikkerheten (jf. DSB, 2012, s. 24). Cyberdomenets natur skaper også helt spesifikke utfordringer som gjør det vanskelig å ivareta alle forutsetningene for avskrekking på tvers av de ulike strategiene.

Aktører og vektorer

Sammenlignet med andre domener er det et nærmest ubegrenset antall aktører som kan påvirke sikkerhetssituasjonen i cyberdomenet, både direkte og indirekte. Det kommer hovedsakelig av at tilgangen til og antallet «vektorer» – definert som «[…] *a specific method or technique to access equipment, computers, or systems to deliver a hostile payload for a malicious outcome*» (Jasper, 2015, s. 61) – i det digitale rommet er enormt.

Antallet vektorer, kompleksiteten disse representerer samt raffinementnivået øker daglig. Denne ekspansive økningen muliggjør en rekke handlinger som er (1) utfordrende å detektere eller beskytte seg mot, og (2) av en karakter som er utfordrende å definere fra et sikkerhetsperspektiv. Vektorenes effekt spenner også bredt, fra tjenesteforstyrrelser til manipulasjon og/eller destruksjon av data (Jasper, 2015, s. 62). Tilgjengeligheten og utformingen av vektorer gjør at nærmest «hvem som helst» med tilgang til internett kan påvirke sikkerhetssituasjonen i cyberdomenet. Alt fra store statlige aktører til organiserte grupperinger og enkeltpersoner kan skape uønskede effekter.

Kombinasjonen av det enorme antallet vektorer og mulige aktører gjør det særdeles krevende å generere avskrekking i det digitale rom (Jasper, 2015, s. 78). Primært skyldes dette at omfanget av potensielle sikkerhetstrusler gjør det vanskelig å beskytte seg mot alle trusler eller respondere på hvert enkelt overtramp. Teknikker og prosedyrer for å håndtere enkeltutfordringer er kortlevd, og trusselbildet er svært dynamisk (Iasiello, 2014, s. 55). Videre vil *kredibiliteten* i klassisk avskrekking i praksis utfordres av *kapabiliteten* til å adressere et stort antall aktører med ulike *modus operandi*. Antall aktører er ikke nødvendigvis en utfordring for «broad deterrence» *per se*, men vi mangler *internasjonale normer*, og bredden av aktører gjør det vanskelig å se hvor, hvordan og i hvilken grad det faktisk eksisterer *gjensidig avhengighet*.

Ulike motiver

Motivasjonen til forskjellige aktører utgjør også en utfordring i denne sammenhengen. Motivene strekker seg fra store statlige aktørers strategiske målsettinger av global eller regional karakter til organiserte gruppers eller enkeltpersoners handlinger motivert av kortsiktig økonomisk vinning eller prestisje. Dette gjør at trusselen fra cyberdomenet treffer alle deler av samfunnet. Samtidig er det ikke slik at disse trusselaktørene og deres målsettinger alltid er uavhengige, og isolerte «ikke-kritiske» handlinger kan være del av en større cyberoperasjon. Selv om individuelle effekter

er målbare, er det svært vanskelig å identifisere motivasjonen som ligger bak den enkelte handling, og hvorvidt flere handlinger må ses i sammenheng – og dermed hvordan situasjonen bør håndteres.

Måten de ulike motivasjonsfaktorene kommer til uttrykk på, gjør at det potensielt oppstår konflikter som hindrer relevant samarbeid mellom aktuelle samarbeidspartnere hvis felles innsats er nødvendig for helhetlig håndtering av de forskjellige utfordringene i cyberdomenet. Mellomstatlig kan dertte skyldes at man ikke ser hendelser i sammenheng fordi man av nasjonale sikkerhetshensyn ikke ønsker å dele informasjon, eller fordi man ikke vet hvilken informasjon man burde dele. Men selv internt i stater vil man kunne oppleve interessekonflikter som hindrer en enhetlig tilnærming som avskrekking forutsetter. Eksempelvis kan kommersielle aktører være uvillige til å dele relevante data med statlige aktører i frykt for tapt konfidensialitet som kan påvirke kortsiktige økonomiske forhold (Clinton, 2012). Staten vil på sin side sjelden ønske å dele sine data, metoder eller teknikker med kommersielle aktører, da det kan avsløre kapabiliteter og sårbarheter. Totalt sett blir den helhetlige forståelsen for problemkomplekset og en felles innsats svært vanskelig å oppnå.

Hvis man ser utfordringene knyttet til motivasjon i sammenhengen med dynamikken rundt vektorer og aktører, er det åpenbart at man står overfor en svært kompleks og dynamisk sikkerhetssituasjon. For effektiv håndtering av hendelser må disse forstås i en større sammenheng, slik at innsatsmidlene kan prioriteres der de gir størst effekt – og dette fordrer samarbeid. Et minimum for å ivareta *kredibiliteten* i en avskrekkingsstrategi er en viss transparens mellom aktørene som kan defineres som del av det samme målkomplekset, som grunnlag for (felles) handling.

Attribusjon og proporsjonalitet

Et grunnleggende premiss for avskrekking er evnen til å identifisere *hvem* som har begått handlingene man søker å avskrekke. Per i dag finnes det ingen felles og anerkjent metode for å attribuere påvirkning i cyberdomenet (Iasiello, 2012). Dette skyldes dels mengden aktører og verktøy som tillater næranonymitet på nettet, men kanskje viktigst er det faktum at en rekke vektorer har tekniske egenskaper som forhindrer attribusjon. Dette gjør at aktører kan operere med liten risiko: «[…] the technical properties of cyberattack vectors that prevent attribution allow actors with near anonymity and impunity» (Jasper, 2015, s. 62).

Attribusjonsutfordringen kan deles inn i to kategorier: teknisk attribusjon og menneskelig attribusjon (Boebert, 2010). For å si det enkelt går teknisk attribusjon ut på å analysere seg frem til hvilken vektor og hvilken node som har ført til påvirkning. Menneskelig attribusjon baserer seg på en teknisk attribusjonsanalyse og sammenstiller resultatet med annen informasjon i et forsøk på å peke ut hvilke aktør – personer og/eller organisasjon – som er ansvarlig for påvirkningen.

Fra en forsvarende part sitt perspektiv, og da spesielt småstater, er attribusjonsutfordringen særlig viktig. Som et minimum er korrekt attribusjon essensielt for å kunne vite hvem og hva man i fremtiden bør beskytte seg mot. Enda viktigere er

nødvendigheten av attribusjon for å vurdere om man bør/må respondere, og hvordan. Dette gjelder for alle aktører, men spesielt dersom man skal ha en ambisjon om å utløse reaksjoner fra internasjonale organisasjoner som forvalter global eller regional sikkerhet – som ofte er premisset for småstaters sikkerhet. USA har stadfestet at de vil respondere på trusler i cyberdomenet som på en hvilken som helst annen trussel, og Stoltenberg erklærte i 2016 at større cyberangrep ville kunne utløse en reaksjon fra NATO-alliansen (Reuters, 2016). Det må likevel antas at det påligger den angrepne part (og dennes allierte) en viss bevisbyrde dersom det skal utløse en reaksjon.

I de tilfellene attribusjon er mulig, er den neste utfordringen å identifisere en proporsjonal respons. Det finnes ingen klare, internasjonalt anerkjente retningslinjer for hvordan proporsjonalitetsprinsippet skal forvaltes i cyberdomenet. På det mest grunnleggende nivået er spørsmålet hvorvidt en reaksjon skal forekomme i det samme domenet som den initiale aksjonen. Like viktig er det å definere hva som utgjør «terskelen» for respons. NATO har selv identifisert utfordringen med å definere *hva* som skal utløse en reaksjon, og *hvordan* man eventuelt skal reagere (NATO, 2018). Her er det signifikante forskjeller i fortolkning, noe som kom tydelig til uttrykk etter cyberangrepene mot Estland i 2007. Estiske beslutningstakere anså dette som åpenbar hjemmel for NATOs artikkel V, mens NATO ikke var av samme oppfatning.

Utfordringene knyttet til attribusjon og proporsjonal respons undergraver åpenbart *kredibiliteten* til enhver avskrekkingsstrategi og potensielt samtidig statens kredibilitet i mer absolutte termer. En respons som oppleves som uproporsjonal eller rettet mot feil aktør, kan få vesentlige konsekvenser. Den største risikoen er kanskje at det kan føre til en utilsiktet eskalering av en konflikt som i utgangspunktet heller ikke er reell. I noen sammenhenger vil dette også kunne skyldes tilsiktet cybermanipulasjon fra en aktør som har interesse av å generere konflikt mellom en *andre- og tredje-part* – altså strategisk utnyttelse av utfordringene knyttet til attribusjon. Ettersom en stats overordnede sikkerhetspolitiske kredibilitet er tett knyttet til evnen til å møte *enhver påvirkning* med proporsjonal respons, står man overfor et sikkerhetspolitisk paradoks; selv om staten føler seg forpliktet til gjengjeldelse for å opprettholde egen kredibilitet, vil respons mot feil aktør eller en gjengjeldelse som er utenfor hva som normativt ansees som proporsjonalt, ha motsatt effekt.

Fra et småstatsperspektiv er derfor attribusjons- og proporsjonalitetsspørsmålet særlig viktig, all den tid sikkerheten er betinget internasjonal støtte. Uklarhet rundt disse forholdene vanskeliggjør stadfesting av nasjonal sikkerhetsstrategi, som forutsetter klarhet i hvilken alliert støtte som vil gjøres tilgjengelig når – med tydelige implikasjoner for forutsetningen om tydelig *kommunikasjon*. Så lenge det er knyttet ambiguitet til disse spørsmålene, skaper det et enormt manøverrom for en angriper (Diesen, 2018, s. 25).

Manglende felles grunnlag

Den mest basale utfordringen ved cyberdomenet er et manglende felles grunnlag for å adressere tematikken. Uten felles begrepsapparat, prosedyrer og internasjonal juridisk

presedens er det utfordrende å etablere effektiv avskrekking. Det er fremdeles uenighet mellom de store aktørene når det gjelder enkle ting som terminologi og meningsinnhold i begreper. Mens USA benytter begrepet «cyber security», benytter Kina og Russland «information security» (Iasiello, 2014, s. 57). Denne utfordringen strekker seg forbi semantikk, fordi det påvirker selve *forutsetningen* for tydelig *kommunikasjon*:

> *Without a common lexicon in place, communication between the two sides is fated to remain in disagreement […]. [W]hen addressing hostile activities in cyberspace where the actors are foreign to each other, the inability to communicate further impedes the ability to send clear messages and deescalate tensions.* (Iasiello, 2014, s. 57)

En fullstendig enighet om terminologi er kanskje utopisk, men et minimum er nødvendig for å adressere utfordringene, og det er gjort flere forsøk på å gjøre nettopp dette. Det europeiske initiativet The 2001 Council of Europe's Convention on Cybercrime (Europarådet, 2001) beskriver relativt godt den viktigste terminologien som trengs i cyberdomenet. Det er imidlertid kun et førtitalls stater som har godkjent/ratifisert selve konvensjonen, med Russland og Kina som de største aktørene som har valgt å avstå fra muligheten til å godkjenne den (Iasiello, 2014, s. 57).

Et annet initiativ er NATO sin opprettelse av NATO Cooperative Cyber Defence Centre of Excellence i 2008, som skal ivareta prinsipielle spørsmål om forsvar av alliansen i det digitale rom (NATO Cooperative Cyber Defence Centre of Exellence, 2018). Organisasjonen produserte i perioden 2013–2017 to forskjellige utgaver av en manual som beskriver hvordan NATO blant annet bør forholde seg juridisk til cyberdomenet i internasjonal kontekst (NATO Cooperative Cyber Defence Centre of Exellence, 2017). Manualen adresserer også hvordan og hvorvidt handlinger i cyberdomenet kan defineres som væpnede angrep (Jasper, 2015, s. 68), men dette sammenfaller ikke med vurderingene i NATOs Policy on Cyber Defense (Jasper, 2015, s. 68). Denne dissonansen understreker utfordringen med å etablere et felles rammeverk – selv internt i alliansen.

Parallelt med interne prosesser har NATO også vært en pådriver for å etablere globale normer og regler (NATO, 2018). Som nevnt i innledningen er dette et arbeid som har vært på den internasjonale agendaen lenge. Det er likevel fremdeles internasjonal uenighet om hvorvidt (og i så fall hvordan) eksempelvis internasjonal humanitær rett skal gjøres gjeldende i en cyberkonflikt, og enkle (men avgjørende) spørsmål, som hva som faktisk kan defineres som aggresjon (iht. FN-pakten) i domenet, er ikke klart (Carr, 2011, s. 31). Her synes det åpenbart at enkelte aktører anser det i sin interesse å sørge for at en viss ambiguitet opprettholdes:

> *Ettersom domenet gir rom for å operere offensivt under terskelen for hva som regnes som et væpnet angrep, kan slike operasjoner påvirke maktbalansen mellom stater ved å stjele en stats intellektuelle eiendom eller true kritisk infrastruktur i en aktuell stat i fredstid.* (Aannø, 2018, s. 62)

I mangel på regulering av cyberdomenet – altså evnen til å definere hva som utgjør normbrudd, hva som utgjør terskelen for legitim reaksjon, og hva en legitim reaksjon

er – er det åpenbart vanskelig å *kommunisere* tydelig til potensielle angripere. Uklarhetene i det normative grunnlaget åpner også for at identifiserte aktører kan omgå/unngå reaksjoner fra «offeret» fordi legitimiteten og legaliteten til eventuelle reaksjoner vil kunne trekkes i tvil. Dette undergraver avskrekking generelt, men spesielt avskrekkingsstrategier basert på felles normer.

Strategi for avskrekking i cyberdomenet

> *The emergence of cyber as a separate domain of warfighting does not necessarily offer magic solutions and miraculous short-cuts to achieve strategic goals.* (Sakkov, 2015, s. 9)

Avskrekking som overordnet strategi er ikke nytt (Quester, 1966). Kjernefysisk avskrekking var et svar på en omveltning i den globale sikkerhetspolitiske virkeligheten – ikke ulikt, vil mange påstå, den cyberdrevne sikkerhetspolitiske omveltningen vi ser i dag. Det er derfor ikke unaturlig at man søker å dra paralleller mellom kjente og utprøvde strategier for kjernefysisk avskrekking og avskrekking i cyberdomenet. Samtidig må man være svært bevisst forskjellene, og enkelte har gått så langt som å påstå at «[…] *despite some crossover, there are too many inconsistencies that prevent an even partial adoption of the nuclear deterrence model*» (Iasiello, 2014, s. 61).

Kort fortalt gjør de fire «problemområdene» som er beskrevet over, det vanskelig for enhver stat med ambisjoner om avskrekking i cyberdomenet å tilfredsstille de grunnleggende forutsetningene for *effektiv* avskrekking. Generelt kan man si at for å komme nærmere en reell mulighet for avskrekking i cyberdomenet er det behov for avklaringer på en rekke områder hvor det per i dag er for mange uutforskede variabler og underutviklede konsepter som hindrer effektiviteten (Iasiello, 2014, s. 55). Tydeligst blir dette for de klassiske formene for avskrekking, og spesielt *avskrekking gjennom straff*, som forutsetter større klarhet i det ovennevnte for å implementeres (Nye, 2017). Innenfor *avskrekking gjennom gjensidig avhengighet*, *gjennom nektelse* og *gjennom felles normer* er det kanskje lettere å etablere forutsetninger på kortere sikt.

Avskrekking gjennom gjensidig avhengighet er en tilnærming som spiller på det som ellers kan oppleves som utfordringene med avskrekking i cyberdomenet. Den stadige tettere tilknytningen mellom aktører (stater, organisasjoner og mennesker) skaper flere potensielle sårbarheter, men det kan også gjøre det vanskelig å gjennomføre offensive cyberoperasjoner uten at det forårsaker utilsiktet skade. Ved å styrke globaliseringens fremvekst kan man redusere risikovilligheten hos mulige fiendtlige aktører: «*By more thoroughly entangling both friend and foe the aggregate benefits for maintaining and enhancing good behavior within the cyberspace increase and reinforce risk averse behaviors*» (Brantly, 2018). For småstater er dette praktisk sett kanskje en mer farbar vei fordi det ikke innebærer paritet i offensive og defensive cyberkapasiteter for å ha effekt. Ved å skape sterkere gjensidig avhengighet med samarbeidspartnere og allierte i cyberdomenet vil man også generere en situasjon hvor felles defensive cyberkapasiteter er av interesse, og dermed kunne underbygge en felles (alliert) avskrekking gjennom nektelse.

For småstater vil imidlertid ofte gjensidig avhengighet være svært asymmetrisk og neppe et tilstrekkelig tiltak for å avskrekke alle relevante aktører. Småstater har normalt en relativt svak posisjon i det internasjonale systemet, men de har likevel anledning til å påvirke hvilke normer og regler som ligger til grunn for mellomstatlig interaksjon, og kan gjennom dette i noen grad utjevne ubalansen i «hard makt». Erkjennelsen av dette gjør at småstaters sikkerhetsstrategi tenderer mot å fokusere på «idealistisk og normorientert politikk» som søker å styrke internasjonale institusjoner, normer og lover (Kjølberg, 2016). Stormakter vil alltid til en viss grad operere etter prinsippet «might is right», også utenfor etablerte rammer, men risikerer fremdeles å bli holdt ansvarlig i tråd med disse rammene (Larres, 2015). Ved å jobbe for å etablere og styrke det normative rammeverket for adferd i cyberdomenet vil man kunne generere reell avskrekking gjennom normer. Samtidig vil rammeverket danne et objektivt utgangspunkt for å legitimere klassisk avskrekking.

Å etablere effektfulle rammer for avskrekking i cyberdomenet fordrer imidlertid en kollektiv innsats, og dagens utgangspunkt er ikke det beste. Et godt første steg kan være å konkretisere innsatsen gjennom å etablere en struktur eller organisasjon hvis formål er nettopp å regulere adferd i cyberdomenet, noe som igjen muliggjør realisering av avskrekkingsstrategi. Organisasjonen bør ta utgangspunkt i eksisterende sikkerhetssamarbeid og allianser, men man bør ikke utelukke et bredere interessefellesskap. En modell som kan benyttes som utgangspunkt, er en tidsriktig versjon av Storbritannias Fighter Command – hvis hensikt var avskrekking i luftdomenet (Arquilla, 2015). Uten å gå i videre detalj om hvordan en slik organisasjon bør se ut, synes det åpenbart at å forene innsatsen under enhetlig ledelse ville danne et bedre utgangspunkt for enhver avskrekkingsstrategi. Ved å knytte stormakter til en slik sammenslutning vil man kunne generere et kapasitetsmessig utgangspunkt for klassisk avskrekking, noe som realistisk sett vil være uoppnåelig for småstater utenfor en slik organisasjon.

For småstater vil deltakelse i organisasjonen balansere den normfokuserte politikken med det som i praksis blir en allianseinnretning som kan sikre konkrete nasjonale interesser på kortere sikt (Long, 2016). En balanse mellom det tilsynelatende idealpolitiske og det realpolitiske er en tilnærming vi allerede kjenner fra norsk politikk, strategi og doktriner (se f.eks. Forsvarsdepartementet, 2015; Forsvarsstaben, 2014). Et slikt delt fokus kan kanskje oppleves som motstridende, men er i realiteten svært rasjonelt. Empirien tilsier at internasjonale lover og normer er av begrenset verdi dersom konflikt oppstår mellom småstater og stormakter (Allison, 2009). Allianser og internasjonale rammer blir komplementære verktøy, hvor nettopp allianser og sikkerhetsorganisasjoner sørger for at aktører (gjennom reell trussel om maktbruk) holdes ansvarlig i henhold til gjeldene rammer.

En moderne Fighter Command – eller *Cyber Command* – må også kunne gjøre valg som forplikter deltakende stater, og som dermed regulerer atferd både innad i organisasjonen og mellom organisasjonen og det internasjonale samfunnet for øvrig. En slik organisasjon vil være med på å sette premissene for internasjonal cyberatferd

og dermed være en viktig aktør i den internasjonale normdannelsen. Således tjener en opprettelse av en Cyber Command både behovet for sikkerhet på kort sikt og ønsket om et bedre regulert cyberdomene på lengre sikt. Dette vil også være komplementære og gjensidig forsterkende innsatser, hvor Cyber Command kan styrke arbeidet med opprettelse av rammer, og hvor disse rammene igjen danner et bedre utgangspunkt for hvordan Cyber Command håndterer domenet. Sagt på en annen måte vil Cyber Command danne et robust utgangspunkt for *klassisk avskrekking* samtidig som det muliggjør etablering av det rammeverket som trengs for troverdig *avskrekking gjennom normer*.

Konklusjon: Implikasjoner for småstater

Basert på de utfordringene og mulighetene som eksisterer i cyberdomenet, og de opsjonene avskrekkingsteori tilbyr, hva bør småstater som Norge gjøre? For det første må man erkjenne de begrensningene som naturlig påligger småstater, også i cyberdomenet. Cybersikkerhet er en ressurskrevende eksersis hvor det er rimelig å anta at den beste effekten kan oppnås sammen med andre. For det andre mener vi det er sannsynliggjort at avskrekking har en plass i cybersikkerhetsstrategi, forutsatt at man ikke ser på ulike avskrekkingsstrategier som gjensidige utelukkende, men komplementære. Norge kan underholde flere operasjonslinjer for å oppnå mer robust avskrekking. For det tredje er det viktig at man starter umiddelbart med å utforske hvordan man praktisk skal gå frem for å realisere avskrekking i cyberdomenet, og her er det viktig å tenke både kortsiktig og mer langsiktig. Om en moderne Cyber Command er realistisk eller hensiktsmessig, er vanskelig å si før man har utforsket mulighetsrommet.

Slik situasjonen nå foreligger, representerer påvirkning i cyberdomenet den *klassiske* kinetiske konflikten sin forlengede arm, hvor fornektbarhet er relativt enkelt å oppnå. Vi vurderer det som helt avgjørende å starte et initiativ før «isolasjonstrangen» bak egenutviklede brannmurer og beskyttelsestiltak, et ønske om profitt eller frykten for å bli lurt gjør terskelen enda høyere enn den allerede er. For småstater som Norge er det signifikant å realisere det stormakten USA allerede har stadfestet som en nødvendighet: å opprette en anerkjent internasjonal, tverrsektoriell og tverrdepartemental organisasjon som også innbefatter relevante private aktører med ansvar for og myndighet til å regulere cyberdomenet for felleskapets beste (U.S. Department of Defence, 2014, s. 15). Uten et slikt initiativ vil verden potensielt hurtig befinne seg på kanten av et stup (om vi ikke allerede er der) med god utsikt over et landskap som har klare anarkistiske tendenser, et cyberlandskap brolagt med gode intensjoner, hvor enkeltaktører etter beste evne har forsøkt å regulere atferd, men som i realiteten preges av motstridende og uklare regler og policyer, og hvor alvorlige globale og regionale konflikter av sikkerhetspolitisk karakter kan oppstå med noen få tastetrykk (U.S. Department of Defence, 2014, s. 15). Det bør ikke være behov for cyberekvivalenten til Operation Centerboard (Farrell, 2018) før vi skrider til verket.

Om forfatterne

Marius Kristiansen er en stadig tjenestegjørende norsk hæroffiser. Han startet i Forsvaret i 2001, og har tjenestegjort både i Sjøforsvaret og Hæren. Han har en B.A. i militære studier med fordypning i landmakt og ledelse fra Krigsskolen Linderud, et Advanced Certificate i Terrorism Studies fra University of St. Andrews i Storbritannia, og en M.S. i Defense Analysis fra Naval Postgraduate School i Monterey, California. Njål Hoem er en stadig tjenestegjørende norsk hæroffiser. Han startet i Forsvaret i 2003, og har tjenestegjort i Hæren siden. Han har en B.A. i militære studier med fordypning i landmakt og ledelse fra Krigsskolen Linderud, har studert Leadership and Organizational Psychology ved Handelshøyskolen BI i Oslo, og har en M.Litt. i War Studies fra University of Glasgow.

Litteraturliste

Aannø, S. T. (2018). *Strategisk avskrekking i det digitale rom – Finnes det rasjonelle strategier for små stater?* Oslo: Forsvarets høgskole.

Alllison, R. (2009). The Russian case for military intervention in Georgia: international law, norms, and political calculation. *European Security, 18*(2).

Arquilla, J. (2015). Deterrence after Stuxnet. Communications of the ACM. Hentet 11.09.2018 fra http://cacm.acm.org/blogs/blog-cacm/190371-deterrence-after-stuxnet/fulltext

Beaver, M. (2016). The United Nations and cyberwarfare. I *Cybersecurity.* Hentet 11.09.2018 fra https://globalriskadvisors.com/united-nations-cyber-warfare/

Blanken, L. (2011). Deterrence. I M. Freeman & H. Rothstein (Red.), *Deterrence in gangs and guerrillas: Ideas from counterinsurgency and counterterrorism*. Monterey: Naval Postgraduate School.

Boebert, E. W. (2010). A survey of challenges in attribution, NRC Proceedings. *Proceedings of a Workshop on Deterring Cyberattacks: Informing strategies and Developing Options for U.S. Policy.* Hentet 11.09.2018 fra https://www.nap.edu/read/12997/chapter/5#43

Brantly, A. (2018). Conceptualizing cyber deterrence by entanglement. Hentet 11.09.2018 fra http://www.ou.edu/cis/sponsored_programs/cyber-governance-and-policy-center/blog/conceptualizing-cyber-deterrence-by-entanglement

Carr, J. (2011). *Inside cyber warfare: Mapping the cyber underworld*. O'Reilly Media, Inc.

Clinton, L. (2012). Cyber Security Social Contract. I S. Jasper (Red.), *Conflict and cooperation in the global commons: A comprehensive approach for international security* (s. 185–98). Washington, DC: Georgetown University Press.

Department of Defence (2014). *Quadrennial Defense Review,* Washington, DC: DOD.

Diesen, S. (2018). *FFI rapport 18/00080: Lavintensivt hybridangrep på Norge i en fremtidig konflikt.* Oslo/Kjeller: Forsvarets forskningsinstitutt.

Direktorat for samfunnssikkerhet og beredskap (2012). *Rapport: Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring*. Tønsberg: DSB.

Europarådet (2001). The 2001 Council of Europe's convention on cybercrime. Budapest: COE. Hentet 11.09.2018 fra http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Etteretningstjenesten (2018). *Fokus 2018 – Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.* Oslo: ETJ.

Farrell, D. A. (2018). *Tinian and the bomb: Project Alberta and Operation Centerboard.* Micronesian Productions.

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

Forsvarsdepartementet (2015). *Prop. 151 S (2015–2016) Proposisjon til Stortinget (forslag til stortingsvedtak): Kampkraft og bærekraft – Langtidsplan for forsvarssektoren*. Oslo: FD. Hentet 11.09.2018 fra https://www.regjeringen.no/contentassets/a712fb233b2542af8df07e2628b3386d/no/pdfs/prp201520160151000dddpdfs.pdf

Forsvarsstaben (2014). *Forsvarets fellesoperative doktrine*. Oslo: Forsvarsstaben.

Grøtan, T. O. (2018). SAMRISK-II: New strains of society – hidden, dynamic and emergent vulnerabilities. *LUFTLED – Luftmakttidsskrift*, (2), 26–30.

Handel, M. I. (1990). *Weak states in the international system.* London: Routledge.

Iasiello, E. (2012). Identifying cyber-attackers to require high-tech sleuthing skills. *National Defense Magazine*, desember.

Iasiello, E. (2014). Is cyber deterrence an illusory course of action? *Journal of Strategic Security, 7*(1), 54.

Jasper, S. (2015). Deterring malicious behavior in cyberspace. *STRATEGIC STUDIES QUARTERLY,* AIR UNIV MAXWELL AFB AL. Hentet fra http://www.au.af.mil/au/ssq/digital/pdf/Spring_2015/jasper.pdf

Keohane, R. O. & Nye, J. S. Jr. (1977). *Power and interdependence: World politics in transition.* Boston: Little, Brown.

Kilcullen, D. (2013). *Out of the mountains*. New York: Oxford University Press.

Kjølberg, A. (2016). Foredrag ved Krigsskolen. Linderud/Oslo.

Kjølberg, A. & Nyhamar, T. (2011). *FFI-rapport 2011/01698: Småstater i internasjonale operasjoner*. Kjeller/Oslo: Forsvarets Forskningsinstiutt.

Larres, K. (2015). Superpowers and international governance: A 'might is right' story? *Caucasus International*, 5, 2. Hentet 11.09.2018 fra http://cijournal.az/storage/posts/101/files/Larres.pdf

Long, T. (2016). Small states, great power? Gaining influence through intrinsic, derivative, and collective power. *International Studies Review,* 1–21.

Maass, M. (2009). The elusive definition of the small state. *International Politics.*

Mearsheimer, J. J. (1983). *Conventional deterrence*. Ithaca, NY: Cornell University Press. Hentet 11.09.2018 fra https://books.google.no/books?id=lNwZDgAAQBAJ&printsec=frontcover&dq=conventional+deterrence&hl=no&sa=X&ved=0ahUKEwjI_K-fr9jZAhWGDuwKHYzmD8cQ6AEIKDAA#v=onepage&q=conventional deterrence&f=false

Ministry of Foreign Affairs of Ukraine (2014). Aide memoire on the violation of imperative norms of international law by Russian Federation. Hentet 11.09.2018 fra https://mfa.gov.ua/en/news-feeds/foreign-offices-news/19432-

NATO (2016). NATO Cyber Defence Pledge. Hentet 10.09.2018 fra https://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO (2018). Cyber defence. Hentet 10.09.2018 fra https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO Cooperative Cyber Defence Centre of Excellence (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Hentet 11.09.2018 fra https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf

NATO Cooperative Cyber Defence Centre of Excellence (2018). History. Hentet 11.09.2018 fra https://ccdcoe.org/history.html

Nye, J. S. Jr., (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71.

Reuters (2016). Massive cyber attack could trigger NATO response: Stoltenberg. Hentet 11.09.2018 fra https://www.reuters.com/article/us-cyber-nato/massive-cyber-attack-could-trigger-nato-response-stoltenberg-idUSKCN0Z12NE

Reuters (2018). U.N. chief urges global rules for cyber warfare. Hentet 11.09.2018 fra https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4

Sakkov, S. (2015). Forord i K. Geers (Red.), *Cyber war in perspective: Russian Aggression against Ukraine*. Tallinn: NATO Cooperative Cyber Defence Centre of Exellence Tallinn.

Schelling, T. C. (2008). *Arms and influence: With a new preface and afterword*. New Haven, CT: Yale University Press.

The Guardian (2010). Cyber-warfare is growing threat. Hentet 10.09.2018 fra https://www.theguardian.com/technology/2010/feb/03/cyber-warfare-growing-threat

The Guardian (2017). Dispute along cold war lines led to collapse of UN cyberwarfare talks. Hentet 10.09.2018 fra https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges; https://globalriskadvisors.com/united-nations-cyber-warfare/

United Nations (2003). *UN Doc. 57/239. Creation of a global culture of cybersecurity.* Hentet 11.09.2018 fra http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/57/239

United Nations (2004). *UN Doc. A/RES/58/199. Creation of a global culture of cybersecurity and the protection of critical information infrastructures*. Hentet 11.09.2018 fra http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/58/199

United Nations (2010). *UN Doc. A/RES/64/211. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure*. Hentet 11.09.2018 fra http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/64/211

United Nations (2016). *UN Doc. A/RES/70/174. Thirteenth United Nations Congress on Crime Prevention and Criminal Justice.* Hentet 11.09.2018 fra http://www.un.org/ga/search/view_doc.asp?symbol=a/res/70/174

United Nations (2016). *UN Doc. A/RES/71/28. Developments in the field of information and telecommunications in the context of international security.* Hentet 11.09.2018 fra http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/71/28

Quester, G. H. (1966). *Deterrence before Hiroshima: The airpower background of modern strategy*. New York: Wiley.

Abstract in English

This article explores the possibilities and challenges associated with *deterrence* as strategy in the increasingly significant cyber-domain, from a small state perspective. The authors argue that genuine *cyber-deterrence* is contingent upon the creation of an accountable cyberorganization, with a multinational and multi-departmental/sectorial composition.

The article addresses *classical* and *broader deterrence*, and the criterions that must be met in order to successfully deter; *capability, credibility,* and the ability to *communicate* effectively. From a global perspective, the ability to generate effective deterrence has been key to shape the international security landscape in the period from 1945 to 1990. However, the complexity of the security sector has increased significantly since then – much due to the seemingly ever-growing global connectedness and the emergence of the cyber-domain.

The article further explores and discusses how the criteria for effective deterrence is tested when applied to the cyber-domain, with emphasis on the problems associated with *the number of actors/vectors*, *varying motives* for actions, the *lack of a shared conceptual foundation* as a basis to address the challenges, and differing opinions concerning *attribution and proportionality.* The authors argue that these problems make it difficult, but thus the more important to identify how to generate effective deterrence in the cyber-domain – especially for high-tech small states such as Norway. Effective management of the problem-complex requires exploration of the whole range of deterrence theory over time, and small states must recognize their inherent weaknesses and play to their strengths. The recommendation put forth here is an initial move which allows just that, and which at the same time sets the stage for more elaborate strategies that exploit the complementary effects of different dimensions of and approaches to deterrence.

Keywords: collective security · international law · deterrence · small state · cyber