International cybernormfremme. Hvordan løsnes hårdknuden?

Temanummer: Cybersikkerhed

Der er ikke mange forhåbninger til de igangværende globale drøftelser om normer for ansvarlig statslig adfærd i cyberspace. Men hvorfor er de internationale normforhandlinger strandet og den vestlige koalitions normstrategi fejlet? Og kan en småstat som Danmark være normentreprenøren, der skubber den vestlige cybernormdagsorden fremad? Med afsæt i normlitteraturen i International Politik peger denne artikel på, at den nuværende kamp om internationale cybernormer er karakteriseret ved gensidige beskyldninger om hykleri, hvilket, når det rettes mod USA og dets allierede, hovedsageligt skal forstås i lyset af Snowden-afsløringerne og manglende anerkendelse af den efterretningsnorm, der dominerer i cyberspace. En begyndende vestlig åbenhed om og nuancering af statslig brug af cyberkapaciteter giver mulighed for, at Danmark kan blive et foregangsland, der udvikler de nødvendige politiske afklaringer og deler "best practices" og derved bidrager med de vigtige referencepunkter, som andre stater kan finde tiltrængt inspiration i. Men det kræver, at danske myndigheder er villige til internt at afveje og nå til enighed om en række svære spørgsmål om, hvornår og hvor meget man ønsker at bruge hackere i udenrigs- og sikkerhedspolitikken og eksternt investerer diplomatisk.

JEPPE TEGLSKOV JACOBSEN
adjunkt,
Forsvarsakademiet,
jeja@fak.dk

Utroværdighed er kerneudfordringen for den vestlige koalitions normfremme

"*The United States will promote a framework of responsible state behavior in cyberspace built upon international law, adherence to voluntary non-binding norms of responsible state behavior that apply during peacetime, and the consideration of practical confidence building measures to reduce the risk of conflict stemming from malicious cyber activity*" (2019 US National Cyber Strategy, Trump, 2018: 20)

"*We should pursue shared prosperity and shared responsibility. … China will stay committed to upholding multilateralism, follow the basic principles governing international relations based on the UN Charter, build more partnerships in cyberspace, and work with all parties to forge a cyberspace that is peaceful, secure, open, cooperative and with a sound order and build a community with a shared future in cyberspace*" (Wang Lei, Coordinator for Cyber Affairs, Ministry of Foreign Affairs of the People's Republic of China, 2019).

Ansvarlighed er nøglebegrebet, når diplomater drøfter, hvordan stater bør agere i cyberspace. Men hvad ansvarlig adfærd helt præcist dækker over, er der langt fra enighed om – og det er til trods for, at en myriade af internationale processer er blevet sat i søen for at finde fælles fodslag. FN har siden 2004 haft seks forskellige grupper af udvalgte regeringseksperter for cyber- og

informationssikkerhed (UNGGE), hvilket siden 2018 har været suppleret af en arbejdsgruppe åben for alle FN's medlemsstater (OEWG). Samtidig har OSCE, EU og Shanghai Cooperation Organisation samt ekspertkommissioner som The Global Commission on the Stability of Cyberspace, det fransk- og Microsoft-ledede initiativ The Paris Call og den privatdrevet Cybersecurity Tech Accord alle forsøgt at udarbejde og udbrede fælles normer for ansvarlig statslig adfærd i cyberspace (Meyer, 2020; Ruhl et al., 2020).

Men positionerne forbliver hårdt optrukket, og ingen nævneværdige fremskridt er i sigte. En række ligesindede lande, med USA og Storbritannien i spidsen ("den vestlige koalition")[1], abonnerer på frivillige og ikkebindende cybernormer, som søger at fremme adfærd, der blandt andet skal forhindre statsstøttet tyveri af private virksomheders intellektuelle rettigheder, statslig beskyttelse af kriminel aktivitet online og påvirkning af valg samt minimere risikoen for militær eskalation ved at forpligte sig på at overholde eksisterende international ret (Maurer, 2019). Modsat står stater som Rusland, Kina og Iran, der ønsker fuld kontrol over datastrømmende på deres suveræne territorier for derved at forhindre farlig og destabiliserende onlineindhold. Samtidig problematiserer disse stater, at der på nuværende tidspunkt foregår en militarisering af cyberspace, hvilket de søger at begrænse ved hjælp af en bindende cyberkonvention (Erskine og Carr, 2016; Henriksen, 2019). Multinationale virksomheder som Microsoft er ligesom sidstnævnte bekymrede for en øget militær tilstedeværelse i cyberspace, men ønsker først og fremmest normer, der minimerer udnyttelse af kommercielle it-produkter og samtidig beskytter brugeres privatliv globalt (Christensen og Liebetrau, 2019).

Centralt for de diplomatiske slagudvekslinger om definitionen af ansvarlig statslig adfærd i cyberspace er kampen om troværdighed. Det er derfor ikke underligt, at beskyldningerne om hykleri ofte tages i brug af alle de involverede parter. Mærkatet "utroværdig" bruges her ikke blot til at påpege fundamentale paradokser i andre aktørers forståelser af, hvad cyberspace er og bør være. Det er også et forsøg på at få den store gruppe af endnu uafklarede stater til at abonnere på én specifikt forståelse af ansvarlig cyberadfærd. Håbet er, at dette vil skabe en global normkaskadeeffekt. Men hvorfor har det været så nemt at pådutte den vestlige koalition mærkatet "utroværdig"? Og hvordan kan en småstat som Danmark spille en rolle i forsøget på at løse den cyberdiplomatiske hårdknude?

I forsøget på at adressere disse problematikker tager artiklen afsæt i den eksisterende litteratur om normer i International Politik (IP). Efter at have gennemgået kernebegreberne og diskussionerne i denne litteratur og sat dem i konteksten af den nuværende strid om cybernormfremme vender artiklen sig mod en af kerneudfordringerne for den vestlige koalitions normfremme, nemlig kritikken om utroværdighed. I forlængelse heraf peger artikel fremad på de muligheder, som Danmark har fået ift. at blive cybernormentreprenør.

Fra normbegrebet i IP til cybernormerfremme i praksis

Hvad mener politologer egentlig, når de bruger ordet international norm? I den liberalkonstruktivistiske tradition inden for internationalpolitisk teori, hvor normdiskussionerne er mest præsente, defineres normer oftest som de kollektive forventninger til passende adfærd for en bestemt gruppe af aktører (Katzenstein, 1996: 5). En succesfuld international norm er således en norm, der har opnået status af at være "internaliseret" og derfor tages for givet som "den rigtige adfærd" for de aktører, der ønsker at se sig selv som en del af et globalt fælleskab af stater. De klassiske casestudier er her udbredelsen af menneskerettighederne (Risse, Ropp og Sikkink, 1999), fremkomsten af et tabu for brugen af kemiske våben og atomvåben (Price og Tannenwald, 1996) og opgøret med apartheid (Klotz, 1995).

Men en ny norm bliver imidlertid ikke bare uden videre accepteret, når den fremsættes og promoveres. Den vil derimod altid være genstand for forhandling og stridigheder, som ikke nødvendigvis er overstået, når en konvention er underskrevet. Martha Finnemore og Duncan B. Hollis (2016: 428) understreger eksempelvis, at normer altid har en dynamisk karakter og bør forstås som en proces, hvor de involverede parter løbende genfortolker betydningen af normen (Wiener, 2008). Det betyder, at en norm ikke nødvendigvis bliver efterlevet, som den oprindeligt var tiltænkt, og at de involverede parter derfor ofte møder beskyldninger om hyklerisk adfærd. Men dermed ikke sagt, at de enkeltaktører, der i udgangspunktet forsøgte at promovere en bestemt norm, er ligegyldige. Disse såkaldte normentreprenører påvirker, hvad der kommer på dagsordenen; de genererer nye måder at tale om og forstå en given problemstilling på og de mobiliserer forskellige værktøjer, heriblandt incitamenter, overtalelse og socialisering, i de vedvarende forsøg på at udbrede en norm (Finnemore og Sikkink, 1998: 897; Björkdahl, 2002: 44; Finnemore og Hollis, 2016: 448–53). Håbet for normentreprenøren er at skabe en kaskadeeffekt (Finnemore og Sikkink, 1998: 902), hvor flere og flere aktører begynder at acceptere og efterleve normen. Normfremme handler derfor ikke udelukkende om at engagere stormagter. Det kan i lige så høj grad være en kamp om for eksempel at få det stille flertal af stater, der endnu ikke har taget stilling, til at indarbejde normen.

> **Håbet for normentreprenøren er at skabe en kaskadeeffekt, hvor flere og flere aktører begynder at acceptere og efterleve normen**

Kampen om normerne for ansvarlig statslig adfærd i cyberspace illustrerer, hvordan forskellige normentreprenører og værktøjer, der arbejder på både bilateralt, regionalt og globalt plan, kan være i spil på samme tid – og trække i forskellige retninger. Louise Marie Hurel og Luisa Cruz Lobato (2018) peger eksempelvis på, at Microsoft forsøger at udnytte sin økonomiske og tekniske kapital til positionere sig som en troværdig og ansvarlig diplomatisk stemme og derved fremme en ændring i staters adfærd i cyberspace, så mi-

litær og efterretningstjenesters udnyttelse af it-sårbarheder i kommercielt software begrænses. Microsofts primære værktøj er overtalelse. Højtstående Microsoft-ansatte gør således flittigt brug af saglige og faktuelle præsentationer, veldesignede brochurer og fængende idéer om behovet for en digital Genèvekonvention eller et digitalt Røde Kors i forsøget på at få stater til at indse, at sikkerhed i cyberspace først og fremmest bør knytte sig til beskyttelsen af civile borgeres (eller mere præcist, globale forbrugeres) fundamentale frihedsrettigheder (Microsoft, 2015; Smith, 2017; 2018). Men multinationale tech-virksomheder som Microsoft – eller diverse netværk af menneskerettighedsforkæmpere for den sags skyld – er ikke de eneste normentreprenører i cyberspace.

USA kan også siges at være en normentreprenør. Duncan B. Hollis (2017) viser, hvordan Obama Administrationen engagerede forskellige normfremmestrategier, da de i UNGGE rapporten fra 2013 formåede at få eksisterende international ret anerkendt som gældende i cyberspace og senere formåede at lande en bilateral aftale med Kinas præsident Xi Jinping om, at ingen af partnerne ville støtte kommerciel cyberspionage. Hvor overtalelse var hjørnestenen i førstenævnte, brugte Obama Administrationen en lang række værktøjer til at opnå en bilateral aftale om cyberspionage med Kina, heriblandt lækkede overvejelser om mulige amerikanske sanktioner, naming and shaming, rejse af tiltale mod kinesiske hackere og udnyttelse af Xi Jinpings indenrigspolitiske agenda om bekæmpelse af statslig korruption (Harold, Libicki og Cevallos, 2016; Hollis, 2017: 12–4). Men begge aftaler viser også, at normudviklingen ikke stopper, når en rapport eller en aftale er blevet præsenteret.

Obama-Xi-aftalen førte til en kaskadeeffekt, hvor flere stater herunder Storbritannien pressede på for lignende aftaler, hvilket førte til en bredere støtte til normen i G-20-sammenhæng (Segal, 2016). Men selvom den kinesiske spionage mod amerikanske virksomheder faldt i månederne efter aftalen, har både USA og Storbritannien ved flere lejligheder sidenhen beskyldt Kina for ikke at overholde aftalen (Bond og Sevastopulo, 2018). Om dette skyldes manglende kinesisk oprigtighed fra starten, eller om det skyldes den generelle forringelse af det amerikansk-kinesiske forhold efter Donald J. Trump overtog præsidentembedet, forbliver spekulation. Under alle omstændigheder vidner det om, at normen endnu ikke er internaliseret. Det kinesiske behov for åbent at afvise, at man bryder aftalen, understreger imidlertid, at statsstøttet kommerciel cyberspionage offentligt anses som uacceptabel statslig adfærd.

Den amerikansk promoverede norm om, at international ret gælder i cyberspace har taget en anden udvikling end Obama-Xi-aftalen. Her er efterfølgende UNGGE-forhandlinger sidenhen gået i stå grundet uenigheder om, *hvad* det egentlig betyder, at international ret også gælder i cyberspace (Grigsby, 2017; Maurer, 2019). I denne sammenhæng kan Kina og Rusland også siges at agere som en normentreprenører.[2] Begge stater spiller en aktiv rolle i forsøget på at skabe en norm om, at det internationale retsprincip om suverænitet bør opretholdes i cyberspace (Henriksen, 2019: 5). På den måde,

som Hollis (2017: 13) også påpeger, kan én normfortolkning laves om og ende med at betyde noget helt andet, end hvad der var tiltænkt fra den oprindelige normentreprenørs side. Som følge heraf foregår striden om cybernormer på nuværende tidspunkt på et institutionelt plan, hvor Rusland succesfuldt har advokeret for, at normdrøftelserne skal finde sted i et åbent FN-spor, OEWG, hvor alle stater kan deltage (og hvor vestlige stater er i undertal), mens USA har genoptaget UNGGE-sporet i en snævrere kreds (Grigsby, 2018). Samtidig advokerer Rusland og Kina – ligesom Microsoft – for etableringen af en omfattende forhandlingsrunde om en digital konvention, hvilket de vestlige stater møder med beskyldninger om hyklerisk adfærd på grund af manglende tro på russisk og kinesisk efterlevelse.

Det er ikke kun Rusland, Kina og deres cybernorm-allierede, der beskyldes for at være hykleriske og utroværdige. Den kritik tilfalder også USA, Storbritannien og deres ligesindede. Og kritikken er ikke helt uberettiget. Hvor jeg i dette afsnit har sat centrale teoretiske normbegreber i kontekst af de igangværende normkampe i cyberspace, vil det næste afsnit se på, hvorfor USA og dets allierede kan tolkes som hykleriske og utroværdige i deres normfremme.

Hvorfor fremstår USA og vestlig normfremme utroværdig?

Edward Snowdens afsløringer om NSA's omfattende overvågningsaktiviteter har givet ammunition til skeptikerne af oprigtigheden af de amerikanske forsøg på at fremme normer for ansvarlig adfærd både i og uden for cyberspace (Farrell og Finnemore, 2013). For det første fremstod de amerikanske forsøg på at promovere frihedsrettigheder online ved at kritisere andre staters overvågning af egne borgere pludselig noget dobbeltmoralske – bedst illustreret med daværende udenrigsminister Hillary Clintons meget omtalte "Internet Freedom"-tale fra 2010, hvor netop privatlivets fred online blev indædt forsvaret (Clinton, 2010). Med udgangspunkt i Snowden-afsløringerne er USA for det andet blevet kritiseret – blandt andet af Kina – for hyklerisk adfærd i forbindelse med de amerikanske forsøg på at konstruere en norm, der forhindrer, at stater giver egne virksomheder en konkurrencefordel ved hjælp af cyberspionage. Her refereres ofte til det faktum, at NSA har spioneret på flere private firmaer som brasilianske PetroBras og kinesiske Huawei (Sheehan, 2014). For det tredje har Microsoft efter Snowden-afsløringerne været vedholdende i deres kritik af staters opkøb og udnyttelse af sårbarheder i it-systemer med reference til, at det underminerer den amerikanske regerings eksplicit artikulerede vision om et frit, åbent, sikkert og pålideligt internet (Obama, 2011; cf. Neutze og Nicholas, 2013; Smith, 2017).

» **Allerede inden Snowdens afsløringer blev der stillet spørgsmålstegn ved oprigtigheden af USA's visioner om et pålideligt og sikkert internet**

Allerede inden Snowdens afsløringer blev der stillet spørgsmålstegn ved oprigtigheden af USA's visioner om et pålideligt og sikkert internet. Det skyldes først og fremmest Stuxnet – computerormen, der i en årrække ødelagde centrifuger til berigelse af uran på et atomanlæg i Iran, og som The New York Times-journalist David E. Sanger afslørede var af amerikansk-israelsk oprindelse (Sanger, 2013: 188–225; 2018: 7–36). Ormen udnyttede it-sårbarheder i en række kommercielle software, eksempelvis Microsoft Windows, som bruges overalt i verden. Og elementer af Stuxnets kode har fundet vej til andet malware, der bruges til kriminalitet og spionage (Simonite, 2012). USA var ikke villige til at bekræfte anklagerne om, at Stuxnet var amerikansk, men har siden langsomt tilpasset den internationale normfremme, så militær anvendelse af cyberangreb, der udføres i overensstemmelse med international ret, nu promoveres som legitim (Jacobsen og Ringsmose, 2017).

Modsat fik USA hurtigt forfattet en række modsvar til Snowden-afsløringerne. For det første insisterede NSA på, at overvågningen skete inden for amerikansk lov, og at NSA derfor *ikke* indhentede og opbevarede data på alle amerikanere (Greenwald og MacAskill, 2013). For det andet forsikrede den daværende amerikanske chef for de nationale efterretningstjenester, James Clapper, om, at motivationen bag spionagen på udenlandske firmaer udelukkende var et forsøg på at få viden om andre staters økonomiske politik, for national sikkerhedshensyn og for få tidlige indikationer på finansielle kriser (Sheehan, 2014; Libicki, 2017: 10). Og for det tredje har de to seneste cybersikkerhedskoordinatorer i det Hvide Hus, Michael Daniel og Rob Joyce, forsikret om, at USA ikke bare udnytter alle it-sårbarheder, de identificerer. I stedet har man etableret en grundig intern procedure, der skal afgøre, hvornår USA frigiver it-sårbarheder til virksomhederne, og hvornår det er forsvarligt, at man beholder dem (Daniel, 2014; Joyce, 2017).

Fra et normfremmeperspektiv lader disse svar dog ved nærmere eftersyn en del tilbage at ønske. Ben Buchanan (2020: 13–39) beskriver eksempelvis, hvordan NSA gennem samarbejdspartnere både i form af amerikanske virksomheder og internationale allierede deler data og efterretninger om de individer, som de amerikanske efterretningstjenester ikke umiddelbart har lov til at indhente og opbevare personlig data om. Dernæst er det indlysende, at NSA's overvågning af udenlandske virksomheder med henblik på at forstå et lands økonomiske politik styrker amerikanske positioner, når der skal forhandles handelsaftaler, hvilket i sidste ende uundgåeligt giver amerikanske virksomheder en konkurrencefordel. USA's forsøg på udelukkende at rette opmærksomheden på tyveri af intellektuelle rettigheder fremstår således primært som en sproglig undvigemanøvre. Sidst indeholder USA's procedure for deling af it-sårbarheder en række undtagelser, der i lyset af NSA's position øverst i de institutionelle cyberhierarki i USA (Jacobsen, 2020: 17), gør bevaring og udnyttelse af sårbarheder i indhentningsøjemed mere sandsynlig (Ambastha, 2019).

Men problemet for USA's normfremme er ikke blot, at skeptikere relativt nemt kan afvise modsvarene. Den primære udfordring knytter sig til det faktum, at forsøgene på at konstruere modsvarene underkender en dominerende efterretningsnorm i cyberspace. Forsøget på at undgå en offentlig diskussion af denne norm er hovedårsagen til, at USA og de vestlige allierede fremstår utroværdige.

Den begyndende accept af en dominerende efterretningsnorm

Siden internettets fremkomst har efterretningstjenester og efterretningstænkning domineret staters interaktioner i cyberspace. Denne kampplads er kendetegnet ved juridiske gråzoner, ved konstant kontakt mellem egne og fjendes spioner og ved at forsøg på at bedrage og opnå relative fordele tages, når mulighederne opstår (Jacobsen, 2019: 248). Men i cyberkonfliktlitteraturen diskuteres efterretningstjenesternes rolle hovedsageligt ved hjælp af et militært begrebsapparat. På den ene side ses egne efterretningstjenesters dominerende position her som en mulig hindring for den militære brug af offensive cyberspaceoperationer, da den malware, der kan bruges til både spionage og angreb, kun sjældent vil blive brugt til sidstnævnte på grund af risikoen for at kompromittere fremtidig indhentningsarbejde (Nakashima, 2016; Conti og Raymond, 2017; Smeets, 2017; Klipstein, 2019). På den anden side ses fremmede efterretningstjenesters cyberaktiviteter under grænsen for væbnet konflikt ofte som eksempler på manglende afskrækkelse og dermed som alvorlige nationale sikkerhedsproblematikker, der ultimativt indeholder et nukleart eskalationspotentiale (Crosston, 2011; Jasper, 2015; Buchanan, 2017; Kello, 2017: 195–211).

Men en manglende åben anerkendelse og diskussion af den eksisterende efterretningstænkning, der naturligt bevæger sig i gråzonen og ikke nødvendigvis meningsfyldt lader sig afskrække, påvirker troværdigheden af den internationale normfremme. Ønsker den vestlige normkoalition at svække beskyldningerne om utroværdighed, må USA og dets allierede skabe mere klarhed om, hvordan statslig adfærd i cyberspace kan tage sig ud i lyset af den dominerende efterretningsnorm.

En begyndende åbenhed herom er dog langsomt ved at indfinde sig i for eksempel USA, Australien og Storbritannien (Fischerkeller og Harknett, 2017; Maurer, 2019: 14). US Cyber Command fremlagde eksempelvis i 2018 et visionspapir, der netop åbent fremlagde, at man aktivt søger vedvarende at være til stede i fjendens netværk, og at der er en villighed til at forsvare nationale sikkerhedsinteresse fra denne position (Cyber Command, 2018). Disse formuleringer fandt også vej til Trump Administrationens nationale cybersikkerhedsstrategi (Trump, 2018), og de er blevet åbent udmøntet eksempelvis i NSA's forstyrrelse af russiske serverer, der spredte misinformation forud for midtvejsvalget i 2018 (Nakashima, 2019). Både den britiske justitsminister, Jeremy Wright, og det amerikanske justitsministeriums juridiske chef, Paul Ney, har også nuanceret fortolkningen af anvendelsen af suverænitetsprincip-

pet i konteksten af staters cyberoperationer (Waxman, 2018; Buchan, 2020). Ney drager eksempelvis en parallel mellem cyberoperationer og konventionel (kontra)spionage, hvilket han bruger til at konstruere et argument for, at det ikke er forbudt at hacke fremmede staters netværk (Schmitt, 2020).

> **I de nuværende forhandlinger forsøger vestlige stater stadig at få andre stater til at acceptere de omhyggeligt fremstillede og indforståede sproglige formuleringer, der implicit retfærdiggør vestlig efterretningsadfærd. Men de sproglige finurligheder er efterhånden velkendte af alle parter, og derfor fremstår cyberdiplomatiet ikke længere troværdigt**

Diskussionerne om en mere nuanceret brug af cyberkapaciteter, der anerkender konstant kontakt i cyberspace, mangler stadig at blive ekspliciteret i de konkrete internationale drøftelser om cybernormer. I de nuværende forhandlinger forsøger vestlige stater stadig at få andre stater til at acceptere de omhyggeligt fremstillede og indforståede sproglige formuleringer, der implicit retfærdiggør vestlig efterretningsadfærd. Men de sproglige finurligheder er efterhånden velkendte af alle parter, og derfor fremstår cyberdiplomatiet ikke længere troværdigt, hvis det fortsætter med blot at insistere på, at man overholder international ret, beskytter private frihedsrettigheder og er ansvarlig i relationen med den private it-sektor.

Givet ovenstående udviklinger er der derfor behov for svar på en række konkrete spørgsmål: Hvornår og med udgangspunkt i hvilke retningslinjer forstyrrer eller manipulerer vestlige stater udenlandske servere i forsøget på at forhindre spionage, overbelastningsangreb eller falske nyheder? Hvornår og i hvilken grad mener vestlige stater, at det er acceptabelt at hacke og frigive fortrolige oplysninger om for eksempel statslederes korrupte adfærd for at fremme vores udenrigspolitiske dagsorden? Og hvad er vores politik i forhold til at købe cyber-værktøjer fra private virksomheder, der også sælger deres produkter til stater med dårlige menneskerettighedsstandarder? De vestlige lande har både intra- og interstatsligt vanskeligt ved at nå til enighed om svarene på disse spørgsmål. Men trods de vanskelige svar og afvejninger, der venter forude, står en småstat som Danmark med gode kort på hånden, hvis de ønsker at indtage rollen som normentreprenøren, der forsøger at løsne hårknuden i cyberspace. Det næste afsnit uddyber, hvorfor og hvad dette kræver fra dansk side.

Det gode eksempel: Danmark som cybernormentreprenør

Småstaters mulighed for at få indflydelse udover, hvad deres økonomiske og materielle magt berettiger, er længe blevet studeret (Ingebritsen et al., 2006; Steinmetz og Wivel, 2010). Hvor traditionelle forklaringer knytter sig til internationalt renommé, specifik ekspertise og diplomatiske evner (Ingebritsen, 2002; Tarp og Hansen, 2013), har flere studier om cybernormfremme

ydermere påpeget, at netop den til stadighed spæde klarhed om de politiske rammer i cyberspace giver småstater – der evner at nå til enighed internt – relativ stor indflydelse på politikkens udvikling (Crandall og Allan, 2015; Jacobsen, 2018). Eksempelvis har Estland, efter landet blev ramt af et cyberangreb i 2007, investeret mange ressourcer i at positionere sig som cyberdiplomatisk nation og har via en række nationale strategier, initiativer og policy-papirer formået at sætte sit præg på forståelsen af cyberpolitikken i EU (Crandall og Allan, 2015: 352). Med andre ord kan åbenhed om gode erfaringer og deling af konkrete afklaringer gøre en stat til normentreprenør, fordi disse informationer bidrager med de efterspurgte eksempler og referencepunkter, som andre aktører kan finde tiltrængt inspiration i, men som også aftvinger en stillingstagen fra disse aktører.

Danmark er i udgangspunktet godt placeret til at blive cybernormentreprenør, hvis man antager, at internationalt renommé og ekspertise er nøgleparametre for småstatslig indflydelse. Danmark anses for førende på det digitale område i EU (EU Commission, 2017) – et image som Danmark med oprettelsen af verdens første tech-ambassadør og en generel styrkelse af repræsentationen i diverse internationale cyberfora har forsøgt at sprede globalt (Regeringen, 2018: 42). Derudover er Danmark blandt de ni medlemslande, der har tilbudt at bidrage til offensive cyberkapabiliteter til NATO Cyberspace Operations Centre (Vavra, 2019) og blandt de første til at udgive en værnsfælles doktrin for militære cyberspaceoperationer (Forsvarsakademiet, 2019). Men det kræver mere end et velplejet renommé at blive normentreprenør. I den resterende del af afsnittet peges der på to centrale elementer: Intern afklaring og ekstern promovering.

» **Danmark er i udgangspunktet godt placeret til at blive cybernormentreprenør, hvis man antager, at internationalt renommé og ekspertise er nøgleparametre for småstatslig indflydelse. Danmark anses for førende på det digitale område i EU**

Skal Danmark blive global cybernormentreprenør, må den danske regering nødvendigvis tackle nogle af de svære spørgsmålet listet i det forrige afsnit. Og de må gøre det åbent. Hvis ovennævnte spørgsmål om, hvornår Danmark hacker sig ind i, manipulerer og forstyrrer servere i andre stater, lækker information, og gør brug af tvivlsomme it-firmaer, skal afklares, er det ikke tilstrækkeligt med klassificerede diskussioner i folketingsudvalg eller i forsvaret. Det kræver, at Udenrigsministeriet kommer på banen og afklarer de muligheder og risici, som en udenrigs- og sikkerhedspolitisk brug af cyberkapacitet medfører. Det kræver, at Erhvervsministeriet, private virksomheder og ikke-statslige organisationer får mulighed for at bidrage med deres bekymringer om en øget sikkerhedspolitisk tilstedeværelse i cyberspace. Og det kræver, at det danske forsvar afgiver noget af det ejerskab over de offensive cyberkapacite-

ter, som lige nu kun indgår i den militære værktøjskasse. Dette kræver måske endda et nyt juridisk grundlag for en bredere brug af de kompetencer, som lige nu sidder i Forsvarets Efterretningstjeneste (Liebetrau, 2020).

Åbenhed og politisk diskussion om disse afvejninger – herunder også om de operative, juridiske og strategiske erfaringer som Danmark har gjort sig i sin hidtidige brug af cyberoperationer – er nødvendig, hvis Danmark i dag skal tages seriøs som ledende normentreprenør i cyberspace. Men diskussionerne og afvejningerne kan samtidig meget vel betyde, at Danmark må acceptere, at man ikke kan stå lige stejlt på samtlige værdipolitiske, økonomiske og sikkerhedspolitiske elementer i den nuværende vestlige normfremmestrategi på samme tid. En småstat som Danmark bør prioritere, hvilken cybernorm man ønsker at være primær repræsentant for. Det kunne være en norm, der forsvarer civil borgeres online frihedsrettigheder globalt. Eller en afklaring af, hvordan stater juridisk bør vurdere internationale principper, som for eksempel proportionalitet og diskrimination, når de agerer i fremmed netværk. Eller det kunne være en norm med henblik på at udvikle et seriøst internationalt samarbejde, der skal forhindre og efterforske cyberkriminalitet på tværs af grænser.

Formår Danmark faktisk at levere fokuserede og prioriterede hvidbøger om officielle retningslinjer for og juridiske afklaringer på ovennævnte spørgsmål, er det dog kun det første skridt hen imod konsoliderede og ultimativt internaliserede internationale cybernormer. Det virkelige diplomatiske arbejde starter først, når de danske positioner skal promoveres internationalt. På trods af at der mangler konkrete referencepunkter for ansvarlig statslig adfærd i cyberspace, er det langt fra sikkert – hvis ikke direkte usandsynligt – at andre stater, der præsenteres for de danske fortolkninger og konklusioner, bare accepterer og internaliserer disse. Her er ligesindede lande i Norden og andre små digitaliserede og cyberfokuserede lande som Estland og Holland oplagte samarbejdspartnere.

det kræver en vedholdende diplomatisk indsats at argumentere overbevisende for de danske positioner og afvejninger i bredere fora. Og overtalelse er ikke nødvendigvis et tilstrækkeligt værktøj

Men det kræver en vedholdende diplomatisk indsats at argumentere overbevisende for de danske positioner og afvejninger i bredere fora. Og overtalelse er ikke nødvendigvis et tilstrækkeligt værktøj. Den bredere værktøjskasse må sandsynligvis også i spil. I nogle bilaterale relationer vil dansk cybernormfremme således med fordel kunne sammentænkes med handelssamarbejder, i forsøget på at skabe incitamentsstruktur. Og i andre tilfælde vil organisatorisk og teknisk kapacitetsopbygning i partnerlande – "socialisering", som Hollis (2017) kalder det – kunne vise sig fordelagtig for cybernormfremmen. Sådanne danske strategier vil selvsagt komme til kort over for stormagter som

Rusland og Kina. Men over for den store mængde af uafklarede stater, hvor størstedelen i øjeblikket læner sig mod den russisk-kinesiske tilgang i diverse cyberfora, vil veltilrettelagte incitaments- eller socialiseringsstrategier kunne påvirke den interne formning af normerne for statslig adfærd i cyberspace.

Men selv hvis den danske regering beslutter sig for at give udenrigspolitikken det tilstrækkelige ressourceløft til, at ovenfornævnte normfremmeindsatser kan lade sig gøre, er det umuligt at styre, hvordan de danske cybernormer vil blive fortolket og genfortolket. Amitav Acharya (2004) viser eksempelvis, hvordan indoptagelsen af en norm aldrig er passiv, men afhænger af den lokale, normative kontekst, hvori normfortolkningerne foregår, og som de transnationale normer skal tilpasses til. Og Charlotte Epstein (2012) viser, hvordan normfremme ofte indeholder en "infantilisering" af de aktører, hvis adfærd der ønskes ændret eller påvirket, med det resultat, at nye positioner kan opstå i modsætning til normentreprenørens oprindelige dagsorden. I kontekst af dansk cybernormfremme er fuldgruberne således mange og uforudsigelige. Der vil således altid være en risiko for, at partnerlande vil bruge de kompetencer, som dansk cyberkapacitetsopbygning har leveret, på en måde som Danmark anser for uansvarligt. Om det så drejer sig om overvågning af dissidenter, industrispionage, spredning af misinformation eller accept af cyberkriminalitet, må tiden vise. Danmark må være villig til at acceptere disse risici, hvis man vil være normentreprenør i cyberspace.

Dansk diplomati i kampen mod en balkanisering af internettet

Forhandlingerne om ansvarlig statslig adfærd i cyberspace står i stampe. Denne artikel lokaliserede de vedholdende beskyldninger om vestlig hykleri som et kerneproblem for den vestlige koalitions manglende evne til at skabe fremskridt. Frem for det vestlige diplomatis sproglige finurligheder i diverse forhandlingsrunder, argumenterede artiklen for, at en begyndende anerkendelse og åbenhed om de praktiske implikationer af en dominerende efterretningsnorm i cyberspace er et skridt i den rigtige retning. I lyset heraf pegede artiklen også på, at Danmark har gode muligheder for at påtage sig rollen som normentreprenøren, der deler erfaringer og politiske afklaringer og derved påvirker cybernormdagsordenen fremadrettet. Men det kræver politiske investeringer, kompromisvillighed, vedholdenhed og ikke mindst mod.

Og der er meget på spil. Risikoen ved *ikke* at gøre noget kan meget vel være en balkanisering af internettet – hvad Chris C. Demchak og Peter Dombrowski (2011) har kaldt fremkomsten af et "cybered Westphalia". Det betyder, at stater sandsynligvis vil kunne tilegne sig fuld kontrol med alt det data, der opbevares på eller rejser igennem servere på deres suveræne territorier, men det betyder også, at informations- og kommunikationsteknologier ikke nødvendigvis længere er kompatible på tværs af grænser eller regioner. Resultatet vil blive ét kinesisk internet, ét russisk internet, ét europæisk internet og ét amerikansk internet. Og vi oplever allerede den geopolitiske kamp om forskellige standarder, leverandører og – mere fundamentalt – forståelser af

dataejerskab udspille sig på relaterede områder som kunstig intelligens og 5G. En sikkerhedspolitisk konkurrencelogik og den dertilhørende balkanisering er ikke blot skadeligt for de økonomiske bånd mellem stormagter og den globale økonomi i bredere forstand, men en opsplitning af den digitale verden risikerer også at fostre mistillid og ustabilitet.

Noter

1 I denne artikel dækker "den vestlige koalition" over USA, Canada, Australien og New Zealand samt størstedelen af de europæiske lande. Trods interne uenigheder arbejder denne gruppe af lande ofte sammen og forsøger at skabe fælles positioner i eksempelvis FN.

2 For en gennemgang af ikke-vestlige, ikke-liberale aktører som normentreprenører, se Carmen Wunderlich (2020).

Bibliografi

Acharya, A. (2004), "How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism", *International Organization*, 58(2): 239–75.

Ambastha, M. (2019), "Taking a Hard Look at the Vulnerabilities Equities Process and its National Security Implications", *Berkeley Technology Law Journal*, 23. april, https://btlj.org/2019/04/taking-a-hard-look-at-the-vulnerable-equities-process-in-national-security/.

Björkdahl, A. (2002), *From idea to norm: promoting conflict prevention*, Lund: Lund University.

Bond, D. og D. Sevastopulo (2018), *US and UK accuse China of cyber espionage campaign*, *Financial Times*, www.ft.com/content/f5f0b42c-046c-11e9-99df-6183d3002ee1

Buchan, R. (2020), "When More is Less: The US Department of Defense's Statement on Cyberspace", *EJIL: Talk!*, 30. marts, www.ejiltalk.org/when-more-is-less-the-department-of-defenses-statement-on-cyberspace/.

Buchanan, B. (2017), *The Cybersecurity Dilemma – Hacking, Trust, and Fear Between Nations*, New York: Oxford University Press.

Buchanan, B. (2020), *The hacker and the state cyber attacksand the new normal of geopolitics*, Cambridge, MA og London: Harvard University Press.

Christensen, K.K. og T. Liebetrau (2019), "A new role for "the public"? Exploring cyber security controversies in the case of WannaCry", *Intelligence and National Security*, 34(3): 395–408.

Clinton, H. (2010), "Remarks on Internet Freedom". The Newseum, Washington D.C., 21. januar, 2009-2017. state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

Conti, G. og D. Raymond (2017), *On cyber: towards an operational art for cyber conflict*, New York: Kopidion Press.

Crandall, M. og C. Allan (2015), "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms", *Contemporary Security Policy*, 36(2): 346–68.

Crosston, M.D. (2011), "World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence", *Strategic Studies Quarterly*, 5(1): 100–16.

Cyber Command (2018), *Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command*, www.hsdl.org/?abstract&did=812923.

Daniel, M. (2014), "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities, White House Blog", https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

Demchak, C.C. og P. Dombrowski (2011), "Rise of a Cybered Westphalian Age", *Strategic Studies Quarterly*, 5(1): 32–61.

Epstein, C. (2012), "Stop Telling Us How to Behave: Socialization or Infantilization?", *International Studies Perspectives*, 13(2): 135–45.

Erskine, T. og M. Carr (2016), "Beyond "Quasi-Norms": The Challenges and otential of Engaging with Norms in Cyberpspace", i A.-M. Osula og H. Rõigas, red., *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn: NATO CCD COE Publications, pp. 87–109.

EU Commission (2017), "How digital is your country? Europe improves but still needs to close digital gap". European Commission – Press Release, http://europa.eu/rapid/ press-release_IP-17-347_en.htm.

Farrell, H. og M. Finnemore (2013), "The End of Hypocracy", *Foreign Affairs*, 92(6): 22–6.

Finnemore, M. og D.B. Hollis (2016), "Constructing Norms for Global Cybersecurity", *The American Journal of International Law*, 110(3): 425–79.

Finnemore, M. og K. Sikkink (1998), "International Norm Dynamics and Political Change", *International Organization*, 52(4): 887–917.

Fischerkeller, M.P. og R.J. Harknett (2017), "Deterrence is Not a Credible Strategy for Cyberspace", *Orbis*, 61(3): 381–93.

Forsvarsakademiet (2019), *Værnsfælles Doktrin for Militære Cyberspaceoperationer*, København: Forsvarsakademiet.

Greenwald, G. og E. MacAskill (2013), "Boundless Informant: the NSA's secret tool to track global surveillance data", *The Guardian*, 11. juni, www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining.

Grigsby, A. (2017), "The End of Cyber Norms", *Survival*, 59(6): 109–22.

Grigsby, A. (2018), "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased", *CFR Blog*, 15. november, www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

Harold, S.W., M.C. Libicki og A.S. Cevallos (2016), *Getting to Yes with China in Cyberspace:* Santa Monica, CA: RAND, www.rand.org/pubs/research_reports/RR1335.html.

Henriksen, A. (2019), "The end of the road for the UN GGE process: The future regulation of cyberspace", *Journal of Cybersecurity*, 5(1): 1–9.

Hollis, D.B. (2017), *China and the US Strategic Construction of Cybernorms: The Process Is the Product*, Aegis Paper Series No. 1704, Stanford University.

Hurel, L.M. og L.C. Lobato (2018), "Unpacking cyber norms: private companies as norm entrepreneurs", *Journal of Cyber Policy*, 3(1): 61–76.

Ingebritsen, C. (2002), "Norm Entrepreneurs – Scandinavia's Role in World Politics", *Cooperation and Conflict*, 37(1): 11–23.

Ingebritsen, C. et al., red. (2006), *Small states in international relations*, Seattle, WA: University of Washington Press.

Jacobsen, J.T. (2018), "En" digital Genèvekonvention" er ikke i Danmarks interesse", *Internasjonal Politikk*, 76(2): 73–88.

Jacobsen, J.T. (2019), "NATOs offensive cyberspaceoperationer. Muligheder og udfordringer ved NATOs forespørgselsdrevne og effektbaserede tilgang", *Internasjonal Politikk*, 77(3): 241.

Jacobsen, J.T. (2020), "Lacan in the US cyber defence: Between public discourse and transgressive practice", *Review of International Studies*, First View, 1–19.

Jacobsen, J.T. og J. Ringsmose (2017), "Cyber-bombing ISIS: why disclose what is better kept secret?", *Global Affairs*, 3(2): 125–37.

Jasper, S. (2015), "Deterring Malicious Behavior in Cyberspace", *Strategic Studies Quarterly*, 9(1): 60–85.

Joyce, R. (2017), "Improving and Making the Vulnerability Equities Process Transparent is the Right Thing to Do", *Whitehouse.gov*, 15. november, www.whitehouse.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/.

Katzenstein, P.J. (1996), "Introduction: Alternative perspectives on national security", i P.J. Katzenstein red., *The culture of national security: Norms and identity in world politics*. New York, NY: Colombia University Press, pp. 1–32.

Kello, L. (2017), *The virtual weapon and international order*, New Haven og London: Yale University Press.

Klipstein, M. (2019), "Seeing is Believing: Quantifying and Visualizing Offensive Cyber Operations Risk", *The Cyber Defense Review*, 4(1): 85–106.

Klotz, A. (1995), *Norms in international relations: the struggle against apartheid*, Ithaca: Cornell University Press.

Libicki, M. (2017), "The Coming of Cyber Espionage Norms", i Rõigas, H. et al., red., *9th International Conference on Cyber Conflict. Proceedings 2017*, Tallinn: NATO CCD COE Publications, pp. 7–24.

Liebetrau, T. (2020), *Dansk offensiv cybermagt mellem angreb, spionage og forsvar: En komparativ analyse på tværs af Europa*, Københavns Universitet: Center for Militære Studier, 50.

Maurer, T. (2019), "A Dose of Realism: The Contestation and Politics of Cyber Norms", *Hague Journal on the Rule of Law*.

Meyer, P. (2020), "Norms of Responsible State Behaviour in Cyberspace", i M. Christen, B. Gordijn og M. Loi, red. *The Ethics of Cybersecurity*. Cham: Springer International Publishing, pp. 347–60.

Microsoft (2015), "International Cybersecurity Norms – Reducing conflict in an Internet-dependent world", www.microsoft.com/en-us/cybersecurity/content-hub/reducing-conflict-in-Internet-dependent-world.

Nakashima, E. (2016), "Obama to be urged to split cyberwar command from NSA", *Washington Post*, 13. september.

Nakashima, E. (2019), "U.S. Cyber Command operation disrupted internet access of Russian troll factory on day of 2018 midterms", *Washington Post*, 27. february.

Neutze, J. og J. P. Nicholas (2013), "Cyber Insecurity: Competition, Conflict, and Innovation Demand Effective Cyber Security Norms", *Georgetown Journal of International Affairs*, 3–15.

Obama, B.H. (2011), *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington D.C.: The White House Office.

Price, R.M. og N. Tannenwald (1996), "Norms and deterrence: The nuclear and chemical weapons taboos", i P. J. Katzenstein, red. *The culture of national security. Norms and identity in world politics*. New York, NY: Colombia University Press, pp. 114–52.

Regeringen (2018), "National strategi for cyber- og informationssikkerhed 2018-2021", Regeringen.

Risse, T., S.C. Ropp og K. Sikkink, red. (1999), *The power of human rights: international norms and domestic change*. Cambridge: Cambridge University Press.

Ruhl, C. et al. (2020), "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads", *Working Paper*, Washington D.C.: Carnegie Endowment for International Peace,. 32.

Sanger, D.E. (2013), *Confront and conceal: Obama's secret wars and surprising use of American power*, New York: Broadway Paperbacks.

Sanger, D.E. (2018), *The perfect weapon: war, sabotage, and fear in the cyber age*, New York: Crown Publishers.

Schmitt, M. (2020), "The Defense Department's Measured Take on International Law in Cyberspace, Just Security", www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/.

Segal, A. (2016), "The U.S.-China Cyber Espionage Deal One Year Later, Council on Foreign Relations", *Net Politics Blog*, www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.

Sheehan, M. (2014), "China Mocks U.S. 'Hypocrisy' On Hacking Charges", *Huffington Post*, www.huffpost.com/entry/china-cyber-spying_n_5356072.

Simonite, T. (2012), "Stuxnet Tricks Copied by Computer Criminals", *MIT Technology Review*, www.technologyreview.com/2012/09/19/115189/stuxnet-tricks-copied-by-computer-criminals/.

Smeets, M. (2017), "Organisational integration of offensive cyber capabilities: A primer on the benefits and risks", i *2017 9th International Conference on Cyber Conflict (CyCon)*. IEEE, 1–18.

Smith, B. (2017), "The need for a Digital Geneva Convention", *Microsoft Blog*, 14. februar, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Smith, B. (2018), "34 companies stand up for cybersecurity with a tech accord", *Microsoft Blog*, 17 April, https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord/.

Steinmetz, R. og A. Wivel, red. (2010), *Small States in Europe: Challenges and Opportunities*, Farnham: Ashgate.

Tarp, M.N. og J.O.B. Hansen, (2013), "Size and Influence. How small states influence policy making in multilateral arenas", *DIIS Working Paper* 11. København: Dansk Institut for Internationale Studier

Trump, D.J. (2018), "National Cyber Strategy of the United States of America", The White House.

Vavra, S. (2019), "NATO cyber-operations center will be leaning on its members for offensive hacks, CyberScoop", www.cyberscoop.com/nato-cyber-operations-offensive-hacking-neal-dewar/.

Wang, L. (2019), "Speech by WANG Lei, Coordinator for Cyber Affairs, at the 6th World Internet Conference, Ministry of Foreign Affairs of the People's Republic Of China", www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/t1710346.shtml.

Waxman, M. (2018), "U.K. Outlines Position on Cyberattacks and International Law", *Lawfare blog*, www.lawfareblog.com/uk-outlines-position-cyber attacks-and-international-law.

Wiener, A. (2008), *The Invisible Constitution of Politics: Contested Norms and International Encounters*, Cambridge: Cambridge University Press.

Wunderlich, C. (2020), *Rogue states as norm entrepreneurs: black sheep or sheep in wolves' clothing?* Cham: Springer.