Fagfellevurdert

Internasjonal POLITIKK
Skandinavisk tidsskrift for Internasjonale Studier

Årgang 77, Nummer 3, side 278-287, 2019, ISSN 1891-1757, www.tidsskriftet-ip.no, Publisert september 2019

Fokus: Cybersikkerhet

Avskrekke hvem? Betydningen av strategisk kultur for cybersikkerhet

Lars Gjesvik*
Norsk utenrikspolitisk institutt (NUPI)

Emil Jørgensen Øverbø
Norsk utenrikspolitisk institutt (NUPI)

Sammendrag

Det er en pågående debatt i akademia om hvorvidt og hvordan man kan benytte avskrekkingsteori i cyberdomenet. Avskrekking var originalt en teori utviklet for å unngå konvensjonell eller nukleær krig. I diskusjonen om cybersikkerhet har det blitt påpekt en rekke tekniske problemer med å overføre en teori fra den fysiske verden til cyberdomenet. Vi anerkjenner disse tekniske utfordringene ved avskrekking i cyberdomenet, men i denne artikkelen ønsker vi å belyse et annet aspekt ved avskrekking, nemlig samspillet mellom sosiale og tekniske faktorer ved avskrekking i cyberdomenet. I denne artikkelen vil vi diskutere hvordan avskrekking som strategi i cyberdomenet vil påvirkes av den spesifikke strategiske kulturen i et land. For å belyse argumentet vil vi benytte Kina som en casestudie. Motsetninger mellom kinesisk og «vestlig» strategisk kultur resulterer i konkrete forskjeller i hvordan Kina og vestlige land agerer i cyberdomenet. Ved å benytte fire komponenter av avskrekkingsteori (nektelse, gjengjeldelse, gjensidig avhengighet og normer) ønsker vi å vise hvordan en dyptgående innsikt i en stats sikkerhetspolitikk og strategiske kultur kan anvendes til å skreddersy en mer effektiv avskrekkingsstrategi og styrke evnen til å forhindre uønsket aktivitet.

Nøkkelord: avskrekking · avskrekkingsteori · cyber · cyberdomenet · strategisk kultur · Kina · sikkerhetspolitikk

*Korrespondanse: Lars Gjesvik, e-post: larsg@nupi.no

Citation: Lars Gjesvik og Emil Jørgensen Øverbø (2019). Avskrekke hvem? Betydningen av strategisk kultur for cybersikkerhet. Internasjonal Politikk, 77(3): 278–287. http://dx.doi.org/10.23865/intpol.v77.1396

Avskrekking og cybersikkerhet

Avskrekking som begrep fikk sitt gjennombrudd i den sikkerhetspolitiske diskursen og akademia under den kalde krigen. Helt grunnleggende går avskrekking ut på å overbevise en potensiell motstander om å avstå fra visse handlinger ved å høyne den potensielle kostnaden ved slike handlinger (Nye, 2017). Forståelsen av avskrekking har vært sterkt påvirket av nettopp den kalde krigen, og særlig av den eksistensielle trusselen om angrep med atomvåpen. Ettersom bruken av atomvåpen hadde vist seg å ha katastrofale følger, forsøkte de to blokkene i den kalde krigen å avskrekke hverandre fra å angripe ved å true med massiv gjengjeldelse. På denne måten ble trusselen om *gjensidig ødeleggelse* en stabiliserende faktor, et angrep ble utenkelig fordi konsekvensene ville vært så omfattende (Freedman, 2013, s. 177).

Ettersom den kalde krigen aldri ble varm, har avskrekking blitt vurdert som en vellykket strategi av flere (Freedman, 2013, s. 158). Dette har igjen ført til at strategien blir forsøkt anvendt på nye sikkerhetsutfordringer, som cybersikkerhet.[1] *Hvordan* avskrekking i cyberdomenet kan gjøres, har derimot vært mer omstridt, med en rekke argumenter om særegne utfordringer ved *cyberavskrekking*.[2] Noen av de særegne utfordringene som har blitt pekt på, er bruken av uoppdagede digitale sårbarheter (såkalte «zero-days»), noe som gjør det vanskelig å *forhindre* hendelser fra å inntreffe (Bendiek & Metzger, 2015, s. 7).Videre har det blitt hevdet at den økende kompleksiteten i nettverk gjør at angriperen har en strukturell fordel som kompliserer avskrekking (Nye, 2017). Et annet argument som ofte nevnes, er problemet med å *attribuere* angrep. Mulighetene for å skjule opprinnelsen til cyberangrep gjør at en angriper ofte kan kamuflere sin identitet, noe som gjør det vanskeligere å reagere og gjengjelde i ettertid (Rid & Buchanan, 2015). I tillegg er det forholdsvis vanlig at stater bruker private aktører eller kriminelle til å utføre angrepene for seg, slik at de senere kan nekte for at det faktisk var dem som stod bak (Collier, 2017).

Disse problemene har ført til at flere avskrekkings og cybereksperter har sådd tvil om avskrekking i det hele tatt er en passende strategi for cyberdomenet.[3] Overvekten av artikler som drøfter denne problematikken, tar utgangspunkt i cyberdomenets unike karakter, men et aspekt ved avskrekking som har fått mindre oppmerksomhet, er samspillet mellom teknologi og den bredere sosiale og kulturelle konteksten. Denne artikkelen vil argumentere for viktigheten av historie og kultur for fungerende avskrekkingsstrategier. Denne tilnærmingen gjør det mulig å belyse hvordan slike sosiale faktorer bidrar til å forme de teknologiske rammebetingelsene, som igjen vil påvirke hvordan avskrekking som konsept kan fungere (Dunn Cavelty, 2018).

---

[1] Cybersikkerhet referer i denne sammenhengen til beskyttelse mot trusler i og fra digitale teknologier og komponenter. Cyberdomenet referer til det virtuelle miljøet disse truslene opererer i.

[2] Se blant annet Rid & Buchanan, 2015; Lindsay, 2015; Tor, 2017; Libicki, 2009; Singer & Friedman, 2014; Lawson, 2017; Segal, 2017; Sulmeyer, 2018; Muller & Stevens, 2017.

[3] Se blant annet Libicki, 2009; Taddeo, 2018; Harknett, 1996; Brantly, 2018.

I denne teksten vil vi derfor diskutere hvorfor avskrekking som strategi i cyberdomenet ikke kan forstås uavhengig av den strategiske kulturen i landet man ønsker å avskrekke. Ved å ta i bruk Kina som et eksempel ønsker vi å vise hvordan man ved hjelp av målrettet avskrekking (*tailored deterrence*) kan tilpasse cyberavskrekkingsstrategier til å bli mer effektive. Som teoretisk rammeverk vil vi ta i bruk Joseph Nyes konseptualisering av avskrekking ved nektelse, straff, normer og gjensidig avhengighet for å belyse vårt argument.

Avskrekkingens mekanismer

Joseph Nye (2017) argumenter for at avskrekking i cyberdomenet opererer gjennom fire mekanismer: gjengjeldelse, nektelse, normer og gjensidig avhengighet. Disse fire mekanismene vil alle i varierende grad være relevante for å avskrekke cyberangrep (Nye, 2017). Avskrekking ved gjengjeldelse var grunnsteinen i nukleær avskrekking og baserer seg på trusselen om å gjengjelde et angrep. Denne formen for avskrekking blir ofte hevdet å være mindre relevant for cybervåpen grunnet problemene med å slå fast hvor et angrep stammer fra. Likevel har gjengjeldelse blitt hevdet å være et nyttig verktøy for å avskrekke, og da særlig som et ledd i et bredere spekter av politiske og økonomiske virkemidler (Nye, 2017).

Nektelse som mekanisme har også blitt tilpasset de skiftende digitale rammebetingelsene. I senere tid har man skiftet fokus fra å nekte angrep, som er vanskelig grunnet den økende kompleksiteten i digitale nettverk, for i stedet å vektlegge *resiliens*. Ved å gjøre ulike systemer vanskeligere å infiltrere samt minske konsekvensen av en infiltrasjon må den angripende part bruke flere ressurser for mindre gevinst. Dette vil igjen bidra til å gjøre digitale angrep mindre effektive og dyrere, noe som vil ha en avskrekkende effekt (Nye, 2017).

De to mekanismene beskrevet over, er allment akseptert som hovedmekanismene for avskrekking, men Nye trekker frem to andre mekanismer som også er av betydning. Den første er gjensidig avhengighet, eller faren for at et angrep vil ramme en selv eller andre stater. Et slikt angrep vil enten skade ens egne interesser eller risikere å trekke tredjeparter inn i konflikten. Dette er særlig relevant for cyberavskrekking på grunn av den høye graden av sammenkobling av digitale systemer, noe som øker risikoen for utilsiktede konsekvenser. Risikoen for slike effekter vil ifølge Nye virke avskrekkende for en potensiell angriper. Den siste mekanismen, normer, antar at stater ikke vil utføre angrep som bryter sterkt med rådende oppfatninger av hva som er rett og galt. Risikoen for internasjonal fordømmelse vil derfor forhindre visse typer angrep og våpen. For cyberavskrekking har det blitt trukket frem at normer er mindre relevant for å stoppe bruken av en viss type *våpen,* men at det heller vil være en brems for angrep på visse typer *mål,* hvor kritisk sivil infrastruktur har blitt foreslått som et eksempel (Nye, 2017).

Dragen i cyberdomenet

Strategisk kultur har sitt utspring i hver enkelt stats kultur og historiske bakgrunn. Disse faktorene gir sterke føringer for hvilke sikkerhetsmål man forsøker å oppnå, og hvilke virkemidler som er legitime i å nå disse målene. Ulike strategiske kulturer kan dermed oppfatte en sikkerhetsutfordring ulikt og ha vidt forskjellige strategier og virkemidler for å møte denne (De Wijk, 2012). For det kinesiske regimet har de strategiske hovedprioriteringene blitt oppsummert som følger: å beholde det kommunistiske regimet, å opprettholde økonomisk vekst, å bevare stabilitet innad, å bevare nasjonal suverenitet og å sikre Kinas status som global stormakt (Heinl, 2017). Mens de strategiske prioriteringene har ligget fast i lang tid, har det blitt argumentert for at det kinesiske regimet har inntatt en mer konfronterende posisjon de siste årene (Inkster, 2016). Digital politikk, både med tanke på nasjonal sikkerhet, bevaring av stabilitet innad og sikring av økonomisk vekst, har blitt et viktig element i den endrede kinesiske utenrikspolitikken og retorikken (Heinl, 2017; Webster et al., 2017; Triolo et al., 2017; Creemers, 2017). Den kinesiske tilnærmingen til cybersikkerhet har noen klare motsetninger til den «vestlige» forståelsen av sikkerhetsutfordringene. I den vestlige forståelsen har den primære trusselen vært enten tyveri av sensitiv informasjon eller sabotasje av kritiske funksjoner, mens den kinesiske tilnærmingen i større grad vektlegger innhold og meningsytringer som sikkerhetstrusler (Lindsay et al., 2015).

Totalt sett fører disse kulturelle og strategiske prioriteringene til at visse definerende trekk ved digitalisering blir oppfattet forskjellig i Vesten og hos kinesiske styresmakter (Zheng, 2015). Prinsipper som fri flyt av informasjon og deling av ideer, grunnsteiner i filosofien internett er bygget på, blir i mye større grad sett på som et problem og en sikkerhetsutfordring i den kinesiske konteksten (Lu Wei, 2014). Samtidig argumenter det kinesiske regimet for at suverenitetsprinsippet også gjelder for digital kommunikasjon og informasjon, sammenstilt i begrepet «cybersuverenitet». Dette begrepet bygger på et argument om at kinesiske myndigheters rett til å styre og kontrollere «sin» digitale sfære er like sterk som deres suverenitet over det fysiske territoriet som utgjør Kina. (Raud, 2016; Austin, 2014). Riktignok er det også i vestlige land et økt fokus på statlig kontroll over digitale teknologier,[4] men utviklingen er betydelig sterkere i mer autoritære land som Kina, Iran og Russland (Morgus et al., 2018)

I de senere år har det kinesiske regimet gått langt i å omgjøre disse perspektivene til praktisk utenrikspolitikk. I offisielle publikasjoner, strategier og notater er betydningen av digital suverenitet understreket og fremhevet (Heinl, 2017). Dette gjenspeiler seg i kinesiske myndigheters skepsis til amerikanskeide selskaper og

[4] Se for eksempel den norske debatten om digitalt grenseforsvar og tilrettelagt innhenting.

tjenesteleverandører. Det er et økende fokus på leverandører av teknologi og et ønske fra kinesiske myndigheter om å minske avhengigheten av utenlandske programvarer og teknologier (Creemers, 2017). Videre har man innført strenge regler for oppbevaring av data og promotert kinesisk teknologier og selskaper, også utenfor statens grenser (Inkster, 2016). Det mest omtalte av tiltakene har vært opprettelsen av den såkalte kinesiske brannmur, som filtrerer innhold fra resten av verden før det når kinesiske brukere (Weaver 2015). De siste årene har en strengere politikk mot virtuelle private nettverk gjort mulighetene for å omgå denne filtreringen vanskeligere (Pham, 2017). Etter at en ny cybersikkerhetslov trådte i kraft i juni 2017, har man også sett en rekke mindre tiltak, som regulering av medier, sterkere beskyttelse av data, byråkratisk omorganisering og et bredt spekter av reguleringer og standarder (Triolo et al., 2017).

Sikkerhetskultur og avskrekking

Ulike strategiske kulturer påvirker avskrekking som konsept på flere måter, både direkte og indirekte. I denne artikkelen vil vi fokusere på to måter kulturelle forskjeller påvirker mulighetene til cyberavskrekking på. Den første av disse dreier seg om konkrete uenigheter rundt konsepter og ideer og ulike virkelighetsoppfatninger. Å se ulikt på et problem innebærer at dette må «oversettes» slik at to parter kan snakke sammen og forstå hverandre. Et viktig poeng er dermed om både Kina og vestlige land har den samme forståelsen av cybersikkerhet og konseptet avskrekking. Den andre mekanismen handler om hvordan strategisk kultur gjenspeiles i de faktiske tekniske komponentene. På et grunnleggende nivå handler cybersikkerhet om infrastruktur, servere og protokoller for kommunikasjon. Ulike kulturelle og sosiale oppfatninger gjør at cyberdomenet ikke bare forstås annerledes, men at det helt konkret *er* annerledes.

Et naturlig sted å starte er de ulike forståelsene av begrepet *avskrekking* i kinesisk og vestlig litteratur. Ettersom avskrekking har vært et så viktig begrep i den vestlige litteraturen, særlig i etterkant av den kalde krigen, har man gått langt i å anta at dette er et universalt begrep. Resultatet har vært at kinesisk atomvåpenpolitikk har blitt lest fra et avskrekkingsperspektiv (Lewis, 2008). Et spørsmål verdt å stille seg, er om avskrekking har hatt den samme betydningen i kinesisk strategisk tenkning, og om konseptet var like utviklet og enhetlig som i vestlig tenkning (Taylor & Medeiros, 2011). Relatert til dette, og vel så relevant, er i hvilken grad vestlige strateger er i stand til å ta inn over seg den kinesiske forståelsen av avskrekking. Som et eksempel har argumentet om et mer selvsikkert og konfronterende kinesisk regime blitt kritisert for å være en feillesing av tidligere oppførsel (Johnston, 2013). For at avskrekking skal fungere, er det essensielt med vellykket kommunikasjon mellom den avskrekkende part og mottakeren. Forvirring og misforståelser rundt motpartens prioriteringer og logikk vanskeliggjør avskrekking. Dette taler for en tilpasning til ulike lands kulturer (Lantis, 2009).

De ulike oppfatningene stopper ikke ved begrepet avskrekking. Det finnes også ulike oppfatninger av hva cybersikkerhet er. Uenighet om hvorfor digitale teknologier er et sikkerhetsproblem, gjør det vanskelig å bli enig om hvordan man skal forhindre uønsket aktivitet. Uten en felles forståelse av hva som er skadelig aktivitet, er det vanskelig å lykkes med gjensidig avskrekking. Et eksempel på dette er utviklingen innen spionasje, hvor cyberangrep har blitt et utbredt virkemiddel for denne type «gråsone»-aktiviteter (Rid, 2011, s. 82). Fra vestlig side har den utbredte kinesiske bruken av industrispionasje for å stjele informasjon fra private selskaper vært et omstridt tema, ettersom statlig spionasje mot private selskaper anses som illegitime mål i Vesten (U.S. Department of Justice, 2018). Den tettere koblingen mellom kinesiske selskaper og regimet, som mest tydelig har blitt problematisert i den økende konflikten rundt Huawei, tyder på at skillelinjen mellom offentlig og privat er mindre markant i kinesisk kontekst (Al Jazeera, 2019). De to ulike oppfatningene av hva som er «legitim» spionasje, resulterer i ulike virkemidler. I en slik kontekst vil det være mer relevant med trusler om *gjengjeldelse* og *kommunikasjon* av ens egen posisjon og prioriteringer, slik det var tilfellet da Kina og USA kom til en enighet om økonomisk spionasje i 2015 (Gomez, 2017). Videre gjør uenigheter om hva cybersikkerhet egentlig *er*, at det blir vanskeligere å utvikle internasjonale normer. Den økte konflikten i internasjonale fora gjør at normer blir et mindre relevant virkemiddel mellom stater som har ulike oppfatninger, slik Kina og Vesten har i dag (Tikk & Kerttunen, 2018)

Et tredje og siste argument dreier seg mindre om ulike forståelser av avskrekking og cybersikkerhet og mer om hvordan ulike forståelser resulterer i andre teknologiske virkeligheter. Teknologi og teknologisk utvikling oppstår ikke i et vakuum, men i samspill i en større sosial kontekst som former hvordan teknologien fungerer (Rid, 2016; Jasanof, 2004). Det er allerede i dag en tiltakende konflikt mellom Vesten og Kina om leveranser av teknologi og bruken av utenlandske selskaper. Vestlige land peker i stor grad på risikoen for spionasje, sabotasje og kritisk infrastruktur og misbruk av private selskaper, med referanse til den kinesiske sikkerhetsloven for å begrunne sin mistillit (Al Jazeera, 2019). Samtidig har kinesiske myndigheter stengt selskaper som Google og Facebook ute, ettersom disse ikke er villige til å lagre data lokalt i Kina (Sacks, 2018). Uenigheten og mistilliten når det gjelder felles regler for digital teknologi, resulterer dermed i stadig mer separate nettverk og systemer, ettersom stater stenger ute teknologi fra land de ikke er alliert med.

Hva er så konsekvensene av dette for avskrekking? Et viktig poeng er at ulike systemer risikerer å undergrave gjensidig avhengighet som en konfliktdempende mekanisme. Stadig mer ulike systemer i Kina og Vesten vil minske relevansen av en slik avhengighetslogikk. Som et illustrerende eksempel kan vi se på et angrep mot ukrainske selskaper sommeren 2017. NotPetya-skadevaren, høyst sannsynlig et russisk angrep på Ukraina, spredde seg via et ukrainsk firma som leverte ett av de to regnskapsprogramvarene som selskaper i landet var pålagt å bruke. Ved å bruke dette sær ukrainske selskapet som angrepsvektor har det blitt spekulert i at man ville begrense skadeomfanget til mål kun i Ukraina. Men ettersom angrepet

også utnyttet en sårbarhet i Windows, ble den faktiske spredningen mye større, og en rekke selskaper utenfor Ukraina ble rammet (Greenberg, 2018). Risikoen ved mer atskilte systemer og teknologier er at slike uintenderte konsekvenser blir mindre utbredt, noe som potensielt vil senke terskelen for å gjennomføre digitale angrep. Dersom ulike kulturelle og historiske erfaringer resulterer i ulike teknologiske systemer, vil avskrekking måtte tilpasses denne nye virkeligheten. Gjensidig avhengighet og normer vil bli mindre relevante mekanismer i de tilfellene hvor det er stor uenighet om hva cybersikkerhet faktisk er, både fordi stater ikke vil klare å enes om felles regler å basere seg på, og fordi uenigheten vil kunne resultere i vidt ulike teknologiske økosystemer. I en slik situasjon vil man måtte lene seg tyngre på mekanismer som nektelse og straff, fordi normer og gjensidig avhengighet vil ha mindre relevans. Hvis systemene blir mindre sammenkoblet, kan til og med straff som avskrekkingsstrategi bli *mer* effektivt, nettopp fordi angrep vil kunne bli mer målrettet.

Konklusjon

Den stadig økende betydningen av digital teknologi i moderne samfunn har gjort spørsmålet om cybersikkerhet til et av de mest omtalte temaene i internasjonal politikk. En av de store debattene omhandler avskrekking og i hvilken grad begrepet er anvendbart i cyberdomenet. Denne debatten har i stor grad handlet om de teknologiske særegenhetene, slik som utfordringene med å attribuere angrep, den høyere tilgjengeligheten til digitale våpen og den lavere terskelen for angrep. Denne typen argumenter tar i stor grad utgangspunkt i at teknologien er lik for alle og har samme påvirkning på tvers av sosiale og kulturelle kontekster. Selv om denne typen argumenter har mye for seg, har vi i denne artikkelen belyst hvordan stater oppfatter og anvender teknologi ulikt, og at ulike strategiske kulturer dermed krever ulike fremgangsmåter for avskrekking. Vi har trukket frem tre måter strategisk kultur påvirker avskrekking i cyberdomenet på: Ved at stater forstår avskrekking forskjellig, ved at stater har ulik forståelse av cybersikkerhet og av hvordan/hvorfor digitalisering kan være en sikkerhetsutfordring, og ved at disse forskjellene gjenspeiler seg i stadig mer differensierte teknologier og systemer.

Ved å anvende dette rammeverket på forholdet Vesten-Kina har vi vist hvordan de ulike strategiske kulturene har stor innflytelse på avskrekking. De forskjellige oppfatningene i Vesten og Kina gjør visse mekanismer for avskrekking mindre relevant, som normer og gjensidig avhengighet, mens andre, som nektelse og straff, kan bli mer relevant. Mens de konkrete mekanismene kan debatteres, vil det overordnede poenget være gjeldende: Den kulturelle konteksten vil være like styrende for hvordan og i hvilken grad cyberavskrekking fungerer, som teknologien i seg selv. Ved å komplementere teknologisk forståelse med særegenhetene ved en strategisk kultur vil et klarere bilde av mulighetene for cyberavskrekking tre frem, og behovet for tilpassede avskrekkingsstrategier vil bli tydelig.

Om forfatterne

Lars Gjesvik er doktorgradsstipendiat ved NUPI og Universitetet i Oslo. Han ser på de politiske aspektene ved fiberoptiske kabler og internettinfrastruktur. Emil Jørgensen Øverbø er utdannet statsviter med mastergrad i Peace and Conflict Studies ved Universitetet i Oslo. Han jobber til daglig som risiko- og sårbarhetsanalytiker for Forsvarsbygg. Han har tidligere jobbet som vitenskapelig assistent på Nupi. Hans akademiske spesialisering er innenfor europeisk sikkerhetspolitikk og avskrekkningsteori.

Kilder

Al Jazeera (2019). China, US continue tit-for-tat row over Huawei. Hentet 18. februar 2019 fra https://www.aljazeera.com/news/2019/02/china-continue-tit-tat-row-huawei-190216144833685.html

Austin, G. B. (2014). Managing Asymmetries in Chinese and American Cyber Power. *Georgetown Journal of International Affairs*, IV, 2014.

Bendiek, A. & Metzger, T. (2015). Deterrence theory in the cyber-century. Working Paper RD EU/Europe, 2015/02, May SWP Berlin.

Betz, D. J. & Stevens, T. (2011). Cyberspace and sovereignty. I *Cyberspace and the State*, [ufullstendig referanse]

Brantly, A. F. (2018). The cyber deterrence problem, for *Nato Cooperative Cyber Defence Centre of Excellence*, Tallinn 2018 [ufullstendig referanse]

Collier, J. (2017). Proxy actors in the cyber domain: Implications for state strategy". *St Antony's International Review, 13*(1), 25–47.

Creemers, R. (2017). Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China, 26*(103), 85–100.

De Wijk, R. (2012). Hybrid conflict and the changing nature of actors. I *The Oxford handbook of war*, [ufullstendig referanse]

Dunn Cavelty, M. (2018). Cybersecurity research meets science and technology studies. *Politics and Governance, 6*(2), 22–30.

Fravel, M. T., & Medeiros, E. S. (2011). China's search for assured retaliation: The evolution of Chinese nuclear strategy and force structure. *International Security, 35*(2), 48–87.

Freedman, L. (2013). *Strategy, a history.* Oxford: Oxford University Press.

Gomez, M. A. (2017). Beyond ones and zeroes: Reframing cyber conflict. *International Affairs*, Spring 2017.

Greenberg, A. (2017). The White House blames Russia for NotPetya, the "most costly cyberattack in history". *Wired,* 15. februar 2018. Hentet 24. mai 2018 fra https://www.wired.com/story/white-house-russia-notpetya-attribution/

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history". *Wired*, 22. august 2018. Hentet 13. september 2018 fra https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Guangqian, P. & Youzhi, Y. (2005). *The science of military strategy.* Beijing, Military Science Publishing House.

Harknett, R. (1996). Information warfare and deterrence. *Parameters, 26*(3).

Heinl, C. H. (2017). New trends in Chinese foreign policy: The evolving role of cyber. *Asian Security*, 2017.

Inkster, N. *China's cyber power.* Milton Park, Abingdon: Routledge.

Jasanoff, S. (2004). *States of knowledge: The co-production of science and social order.* Milton Park, Abingdon: Routledge.

Johnston, A. I. (2013). How new and assertive is China's new assertiveness? *International Security, 37*(4), 7–48.

Lantis, J. S. (2009). Strategic culture and tailored deterrence: Bridging the gap between theory and practice. *Contemporary Security Policy*, *30*(3), 467–485. https://doi.org/10.1080/13523260903326677

Lawson, E. (2017) *Cyber security: Deter or die?* Hentet 16. april 2017 fra https://rusi.org/commentary/cyber-security-deter-or-die

Leonard, M. (Red.) (2016). *Connectivity wars: Why migration, finance and trade are the geo-economic battlegrounds of the future*. London: European Council on Foreign Relations.

Lewis, J. (2018). Minimum deterrence. *Bulletin of the Atomic Scientists, 64*(3), 40.

Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. Hentet 20. mai 2018 fra https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Lindsay, J. R. (2015). Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity, 1*(1), 53–67.

Lindsay, J. R., Cheung, T. M. & Reveron, D. S. (2015). *China and cybersecurity*. Oxford: Oxford University Press.

Lu Wei (2014). Cyber sovereignty must rule global internet. *Huffington Post*, 15. desember 2014. Hentet 14. april 2017 fra http://www.huffingtonpost.com/lu-wei/china-cyber-sovereignty b 6324060.html

Morgus https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/ [ufullstendig referanse]

Muller, L. & Stevens, T. (2017). Upholding the NATO cyber pledge cyber deterrence and resilience: Dilemmas in NATO defence and security politics. *NUPI Policy Brief.* Oslo: Norsk utenrikspolitisk institutt.

Nakashima, E. (2016). Cyber researchers confirm Russian government hack of Democratic National Committee. The Washington Post, 20. juni 2016. Hentet 5. september 2018 fra *https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3 719-11 e6-9ccd-d6005beac8b3_story.html?noredirect=on&utm_term=.0c8f70b1a0f*

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

Pham, S. (2017, 24. januar). China fortifies great firewall with crackdown on VPN's. *CNN Business*. Hentet 22.04.2017 fra http://money.cnn.com/2017/01/23/technology/china-vpn-illegal-great-firewall/

Raud, M. (2016). China and cyber: Attitudes, strategies, organization. Rapport for *Nato Cooperative Cyber Defence Centre of Excellence,* Tallinn.

Rid, T. (2011). *Cyber war will not take place.* Sted, India: Oxford University Press.

Rid, T. & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37.

Rid, T. (2016). *Rise of the machines.* London: Scribe Publications.

Sacks, S. (2018, 18. juni). Beijing wants to rewrite the rules of the internet. *The Atlantic*. Hentet 05.01.2019 fra https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/

Segal, A. (2017, 24. juli). Which cyberattacks should the United States deter, and how should it be done?" Blog Post for Council on Foreign Relations.

Singer, P. W. & Friedman, A. (2014). *Cybersecurity and cyberwar – what everyone needs to know.* New York: Oxford University Press.

Slayton, R. (2017). What is the cyber offense-defense balance? *International Security, 41*(3).

Solon, O. (2017, 13. september). US Government bans agencies from using Kaspersky software over spying fears. *The Guardian*. Hentet 15.09.2018 fra https://www.theguardian.com/technology/2017/sep/13/us -government-bans-kaspersky-lab-rus sian-spying

Sulmeyer, M. (2018). How the U.S. can play cyber-offence. *Foreign Affairs.* Hentet 17.09.2018 fra https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense

Taddeo, M. (2018). The limits of deterrence theory in cyberspace. *Philosophy & Technology, 31*(339). Hentet fra https://doi.org/10.1007/s13347-017-0290-2

Tikk, E. & Kerttunen, M. (2018). International cybersecurity: Orchestral manoeuvres in the dark. *NUPI Policy Brief.* Oslo: Norsk Utentrikspolitisk Institttut.

Tor, U. (2017). 'Cumulative deterrence' as a new paradigm for cyber deterrence. *Journal of Strategic Studies, 40*(2), 92–117.

Triolo, P., Sacks, S., Webster, G. & Creemes, R. (2017). China's cybersecurity law one year on. *Cybersecurity Initiative*. Hentet 10.09.2018 fra https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/

U.S. Department of Justice (2018). Two Chinese hackers associated with the ministry of state security charged with global computer intrusion campaigns targeting intellectual property and confidential business information. Hentet 20.12.2018 fra https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

Waddell, K. (2017, 13. januar). Why elections are now classified as 'critical infrastructure'. The Atlantic. Hentet 20.04.2017 fra https://www.theatl antic.com/technology/archive/2017/01/why-the-governmentclassified-elections-as-critic al-infrastructure/513122/

Weaver, N. (2015, 5. juni). How China's 'great cannon' works – and why we should be worried. *CNN*. Hentet 16.04.2017 fra http://edition.cnn.com/2015/06/04/opinions/china-great-cannon/

Webster, G., Creemers, R., Triolo, P. & Kania, E. (2017). China's plan to 'lead' in AI: Purpose, prospects, and problems. *Cybersecurity Initiative*. Hentet 10.09.2018 fra https://www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-purpose-prospects-and-problems/

Zheng, Y. (2015). From cyberwarfare to cybersecurity in the Asia-Pacific and beyond. I Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (Red.), *China and cybersecurity.* Oxford: Oxford University Press.

Zhong, R., Mozur, P. & Nicas, J. (2018, 17. april). Huawei and ZTE hit hard as U.S. moves against Chinese tech firms. *The New York Times*. Hentet fra https://www.nytimes.com/2018/04/17/technology/huawei-trade-war.html lest 05.09.2018

Abstract in English

There is an ongoing debate in academia about if and how deterrence theory may be used in cyberspace. Deterrence was originally a theory developed for avoiding conventional and nuclear war. In the current discussion on cyber security, there has been pointed out a range of technical problems of transferring a theory about the physical world to cyberspace. We recognize these challenges of deterrence in cyberspace, but in this article we want to shed light on a different aspect of deterrence. That is the interplay between social and technical factors of deterrence in cyberspace. In this article we will discuss how deterrence as a strategy in cyberspace is influenced by the specific strategic culture of a country. We will use China as a case study to showcase our argument. Contrasts between Chinese and "Western" strategic culture results in concrete differences in how Chinese and Western countries act in cyberspace. By utilizing four components of deterrence theory (denial, punishment, entanglement and norms), we will show how an in-depth knowledge of a state's security policy and strategic culture may be used to tailor a more effective deterrence and enforce the capacity of hindering unwanted activity.

Keywords: deterrence · cyberspace · strategic culture · China