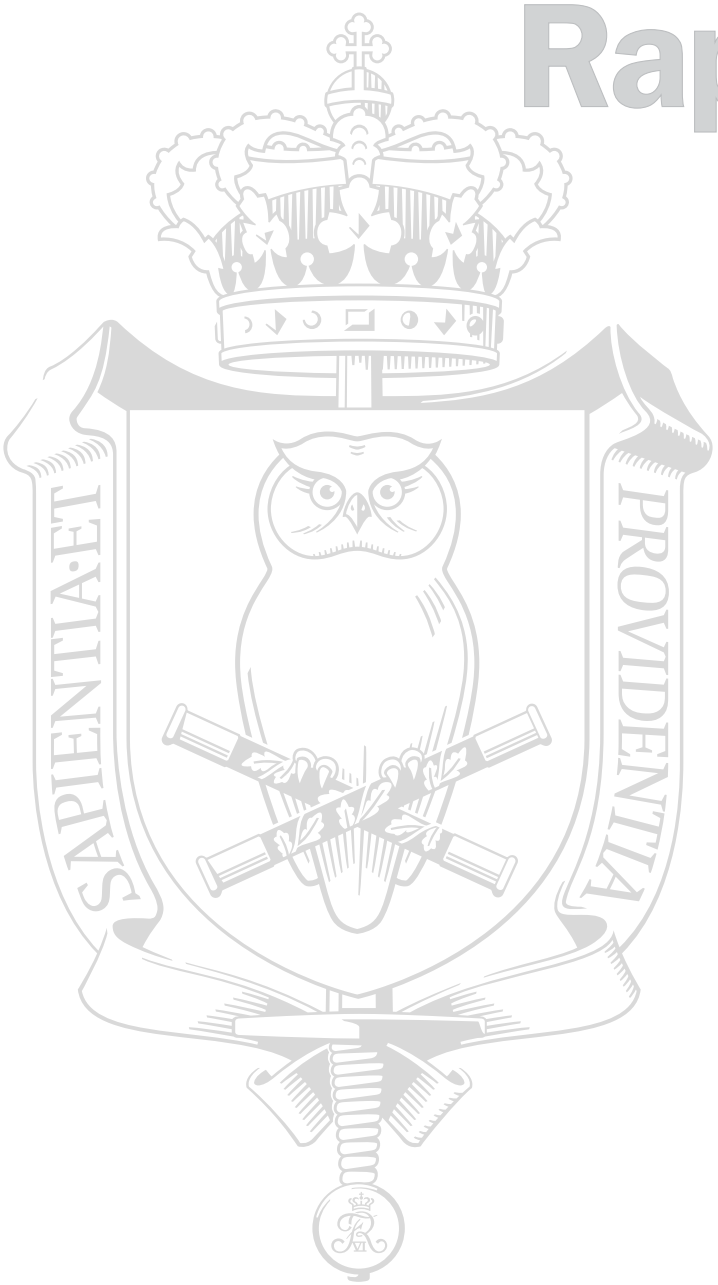
FORSVARET

Rapport

FEBRUAR 2018



Cybermagt er spoilermagt

Hvordan tæmmer vi våbenkapløbet i cyberspace og hæmmer destabiliseringen af internationale relationer?

Af studielektor Dorthe Bach Nyemann, Institut for Strategi, Forsvarsakademiet

FORSVARSAKADEMIET

FORSVARSAKADEMIET

Cybermagt er spoilermagt - Hvordan tæmmer vi våbenkapløbet i cyberspace og hæmmer destabiliseringen af internationale relationer?

Ved studielektor Dorthe Bach Nyemann, Institut for Strategi, Forsvarsakademiet[1]

1) Tak til Jørgen Staun for støtte og gode råd og for at holde mig på sporet undervejs i skriveprocessen.

København februar 2018
Forsvarsakademiet
Svanemøllens Kaserne
Ryvangs Allé 1
2100 København Ø
Tlf.: +45 728 17000
Ansvarshavende redaktør: Anja Dalgaard-Nielsen, Chef for Institut for Strategi
Layout: FAK
ISBN: 978-87-7147-222-6

INDHOLDSFORTEGNELSE

Abstract

Cyberspace udgør en arena for magtanvendelse, der giver særlige vilkår og muligheder for destabiliserende aktiviteter af afgørende betydning for forholdet mellem stater. Gennem denne rapport søges det påvist, at cybermagt først og fremmest er en spoilermagt, der kan være med til at undergrave centrale institutioner i staten. Samtidig øges de internationale spændinger, når der skabes gensidig usikkerhed om motiver, kapabiliteter, respons og adfærd i cyberspace. Denne usikkerhed er med til at accelerere et våbenkapløb om cyberkapabiliteter og øge sikkerhedsdilemmaet mellem stater. Det sker særligt, fordi anvendelse af cybermagt synes at privilegere offensive handlinger uden forvarsel. Karakteren af cyberspace fremmer vedvarende spionage og kontinuerlig udvikling af nye metoder til senere anvendelse. Cybermagt er først og fremmest en spoilermagt, men den har også eskalationspotentiale og kan lede til mere alvorlige konflikter mellem stater. Rapporten diskuterer flere mulige gensidigt afhængige strategier, som stater kan tage i anvendelse for at tæmme og hæmme den negative udvikling. Der peges på flere veje til at opnå mere klar kommunikation om grænser for og konsekvenser af adfærd i cyberspace. Det handler om at kombinere afskrækkelsesstrategier med normskabelse og samarbejde.

Rapportens spørgsmål

Cyberspaces betydning for staterne er omfattende og svær at få greb om. De seneste års udvikling har vist, at de vestlige stater er blevet langt mere sårbare og gennemtrængelige end tidligere på grund af den accelererende digitalisering. Det er blevet meget lettere at foretage destabiliserende aktiviteter via cyberspace uden for myndighedernes kontrol og regulering (Bradshaw & Howard, 2017.12) (Kragh & Åsberg, 2017) (Hennessey, 2017). Statens indre forhold, den kritiske infrastruktur og bærende demokratiske institutioner påvirkes ofte af både ikkestatslige aktører og fremmede statsmagter (Hansen, 2017:06, s. 21-24). Herved bliver det mere og mere tydeligt, at cyberspace er særlig velegnet til at spoile, undergrave og bryde ned. Selv om det er svært at få øje på motivet bag det enkeltstående tilfælde, sker der langsomt en udhuling og undergravning af tilliden til de institutioner, der bærer det liberale demokrati og vores fælles internationale institutioner.

Den undergravning giver samtidig plads til, at andre dagsordner end de liberaldemokratiske og andre internationale spilleregler end de vestligt funderede kan få øget betydning (Hennessey, 2017, s. 39). Samlet set rejser disse observationer en række spørgsmål. For hvad er det egentlig ved karakteren af cyberspace, der så afgørende ændrer vilkår og muligheder for staterne og den internationale stabilitet? Hvad er rækkevidden og betydningen af de destabiliserende aktiviteter og det tilhørende våbenkapløb i cyberspace? Og kan stater eller andre aktører begrænse de negative implikationer for international politik?

Denne rapport sætter cybermagt anvendt med destabilisering som mål på dagsordnen og undersøger, hvordan cyberaktiviteter påvirker statens sikkerhed og integritet samt de internationale relationer i allerbredeste forstand.[1]

Cybermagt og destabilisering diskuteres ud fra følgende tre spørgsmål:

1. Hvilke egenskaber ved cybermagt skaber særlige vilkår for at fremme destabilisering?
2. Hvordan påvirker aktiviteter i cyberspace sikkerhedsdilemmaet mellem stater?
3. Hvilke strategier kan stater tage i anvendelse for at hæmme destabiliserende cyberaktiviteter?

Rapportens antagelser og fremgangsmåde

I anstrengelserne for at komme en dybere forståelse af cyberaktiviteters rolle og betydning nærmere anlægges her i rapporten et realistisk og rationalistisk blik. Cyberaktiviteter anskues i et magtperspektiv med særlig fokus på staten og dennes muligheder både for at udnytte cyberdomænets potentialer, men også for at skærme sig fra dem. Denne orientering mod staten er valgt, til trods for at netop cyberspace i særlig grad udfordrer vores opfattelse af, hvor magten er, hvem de relevante aktører er, og hvad statens nationale sikkerhed og interesser omfatter og vedrører. Cybermagt forstås ligeledes som en strategi anvendt bevidst af bestemte aktører i håbet om at opnå en ønsket effekt. Aktørerne og deres mål kan være vanskelige at få indsigt i, men det er ikke desto mindre magtprojektion i

1) Når præfikset cyber anvendes foran begreber som magt, kapabilitet eller angreb, angiver det "cyber-enabled activities" (White House, 2016), dvs. cyberbaserede aktiviteter, der udnytter det potentiale, som cyberspace giver, for at optimere effekten af handlinger, der i andre domæner kun vanskeligt kunne få tilsvarende konsekvenser eller virkning. Begrebet henviser altså til alle slags aktiviteter, lovlige som ulovlige, skjulte som åbenlyse, der benytter cyberspace.

klassisk forstand – hvor man søger at få andre til at gøre noget, de ellers ikke ville have gjort – der er genstand for analysen her.

Når cybermagt undersøges i en strategisk ramme, rettes blikket mod stater og deres bevidste anvendelse og opbygning af cyberkapabiliteter. Josef Nye påpeger, at der med skabelsen af cybermagt ikke bare sker en forskydning af magt fra et centrum til et andet, men i stedet en magtdiffusion, hvor staterne kommer i stærk konkurrence med andre aktører og får tiltagende svært ved at kontrollere egne samfund (Nye, The Future of Power, 2011, s. 114). Denne pointe er imidlertid ikke i modstrid med antagelserne i denne rapport. Magtdiffusion og det voksende antal aktører i cyberspace er netop de vilkår, der er udgangspunktet for at forstå staters adfærd i cyberspace. På samme vis taler Nyes magtbegreb direkte ind i de vanskeligheder, som staterne har, med at afværge den tiltagende destabilisering, trods akkumuleringen af cyberkapabiliteter overalt i det internationale system.

Når rapporten her sætter fokus på destabilisering som et mål i sig selv, er det særligt aktiviteter, der er under tærsklen for et væbnet angreb, som er interessante. De aktiviteter, som rapporten beskæftiger sig med, er derfor sjældent ulovlige og har ikke nødvendigvis fysiske konsekvenser. Man kan i stedet sige om aktiviteterne, at de er uvenlige. Derfor er den enkelte aktivitet hverken en trussel eller en fjendtlig handling, men samlet set er cyberaktiviteter mulighedsskabende for eksterne aktører, uden at det behøver at udvikle sig til en egentlig voldelig konflikt. Hvis vi anskuer interessekonflikter mellem stater som en permanent tilstand, hvor klassisk våbenmagt er en sekundær ressource, og hvor andre mere indirekte metoder er centrale for at opnå egne politiske mål (Tzu,S. 2010, s. 122,154, 127), bliver det nemmere at få øje på betydningen af cyberaktiviteter og motiverne bag en række forskellige og hver for sig ret betydningsløse hændelser.

Rapporten tager indledningsvis fat på at diskutere cybermagtens egenskaber. Magten karakteriseres først og fremmest som en spoilermagt, der indirekte, vedholdende og spredt kan nedbryde og undergrave vertikal og horisontal legitimitet i staterne. Herefter søger rapporten at afklare, hvorvidt cyberaktiviteter kan have mere vidtgående konsekvenser for relationerne mellem stater, ved at se på, om den tiltagende anvendelse af cybermagt fører til aktivering af sikkerhedsdilemmaet. Dette afklares ved at undersøge 1) forholdet mellem offensiven og defensiven i cyberspace, 2) en mulig eskalering af cybermagt fra spoilermagt til egentlig militær anvendelse samt 3) problemet med de skjulte cyberkapabiliteter, der vanskeliggør staternes indsigt i hinandens intentioner, motiver og muligheder.

Rapportens anden del diskuterer, hvilke strategier staterne kan tage i anvendelse for at forhindre den destabiliserende adfærd og det tiltagende våbenkapløb i cyberspace i at fortsætte ukontrolleret. Den peger på to forskellige typer af strategier, som understøtter hinanden i relation til cybermagt. Den ene strategi retter sig mod mere effektiv afskrækkelse og risikohåndtering. Den anden retter sig mod normskabelse og international regulering.

Cybermagt er spoilermagt

En dybere forståelse af cyberaktiviteters betydning kræver, at de ses i sammenhæng med staters øvrige strategier for at opnå deres politiske mål i fredstid så vel som under konflikt. Anvendelsen af cyberkapabiliteter udgør altså en *mulig* magt på linje med andre magtformer. Det særlige ved magt

i cyberspace er dog, at den kan påvirke alle andre domæner – land, sø, luft og rum – simultant eller udvalgte domæner, afhængig af hvilken effekt der søges opnået. Cyberkapabiliteteter muliggør herved øget magt i alle andre domæner og øger samtidig statens evne til at påvirke mange forskellige sektorer, private som offentlige. Den kan skabe effekter i hele staten: den finansielle sektor, sundhedsområdet, landbrugsproduktionen, transport og energi, telekommunikation, forsvaret osv.

Transformationen af cyberkapabiliteter til destabiliserende politiske mål kan beskrives som en strategisk proces, hvor "manging context for continuing advantage according to policy" er en fortløbende og aldrig afsluttet aktivitet (Sheldon, 2012, s. 208). Når "managing context" udgør den strategiske anvendelse af cyberaktiviteter, er det nemmere at forstå, hvordan destabilisering eller spoiling bliver et mål i sig selv, og hvorfor aktiviteterne sjældent når tærsklen for et væbnet angreb. Det kan skyldes, at den bedste strategiske anvendelse af cyberkapabiliteter *ikke* er at gøre det samme, som konventionelle våben kan med stor effekt og præcision, men at bruge cybermagt, der hvor den kan gøre det, andre virkemidler ikke kan – nemlig at skabe de rette præmisser for politisk forandring. Anvendelse af cybermagt til svækkelse af en stats horisontale eller vertikale legitimitet kan få effekter, der langt overstiger tidligere tiders informationsoperationer, spionagevirksomhed eller propaganda (Hansen, 2017:06, s. 10). "Skabelse af den rette præmis" eller "managing context" giver dog indtryk af et virkemiddel, der er mere effektivt, end det i virkeligheden er. Cyberaktiviteter har ofte en indirekte effekt. På trods af deres mulige ødelæggende og manipulerende funktion, selv i meget digitalt sårbare stater, har de endnu ikke virket tvingende i forhold til at ændre en konkret adfærd. Det klassiske eksempel er Estland 2007, hvor Estland, på trods af massive langvarige cybernedbrud kombineret med højlydte russiske protester, trusler og diplomati samt demonstrationer fra russiske mindretal i Estland, ikke lod sig tvinge til en bestemt handling – nemlig at lade et tidligere russisk krigsmonument blive stående i Tallinn (Sheldon, 2012, s. 214-215). Her var forholdene for påvirkning ellers særlig gunstige: Estland er meget sårbar over for uvenlige cyberaktiviteter grundet den høje grad af digitalisering af samfundet. Det er samtidig en småstat med stor afhængighed af russisk energi og med et stort russisk mindretal. I virkeligheden kunne man hævde, at de anvendte cyberaktiviteter fik den helt modsatte effekt end den tilstræbte. Estland fik nemlig efterfølgende NATO til at sætte fokus på cyberkapabiliteter og de baltiske landes generelt sårbare situation, og landet blev det sted, hvor alverdens folkeretseksperter samlede deres viden om cyber, folkeret og især humanitær folkeret i forbindelse med væbnede konflikter med udgivelsen af Tallinnmanualen (Schmitt, 2017) (Libicki, 2009, s. xv). NATO etablerede endvidere et Center of Excellence i Estland med fokus på bekæmpelse af cybertrusler. Her udvikles i dag nogle af de mest avancerede øvelser til bekæmpelse af cyberangreb. Det er desuden lykkes Estland at mobilisere befolkningen over for digitale trusler, og landet har således som det første land i verden oprettet et cyberhjemmeværn med både teknisk, juridisk, strategisk og organisatorisk ekspertise, som først og fremmest stilles til rådighed af eksperter, der arbejder i den private sektor i Estland.

Skabelsen af den rette præmis for videre politisk indflydelse betyder altså ikke, at man med cybermidler kan skabe en helt bestemt præmis, men det muliggør politisk forandring ved at bearbejde grupper, skabe usikkerhed i forskellige sektorer eller udstille samfundsmæssige svagheder både i de offentlige institutioner og blandt private aktører. Ud fra denne forståelse bliver det også klart, hvordan cyberaktiviteters mange divergerende mål og fremtrædelsesformer tilsammen kan være virkningsfulde: Cybermagt er altså først og fremmest en spoilermagt, der bryder ned, så andet kan

sættes i stedet. Dens primære funktion er at virke nedbrydende. Det peger også på et andet forhold ved cybermagt som et strategisk værktøj: at dens anvendelse nødvendigvis må være vedvarende – før, under og efter en eventuel konflikt. Det er et strategisk værktøj, der er med til at underminere grænserne mellem konflikt og fred (Libicki M. , 2017, s. 15).

Når vestlige demokratier planlægger strategier for cyber- og informationssikkerhed, er det derfor langt fra nok at tænke i sikring og monitorering af de sektorer, der vurderes at have en kritisk infrastruktur i forhold til statens vitale funktioner og sikkerhed. Det er også nødvendigt at forholde sig til andre destabiliserende cyberaktiviteter, herunder særligt i forhold til de institutioner, der er grundlaget for vores demokratiske system: partier og interesseorganisationer, valgprocedurer, sociale medier, klassiske medier, opinionsmålingsinstitutter mv. (Singer, 2017, s. 4) (Tikk-Ringas, 2015, s. 120). Obamaadministrationen nåede da også lige at sætte valgsystemer på listen over kritisk infrastruktur via Homeland Security Department for herved at tydeliggøre, at angreb herpå udgør "an unusual threat to the national security, foreign policy and economy of the United States" (Marks, 2017, s. 7).

Det er samtidig klart, at cybermagt kan anvendes til mere og andet end destabilisering. Det betyder, at de værktøjer, som udvikles i cyberspace til informationsindhentning og destabiliserende tiltag i fredstid, indeholder muligheder for eskalation. Cyberkapabiliteter udviklet alene til destabiliserende formål formår herved alligevel at øge sikkerhedsdilemmaet mellem stater. Og de selvsamme cyberkapabiliteter kan anvendes til at forsvare sig mod angreb, til selv at foretage efterretningsindhentning eller til offensive cyberoperationer som en del af statens militære kapabilitet (Gartzke & Lindsay, 2015, s. 325).

Cyberaktiviteter og betydningen af sikkerhedsdilemmaet mellem stater

I starten af 50'erne introducerede John H. Herz begrebet sikkerhedsdilemma som et grundvilkår i internationale relationer (Herz, 1950). Mange har tolket Herz på en sådan måde, at sikkerhedsdilemmaet i virkeligheden bliver et paradoks: Jo mere sikkerhed, der søges via magtakkumulation, jo mere får det andre til at søge samme magt, og det gør den første gruppering mere usikker, hvilket skaber et behov for endnu mere magtakkumulation – en negativ og irreversibel spiral. Ken Booth og Nicholas J. Wheeler mener imidlertid, at vi herved misser pointen med begrebet (Booth & Wheeler, 2008, s. 9). Det centrale ved dilemmaet er, at den grundlæggende usikkerhed i internationale forhold vedrører to forhold: vores fortolkning af modpartens intentioner og vores mulige respons. Dilemmaet ligger i, at vores tolkning af modpartens intentioner – lige meget om den er positiv eller negativ – kan vise sig at være forkert, og ligeledes vil vores respons være genstand for tilsvarende usikkerhed. Dilemmaet er en konsekvens af den grundlæggende dualisme i den menneskelige eksistens i relationen mellem frygt og afhængighed (Booth & Wheeler, 2008, s. 22). Sikkerhedsdilemmaet handler i virkeligheden om kommunikation mellem stater. Hvis en stat ønsker at udvise (vilje)styrke og troværdighed, risikerer den at blive opfattet som aggressiv og truende, hvis kommunikationen mislykkes. Og hvis den signalerer fredelige intentioner via tilbageholdenhed i oprustning, bliver den måske opfattet som svækket – en, der kan overvindes, eller hvis interessesfære er til forhandling. Det generelle spændingsniveau mellem de centrale internationale aktører er den afgørende faktor for, hvordan vi tolker andre staters adfærd, om et våbenkapløb er rationelt, og i hvor høj grad det vil stimulere et sikkerhedsdilemma (Glaser,

2004, s. 46,48). Når det kommer til cyberspace, er vilkårene for kommunikation via oprustning eller nedrustning imidlertid ganske anderledes end ved konventionel oprustning.

Ved at betragte cybermagt og dens unikke egenskaber peger denne rapport på tre elementer, der er afgørende for at komme nærmere en forståelse af udviklingen i sikkerhedsdilemmaet mellem stater på cyberområdet. Det første centrale element er den særlige "geografi", som cybermagt udfolder sig i. Det andet element er cybermagts potentiale til at eskalere fra at være en destabiliserende kraft til at være et effektivt middel i en konventionel krig mellem stater, der kan øge effekten af andre domæners virkemidler. Det tredje element er det mørklagte udviklingsniveau af cyberkapabiliteter samt muligheden for anonymitet – en væsentlig parameter for staters gensidige usikkerhed. I cyberspace er det særlig vanskeligt at identificere modpartens motiver, handlinger, styrker og muligheder. Samlet set er det rapportens pointe, at passende intention og respons i cyberspace er endnu mere vanskelig, end når det gælder det konventionelle område. De tre elementer diskuteres mere indgående nedenfor.

Geografi, cybermagt og sikkerhedsdilemmaet

Ifølge Robert Jervis (Jervis R. 1978, s. 194-199) er geografi en væsentlig parameter for, hvorvidt offensiven eller defensiven i forholdet mellem stater står stærkest, samt i hvor høj grad sikkerhedsdilemmaet aktiveres i forbindelse med oprustning. Jo større og mere besværlige afstande, der er mellem parterne, og jo større sårbarheden er i bevægelsen fra eget område til modstanderens, jo større fordel har defensiven. Når afstanden er stor, kan man tillige opbygge defensive kapabiliteter, have troppebevægelser og lignende uden at øge sikkerhedsdilemmaet, idet sådanne synlige forberedelser ikke samtidig kan tolkes som en styrkelse af ens offensive kapabiliteter. Store, observerbare afstande giver mulighed for, at forsvaret kan forberede sig, ligesom det øger modstanderens logistiske udfordringer. Afstandene vil i sig selv udgøre en væsentlig hindring for, at der opstår voldelig konflikt mellem parterne. Logikken er lige modsat for letindtagelige områder med korte geografiske afstande. Her er der øget risiko for konflikt: Det er langt lettere at provokere sikkerhedsdilemmaet. Og her belønnes overraskelsen. Det er klare fordele ved præventive angreb og offensiv tænkning i det hele taget. Denne opfattelse af betydningen af geografisk nærhed finder vi ikke kun hos realistiske tænkere, men også i teorien om regionale sikkerhedskomplekser. Barry Buzan slår således fast: "Because threats operate more potently over short distances security interactions with neighbours will tend to have first priority. Seen from the top down, security complexes are generated by the interaction of anarchy and geography" (Buzan, 1991, s. 191). Geografisk nærhed er altså central for tænkning om trusler, og hvordan de fortolkes og besvares.

Geografisk nærhed er særlig relevant, hvad angår beskyttelsen af eget territorium. Centrale interessekonflikter mellem stormagter er dog sjældent alene forbundet med territorium og befolkning, men i høj grad knyttet til områder, der ikke tilhører nogle af parterne, men hvor der er modstridende interesser. Herved udvides zonen, hvor et sikkerhedsdilemma kan opstå, samt den rolle, geografi spiller i det konkrete eksempel. Fortolkning af intention og respons kommer i de situationer til at gælde langt bredere og vedrøre alle zoner for indflydelse og indblanding.

Hvordan kan disse to teoretiske pointer knytte an til cybermagt, som den forstås i denne rapport? For det første hævdes det, at det centrale mål med cybermagt er destabilisering. Det betyder, at det

område, der er under påvirkning, er staten og alle de elementer, der udgør et samfunds sammenhængskraft. For det andet handler det om at influere befolkningen og dennes opfattelse af statsmagten, dens værdier og institutioner som legitime og troværdige. For det tredje er geografi forstået som afstand ikke meningsfuldt i cyberspace. Det rette digitale "våben" kan nå sit mål uden tidsmæssige forhindringer, uden hensyn til afstande og oftest uden logistik. En række af de muligheder, der findes, for påvirkning i cyberspace er nok problematiske, men langt fra noget, man aktivt kan opsætte værn imod. Det gælder trolling, informationspåvirkning via blogs, betalte chattere, propaganda via falske nyheder, manipulation og fordrejninger af data mv. Andre anvendelser af cybermagt til f.eks. at spionere eller hacke sig ind i private eller offentlige institutioner kan man bedre styrke sit cyberforsvar imod. Her gælder imidlertid det forhold, i relation til sikkerhedsdilemmaet, at vi ikke kan "se modstanderen på vej mod angrebet." Udvikling af kapabiliteter, mobilisering af personer til deployering, logistiske tilpasninger, anskaffelse af materiel – alle disse forhold giver i den fysiske verden tid til at forberede et forsvar samt mulighed for at mobilisere, igangsætte politiske forhandlinger, aktivere støtte fra allierede mv. I cyberspace er der ikke forskel på nærhed og distance – her er truslen fra naboer ikke større, mere potent regionalt. I cyberspace befinder stormagter og småstater sig på den samme globale spilleplade. Her er ingen nære trusler at give primat eller førsteprioritet.

Hvis vi skal søge at inddrage ovenstående forståelse af cybermagts påvirkning af sikkerhedsdilemmaet, foregår cyberaktiviteter i et rum, hvor geografiske grænser er letindtagelige. Den offensive kapabilitet nyder fordelene ved usynlig forberedelse og muligheden for at bevæge sig uden tid i det digitale landskab. Vi må derfor forvente, at cybermagt skaber øget tvivl om både de andres intentioner, og hvilken respons der er passende. Samlet set betyder det en klar provokation af sikkerhedsdilemmaet. Cyberkapabiliteternes særlige karakter ansporer til præventiv frem for afventende adfærd. Når vi ikke kan aflæse en potentiel modstanders adfærd og er usikre på dennes intentioner, må vi forberede os på det værste og eventuelt foregribe en mulig handling (Glaser, 2004, s. 48). Anarkiets dynamik står så meget desto stærkere, når tid og rum opløses. På basis af denne logik er potentialet for konflikt overhængende. Sikkerhedsdilemmaet vedrører samtidig meget mere end de militære magtmidler. Det er relevant i relation til alle samfundets sektorer og på alle områder, der kan udfordre statens stabilitet, integritet, suverænitet og vitale interesser. Selv hvis ovenstående analyse skulle være forfejlet, er alene forestillingen om, at det er offensiven, der har fordelen, med til at drive våbenkapløbet i cyberspace frem (Slayton, 2017, s. 72). Af samme grund ses udviklingen af cyberkapabiliteter at være karakteriseret af eksponentiel vækst blandt alle verdens (stor)magter. Den daglige intensivering af uvenlige aktiviteter i cyberspace er et klart tegn på domænets tiltagende betydning, ikke mindst for opfattelsen af trusselsniveauet mellem stater.

Samtidig er det afgørende at diskutere, om sikkerhedsdilemmaet kan anvendes, når vi ser på cybermagt som spoilermagt. Kan overvejelser om gensidig militæroprustning flyttes ud af kontekst og ind i et perspektiv, der handler om holdningspåvirkning af en befolkning? Giver det mening at slutte, at vi vil se et øget konfliktpotentiale mellem stater baseret på et virkemiddel, der mest af alt handler om at skabe præmisser for politisk forandring i en stat, før eller helt uden at voldelig konflikt er en del af kabalen? En af grundene til, at det faktisk giver mening, er, at cybermagt – selvom den nuværende strategiske anvendelse er destabilisering – har potentiale til at skabe stor effekt, i det øjeblik en konflikt eskalerer. Sikkerhedsdilemmaets relevans i cyberspace er derfor afhængig af den mulige eskalering fra ikkevoldelige destabiliseringstiltag til klar militær anvendelse af cyberkapabiliteter.

En sådan eskalering er mest relevant for stater og mindre for de ikkestatslige aktører, der nok kan "spoile" via cyberbaserede aktiviteter, men som ikke kan drive det videre og udfordre den grundlæggende magtbalance mellem stater. Magtens diffusion, som Nye pegede på, får nok "temperaturen til at stige" i det internationale samfund med øget uforudsigelighed og destabilisering til følge, men det ændrer ikke ved staternes fortsatte centrale betydning i internationale relationer.

Cybermagt, eskalationspotentiale og sikkerhedsdilemmaet

Et centralt spørgsmål er altså, om cybermagt har eskalationspotentiale. Som påpeget tidligere er destabilisering mulighedsskabende for en videre politisk udvikling, men det kan også føre til intensivering og udløsning af andre mekanismer, når det gunstige øjeblik opstår. Derfor kan cybermagt, forstået som evnen til at skabe destabilisering via tiltag i cyberspace, ikke bare isoleres og defineres som en proces, der foregår under tærsklen til voldelig konflikt; cybermagt kan ligeledes have "spillover" effekter til militære operationer og herved mere direkte betydning for sikkerhedsdilemmaet. Allerede i 1998 skrev den russiske udenrigsminister til FN's generalsekretær med en bekymring om, at udviklingen i det, han kaldte "informationsvåben", kunne undergrave den internationale stabilitet og sikkerhed gennem nedbrydning af principper om magtanvendelsesforbuddet, ikkeindblanding i staters interne affærer samt respekt for menneskerettigheder og frihed (Tikk-Ringas, 2015, s. 117). Rusland fremlagde et udkast til en resolution med følgende ordlyd:

Advisability of developing international legal regimes to prohibit the development, production or use of particularly dangerous forms of information weapons, and of taking measures to combat information terrorism and crime, including the establishment of an international system (centre) for monitoring threats to the security of global information and telecommunications systems. (UN Disarmament Committee, 1998)

Det har altså længe været en almindelig opfattelse, at udviklingen i informationsteknologi har potentiale til at skabe generel destabilisering, men også til at eskalere til de mest farlige og ødelæggende operationer.

Når vi skal undersøge, hvordan og i hvilken udstrækning cybermagt og udviklingen af denne kan påvirke sikkerhedsdilemmaet mellem stater, er det nødvendigt at anskue cybermagt fra en ny vinkel. Det er ikke nok at se på, hvad magten kan anvendes til at opnå og med hvilken effekt. Det er heller ikke tilstrækkeligt at se på dens unikke karakter eller evne til at influere alle sektorer og domæner på forskellig vis. Nej, vi må også søge at beskrive de dimensioner, en oprustning i cyberspace baserer sig på. Gregory Rattray har foreslået fire fælles dimensioner til at forstå styrkeforholdet mellem domænerne land, sø, luft, rum og cyberspace:

a. Teknologisk udvikling og forspring
b. Evne til hastighed og mængde af operationstyper
c. Kontrol over områder
d. National mobilisering (Langø, 2016, s. 19)

Ændringer i styrkeforholdet mellem stater kan altså læses af fortolkninger af udviklingen af kapabiliteterne inden for disse forskellige dimensioner.

Teknologisk forspring og udvikling skal her forstås som digitalisering og opkobling af hele samfundet og som udvikling af nye teknologier til militær og ikkemilitær anvendelse.

Hastighed knytter sig til automatisering af instrumenter i cyberspace og øget forbundenhed, mens mængden af operationstyper knytter sig til cyberinstrumenternes mulige succesfulde integration i forskellige operationer, defensive som offensive.

Kontrol i cyberspace vedrører både kontrol over den fysiske infrastruktur og evnen til at øve indflydelse og kontrol over samfundets mange sektorer og tilknyttede ikkestatslige aktører, der kan angribes via cyberdomænet, men som også kan anvendes aktivt i en operation rettet mod andre.

Det sidste område er national mobilisering, hvor det er afgørende for styrkeforholdet på cyberområdet, hvorvidt staten systematisk kan udnytte ekspertise fra den private sektor, og hvor statens evne til at kombinere økonomisk, militær og diplomatisk magt i en samlet "whole of nation approach" rettet mod bestemte mål vurderes.

Cybermagt er altså meget mere end skræddersyede våben og aktiviteter til anvendelse i cyberspace. Stærke enkeltstående våben, der kan udvikles af ikkestatslige aktører eller få tekniske eksperter, og som kan holdes skjult for omverdenen frem til deres anvendelsestidspunkt, er altså ikke det, der udgør en stats cyberkapabilitet. Selv om den konkrete udvikling af tekniske metoder til frembringelsen af "våbensystemer" i cyberspace er mørklagt, kan en monitorering af kapabilitetsudviklingen inden for de fire dimensioner, der er præsenteret her, give et godt billede af de kapabiliteter, en stat eller ikkestatslig aktør ligger inde med. Herved kan analyser afsløre aktørens muligheder for eskalation inden for cyberdomænet samt for at agere mere og andet end spoilermagt.

Udviklingen af cyberkapabiliteter kan øge sikkerhedsdilemmaet, fordi det er så vanskeligt at forbedre sit forsvar i cyberspace, uden at det giver anledning til en negativ fortolkning af egne, men også af en modstanders fremtidige intentioner og mulige respons i en konfliktsituation. For at udvikle cybervåben må man udpege og undersøge fjendtlige netværk i fredstid. Udpegning af og informationsindhentning fra eventuelle fremtidige fjender er altid politisk sprængfarligt – hvis altså aktiviteterne opdages (Jacobsen, 2016) (Buchanan, 2016, s. 23). I et realistisk perspektiv er det vanskeligt at forestille sig, hvorvidt det er muligt at overbevise eventuelle modstandere om ens motiver. Der er en klar sammenhæng mellem udvikling af de fire dimensioner af kapabiliteter til cyberforsvar nævnt ovenfor og den mulige offensive anvendelse af samme (Slayton, 2017, s. 73). Styrkelsen af eget cyberforsvar involverer egentlig organisatorisk integration af offensive cyberkapabiliteter, og det betyder intensivering af sikkerhedsdilemmaet, selv om det ikke er tiltænkt (Smeets, 2017, s. 27).

Endnu et forhold er værd at tage med i overvejelserne om en mulig eskalation: den manglende udvikling af diplomatiske normer i cyberspace. En hændelse i cyberspace er i dag underlagt en langt mere "tilfældig" fortolkning, end hvis samme handling fandt sted i den fysiske verden. Normdannelsen eller den intersubjektive forståelse af, hvornår noget er tyveri, spionage, manipulation, sabotage eller endda et væbnet angreb, er i sin vorden internationalt. Denne usikkerhed fører til, at handlinger, der i dag tillades i cyberspace, er sjældne eller yderst problematiske uden for cyberspace og normalt bliver mødt med klare sanktioner. Hvis der ikke er et match mellem, hvad forskellige stater finder, er

uacceptabelt eller ligefrem kan tolkes som angrebshandlinger som en del af en international konflikt, øges muligheden for overraskende modsvar eller eskalering betydeligt (Andres, 2012, s. 95).

Cybermagt, den mørklagte kapabilitetsudvikling og sikkerhedsdilemmaet

For private virksomheder, nationale myndigheder og sikkerhedsindustrien er fordelene ved at hemmeligholde forhold i cyberdomænet overvældende. Det handler om konkrete indbrud, mulige sikkerhedsforanstaltninger, evnen til at opdage brud og deres ophav. Desuden er efterretningstjenesternes egne muligheder for spionage enormt store og profitable, og deres interesse i at dele viden om cyberhændelser med andre minimal (Andres, 2012, s. 93). I cyberspace vinder den intervenerende handling derfor af mindst tre grunde:

1. Efterretningers værdi er meget stor i forhold til risikoen for at blive opdaget/modsvaret.
2. Et effektivt forsvar i cyberspace nødvendiggør, at staten kan intervenere i modstanderens systemer.
3. Våbensystemer i cyberspace kan plantes, før en eventuel konflikt opstår, og det kan blive relevant at udløse dem.

Defensive tiltag i cyberspace kan derfor meget let tolkes som en optrapning, idet det er ganske vanskeligt at signalere den rette intention, når man søger at gøre noget ubemærket og uset, omend hensigten er defensiv (Hennessey, 2017, s. 45). Det gør overgang mellem freds- og krigstid mere glidende end under klassiske konventionelle konflikter (Andres, 2012, s. 94-95) (Slayton, 2017, s. 87). Denne dimension ved cyberkapabiliteterne er med til at understøtte en tendens, vi så i ovenstående undersøgelse af geografiens betydning og cybermagts potentiale for eskalation til andre domæner samt til anvendelse i sammenhæng med egentlige militære operationer. Når dette kombineres med den manglende normdannelse for fortolkning af adfærd i cyberspace og den brede palet af aktører og sektorer, der optræder i cyberspace, øges usikkerheden blandt staterne markant.

Hvis stabilitet og en gennemskuelig magtbalance mellem stater er den tilstand, der er mest eftertragtelsesværdig i internationale relationer, står vi over for noget af en udfordring. Rapporten her peger på en række forhold ved cybermagt, der trækker i den helt modsatte retning. Opsummeret betyder det:

- Cybermagt er effektiv som et strategisk værktøj til at skabe ustabilitet på alle tænkelige niveauer i staten og bryder hermed statens integritet og suverænitet effektfuldt. Cybermagt er en stærk spoiler.
- Cybermagt er langsom i sin tilblivelse, men kan aktiveres uden forvarsel og implementeres uafhængig af logistisk eller synlig mobilisering og kan kun delvist og vanskeligt afværges.
- Cybermagt er effektiv til destabilisering i fredstid, men kan ligeledes anvendes og implementeres i militære operationer og er herved et klart offensivt instrument med stort eskalationspotentiale.
- Cybermagts store værdi i forbindelse med efterretningsindhentning, de manglende internationale normer om dens anvendelse samt cyberkapabiliteters ret usynlige udvikling gør accelerationen af våbenkapløbet vanskelig at be- og afgrænse.

Alle disse forhold peger frem mod den rationelle konsekvens, at staterne bør opruste massivt på cyberområdet (Glaser, 2004, s. 47,48),[2] at offensive handlinger betaler sig, og at sikkerhedsdilemmaet, trods den umiddelbare ikkemilitære anvendelse af instrumenterne, i høj grad er aktiveret. Det interessante spørgsmål er derfor: Kan man gøre noget for at forhindre, at spoileradfærd eskalerer til international konflikt, og kan man hæmme det tiltagende våbenkapløb?

Der synes at være mindst to veje at gå, begge ufuldkomne i håndteringen af cybertrusler – men i forening og samtidigt måske den rette medicin til at hæmme både våbenkapløbet og destabiliseringen. Den ene metode handler om afskrækkelse og risikohåndtering i bredeste forstand, den anden om dialog, normopbygning og fælles regulering af cyberspace til fælles gavn og forudsigelighed. Begge metoder handler om klar kommunikation om grænser og konsekvenser for adfærd i cyberspace (Hennessey, 2017, s. 40).

Afskrækkelse, risikohåndtering og international normdannelse om adfærd i cyberspace

Skal våbenkapløbet i cyberspace tæmmes, og spoileradfærden begrænses, er det afgørende, at staterne udvikler nogle brugbare strategier. Cybermagtens anderledes virkemåde, hvis væsentligste dynamikker, rapporten har diskuteret, betyder, at gængse strategier til at begrænse konfliktopbyggende adfærd må omtænkes og tilpasses det nye domæne. Det er ikke en simpel manøvre at omstille sig til at kommunikere og respondere på aktiviteter i cyberspace på en måde, der fremmer gennemskuelighed og troværdighed over for andre aktører. Hvordan kommunikerer man grænser for acceptabel adfærd og passende konsekvenser i cyberspace? Hennessey peger på fire forhold, som er vanskelige, men nødvendige at kommunikere i cyberspace, hvis målet er at mindske sikkerhedsdilemmaet og fremme forudsigelighed og klare intentioner.

For det første skal der ske en offentlig og overbevisende attribution af hændelser til en bestemt aktør. For det andet skal der tilstræbes klar kommunikation om tærskler for acceptabel og ikke acceptabel adfærd i cyberspace. Denne kommunikation skal bakkes op af forventningen om troværdig og proportional respons. Og sidst men ikke mindst er det nødvendigt at overbevise omverdenen om, at man besidder passende kapacitet til at respondere (Hennessey, 2017, s. 40).

Det er først i de senere år, at man har set en udvikling, der søger at leve op til disse fire anbefalinger. Hvis man tager indblandingen i valget i USA i 2016 som en konkret case, er der flere ting, som springer i øjnene. USA var meget sen til at drage nogen til ansvar for indblandingen i valget og afholdt sig fra at fremlægge klar og utvetydig dokumentation for sine anklager mod Rusland. Så sent som i 2015 opdaterede USA sin cyberafskrækkelsespolitik. Den nye politik fra 2015 havde imidlertid fortsat meget snævret definerede tærskler for adfærd i cyberspace, hvor modsvar eller gengældelse kan forventes. Dette gjaldt trusler mod menneskeliv, kritisk infrastruktur, økonomisk sikkerhed og

2) Glaser (2004) peger på en række rationelle grunde for stater til at indgå i et våbenkapløb, der efter hans vurdering faktisk kan være med til at undgå voldelig konflikt mellem stater, selv om sikkerhedsdilemmaet aktiveres i processen: a) hvis internationale forhold nødvendiggør militær konkurrence, b) ved skifte i offensiv/defensiv-balancen mod offensiven, c) usikkerhed omkring modstanderens motiver og intentioner, d) hvis en stat med aftagende magt kan opruste og herved opnå fordele og muliggøre præventive tiltag, e) teknologisk udvikling, der nødvendiggør tilegnelsen af nye våben for ikke at svække magtbalancen. Alle disse delelementer er til stede i udpræget grad i den internationale udvikling på cyberområdet, der er opregnet i ovenstående kapitel, og det forklarer derfor ganske godt våbenkapløbets dynamikker i dette nye domæne.

militær kommandokontrol, mens angreb på centrale amerikanske værdier som ytringsfrihed og andre væsentlige grundlag for det liberale demokrati ikke var inddraget. Herudover har det været ganske usikkert, hvordan eller hvor voldsomt USA vil modsvare uacceptabel adfærd. Det har i lang tid været en pointe i sig selv, at USA har signaleret tvetydighed og usikkerhed om forventede modsvar ved hacking: "[R]esponse would be proportional, perhaps not visible and at a time and place of its choosing" (Hennessey, 2017, s. 44). Selv efter indblandingen i de amerikanske valghandlinger var den officielle respons ret afdæmpet med udvisning af diplomater, begrænsede økonomiske sanktioner og lukning af to russiske matrikler i USA.

En anderledes tilgang, hvor man mere tydeligt tør lægge beviser frem, være mere klar i forhold til acceptabel adfærd og reagere på en mere forudsigelig og proportional måde, vil styrke afskrækkelsesmomentet, fremme en klar normdannelse samt gøre risikoen ved uvenlig cyberadfærd mere åbenbar (Libicki M. , 2017, s. 16-17). Det indebærer imidlertid også en række risici, som staterne indtil nu har værget sig imod, herunder især at ingen ønsker at fremsætte røde linjer, der skal give bestemte svar – slet ikke når vi bevæger os i den grå zone under tærsklen for væbnede angreb og måske også under grænsen for ulovlig magtanvendelse.

En mindre ambitiøs og også mindre risikabel strategisk tilgang er derfor at arbejde parallelt med to mulige måder at håndtere uvenlige cyberaktiviteter i fremtiden: afskrækkelse af de værste/farligste aktiviteter, risikohåndtering i forhold til de øvrige samt et parallelt spor, der sætter dialog, normdannelse og regulering af cyberadfærd og anvendelse af cybermagt på dagsordenen.

Afskrækkelse

Begrebet afskrækkelse knytter sig traditionelt til en snæver sikkerhedsopfattelse, hvor militære trusler mod statens eksistens søges effektivt afværget. I en meget snæver forstand knytter afskrækkelse sig til en trussel om gengæld med anvendelse af militær magt. Skal afskrækkelse virke, må modstanderen være overbevist om, at der både er vilje og evne til at sætte gengældelsen i værk, hvis det viser sig nødvendigt (Art, 1980, Vol. 4, Issue 4, s. 6). Trusler identificeres ud fra en analyse, der fokuserer på mulige fjendtlige aktører, disses militære kapabiliteter og vilje til at angribe samt mulige motiver. Afskrækkelse kræver normalt opbygning af kapabiliteter alene eller i en alliance, der får en potentiel modstander til at opgive på forhånd, fordi den forventede modstand bliver for voldsom, eller den efterfølgende straf for stor. Nogle sætter lighedstegn mellem effektiv afskrækkelse og total prævention. Det giver imidlertid ikke mening i cyberspace (Nye, 2017, s. 45). Med udgangspunkt i Snyders definition på afskrækkelse – "dissuading others by a threat of sanction or promise of reward" – skal vi ifølge Nye ikke alene tænke afskrækkelse som knyttet til anvendelsen af militær magt. Afskrækkelse kan også ske ved appel til den andens moral eller, måske mere realistisk, dennes frygt for tab af moralsk anseelse og legitimitet blandt allierede i det internationale samfund generelt eller i egen befolkning (Nye, 2017, s. 52). Nye peger på en række tiltag, der kan være med til at understøtte afskrækkelse i cyberspace, især hvor succeskriteriet ikke er fuldt stop, men at nedbringe og vanskeliggøre cyberangreb ved at øge omkostningerne samt nedbringe mængden af fordelene.

Som det fremgår af USA's internationale strategi for cyberspace, kan et modsvar komme fra et hvilket som helst våben efter eget ønske og begrænser sig derfor ikke til de kapabiliteter, der er til rådighed i cyberdomænet:

We reserve the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. (White House, 2011, s. 14)

Yderligere konkluderer USA's Defense Science Board, at "nuclear weapons remain the ultimate response and anchor of the deterrence ladder" (Nye, 2017, s. 55).

Opstår der en situation, hvor vi bevæger os mod voldelig konflikt med udgangspunkt i aktiviteter, der startede i cyberspace, er det bedre at afskrække med konventionelle eller sågar nukleare kapabiliteter, også over for voldelige angreb involverende cyberspace, fremfor at svare igen i samme domæne eller at anvende en cyberkapabilitet, der alene kan afskrække andre fra angreb (Libicki M. , 2017, s. 17) (Nye, 2017, s. 55,63).

Selv om afskrækkelse i cyberspace i en vis udstrækning lader sig gøre, er det særlig vanskeligt, når vi taler om aktiviteter, der retter sig mod destabilisering. Disse tiltag er netop ikke karakteriseret ved angreb, men kan oftest karakteriseres som uvenlige handlinger begået af en skøn blanding af aktører med forskellige mere eller mindre koordinerede formål og planer. Når det vedrører handlinger under tærsklen for angreb, er afskrækkelsesstrategier langt mindre virkningsfulde (Nye, 2017, s. 63). Her kan det rette redskab være en supplerende strategi med fokus på risikohåndtering.

Risikohåndtering

Anskuer vi cyberspace som et unikt domæne med andre muligheder og relationer end de andre domæner, afskrækkelse normalt tænkes i, giver det måske god mening at overveje at supplere afskrækkelsesbegrebet med en anden tilgang, særligt når vi sætter fokus på de aktiviteter, der ligger under tærsklen for magtanvendelse. Karsten Friis og Erik Reichborn-Kjennerud slår i en artikel fra 2016 til lyd for, at trusselsbegrebet erstattes med risici, og afskrækkelse på den baggrund suppleres med risikohåndtering (Friis & Reichborn-Kjennerud, 2016). Som den første del af denne artikel også pegede på, er cyberdomænet velegnet til aktiviteter, der handler om at indhente information og påvirke hele spektret af statens funktionsmåder samt relationer i civilsamfundet eller i det private erhvervsliv. Destabilisering er en vedvarende strategi, som en myriade af aktører bidrager til på alle niveauer og med skiftende intensitet, kompetence og formål. Selv om det er muligt at pege på de mest avancerede cyberspaceaktører og opnå en dybere forståelse af deres motiver, vilje og evner, er det langt fra en tilfredsstillende måde at forholde sig til alle uvenlige aktiviteter i cyberspace. Desuden har det i sig selv en eskalerende effekt at tale om myriaden af cyberhændelser ud fra en trusselsterminologi (Macák, 2017, s. 140). I stedet opfordrer Friis og Reichbourn-Kjennerud til, at vi betragter cyberspace som et risikofyldt domæne, hvor det centrale er at sætte fokus på egne sårbarheder, afhængighed og resiliens og fremfor afskrækkelsestrategier at arbejde med "governance of risks" (Friis & Reichborn-Kjennerud, 2016, s. 40). Denne tankegang retter sig særligt mod håndtering af cyberbaserede aktiviteter i fredstid.

I de situationer, hvor vi befinder os under tærsklen for et væbnet angreb, vil vi derfor se klassiske afskrækkelsesstrategier brugt i kombination med værktøjer til risikohåndtering. Kan dette så ske uden at aktivere sikkerhedsdilemmaet? Det overraskende svar er i mange tilfælde: ja. Og det er der flere grunde til (Cooper, 2012, s. 112-116). Det gælder først og fremmest om at have fokus på resiliens og minimering af "risks by denial": Det centrale er her at gøre det langt mindre attraktivt for angriberen at forsøge en infiltration. Resiliens og minimering af fordele ved indtrængning er virkningsfuldt over for kendte grupperinger, men virker også på andre ukendte aktører (Nye, 2017, s. 56). Det handler tillige om at øge omkostningerne ved en adfærd, der har til formål at udnytte det digitale netværk, og det kan gøres ved hjælp af en bred vifte af tiltag (Singer, 2017, s. 3). Afgørende for effektiv minimering af risici er, at man søger at mindske den værdi, en potentiel modstander forventer at opnå ved en succesfuld cyberaktivitet. Det gøres for eksempel ved at sprede oplysninger om de anvendte metoder eller udvikle effektive backupmekanismer til at håndtere nedbrud eller overbelastning af nettet. Tilsvarende og parallelt med, at man mindsker værdien ved en uvenlig cyberaktivitet, skal det gøres mere usikkert, om handlingen overhovedet vil lykkes. Altså skal sandsynligheden for, at aktionen vil virke, svækkes. Det stiller modstanderen over for to negative forhold i dennes samlede analyse af, om det kan betale sig at afprøve en uvenlig cyberaktivitet. Ved succes er udbyttet kvalitetsmæssigt begrænset, ligesom muligheden for overhovedet at opnå et udbytte er faldende. Samlet set virker disse tiltag mod uvenlige cyberbaserede aktiviteter, uden at det på nogen måde påvirker forholdet mellem aktørerne, og uden at sikkerhedsdilemmaet øges (Cooper, 2012, s. 109). Konkret kan der peges på en række væsentlige tiltag såsom systematisk patruljering af egne kritiske netværk i samarbejde med private virksomheder, civilsamfund og lignende. Her er støtte til opbygningen af internationale kapabiliteter i efterforskningsarbejdet samt til deling af informationer om kendte metoder til indtrængning og forhindring heraf helt afgørende i kampen mod destabiliserende tiltag (Nye, 2017, s. 62) (Hohmann, Pirang, & Benner, 2017). EU er kommet langt i arbejdet med at udarbejde fælles standarder for sikkerhed og databeskyttelse, sektorspecifikke krav og krav om gennemskuelig organisation til håndteringen af sikkerhedsbrud med overraskende hurtig implementering i medlemslandene af det såkaldte NIS-direktiv fra 2016 (twobirds.com, 2018) (EU 2016/1148).

Ovenstående forskellige tiltag kommunikerer ikke grænser og konsekvenser med den klarhed, Hennessely anbefaler. De giver en forventning om øgede og stigende omkostninger ved at gennemføre et eventuelt angreb samt faldende forventede fordele eller effekt i det system, der er under angreb. Samarbejde om efterretningsarbejde, styrket modstandsdygtighed i kritisk infrastruktur, forøgelse af det generelle forsvar i cyberspace og tydelig kommunikation om muligheder for gensvar via andre midler end cyberkapabiliteter giver et godt billede af de problemer, en potentiel aktør står til at møde. Den anden del af ligningen handler om kommunikation om grænser for adfærd. Her er *naming* and *shaming* én vej at gå. En anden er proaktivt at opbygge internationale normer for og regulering af adfærd i cyberspace.

Dialog om normer og regulering i cyberspace

Normudvikling og tydeliggørelse af acceptabel og ikkeacceptabel adfærd kræver en ændring i den politiske reaktion på uvenlige handlinger i cyberspace. Handlinger skal aktivt fordømmes og besvares. Stater skal opfylde deres pligter vedrørende kontrol under deres jurisdiktion – også i cyberspace (Cooper, 2012, s. 115). Normudvikling nationalt og internationalt via øget intolerance, højere straffe

ved ulovlige handlinger samt retsforfølgelse til skræk og advarsel er en god vej at gå. Med et skifte fra orientering mod trusler og afskrækkelse til fordel for sårbarhed og risikohåndtering dykker vi ned i den liberale værktøjskasse for at mindske sikkerhedsdilemmaet mellem stater. En mere tydelig og kontinuerlig statspraksis med bestemte sanktioner knyttet til bestemt adfærd vil give bedre forudsætninger for at tolke adfærd i cyberspace – både hvad angår motiver og respons, de to elementer i sikkerhedsdilemmaet, som Herz oprindelig pegede på. Det vil skabe noget af den forudsigelighed, der i dag efterspørges i cyberspace, og som giver et forfejlet indtryk af "Det Vilde Vesten". EU er faktisk gået foran på dette område og har ud over NIS-direktivet udviklet en Cyber Diplomacy Toolbox, der netop skal kommunikere øgede omkostninger ved anvendelse af uvenlige cyberaktiviterer og herved øge mulighederne for afskrækkelse via forudsigelige, konsekvente modsvar:

The EU stresses that clearly signaling the likely consequences of a joint EU diplomatic response to such malicious cyber activities influences the behavior of potential aggressors in cyberspace thus reinforcing the security of the EU and its Member States. (Council of the European Union, 9916/17, s. 5)

I 2003 reflekterede Herz selv over betydningen af sikkerhedsdilemmaet i dag, og hvilke muligheder der findes for at begrænse eller "tæmme" det:

Half a century ago I looked for an approach to overcome the extremes of power politics by an attitude I called "realistic liberalism"… I knew it would be difficult in a system of international anarchy. But what can be done shows in the surprising success of European nations. Still sovereign and independent, the members of the European Union have reached a stage of trust and collaboration where war between any of them has become unthinkable. There too, awareness of the dual threat to human survival, the nuclear and the ecological one, has led to increased willingness to make economic sacrifices and even changes in lifestyles needed to avoid mortal dangers to human survival. (Herz, 2003, s. 416)

Omend mange nok i dag ville pege på de åbenbare svagheder ved det europæiske projekt, kan citatet ovenfor alligevel bruges som afsæt til at overveje en række forhold, der er centrale for en analyse af udviklingen i cyberdomænet og betydningen af sikkerhedsdilemmaet mellem stater. Skal man overvinde magtpolitikkens logik, kræver det altså ifølge Herz en nødvendighed i form af en sikkerhedstrussel. Denne overvindelse skal ske via et villet, tillidsfuldt, forpligtende, kontinuerligt samarbejde. Spørgsmålet er, om destabilisering forårsaget af aktiviteter under tærsklen for væbnet angreb, diffuse, vedvarende og spredt ud på mange sektorer, udført af utallige forskelligartede aktører, skaber en "brændende platform" for sådanne samarbejder? Er destabiliserende cyberaktiviteter egentlige sikkerhedstrusler? Kan de sidestilles med essentielle trusler som atomkrig eller et økologisk sammenbrud? Og hvis ikke, hvordan aktiveres så de liberale virkemidler i værktøjskassen, international normdannelse, tillidsskabende mekanismer, institutionelt samarbejde og folkeretlig regulering, som kan være med til at afbøde virkningerne af den accelererende udviklingen i cyberdomænet på sikkerhedsdilemmaet mellem stater?

Det har vist sig langt vanskeligere, end man kunne forestille sig, at etablere fælles internationale normer for cyberaktiviteter. En af de væsentligste problemstillinger vedrører de forskellige værdier og mål, der adskiller vestlige og ikkevestlige stater, når det gælder kontrol med og overvågning af information. Med Rusland og Kina i spidsen har de ikkevestlige stater i ganske lang tid arbejdet på at

udforme nogle særlige traktater til regulering af cyberområdet eller nærmere bestemt området for informationsudvikling. Samtidig har USA og mange af de øvrige vestlige stater fastholdt, at cyberspace udmærket lader sig regulere via gældende internationale regler og principper (Tikk-Ringas, 2015, s. 119-125) (Schmitt, 2017) (Jacobsen, Danmark bør undgå en "digital Genèvekonvention" - En prioritering af Danmarks cyberpolitik, 2017, s. 8-11). Over tid er der via debatter særligt i fora som UN Group of Governmental Experts (GGE) og UN Disarmament Committee sket tilnærmelser mellem de to yderpunkter, og i dag synes der at være enighed om, at principperne for staters suverænitet, lighed og ret til ikkeindblanding i interne anliggender også gælder i cyberspace. Uenigheder skal løses med fredelige midler, og international ret og den humanitære folkeret kan anvendes på cyberområdet. Her finder også de bærende principper som humanitet, nødvendighed, proportionalitet og distinktion anvendelse (Tikk-Ringas, 2015, s. 124,125). Da det på mange måder er umuligt at indgå aftaler om våbenkontrol eller nedrustning i cyberdomænet, er det afgørende, at cyberinstrumenter ikke tages i anvendelse mod ulovlige mål. Dette er reguleret i den humanitære folkeret, men skal efter USA's mening ligeledes gælde i fredstid, hvor den humanitære folkeret ellers ikke finder anvendelse (Nye, 2017, s. 61). Herudover er der et stærkt fælles ønske om at udvikle politisk bindende normer for acceptabel statsadfærd i cyberspace. Blandt andet Rusland tilslutter sig denne mulighed, når nu det ikke er muligt at indgå en særlig traktat på området.

Norms reflect the international community´s expectations, set standards for responsible State behavior, and allow the international community to assess the activities and intensions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development (The 2015 repport of the Group of Governmental Experts, 2015).

Citatet her afslører flere interessante forhold ved regulering af cyberspace. For det første er der enighed om, at manglende regulering af området skaber usikkerhed og er en udfordring for international fred og sikkerhed, samt at det er med til at hæmme både sikkerheden generelt og den mulige realisering af teknologiens potentialer. Hvilke normer der så skal gælde i cyberspace, er det vanskeligt at finde frem til af mindst fire gode grunde:

1. USA's frygt for alle tiltag til regulering på cyberområdet, der kan være med til at legitimere repressive staters praksis overfor for informationsudveksling (Tikk-Ringas, 2015, s. 125,126).
2. Vanskelighederne med at beskrive fælles normer på et område, hvor de tekniske muligheder hele tiden øges og ændres.
3. Uenigheder om regulering af praksis vedrørende spionage, overvågning, national suveræntitet og mulig governance i cyberspace baseret på modstridende nationale interesser på området.
4. Den tiltagende generelle forværring af forholdet mellem stormagterne i det internationale system grundet blandt andet udviklingen i Krim, det østlige Ukraine og Syrien.

Så sent som ved FN's generalforsamling i 2016 blev der endnu en gang efterspurgt fælles normer til forebyggelse af cyberangreb, herunder klare normer for ansvarlig statsadfærd (Australien) og accept af en "no first use standard" for offensive cyberoperationer (Venezuela) (General Assembly, First Committee, 2016, s. 8,9,11). Desværre så man i sommeren 2017, at det ikke var muligt i GGE at blive enige om en ny rapport med anbefalinger til normer på cyberområdet. Faktisk er enigheden

fra 2015 vedrørende retten til selvforsvar i cyberspace ved at smuldre, og der er ingen fremgang at spore, hvad angår etablering af fælles normer for adfærd i fredstid (Nye, Controlling Cyber Conflict, 8. august 2017 (b), s. 2). Det forværrede forhold mellem stormagterne synes at være den afgørende årsag til den manglende vilje til at fortsætte de gode takter i GGE, og de fleste eksperter er skeptiske over for, om der i det regi kan ske fortsat normudvikling, eller om det kan ske i FN-sporet i det hele taget i den kommende tid (Nye, Controlling Cyber Conflict, 8. august 2017 (b), s. 3) (Sukumar, 2017). Uenighederne i det internationale samfund er en fortsat forhindring for, at sikkerhedsdilemmaet kan svækkes med tillidsskabende tiltag, at afskrækkelse fremtræder mere troværdig og kalkulerbar for alle typer af uvenlige cyberhandlinger, og at aktører, der bedriver disse handlinger, bremses og kommer under kontrol. Så længe stormagterne har så differentierede holdninger til, hvad der skal gælde af normer for informationsudveksling (Booth & Wheeler, 2008, s. 88), er det meget vanskeligt at udvikle både sædvaner og *soft law* på cyberområdet i et omfang, der kan imødekomme udfordringerne med cyberaktiviteter med destabiliserende konsekvenser.

Den generelle negative udvikling i forholdet mellem stormagterne og den dertilhørende svækkelse af viljen til at indgå og efterleve fælles normer på cyberområdet betyder, at mere decentrale og emnespecifikke processer tager over. Til eksempel har The Hauge Centre for Strategic Studies taget initiativ til The Global Commission on the Stability of Cyberspace (GCSC), der arbejder målrettet på at etablere fælles normer til beskyttelse af internettet sammen med en række medlemmer spredt over hele verden, som både repræsenterer stater, industri og civilsamfund med legitimitet vedrørende forskellige aspekter af internettet. De fælles normer, man arbejder hen imod, er:

State and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace. (The Hauge Center for Strategic Studies, 2017)

Man må også forvente, at de vestlige stater vil gå sammen om en række principper vedrørende eksempelvis indblanding i valg, anvendelse af information fra spionage (Libicki M. , 2017) eller yderligere afgrænsning af kriminelle aktiviteter, samt at industrien og samarbejdsorganisationer som EU og G7 går sammen om standarder for sikkerheden i *Internet of things* mv. I sommeren 2017 gik man f.eks. sammen om en deklaration om privillige normer til G7 mødet, der bygger ekspicit videre på GGE gruppens arbejde (G7 - Declaration, 2017). Herved sker der en inkrementel, partiel og decentral kommunikation om, hvad der er acceptabelt og ikke acceptabelt, når vi taler om cyberbaserede aktiviteter. Kommunikationen om grænser forbedres, selv om den ikke nyder universel tilslutning eller understøttes af enighed om reglers udstrækning og gyldighed på cyberområdet (Nye, Controlling Cyber Conflict, 8. august 2017 (b), s. 3). Den er asynkron, ukoordineret og bagud i forhold til kreative cyberaktiviteters gennemførelse – men er trods alt en fremadskridende proces.

Konklusion

Denne rapport har haft som ambition at opnå større forståelse af cyberspace som arena for magtanvendelse mellem aktører, særligt i relation til destabilisering. Rapporten har undersøgt, i hvilken udstrækning aktiviteter i cyberspace påvirker sikkerhedsdilemmaet mellem stater, og den har peget på en række faktorer, der fremmer våbenkapløbet mellem stater på dette nye område. Via kendskab til

cybermagts særlige egenskaber og muligheder har rapporten opstillet to veje til at hæmme de negative konsekvenser af cybermagts betydning. Den har peget på afskrækkelse og risikohåndtering samt fortsat dialog og normskabelse ved inddragelse af alle interessenter, stater som ikkestatslige aktører.

Cybermagt som spoilermagt

Cybermagt er en indirekte magt, der ikke gennemtvinger bestemte politiske handlinger, men er et effektivt middel til at bane vej for indre forandringer i statens politiske fundament. Cyberaktiviteter kan være med til at skabe et mere ustabilt, svækket og stresset politisk styre samt mere uforudsigelige internationale relationer. Cybermagt er altså i første omgang en "spoilermagt" – en magt, der undergraver, snarere end bygger op. Det kan udnyttes af statslige såvel som ikkestatslige aktører.

I dag er sikkerhedsdilemmaet mellem stater øget på grund af det accelererende våbenkapløb i cyberspace. Det betyder, at staterne bliver mere og mere usikre på to dimensioner. Det første vedrører usikkerheden omkring, hvordan man skal tolke de andre aktørers øgede kapabiliteter på cyberområdet samt den voldsomme stigning i antallet af uvenlige cyberaktiviteter. For det andet er staterne usikre på, hvordan de skal reagere på det voksende antal af uvenlige aktiviteter i alle sektorer og på alle niveauer inden for statens egne grænser. Der er heller ingen afklaring, i forhold til hvordan staterne selv skal håndtere våbenkapløbet.

Karakteren af cyberspace øger sikkerhedsdilemmaet

Usikkerheden får staterne til at øge oprustningen i cyberspace. Men der er også en række egenskaber ved cyberspace, der i sig selv er med til at øge sikkerhedsdilemmaet. Rapporten peger på tre centrale elementer: geografi, eskalationspotentialet og den mørklagte kapabilitetsudvikling. Analysen af de tre elementer peger samlet set på, at cybermagt, når vi anskuer den i relation til destabilisering, er indirekte, vedvarende, skjult og indgribende på alle niveauer i staten. Cybermagt opfattes offensivt, kan aktiveres uden forvarsel og uden synlig mobilisering. Den kan anvendes til langt farligere formål end destabilisering, såfremt aktørens øvrige kapabiliteter kan understøtte det.

På trods af ovenstående ændrer våbenkapløbet i cyberspace dog ikke ved den grundlæggende magtbalance mellem staterne eller ved det forhold, at staterne fortsat er de afgørende aktører i internationale relationer. Staterne er fortsat de eneste, der har adgang til den række af støttende funktioner og den organisering og styring, der skal til, for at man kan udnytte cybermagten til mere end at agere "spoiler" eller destabiliserende kraft. Herudover gælder, at staterne er de eneste aktører, der kan flytte konflikten fra cyberspace til konventionel eller nuklear krig.

Strategier til at hæmme og tæmme cybermagt

De strategier, som staterne bør bringe i anvendelse for at håndtere våbenkapløbet i cyberspace, har det tilfælles, at de søger at fremme en mere klar kommunikation. En kommunikation, der vedrører konsekvenser af uvenlig adfærd og grænsen mellem uvenlig og ikkeacceptabel adfærd. Samtidig er det nødvendigt, at staterne fortsat har fleksibilitet og frihed til at vælge respons. Klar kommunikation kræver derfor en tostrenget strategi.

Den ene tilgang understøtter afskrækkelse og risikohåndtering i cyberspace. Den anden styrker dialog og samarbejde omkring normdannelse og regulering samt forskellige tillidsskabende aktiviteter. Afskrækkelse er vanskelig i cyberspace, men langtfra umulig. Afskrækkelse skal dog opfattes mindre definitivt for at være succesfuld og skal kombineres med risikohåndtering, således at fordelene ved ødelæggende aktiviteter mindskes. Samtidig skal staterne signalere øgede forventede omkostninger ved anvendelse af cyberinstrumenter. Det kræver, at staterne faktisk har relevante kapabiliteter til modsvar på angreb eller uvenlige aktiviteter, og i den forstand er et våbenkapløb ikke blot usikkerhedsskabende – det indeholder samtidig et afskrækkelsespotentiale, der i sig selv kan virke dæmpende på sikkerhedsdilemmaet. Afskrækkelsens endelige virkning bakkes op af konventionel eller nuklear afskrækkelse i yderste potens. Dette svækker afgørende cybertruslens eskalationspotentiale.

Allerede i 1950'erne pegede Herz på, at en svækkelse af sikkerhedsdilemmaet først og fremmest kalder på international normdannelse og tillidsskabende mekanismer. Denne rapport peger ligeledes på, at en af de afgørende metoder til at få det accelererende digitale våbenkapløb under kontrol er fortsat at arbejde med normdannelse og tillidsskabelse i cyberspace. Der er en udbredt interesse i, at staterne sætter nye fælles normer for acceptabel adfærd i cyberspace og passende sanktioner ved brud på disse normer. Desværre er der samtidig ret stor splittelse i forhold til, hvordan disse normer skal udkrystallisere sig. Samtidig er det internationale klima for tilslutning til tillidsskabende mekanismer lige nu meget dårligt. Derfor vil vi i de kommende år se udviklingen af normer ske partielt, asynkront, decentralt og forskelligt i relation til forskellige aspekter af internettets funktioner. Vi kommer også til at se andre aktører end staterne gå foran i denne udvikling, indtil et mere gunstigt miljø for fælles aftaler forhåbentlig genopstår.

På trods af udsagn om det modsatte og stigningen i antallet af uvenlige cyberdrevne aktiviteter i 2017 er der ikke udsigt til, at staterne oplever den brændende platform, som Herz så som forudsætningen for, at staterne for alvor vil tæmme våbenkapløbet, svække sikkerhedsdilemmaet og villigt indgå nødvendige aftaler. Det skyldes nok, at cybermagt indtil videre først og fremmest er en spoilermagt og ikke en vital sikkerhedstrussel.

Litteraturliste

Citerede værker

Allan, C. S. (Spring 2013). Attribution Issues in Cyberspace. *Chicargo-Kent-Journal of International and Comrarative Law Vol. 13, Issue 2*.

Andres, R. B. (2012). The Emerging Structure of Strategic Cyber Offense, Cyber Defense and Cyber Deterrence. I D. S. Reveron, *Cyberspace and National Security.* Georgetown University Press.

Art, R. J. (Spring 1980, Vol. 4, Issue 4). To What Ends Military Power? *International Security*, s. 3-35.

Booth, K., & Wheeler, N. (2008). *The Security Dilemma - Fear, cooperation and trust in world politics.* palgrave macmillan.

Bradshaw, S., & Howard, P. H. (2017.12). *Troops, Trolls and Troublemakers: A global Inventory of Organized Social Media Manipulation.* University of Oxford.

Buchanan, B. (2016). *The Cybersecurity Dilemma - Hacking, Trust and Fear between Nations.* Oxford University Press.

Buzan, B. (1991). *People, States and Fear 2nd edition.* Harvester Wheatsheaf.

Commentary: Means, gols and consequences of the pro-Kremlin disinformation campaign. (22.. Februar 2017). Hentet fra evusdisinfo.eu.

Cooper, J. R. (2012). A new Framework for Cyber Deterence. I D. S. (ed.), *Cyberspace and National Security.* Georgetown University Press.

Council of the European Union. (9916/17). *Annex to Draft Council Conclusions on a Framework for a joint EU Diplomatic response to Malicious Cyber Activities.* Brussels 7. June 2017.

EU 2016/1148, NIS direktiv af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for Net- og informationssystemer i hele Unionen.

Executive Order, Taking additional steps to adress the national emergency with respect to significant malicious cyber-enabled activities (The White House 28. December 2016).

Friis, K., & Reichborn-Kjennerud, E. (2016). From Cyber threats to cyber risks. I K. Friis, J. Ringsmose, & (eds.), *Conflict in Cyber Space - Theoretical, strategic and legal perspectives.* Routlegde.

G7 - Declaration. (11.. april 2017). *G7 Declaration on Responsible State Behaivor in Cyberspace*. Lucca, Italien.

Gartzke, E., & Lindsay, J. R. (24:2 2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies*, s. 316-348.

Glaser, C. (Spring, Vol 28, No. 4 2004). When Are Arms Races Dangerous? *International Security*, s. 44-84.

Hansen, F. S. (2017:06). *Russian Hybrid Warfare - A study of disinformation.* DIIS Rapport.

Hennessey, S. (November/December 2017). Deterring Cyberattacks - How to Reduce Vulnerability. *Foreign Affairs*, s. 39-46.

Herz, J. H. (1950). Idealist Internationalism and the Security Dilemma. *World Politics*, s. vol. 2(2) s. 157-180.

Herz, J. H. (2003). The Security Dilemma in International Relations: Background and Present Problems. *International Relations*, s. vol. 17(4) 411-416.

Hohmann, M., Pirang, A., & Benner, T. (2017). *Advancing Cybersecurity Capacity Building.* Global Public Policy Institut.

Jacobsen, J. T. (2016). *Opbygning af offensiv cyberkapabilitet - Næste skridt for Danmarks cybermilitær.* DIIS Policy Brief.

Jacobsen, J. T. (2017). Danmark bør undgå en ”digital Genèvekonvention” - En prioritering af Danmarks cyberpolitik. *Forsvarsakademiet*.

Jervis, R. (Vol. 30, No. 2 1978). Cooperation Under the Security Dilemma. *World Politics*, s. 167-214.

Kragh, M., & Åsberg, S. (2017). Russia´s strategy for influence through public diplomacy and active measures: the Svedish case. *The journal of Strategic Studies*.

Langø, H.-I. (2016). Competing academic approaches to Cyber Security. I J. Ringsmose, & Friis, *Conflicts in Cyberspeace - teoretical, strategic and legal perspectives.*

Libicki, M. (2017). The Coming og Cyber Espionage Norms. I H. Rõigas, R. Jackschis, L. Lindström, & T. Minárik, *Defendig the Core* (s. 7-23). Tallinn: CCDCOE.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar.* RAND Project Air Force.

Macák, K. (2017). From the Vanishing Point Back to the Core: The Impact og the Development of the Cyber Law of War on General International Law. I H. Rõigas, R. Jackschis, L. Lindström, & T. Minárik, *2017 9th International Conference on Cyber Conflict - Defending the Core.* Tallinn: CCDCOE.

Marks, J. (april 2017). The US Does An About-Face on New Cyber Norms. *Defence One - Cyberwarfare*, s. 6-7.

Nye, J. S. (2011). *The Future of Power.* New York: Public Affairs.

Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, s. Vol. 41 (3) pp. 44-77.

Nye, J. S. (8. august 2017 (b)). Controlling Cyber Conflict. *Project Syndicate - The World´s Opinion Page*, 1-4.

Sanger, D. (2016). U.S: Wrestles with How to Fight Back Against Cyberattacks, July, 30. *New York Times*.

Schmitt, M. N. (2017). *Tallinn Maual 2.0 on the international law appicable to Cyber Operations 2. edition.* Cambrigde.

Sheldon, J. B. (2012). Toward a Theory of Cyber Power - Strategic Purpose in Peace and War. I D. S. (ed.), *Cyberspace and National Security.* Georgetown University Press.

Singer, P. (14. Januar 2017). *How America can beat Russia in Cyber War, Despite Trump*. Hentet fra Wired.

Slayton, R. (Vol 41, no. 3 2017). What is the Cyber Offence-Defence Balance? Conceptions, Causes and Assessment. *International Security*, s. 72-109.

Smeets, M. (2017). Organisational Integration of Offensive Cyber Capabilities - A Primer on the Benefits and Risks. I H. Rõigas, R. Jackschis, L. Lindström, & T. Minárik, *2017 9th International Conference on Cyber Conflict - Defending the Core.* Tallinn: CCDCOE.

Sukumar, A. M. (4. Juli 2017). The UN GGE Failed. Is International Lwa in Cyberspace Doomed As Well? *Lawfare*.

The 2015 repport of the Group of Governmental Experts. UN: A/70/150.

The Hauge Center for Strategic Studies. (18. 07 2017). Hentet fra https://hcss.nl/news/global-commission-stability-cyberspace

Tikk-Ringas, D. (2015). *Evolution of the Cyber Domain.* London: The International Insitute for Strategical Studies.

twobirds.com. (23.. Januar 2018). Hentet fra Bird & Bird: https://www.twobirds.com/da/news/articles/2017/denmark/cyber-security-overblik-over-relevant-lovgivning

Tzu, S. (2010). *The Art of War.* Public Domain.

UN Disarmament Committee. (30.. september 1998). Brev fra russisk repræsentation rettet til FN´s generalsekretær. A/C.1/53/3, 30 September 1998.

White House. (2011). *International Stretegy for Cyberspace.*