Fagfellevurdert

Internasjonal POLITIKK
Skandinavisk tidsskrift for Internasjonale Studier

Årgang 77, Nummer 3, side 288-295, 2019, ISSN 1891-1757, www.tidsskriftet-ip.no, Publisert september 2019

Fokus: Cybersikkerhet

Inn i gråsonen: avskrekking som forsvar av cyberspace?

Lilly Pijnenburg Muller*
Norsk utenrikspolitisk institutt (NUPI)

Sammendrag

Selv om det kan hevdes at de ulike elementene som utgjør cyberoperasjoner – undergraving, sabotasje, manipulering, tyveri og desinformasjon – ikke er noe nytt, sprer de seg i dag med en hastighet og i et omfang som er uten historisk sidestykke. Cybersikkerhet er tett sammenvevd med det 21. århundres politiske og militære konflikter. Som NATOs generalsekretær Jens Stoltenberg påpeker, har de fleste konflikter og kriser i våre dager en cyberdimensjon, og det er vanskelig å forestille seg en militær konflikt i dag uten (Stoltenberg, 2016). Av denne grunn har såkalt cyberavskrekking blitt tema for en omfattende militær, politisk og akademisk debatt som kretser rundt et sett av viktige operasjonelle konsepter og overveielser. Et sentralt tema er hvorvidt det *kan* avskrekkes i cyberspace, gitt attribusjons utfordringene som preger etterdønningene av et cyberangrep. Denne artikkelen stiller spørsmål ved om «cyberavskrekking» er mulig og hensiktsmessig, og drøfter nye mulige måter å tenke rundt avskrekking i cyberspace på.

Nøkkelord: avskrekkingsteori · cybersikkerhet · attribusjon · forsvar · offentlig-privat samarbeid

Introduksjon

Et trygt cyberspace er avgjørende i vår såkalte informasjonsalder, hvor samfunnet er grunnleggende avhengig av digital teknologi for å fungere. Digitalisering av

*Korrespondanse: Lilly Pijnenburg Muller, e-post: lilly.muller@nupi.no

Citation: Lilly Pijnenburg Muller (2019). Inn i gråsonen: avskrekking som forsvar av cyberspace?. Internasjonal Politikk, 77(3): 288–295. http://dx.doi.org/10.23865/intpol.v77.1397

samfunnet og vår økende avhengighet av informasjonsteknologi har ført til at nye og hittil ukjente sårbarheter kan bli, og ofte blir, utnyttet av både statlige og ikke-statlige aktører. Offensive cyberoperasjoner utføres ikke bare for kriminell eller kommersiell vinning, men har også fått innflytelse på hvordan internasjonal politikk utføres. Den økte bruken av cyberoperasjoner fra både statlige og ikke-statlige aktører i konflikt og fredstid har gjort sikringen av cyberspace mer komplekst. Dette gjelder for både utformingen av offensive operasjoner og en eventuell avskrekking av dem. Som et resultat har cyberspace blitt akseptert som et nytt krigsdomene, hvor både stater og ikke-statlige aktører konkurrerer i kampen om makt og innflytelse (NATO, 2016).

Denne artikkelen stiller spørsmål ved om såkalt cyberavskrekking er mulig og, i så fall hensiktsmessig. Om ikke, finnes det alternativer? Og hva ønsker stater egentlig å avskrekke i cyberdomenet? For å svare på disse spørsmålene drøfter artikkelen først nøkkelbegreper i tradisjonell avskrekkingsteori og stiller spørsmål ved om disse kan anvendes i cyberspace. Videre påpekes en rekke problemer rundt overførbarheten av eksisterende avskrekkingsmodeller til cyberspace. Avslutningsvis drøftes alternative og komplementære tilnærminger til avskrekking i cyberdomenet. Fellesnevneren for disse komplementære tilnærmingene er at for å lykkes, krever de en nytenking rundt begrepet «cyberavskrekking». Artikkelen argumenterer for at cyberavskrekking må betraktes som en kontinuerlig prosess, som må benytte nasjonale og allierte ressurser fra flere domener i et integrert samspill som et middel for å etablere avskrekking og motstandskraft.

Begrepet avskrekking i militær teori – fra den kalde krigen til i dag

Avskrekking betegner evnen til å overbevise motstandere om at du er i stand til å påføre dem betydelige kostnader eller begrense deres mulige gevinst dersom de skulle begå en offensiv handling mot deg. Avskrekking er en nødvendig delkomponent i militærstrategi og omfatter potensiell eller faktisk anvendelse av makt for å påvirke handlingene til en aktør (Freedman, 2004, s. 26). I motsetning til tvang – som tar sikte på å endre en atferd som allerede er påbegynt – tar avskrekkingsmanøveren sikte på å endre en aktørs atferd før den blir satt i verk. Dette gjøres i følge avskrekkingsteori ved å endre aktørens kostnads- og nyttevurdering av de ulike strategiske valgene som er tilgjengelige (Freedman, 2004; Snyder, 1961). Hvis aktørene oppfatter at den forventede kostnaden av en bestemt handling er større enn den sannsynlige nytteverdien, vil de ifølge teorien bli avskrekket fra å utføre denne handlingen, og *status quo* blir opprettholdt.

Avskrekkingen er dermed betinget av hvorvidt en motstander oppfatter en trussel som troverdig. Det er med andre ord ikke kun avhengig av rent teknisk, men også psykologisk evne. Dette psykologiske aspektet kan illustreres ved forskjellen mellom de to tradisjonelle typene avskrekking: gjengjeldelse og hindring. Den førstnevnte er avhengig av at forsvarerens trussel om å slå tilbake dersom den skulle bli angrepet, blir ansett som troverdig av angriperen, og videre at ethvert forsøk på angrep vil bli gjengjeldt. Den sistnevnte er avhengig av forsvarerens evne til å hindre angriperen

i å oppnå målet sitt (Snyder, 1961). Mens gjengjeldelse innebærer ren maktbruk, inneholder hindring også elementer av kontroll. Hindring i denne forstand har til hensikt å beholde kontroll over situasjonen i så stor grad at motstanderen fratas sine strategiske alternativer, uten nødvendigvis å bli tvunget til å godta et bestemt utfall (Freedman, 2004, s. 37).

Avskrekking ble ansett som en vellykket strategisk modell under den kalde krigen, da stormaktenes gjensidige avskrekking forhindret bruken av atomvåpen. Til tross for perioder med strategisk spenning og eskalering har denne vellykkede forhindringen av atomkrig kommet til å forme etterfølgende debatter om avskrekking som militærstrategi. Dette har hatt ringvirkninger også for andre strategiske domener. Avskrekkingstankegangen slik den ble praktisert i en atomkonflikt, kan imidlertid ikke like enkelt overføres til andre sammenhenger (Harknett, 1994; 2018). Atomvåpen står i skarp kontrast til andre våpen som brukes til avskrekking, spesielt der hvor et mangfold av aktører, intensjoner og teknologiske ressurser eksisterer i tett samspill i en sjablong av konkurrerende kapabiliteter og muligheter (Sterner, 2011).

Selv om kunnskap fra den kalde krigen gir nyttig innsikt i strategisk interaksjon mellom stater, kan en modell for avskrekking i cyberdomenet ikke avledes direkte fra ideen om avskrekking basert på atomvåpen (Lupovici, 2014). I motsetning til atomvåpen, som brukes én gang av en enkelt aktør, og hvor det er tydelig hvor angrepet kommer fra, er «attribusjonsproblemet» et av de første og mest fremtredende problemene som blir identifisert og diskutert av både praktikere og akademikere i debatter om cyberavskrekking.

Et attribusjonsproblem?

William J. Lynn, tidligere viseforsvarssjef i USA, skrev i 2010 at missiler kommer med en returadresse, men det gjør som oftest ikke et datavirus. Videre påpekte han at arbeidet med å identifisere en angriper kan ta måneder, om det det i hele tatt er mulig (Lynn, 2010, s. 99). Hovedbakgrunnen for attribusjonsproblematikken er påstanden om at en aktør som opererer i og gjennom cyberspace, kan skjule kilden til angrepet og dermed sin egen identitet. Når man ikke vet hvem som har til hensikt å utføre et angrep, er det vanskelig å avskrekke fra gjennomføring av det (Lindsay, 2015, s. 8). Tilsvarende, dersom man ikke vet hvem som har utført ett angrep, er det vanskelig å avskrekke aktøren fra å gjenta det.

Den potensielle mangelen på en «returadresse» har lenge vært erkjent som et hinder for muligheten og evnen til å innta en troverdig avskrekkingsposisjon i cyberspace (Lynn, 2010, s. 99). Ut fra denne problematikken hevder teoretikere som Taddeo (2017), Goodman (2010) og Haley (2013) at attribusjon av angrep igjennom cyberspace i beste fall er problematisk, om ikke umulig. Selv om attribusjonsproblemet gjør det mer komplisert å avskrekke en potensiell angriper, er anonymitet imidlertid ikke noe absolutt kjennetegn i cyberspace. Mangel på attribusjonsevne vil ikke nødvendigvis gjøre avskrekkingen mindre effektiv. I tillegg til dette

er attribusjonsproblematikken ikke unik for cyberdomenet; væpnede angrep utføres også ofte anonymt (Elliott, 2011).

Som Lynn (2010) påpekte, kan oppsporing av kilden til et digitalt angrep ta tid – selv om den har blitt kortet betydelig ned ved hjelp av involvering av eksperter fra privat sektor. I tillegg finnes det andre måter å omgå attribusjonsproblemet på. Som Rid og Buchanan (2015) hevder, må attribusjon settes i kontekst. Det er ikke utelukkende avhengig av tekniske forhold. Angrep må vurderes ut fra en større sammenheng og settes inn i en sammenheng (Betz & Stevens, 2011). Attribusjon er like mye en politisk som en teknisk utfordring. Selv om man ikke kan være hundre prosent sikker, er det ikke umulig å attribuere; det kan finnes solid grunnlag for å anta at en bestemt aktør har vært involvert i en cyberoperasjon, selv uten tekniske bevis (Betz & Stevens, 2011). Et eksempel på dette er kongresshøringen om påstått russisk innblanding i det amerikanske presidentvalget i 2016. Alle vitnene bekreftet at etter deres oppfatning var det Russland som sto bak operasjonen, selv uten at det forelå en «smoking gun» på den tiden høringen fant sted (US Senate Select Committee on Intelligence, 2017). Konklusjonen var basert på vurdering av en rekke politiske, tekniske og strategiske faktorer.

Om vi aksepterer premisset at attribusjon ikke nødvendigvis er et like stort problem for avskrekking som det blir hevdet i debatten, stiller spørsmålet seg annerledes. I stedet for å stille spørsmål ved om avskrekking er et problem, burde vi heller stille spørsmål ved hvordan den skal anvendes, og hva stater ønsker å avskrekke.

En revurdering av avskrekkingsparadigmet – nye ideer

Flere forskere har lagt frem forslag til hvordan cyberavskrekking kan virkeliggjøres. Joseph Nye (2012) hevder at nøkkelen til vellykket avskrekking fra cyberangrep ligger i «self-deterrence» – avskrekking som påfører kostnader på både angriperen og den som blir angrepet. Denne ideen er basert på gjensidig avhengighet som gjør at dersom angriperen lykkes med angrepet sitt, vil dette koste både offeret og den som angriper. Argumentet baserer seg på ideen om at dersom to stater er avhengig av de samme tingene, vil et angrep mot «offeret» også påføre agressoren skade. Cyberspace blir her presentert som en global allmenning hvor alle stater har en interesse og goder av å bruke internettet. En slik avhengighet vil hindre et land i å angripe et annet, da en automatisk ikke bare skader «offeret» men også angriperen selv. Det er per i dag ingen formell aksept for cyberspace som en slik global allmenning, men at land er bundet sammen gjennom internett, frykten for en potensiell eskalering og uforutsette utfall av et angrep må tas i betraktning av en potensiell angriper. Jo mer et land er avhengig av digital infrastruktur, desto viktigere vil det være å opprettholde et stabilt og trygt internett (Nye, 2012).

En annen avskrekkingsmodell som baserer seg på at attribusjon ikke nødvendigvis er et problem, omfatter «normbasert avskrekking» fra digitale angrep. Denne modellen, som først ble lagt frem av Freedman i 2004, baserer seg på at, i likhet med atomvåpen, er det ikke bare våpenet i seg selv som må forstås, men også dem som

har tilgang til disse våpnene. Avskrekking blir følgelig ikke utelukkende et spørsmål om teknisk evne til å handle, men også om forståelsen av praksis og de involverte aktørenes motiver og intensjoner om å handle, samt av de sosiale, kulturelle og politiske faktorene som former dem.

Selv om dette er et viktig poeng, vil en slik normbasert avskrekking være mest effektiv mot stater og mindre anvendelig overfor ikke-statlige aktører, da evnen til å kommunisere med disse er mer begrenset. Evnen til å svare på et vellykket angrep fra en ikke-statlig aktør vil også være mindre. For å omgå dette problemet foreslår Uri Tor (2017) et kumulativt avskrekkingsparadigme. Det kumulative paradigmet tar ikke sikte på å forhindre at cyberangrep vil skje, da dette betraktes som urealistisk. Det kumulative avskrekkingsparadigmet tar heller for gitt at cyberaggresjon vil finne sted, og søker snarere å forebygge og begrense slike handlinger gjennom å gå til angrep mot den rivaliserende aktøren. Tor hevder at slike angrep må skje gjentatte ganger som tilsvar på cyberaggresjon over lang tid. Noen ganger vil også den utløsende hendelsen måtte møtes med en uforholdsmessig kraftig respons (Rid, 2012). Det kumulative avskrekkingsparadigmet er dermed av restriktiv snarere enn av absolutt natur. Det forutsetter at ulike former for angrep vil finne sted, med både store og små virkninger, og dermed er det ikke et spørsmål om de vil skje eller ikke. Graden av avskrekking er dermed det viktigste spørsmålet. Et sentralt trekk ved dette paradigmet er at avskrekkingen skjer på tvers av flere domener, og at aktivitetene ikke er begrenset til cyberspace. Det er også behov for kinetiske operasjoner i tillegg til diplomatisk og politisk påvirkning.

Tors rammeverk inneholder elementer av makt, da det ikke kun er rettet mot aggressorens oppførsel, men også er konstruert for å påvirke de andre som deltar i spillet. Mens Nye argumenterer for et fokus på økonomisk sammenveving og normer, beskriver Tor en posisjon som beveger seg bort fra absolutt avskrekking, mot et kumulativt cyberavskrekkingsparadigme som er restriktivt og kontinuerlig. Disse modellene har både styrker og svakheter, men begge understreker hvordan avskrekking av et cyberangrep må ta de faktiske forholdene rundt et angrep i betraktning. Videre viser de kompleksiteten som er involvert. Selv om de har ulikt fokus, antar de ulike modellene at avskrekking av cyberangrep er mulig, og de er innforstått med at det kan finnes mer enn én riktig variant. De erkjenner at det er usannsynlig at cyberavskrekking kan forhindre alle angrep kun ved hjelp av cybermidler. De ulike avskrekkingsposisjonene søker om mulig heller å påvirke konfliktområdet, uten noen forventning om total dominans.

Ut av gråsonen

Cyberavskrekking har blitt et tema for en omfattende militær, politisk og akademisk debatt konsentrert rundt en rekke viktige operasjonelle konsepter og overveielser (Stevens, 2012; Lupovici, 2014; Tor, 2017). Med attribusjonsproblematikken som et sentralt tema har debatten fokusert på hvorvidt cyberavskrekking kan fungere, men med liten konsensus rundt hva man skal forsøke å hindre, og hvordan, og hvilke

konsekvenser en slik forhindring skal føre med seg (Sulmeyer, 2017). Ved å granske begrepet avskrekking har denne artikkelen vist at det dynamiske miljøet, truslenes omfang, mangfoldet av statlige og ikke-statlige aktører og de tekniske utfordringene forbundet med attribusjon, krever en omorientering av hvordan vi tenker rundt avskrekking og de praksisene som er forbundet med dette. En slik nytenking vil med fordel kunne fokusere på det som er særegent for cyberspace, men må også omfatte en oppmyking av ortodokse tanker som er innarbeidet i eksisterende perspektiver. En slik utvidet tankegang kan forskyve de etablerte grensene for teorier knyttet til avskrekking.

Det er ikke kun én form for avskrekking som kan fungere. Cyberspace er komplekst, og et avskrekkingsparadigme må reflektere denne kompleksiteten. Cyberdomenet er et offensivt miljø hvor vi vil fortsette å se en jevn økning i antall cyberangrep. Dette betyr imidlertid ikke at ethvert forsøk på avskrekking vil være forgjeves. I motsetning til avskrekkingsteknikker rundt bruk av kjernevåpen og i andre konvensjonelle sammenhenger er ikke cyberavskrekking avgrenset verken i tid eller til spesifikke hendelser. Cyberangrep kommer i så mange ulike former at vi ikke kan være bundet til å rette avskrekkingen kun mot bestemte typer aggresjon. Slike angrep må settes inn i en bredere politisk kontekst som omfatter en rekke hendelser, og også deres mulige fremtidige ettervirkninger, av ulik skala og type.

Tradisjonelle modeller for avskrekking er utilstrekkelig for å møte trusler i og fra cyberspace i det 21. århundre. Cyberavskrekking er både mulig og gjennomførbart, men vil nødvendigvis bestå av en kumulativ prosess som omfatter mer enn militære midler. Cyberavskrekking er mulig i teorien, men det trengs større klarhet om hvilke handlinger man ønsker å avskrekke, med hvilke verktøy og til hvilken kostnad (Healy, 2017). I motsetning til påstandene om at strukturen av cyberspace gjør avskrekking teoretisk umulig, med tilhørende oppfordringer om å bevege seg bort fra paradigmet for cyberavskrekking generelt, argumenterer denne artikkelen for at avskrekking i cyberdomenet er mulig (Harknett & Nye, 2017). I stedet for å bevege oss vekk fra avskrekking som konsept, bør vi heller stille spørsmål ved om avskrekking i seg selv er løsningen. Det er behov for å fokusere på hva stater ønsker å avskrekke. Hvordan skal den strategiske planen for å avskrekke se ut, og hvordan skal den gjennomføres på tvers av flere domener?

De fleste offensive cyberoperasjoner representerer ikke trusler mot nasjonal sikkerhet på høyt nivå, men kan snarere karakteriseres som kriminelle handlinger. Bekjemping av disse krever tverretatlig og offentlig-privat samarbeid, men vanligvis ikke av militær og transnasjonal karakter. I stedet for konfliktforebygging i tråd med modellen for avskrekking mot bruk av kjernefysiske våpen vil det være mer formålstjenlig å forsøke å påvirke selve konfliktområdet, uten noen forventning om å kunne dominere dette området fullstendig. I likhet med andre former for kriminalitet er slike angrep vanskelige å avskrekke (Nye, 2017). Uten å forestille seg et skarpt skille mellom kriminelle og strategiske cyberangrep der dette ikke finnes, vil det heller være hensiktsmessig å avklare hvilke handlinger og prosesser som utgjør trusler mot

nasjonal sikkerhet, og hvilke som ikke gjør det. Dette vil ha betydelige implikasjoner for avklaringen av forventninger og allokeringen av ressurser og dermed også for effektiviteten av avskrekking i cyberdomenet.

Angrep vil fortsette å forekomme hyppig i det digitale domenet. De er mange, kontinuerlige og tvetydige – og i stadig endring. Konflikt blir på denne måten den «nye normalen» i cyberspace (Korns, 2009). Enhver posisjon for avskrekking må underbygges av en forståelse av at cyberspacemiljøet er av «vedvarende persistens» (Harknett & Goldman, 2016). Forsøk på angrep av varierende størrelse, omfang og virkning vil fortsette å skje. For å lykkes må et fremtidig avskrekkingsregime bevege seg ut over de tradisjonelle militære aspektene rundt avskrekking og knyttes opp mot en bredere sosial og politisk kontekst. Dette kan gjøres ved å koble cyberoperasjoner til andre domener av nasjonal makt i et nøye overveid rammeverk som går på tvers av de ulike domenene. En slik kumulativ prosess omfatter elementer av både makt og avskrekking. Dersom avskrekking og motstandsdyktighet opptrer som integrerte komponenter i denne prosessen, med betydelig overlapp, vil motstandernes kostnads- og nytteanalyser kunne påvirkes. Et slikt rammeverk for cyberavskrekking aksepterer at cyberangrep vil skje, og tar samtidig høyde for at det ikke nødvendigvis er et uttrykk for svikt dersom noen lykkes med et angrep. Dette vil heller kunne anses som en mulighet til å lære og tilpasse seg.

Om forfatteren

Lilly Pijnenburg Muller er doktorgradstipendiat ved War Studies, King's College London og tilknyttet Norsk Utenrikspolitisk Institutt (NUPI). Hun har tidligere jobbet som forsker ved Global Cyber Security Capacity Building Centret ved University of Oxford.

Bibliografi

Betz, D. & Stevens, T. (2011). *Cyberspace and the state: Toward a strategy for cyber-power* (s. 94–95). London: Routledge for the International Institute for Strategic Studies.

Elliott, D. (2011). Deterring strategic cyberattack. *IEEE Security & Privacy, 9*(5), 36–40.

Farwell, J. & Rohizinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 31.

Foerster, S. (2012). Strategies of deterrence. I Jasper, S. (Red.), *Conflict and cooperation in the global commons: A comprehensive approach for international security* (s. 64–65). Washington, DC: Georgetown University Press.

Freedman, L. (2004). *Deterrence* (s. 6–37). Cambridge: Polity Press.

Lupovici, A. (2014). The 'attribution problem' and the social construction of 'violence' Taking cyber deterrence literature a step forward. *International Studies Perspectives*, *17*(3), 322–342.

Goodman, W. (2010). Cyber deterrence: tougher in theory than in practice? *Strategic Studies Quarterly*, 102–35.

Healy, J. (2017). Cyber deterrence is working – so far. *The Cipher Brief*. Hentet 11.11.2018 fra https://www.thecipherbrief.com/cyber-deterrence-is-working-so-far

Harknett, R. J. & Nye, J. S. Jr. (2017). Correspondence is deterrence possible in cyberspace? *International Security*, *42*(2), 196–199.

Harknett, R. J. & Goldman, E. O. (2016). The search for cyber fundamentals. *Journal of Information Warfare*, *15*(2), 81–88.

Harknett, R. J. (1994). The logic of conventional deterrence and the end of the Cold War. *Contemporary Security Policy, 4*(1), 86–114.

Korns, S. W. (2009). Cyber operations: The new balance. *Joint Force Quarterly, 54*(3), 97–102.
Libicki, M. C. (2009). Cyber deterrence and cyberwar. Hentet 05.11.2017 fra http://www.rand.org/pubs/monographs/MG877.html
Lindsay, J. (2015). Tipping the scales: The attribution problem and the feasibility of deterence against cyberattack. *Journal of Cybersecurity, 1*(1), 53–67.
Lupovici, A. (2014). The 'attribution problem' and the social construction of 'violence': Taking cyber deterrence literature a step forward. *International Studies Perspectives, 17*(3), 322–342.
Lynn, W. J. III (2010). Defending a new domain: The Pentagon's cyberstrategy. *Forign Affairs*, *89*(5), 99.
Nye, J. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71.
Rid, T. (2012). Deterrence beyond the state: The Israeli experience. *Contemporary Security Policy, 33*(1), 124–147.
Rid, T. & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37.
Stevens, T. (2012). A cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy, 33*(1), 148–170.
Stoltenberg, J. (2016). Press conference following the North Atlantic Council meeting at the level of NATO Defence Ministers, 14 June. Hentet 08.05.2017 fra http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=end
Snyder, G. H. (1961). *Deterrence and defense: Toward a theory of national security* (s. 14–16). Princeton, NJ: Princeton University Press.
Taddeo, M. (2017). The limits of deterrence theory in cyberspace. *Philos. Technol.* (31), 339–355. https://doi.org/10.1007/s13347-017-0290-2
Tor, U. (2017). 'Cumulative deterrence' as a new paradigm of cyber deterrence. *Journal of Strategic Studies, 40*(1–2), 92–117.
NATO (2016). Cyber defence pledge, 8 July. Hentet 05.08.2017 fra http://www.nato.int/cps/en/natohq/official_texts_133177.htm
Rid, T. & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37.
Sulmeyer, M. (2017). Which cyberattacks should the United States deter, and how should it be done? Hentet 09.02.2018 fra https://www.cfr.org/blog/which-cyberattacks-should-united-states-deter-and-how-should-it-be-done
US Senate Select Committee on Intelligence (2017). Disinformation: A primer in Russian active measures, 30 March.

Abstract in English

Cybersecurity is deeply intertwined with every aspect of today's political and military conflict. In conjunction with the growing acceptance of cyberspace as a military domain, so called "cyber deterrence" has become the subject of extensive military, political and academic debates. Revolving around a set of important strategic and operational concepts the debates are questioning whether deterrence can be achieved in cyberspace. In line with current debates, this article examines if "cyber deterrence" is possible, appropriate, and desirable, yet extends the debate by including new possible ways to think about deterrence and defense in cyberspace. By drawing attention to cyberspace's idiosyncrasies while questioning the orthodoxy of deterrence as a concept, a reconceptualization of "cyber deterrence" that focuses on cyberspace itself is argued for, one which incorporates new outlooks and ideas, some of which may challenge the established boundaries of deterrence theory.

Keywords: compellence · defense · deterrence theory · military power · offensive cyber capabilitie