Fagfellevurdert

Internasjonal POLITIKK
Skandinavisk tidsskrift for Internasjonale Studier

Årgang 76, Nummer 2, side 73–88, 2018, ISSN 1891-5580, www.tidsskriftet-ip.no, Publisert mai 2018

# En "digital Genèvekonvention" er ikke i Danmarks interesse.[1]

Jeppe Teglskov Jacobsen
*Danish Institute for International Studies (DIIS)*

**Sammendrag**

Selvom Danmark såvel som de fleste andre småstater har interesse i bedre it-sikkerhed og juridisk klarhed i cyberspace, er Microsofts forslag om en åbning af forhandlingerne om en bred digital konvention for staters adfærd i cyberspace langt fra i dansk interesse. En åbning risikerer ikke blot at genåbne allerede vedtaget internationale aftaler og underminere eksisterende, ikke-bindende drøftelser om emnet, men ignorerer også de sikkerhedspolitiske gevinster som stater legitimt forfølger i cyberspace. Det betyder dog ikke, at en småstat som Danmark blot må forholde sig passivt på det cyberpolitiske område. Tværtimod. Den politiske uklarhed, der stadig omringer cyberspace, giver småstater mulighed for at "punch above their weight". Således vil et øget danske cyberengagement i EU, NATO, FN og i ikke-statsdrevne forhandlingsfora samt et målrettet samarbejde med både danske og udenlandske virksomheder styrke Danmarks position internationalt og ultimativt sikkerheden i cyberspace.

**Nøgleord:** cyberspace; Microsoft; cyberdiplomati; international ret; småstater

[1]En tidligere version af denne artikel er blevet udgivet som Policy Brief på Forsvarsakademiet: http://www.fak.dk/publikationer/Documents/Prioritising%20Denmark%27s%20Cyber%20Policy.pdf


*Citation: Jeppe Teglskov Jacobsen (2018). «En "digital Genèvekonvention" er ikke i Danmarks interesse». Internasjonal Politikk, 76, 2: 73–88. http://dx.doi.org/10.23865/intpol.v76.1041*

## Indledning

Vi har i den seneste tid set en markant stigning i antallet af episoder, hvor kriminelle ved hjælp af malware har krypteret virksomheders computere og krævet løsesum for at gøre det krypterede data tilgængelig for virksomhederne igen. Denne gidselstagningsteknik, kendt under betegnelsen *ransomware*, kom for alvor i den internationale offentligheds søgelys, da det britiske sundhedsvæsen, NHS, i maj 2017 blev ramt af det verdensomspændende WannaCry-angreb. Da Mærsk en måned senere oplevede omfattende forstyrrelser forårsaget af et lignende angreb, NotPetya, spærrede også danskerne for alvor øjnene op for denne trussel. Hændelserne forekommer særlige, fordi de involverer teknikker til udnyttelse af it-sårbarheder udviklet af National Security Agency (NSA), og fordi disse sårbarheder blev lækket i april i år. NSA har i forlængelse heraf mødt megen kritik for at have udviklet og lagret teknikker, der gør både civile borgere og virksomheder sårbare over for ikke blot ransomware, men alle former for cyberangreb – en kritik NSA-direktør Michael S. Rogers har afvist (Starks 2017). Kritikken fra især den private sektor går på, at NSA i stedet bør arbejde tættere sammen med eksempelvis Microsoft om at gøre cyberspace så sikkert som muligt.

Med udgangspunkt i denne kritik opfordrede Microsofts direktør og chefjurist Brad Smith allerede inden WannaCry til, at der udvikles en "digital Genèvekonvention", en opfordring, der siden hen er blevet præsenteret i både FN og EU og har mødt stor offentlig opbakning (Smith 2017; Microsoft 2017; Kaspersky 2017; Meyer & Stauffacher 2017; UNOG 2017; Neutze 2017). Kort fortalt indeholder Microsofts forslag til en digital konvention 1) et forbud for stater mod at kompromittere private virksomheder og kritiske infrastrukturer, 2) et påbud om, at stater skal samarbejde med den private sektor om at identificere og håndtere it-sårbarheder og cyberhændelser, samt 3) en begrænsning af staters oprustning af cybervåben. Egentlig er Microsofts brug af "Genève" en smule misvisende, da Genèvekonventioner normalt er noget, der udelukkende regulerer krig og ikke staters adfærd mere generelt. Microsofts forslag til en digital konvention er altså mere end blot en regulering af cyberkonflikt, og det består af en nedrustningsaftale, et civilt-militært samarbejde og oprettelsen af et internationalt organ, der skal attribuere cyberangreb. En "digital konvention om staters adfærd i cyberspace" fremfor en "digital Genèvekonvention" havde således været mere retvisende og mindre forvirrende (Minárik & van der Meij 2017) – men måske også mindre fængende.

Det ændrer dog ikke ved, at stater ikke kan sidde Microsofts forslag overhørig. Stater er i dag dybt afhængige af de private teknologivirksomheder, der ejer langt størstedelen af den digitale infrastruktur. Det er således forståeligt, at der både i den politiske og akademisk debat om international cybersikkerhed generelt er enighed om, at den private sektor og NGO'er nødvendigvis må inddrages i politikudviklingen i cyberspace. Dette understreges eksempelvis af de seneste års eksplosive vækst i brugen af begreber som offentligt-privat partnerskab og multistakeholdermodel,

når der skal introduceres løsninger på udfordringerne fra cyberspace (Nye 2014; Carr 2016; Muller 2016). I en situation hvor sammenkoblingen mellem offentlig og privat er uundgåelig, er det nødvendigt, at stater såvel som ikke-statslige aktører forstår den politiske og tekniske kontekst, hvori Microsofts forslag om en international digital konvention er blevet fremsat. Dette er afgørende for, at en fremtidig dialog kan ske på et oplyst grundlag. Artiklens første formål er således at bidrage til et sådant grundlag ved at vurdere Microsofts forslag samt de politiske og tekniske realiteter, som forslaget skal navigere i. Med andre ord, understreger artiklen en velkendt pointe om, at de juridiske ambitioner om en international konvention altid – og således også i cyberspace – foregår på en international politisk kampplads (Reus-Smit 2004).

Ved første øjekast har en småstat som Danmark fordel af, at der internationalt skabes mere juridisk klarhed om staters adfærd i cyberspace. Juridiske rammer er de facto det bedste redskab, hvormed småstater kan holde store stater til ansvar for deres handlinger. Den store udbredelse af it gør ydermere, at Danmark også har interesse i, at produkter fra fx Microsoft, Siemens, Apple, IBM er så sikre som muligt. En generel forbedring af it-sikkerheden begrænser nemlig alle andre staters evne til at spionere mod og angribe via cyberspace. Forhandlinger om en generel konvention om staters adfærd i cyberspace er imidlertid ikke nødvendigvis den mest hensigtsmæssige tilgang for stater som Danmark, der normalt efterspørger international juridisk klarhed. Jeg peger i artiklen på fire hovedargumenter, der gør det politisk og teknisk ufornuftigt at forfølge tanken om en digital "Genèvekonvention":

1. Åbningen af en forhandlingsproces i FN-regi vil med al sandsynlighed føre til diplomatiske drøftelser om emner, som stater, der ønsker et åbent og frit internet, helst ikke ser genåbnet.
2. Åbningen af en forhandlingsproces risikerer at underminere de igangværende formelle og uformelle drøftelser om international ret i cyberspace.
3. Åbningen af en forhandlingsproces strander efter al sandsynlighed på, at en række stater ikke ønsker at afgive muligheden for at udnytte it-sårbarheder til at fange kriminelle, forhindre terrorisme og generel spionage.
4. En digital konvention for staters adfærd i cyberspace er vanskelig at håndhæve.

Disse argumenter betyder imidlertid ikke, at Danmark blot må afholde sig fra at agere på det cyberpolitiske område. Det fører til artiklens andet formål. Den verserende akademiske debat om småstaters mulighed for at "punch above their weight" peger hovedsageligt på specifik ekspertise, internationalt renommé, økonomisk kapacitet eller diplomatiske evner som nøgleforklaringerne (Neumann & Gstöhl 2006; Steinmetz & Wivel 2010; Tarp & Hansen 2013). Anden halvdel af nærværende artikel bygger videre på disse idéer og tager som afsæt, at den til stadighed spæde klarhed om de politiske rammer i cyberspace muliggør, at småstater stadig kan få relativt stor indflydelse på, hvordan politikken på dette område udvikler sig (Crandall & Allan

2015; Nye 2010; Austin 2014). Jeg peger på, at dette i Danmarks tilfælde kræver en styrket indsats på det udenrigs-, forsvars og erhvervspolitiske område.

Lad mig dog først kritisk gennemgå Microsofts forslag om en digital "Genèvekonvention".

## Hvem kan bebrejdes for WannaCry og NotPetya?

Inden vi ser på de eventuelle udfordringer ved en forhandling om en konvention for statslig adfærd i cyberspace, er det værd at kaste et blik på, hvem der kan bebrejdes for forårets ransomwarehændelser samt den utilstrækkelige it-sikkerhed mere generelt. Et sådant blik understreger nemlig, at Microsofts forslag til en konvention kun adresserer én enkelt og selektiv del af problemet.

Den aktør, som har været genstand for mest kritik i forbindelse med ransomwarehændelserne, er NSA. NSA fandt en fejl i Microsoft Windows, udviklede teknikker til at udnytte denne fejl og gemte eller brugte herefter teknikken i sin indhentningsvirksomhed. Det er vanskeligt at kritisere NSA for at gøre det job, som myndigheden er sat i verden for, men en række forhold gør alligevel, at NSA ikke går fri for kritik. For det første er det uklart, om de it-sårbarheder, som blev udnyttet, faktisk har været underlagt den amerikanske procedure, der skal afgøre, om en sårbarhed skal gemmes eller deles med henblik på udbedring (Schwartz & Knake 2016). Da proceduren er klassificeret, er det imidlertid umuligt at vide, hvor brugbar teknikken egentlig var for NSA's indhentningsaktivitet. Kritikken strander således her indtil videre (Knake 2017). Lettere er det at bebrejde NSA for den manglende evne til at undgå lækager. Brad Smith sammenlignede WannaCry med en situation, hvor USA's militær mistede et tomahawkmissil (Guardian Staff 2017). Analogien illustrerer ikke, at der nødvendigvis er et behov for at fjerne tomahawkmissiler eller cybervåben fra USA's våbenarsenal, som Smith ellers insinuerer, men blot et behov for mere og bedre kontrol og sikkerhed omkring opbevaring af disse.

NSA er langt fra den eneste, der kan bebrejdes for ransomwarehændelserne. Det er indlysende, at it-kriminelle og The Shadow Brokers, gruppen, som lækkede NSA-teknikkerne, også spiller en central rolle. Mere interessant er det imidlertid, at Microsoft, de berørte virksomheder og tilhørende it-administratorer samt i sidste ende diverse regeringer også kan bebrejdes, at eksempelvis ransomware har udviklet sig til en så alvorlig sikkerhedsudfordring, som tilfældet er. Langt de fleste virksomheder er i dag afhængige af it-systemer. Det er i sig selv ikke et problem. Problemet opstår, når selvsamme virksomheder flere steder i deres it-infrastruktur har gamle og ikke længere understøttede styresystemer, såsom Windows XP, installeret på deres maskiner. Eller endnu værre: når it-administratorerne ikke har installeret opdateringer for gældende systemer. Det er WannaCry-episoden et eksempel på: Halvanden måned *før* WannaCry udsendte Microsoft en opdatering til sine understøttede styresystemer, som rettede den fejl, NSA indtil da sandsynligvis havde udnyttet. Virksomhederne lærte med andre ord på den hårde måde, at der er behov for grundigere

forståelse af og investering i egen it-infrastruktur, hvis man vil minimere risikoen for ransomware og andre mere alvorlige cyberangreb.

Større investeringer i it-sikkerhed sikrer dog aldrig fuldstændig en virksomhed mod cyberindbrud og -forstyrrelser. Det skyldes, at software sjældent udelukkende gør det, som programmøren eller administratoren ønsker. Programmering og installering af it-systemer er en kompleks opgave, ligesom brugere af it-systemer oftest er uforsigtige i deres omgang med vedhæftede filer, links og lignende. Således er det næsten umuligt at undgå, at udefrakommende personer – uden autorisation – kan få adgang til eller påvirke et it-system.

Det betyder, at de it-virksomheder, som udvikler mange af de styresystemer, applikationer og hardware, vi i dag er afhængige af, også bærer en del af skylden. Microsoft programmerede den fejlbehæftede kode, som NSA og personerne bag WannaCry og NotPetya udnyttede. Softwarefirmaer har modsat medicinal- og bilindustrien intet juridisk ansvar for at sikre, at det produkt, de sender på markedet, er sikkert. Det betyder, at Microsoft har udviklet en forretningsmodel, hvor man løbende sender nye styresystemer på markedet og kun opdaterer de nye produkter og undlader at fortsætte opdateringen af gamle, fejlbehæftede systemer. Det bidrager til problemets omfang. Det rejser spørgsmålet om, hvorvidt Microsoft ikke også kan bebrejdes for ikke i tilstrækkelig grad at beskytte de kunder, som virksomheden har solgt sine produkter til, men som ikke har økonomisk mulighed for at investere i det nyeste, understøttede styresystem.

Microsofts ønske om en digital Genèvekonvention, som skal beskytte civile mod staters uforsvarlige brug af cyberspace, kan anskues fra en anden vinkel end den, Microsoft fremstiller. En digital Genèvekonvention i den form, Microsoft forestiller sig, gengiver kun én version af virkeligheden. Denne version ignorerer, at Microsoft, Google og andre techgiganter fortsat kun har incitament til at investere i udbedringen af fejl og sårbarheder, hvis det vurderes at øge deres samlede økonomiske profit. Uden statslig kompromittering af deres it-systemer har de store techgiganter mindre incitament til at udvikle teknikker og praksisser, der gør programmering bedre fra starten. Derudover skal virksomhedernes profitkalkule tænkes ind. Flere techvirksomheder som fx Microsoft tjener penge på at tilbyde it-sikkerhedsservicer, som i sidste ende beskytter mod bl.a. Microsofts manglende evne til i første omgang at sikre sit eget produkt (Morozov 2017). Hvis Microsoft virkelig ønsker, at techvirksomheder skal være et nyt Røde Kors, som Brad Smith foreslår i sit blogindlæg (Smith 2017), indebærer det, at virksomhedernes "for profit-model" gentænkes.

Det bringer mig til den sidste spiller, der bebrejdes for ransomwarehændelserne og for den generelt utilstrækkelige it-sikkerhed: staterne. Ifølge Microsoft løber staterne fra deres ansvar ved ikke at være nået til enighed om et sæt internationale retningslinjer, som begrænser udnyttelsen af sårbarheder i kommercielle it-systemer, og som pålægger staterne at samarbejde med hinanden og med virksomheder om at styrke it-sikkerheden. Derudover begynder flere og flere uafhængige stemmer i det

it-tekniske miljø at pege på, at staterne bør tage ansvar for at regulere de markedsfejl, der gør det muligt for dårligt programmeret software uhindret at flyde frit rundt på markedet (Schneier 2017). Staterne har tydeligvis ikke i tilstrækkelig grad investeret i og implementeret standarder, der opstiller retningslinjer for, hvornår et produkt er markedsklart. De har ikke – som det ellers er tilfældet på mange andre områder, herunder medicinal- og fødevareområdet – investeret i en myndighed, der kan undersøge og udstille usikre produkter og virksomheder.

Jeg er i dette afsnit tilgået Microsofts forslag om en digital Genèvekonvention fra en lidt bredere vinkel og har dermed vist, at det er udtryk for snæversyn at udråbe staten og dens efterretningstjeneste til syndebuk. Jeg har desuden vist, at det er utilstrækkeligt at pege på en løsning, der udelukkende omfatter stater, deres diplomater og internationale jurister. Det betyder imidlertid ikke, at klarhed omkring de juridiske retningslinjer for statslig adfærd i cyberspace ikke er at ønske. Folkeretten skaber i teorien forudsigelighed og værktøjer til at straffe eller "shame" aktører, når de bryder med de vedtagne regler. Det er godt for de virksomheder og regeringer, der søger stabilitet og status quo internationalt. Men alt imens klarere juridiske rammer i udgangspunktet er ønskværdige, så er idéen om at åbne forhandlingerne om en digital konvention for statslig adfærd uhensigtsmæssig. Det skyldes først og fremmest, at internationale juridiske diskussioner aldrig kan afkobles fra de politiske, praktiske og tekniske realiteter, hvori de foregår. Dette illustreres med fire argumenter for, hvorfor en digital "Genèvekonvention" er en dårlig idé for de lande, der ellers normalt er positive overfor internationale normer og ønsker et frit og åbnet internet:

1. den ignorerer de diplomatiske vanskeligheder, som en sådan åbning indebærer.
2. den de facto underkender potentialerne i de eksisterende formelle og uformelle drøftelser af international ret i cyberspace.
3. den tager ikke hensyn til, at statens udnyttelse af it-sårbarheder også kan gavne den nationale sikkerhed.
4. den overvurderer juraens magt i relation til de praktiske og tekniske håndhævelsesudfordringer, som cyberspace i øjeblikket byder på.

Lad mig se nærmere på disse fire punkter.

## Pandoras æske

Microsofts idé om en digital Genèvekonvention hviler på en antagelse (eller måske et naivt håb?) om, at konventionsforhandlinger i FN blot handler om, at stater møder op og skriver under på de principper og regler, som USA (eller Microsoft) ønsker at knæsætte. Sådan udfolder en diplomatisk forhandling sig selvsagt ikke, og i det konkrete tilfælde har USA, EU-landene og flere andre ligesindede i flere år kæmpet aktivt *imod* åbningen af en diskussion om en ny, bred konvention på det digitale område. Denne gruppe af "allierede" ønsker at tilpasse staters adfærd i cyberspace til eksisterende internationale rammer, og staterne har derfor forhandlet om separate

resolutioner på delelementer af det digitale område, eksempelvis menneskerettigheder og privatlivets fred.

Det følger således af logikken om ikke at slå for stort brød op, at EU og USA – fremfor en ny konvention – forsøger at få flere og flere lande til at skrive under på og videreudvikle den allerede eksisterende, omend forældede, Budapestkonvention for cyberkriminalitet fra 2001. Det skyldes først og fremmest, at "den vestlige koalition" generelt i FN-afstemninger ikke længere kan tage for givet, at de har flertal, og dermed ikke blot kan presse deres egen dagsorden igennem. En åbning af forhandlingerne om en ny digital konvention, som lande som Rusland og Kina har presset på for i årevis, vil betyde en (gen)åbning af en række emner, som de fleste vestlige lande ikke ønsker at drøfte i et interstatsligt forum. Det drejer sig eksempelvis om styringen af internettets protokoller (internet governance), som Vesten i årevis har kæmpet for at regulere gennem et samarbejde med private, frivillige, nonprofitorganisationer og virksomheder og ikke FN – den såkaldte multistakeholdermodel (Muller 2016). Omvendt vil Kina og Rusland efter al sandsynlighed betragte Smiths forslag om en digital Genèvekonvention som en kærkommen mulighed for at genåbne drøftelserne om ytringsfrihed og andre fundamentale menneskerettigheder online samt om, hvorvidt Genèvekonventionerne overhovedet kan gælde i cyberspace (Henriksen 2017: 156-8).

Diplomatiske forhandlinger af denne karakter er med andre ord langsommelige og komplekse, og det er vanskeligt at forudse, hvorvidt et forslag til en konventionstekst ender med det ønskede resultat. Det betyder, at selvom Microsofts anbefalinger til principper for statslig adfærd online givetvis forbedrer it-sikkerheden, er en færdigforhandlet digital konvention ikke nødvendigvis til gavn for Microsoft og andre it-virksomheder (eller vestlige stater generelt). Konventionsforhandlingerne kan meget vel resultere i øget statslig kontrol med data, som for nuværende befinder sig i hænderne på private virksomheder og udgør en vigtig del af virksomhedernes nuværende og fremtidige vækstgrundlag. Det kan derfor heller ikke afvises, at det vil lykkes et flertal af stater i FN at give virksomheder øget juridisk (erstatnings)ansvar, når de udvikler fejlbehæftet software. Begge dele er tidligere blevet luftet i internationale fora (FN's Generalforsamling 2015a), og det er noget, især amerikanske virksomheder har kæmpet imod med henvisning til, at det går ud over væksten i it-sektoren (Goertzel 2016).

Langsommeligheden i store internationale forhandlingsprocesser kan i dette tilfælde også betyde, at den teknologiske udvikling konstant overhaler forhandlingerne. Inertien gør det usandsynligt, at stater ønsker at lukke de forskellige kapitler løbende, hvormed man frasiger sig muligheden for at opnå en trinvis udvikling af de juridiske rammer. Forbrugere og virksomheder vil derfor i mange år skulle gå og vente på, at staterne når til enighed om alle artikler i en ny konvention.

## Eksisterende diplomatiske kanaler

Microsoft anbefaler, at staterne støtter virksomhederne i deres forsøg på at sikre deres produkter, samtidig med at de begrænser udviklingen, opbevaringen og brugen

af cybervåben. Det gælder særligt de våben, der gør det muligt at udnytte virksomhedernes it-sårbarheder. Disse anbefalinger, som blev præsenteret på USA's største cybersikkerhedskonference, RSA, i et blogindlæg (Smith 2017) og efterfølgende for både EU og FN (Neutze 2017; UNOG 2017), ligger fint i forlængelse af det, der allerede er blevet (og fremadrettet vil blive) diskuteret i flere internationale fora. Mange af disse fora er modsat en digital Genèvekonvention ikke juridisk bindende, hvilket på nuværende tidspunkt er det eneste, de deltagende stater og ikke-statslige aktører har kunnet nå til enighed om. Det er derfor, at flere internationale juridiske og politiske eksperter fortsat holder fast i, at ikke-bindende erklæringer synes at være det mest sandsynlige første skridt hen imod mere håndfaste statslige normer for adfærd i cyberspace (Finnemore & Hollis 2016; Tikk-Ringas 2016; Schmitt & Vihul 2014; Nye 2014; Henriksen 2012).

FN's gruppe af regeringseksperter på området (UNGGE) har ad flere omgange udgivet rapporter, hvori man er nået til enighed om en række relaterede emner. Men til trods for at rapporterne er af ikke-bindende karakter, har de vist sig særdeles vanskelige at nå til enighed om. Eksempelvis resulterede den seneste forhandlingsrunde i 2016/17 slet ikke i en ny rapport. Hvis ikke-bindende rapporter ikke kan forhandles, er det usandsynligt, at en bindende Genèvekonvention kan komme på tale. Det betyder imidlertid ikke, at UNGGE og lignende fora ikke er værd at investere i. I de tidligere rapporter nåede gruppen af regeringseksperter til enighed om, at stater anerkender, at eksisterende international ret gælder i cyberspace, at stater ikke bevidst må gøre skade på andres kritiske infrastruktur eller på de enheder, stater anvender til at "brandslukke" cyberangreb (CERT'er), og endelig at stater ikke må bruge stedfortrædere såsom ikke-statslige aktører til at gøre skade på andre i cyberspace (FN's Generalforsamling 2015b). Derudover arbejder forhandlingsdeltagerne både i UNGGE og OSCE fortsat på at skabe platforme for tillidsskabende foranstaltninger. Sådanne foranstaltninger har historisk set været de indledende skridt, der har muliggjort seriøse drøftelser om nedrustning. Alle disse færdigforhandlede elementer risikerer at skulle starte forfra, hvis samtlige medlemsstater i FN sætter sig ned for at begynde officielle forhandlinger om en overordnet digital konvention.

Microsoft pointerer korrekt, at den eksisterende folkeret ikke direkte adresserer – eller i nævneværdig grad begrænser – staters udnyttelse af private it-virksomheders produkter, når cybervåben forberedes, eller cyberspionage udføres. Det mest udførlige akademiske arbejde, der forsøger at afklare eksisterende international ret i cyberspace, Tallinnmanualen 2.0, understreger således, at cyberspionage som sådan ikke er forbudt, medmindre det medfører funktionel skade eller strider mod internationale menneskerettigheder og lignende (Schmitt 2017: 168). Selvom manualen er udarbejdet af akademikere, har den allerede i flere lande vist sig som et centralt referencedokument for de statslige medarbejdere, der skal klarlægge og juridisk vurdere de respektive landes militære brug af cyberspace.

Hvis Microsoft skal gøre sig forhåbninger om at få tilføjet et kapitel om forbud mod statslig udnyttelse af it-sårbarheder hos private virksomheder, bør dette formuleres mere præcist og fokuseret end som et bredt behov for en digital Genèvekonvention. Microsoft får i den henseende mere ud af at fortsætte sit arbejde med i stilhed at søge indflydelse på de stater, der er engageret i igangværende forhandlinger i fx UNGGE, samt at arbejde på, at de anbefalinger, som udvikles, omsættes til bindende internationale praksisser.

Selv hvis det lykkes Microsoft at få en stemme i disse forhandlingsfora, er det meget usandsynligt, at staterne er villige til at lade sig binde juridisk og derved fuldstændig opgive retten til at udvikle, gemme og bruge cybervåben. Jeg peger på to grunde hertil.

## Modsatrettede sikkerhedshensyn

Der er en god grund til, at spionage ikke i udgangspunktet strider mod folkeretten. I forsøget på at forudse og forhindre krige, terrorisme og kriminalitet samt styrke internationale forhandlingspositioner har spionage alle dage været et værdsat redskab for stater. Med udbredelsen og afhængigheden af informations- og kommunikationsteknologi har stater fået en platform, hvor indhentning af store mængder information er blevet nemmere og næsten risikofri. Dygtige hackere i efterretningstjenesterne kan sidde i ro og mag i hjemlandet og lede efter og udnytte it-sårbarheder hos *modstanderen*. Kilden til Microsofts markante intervention udspringer af det velkendte dilemma i cyberspace: at mange af de identificerede og udnyttede it-sårbarheder findes i kommercielle it-produkter, som bruges af statslige institutioner, virksomheder og private borgere overalt på kloden. Dilemmaet opstår, så snart en sårbarhed er identificeret i et system. Her må en efterretningstjeneste nemlig nødvendigvis vurdere, hvilke it-systemer i hjemlandet og hos allierede der er sårbare på grund af it-sårbarheden, samt hvilke andre aktører der har kendskab til, vil få kendskab til og i øjeblikket udnytter den. Sådanne vurderinger kan være særdeles vanskelige.

Statslig udnyttelse af it-sårbarheder kan imidlertid også øge den nationale sikkerhed. Netop anerkendelse af de modsatrettede sikkerhedshensyn har fået USA til at udvikle en officiel (omend klassificeret) procedure for vurdering af, om mulighederne ved udnyttelse af en it-sårbarhed står mål med de potentielle risici, der er forbundet med, at sårbarheden ikke bliver udbedret af den virksomhed, som er skyld i dens eksistens. Hvis man støtter Microsofts dagsorden om mindre statslig oprustning i cyberspace, er et andet og måske vigtigere sted at starte end en konvention for staters adfærd i cyberspace at søge mere åbenhed om, hvad der ligger til grund for de forskellige staters vurderinger af it-sårbarheder. Derudover må støtter nødvendigvis forsøge at overbevise både offentligheden og politikere om, at global it-sikkerhed er en vigtig del af vores "nationale sikkerhed", også selvom det

vanskeliggør politiets og efterretningstjenesternes arbejde: De må nemlig udarbejde argumenter for, at it-sikkerhed er vigtigere end evnen til at dominere (via cyberspace) i fremtidige militære konfrontationer end at have kendskab til andre staters uofficielle holdninger og positioner i vigtige internationale økonomiske og diplomatiske spørgsmål. Det kræver, at Microsoft og andre støtter af en digital konvention seriøst engagerer sig i og konfronterer det dilemma, der eksisterer, i stedet for at ignorere dets eksistens.

Selv hvis diverse techgiganter og deres støtter får succes med at konstruere en fortælling om, at it-sikkerhed skal have mere vægt *på bekostning af* andre former for sikkerhed, er beslutningen om at frasige sig kapaciteten til at udnytte sårbarheder i cyberspace stadig vanskelig. Det skyldes en række både tekniske og politiske faktorer, som jeg vil adressere i det følgende.

## Håndhævelsesproblematik

Som allerede nævnt nåede UNGGE i 2015 til enighed om, at stater ikke må bruge stedfortrædere til at gøre skade på hinanden. Der ligger altså allerede nogle klare linjer, som stater diplomatisk kan referere til, hvis en anden stat eksempelvis forstyrrer en demokratisk valgproces, sådan som USA mener, Rusland gjorde i 2016. UNGGE-konklusionerne er godt nok endnu ikke juridisk bindende, hvilket måske er grunden til, at nogle stater synes at være villige til at ignorere dem. Det er dog langt fra sikkert, at det juridiske ord (i cyberspace) er så stærkt, som Brad Smith og Microsoft håber på.

Cyberspaces tekniske karakter gør det på nuværende tidspunkt vanskeligt at håndhæve en konvention. En meget gentaget grundantagelse om cyberspaces tekniske karakter er, at det er relativt nemt at opnå anonymitet. Det meste onlinekriminalitet bliver ikke opklaret, ligesom man hverken har pågrebet personerne bag WannaCry eller NotPetya. Når en større cyberhændelse finder sted, beskylder den forurettede stat ofte en anden stat for at stå bag – og lige så ofte afviser den beskyldte anklagen. Det forhindrer dog ikke den forurettede stat i at svare igen mod den *formodede* gerningsstat. Fx truede USA Kina med sanktioner for den industrielle cyberspionage, som man mente at kunne spore til den kinesiske stat, og USA udviste femogtredive russiske diplomater, efter at samtlige amerikanske efterretningstjenester havde peget på Kreml som ansvarlig for hackerangrebene på Demokraternes præsidentkampagne. Det er imidlertid ikke klart, hvilke tekniske beviser USA lægger til grund i sin udpegning af bagmanden. Det skyldes først og fremmest manglende amerikansk interesse i at miste den indhentningskapacitet, landet allerede besidder. Afslører man det bevismateriale, de signaturer og teknikker, som man har kendskab til, at modstanderen bruger, kan denne nemlig blot ændre sine praksisser fremadrettet (Jacobsen & Ringsmose 2017). Dette dilemma i forhold til at løfte en bevisbyrde og dermed håndhæve eventuelle internationale regler er en central udfordring i enhver forhandling om en digital konvention.

Brad Smith og Microsoft foreslår med inspiration fra Det Internationale Atomenergiagentur (IAEA), at der oprettes en gruppe af uafhængige tekniske eksperter, som skal fastslå, om et cyberangreb er en statslig aktørs værk. Idéen er bestemt interessant og værd at overveje, men den er også kontroversiel. Det skyldes ikke mindst, at det virker utænkeligt, at nogen stater ville være villige til at lade deltagere fra et sådant internationalt agentur føre fysisk tilsyn med deres efterretningstjenesters arbejde i cyberspace. Uden fysisk tilsyn skal agenturet reelt agere på linje med de cybersikkerhedsfirmaer, såsom CrowdStrike, Kaspersky og FireEye, som allerede i dag grundigt analyserer de eksempler på ulovlig indtrængen, der foregår i cyberspace. På trods af disse firmaers store tekniske kompetencer er det langt fra sikkert, at de har evnerne til at løfte en tilstrækkelig bevisbyrde mod en stat, der gør sig umage for at forblive anonym. En efterretningstjeneste med omfattende overvågningskapacitet, der samtidig selv gør brug af cyberspionage og måske endda informanter på jorden, kan givetvis gøre det. Men man er næppe villig til at lade en international cybervagthund fungere som et de facto-spionagentur i FN.

International "shaming" ved brud på konventioner har til tider vist sig at være et brugbart redskab i international diplomatisk sammenhæng, men det kræver attribution. Medmindre man teknisk vil omkalfatre internettet, er et internationalt cyberagentur uden reelle spionbeføjelser, men med mandat til at efterforske cyberangreb et af de mest konkrete – om end politisk penibelt – bud, vi i øjeblikket har på noget, man på sigt kunne starte på at drøfte.

## En småstats politiske råderum: Danmark som case

Jeg har i ovenstående peget på fire politiske og tekniske grunde til, at bestræbelserne på at etablere en konvention for statslig adfærd i cyberspace er dømt til at mislykkes. Det betyder dog ikke nødvendigvis, at omfanget af cyberkriminalitet og andre cyberhændelser vil fortsætte med at stige i al evighed. En række udviklinger vil muligvis kunne afhjælpe problemet. For det første er der endnu håb om, at den teknologiske udvikling formår at forbedre it-produkter og implementering af disse. For det andet kan det ikke afvises, at de ikke-bindende diplomatiske forhandlinger med tiden faktisk får skabt normer, der fører til mindre statslig indhentnings- og angrebsaktivitet i cyberspace. Og for det tredje sidder især USA, men også Kina og EU med en mulig nøgle til at højne den generelle it-sikkerhed gennem regulering, standarder og nye incitamentsstrukturer.

Det betyder imidlertid ikke, at en småstat som Danmark står uden mulighed for at få indflydelse på udviklingen af den internationale cybersikkerhedspolitik. Matthew Crandall og Collin Allan (2015) har således vist, hvordan en anden småstat – Estland – har udnyttet den omfattende politiske uklarhed omkring cyberspace til at få indflydelse på skabelsen af internationale normer. Estland har, siden landet blev ramte af cyberangreb i 2007, investeret mange ressourcer i at positionere sig som en cyberdiplomatisk nation, der i både EU, NATO og EU fremmer cybersikkerhed

og "internet governance" (ibid.: 352). Det følgende afsnit identificerer tre områder, Danmark kan styrke for at kunne "punch above its weight": det udenrigs-, det erhvervs- og det forsvarspolitike område.

## Styrket cyberdiplomati

Til trods for at Danmark er førende på det digitale område i EU (EU Commission 2017), har vi indtil nu ikke markeret os i særlig grad på det cyberdiplomatiske område. Alt imens flere ligesindede lande har oprettet cyberambassadører, vidner den nye danske techambassadør i Silicon Valley om, at prioriteten ikke er diplomatiske forhandlinger om normer for statslig adfærd i cyberspace, "internet governance" eller sikring af menneskerettigheder online, men i første omgang hovedsageligt på vækstskabelse i it-sektoren. Det betyder ikke nødvendigvis en nedprioritering af it-sikkerhed. Techambassadøren kan eksempelvis med sin samarbejds- og indkøbspolitik være med til at højne efterspørgslen efter sikre it-produkter.

Ønsker den danske regering at have indflydelse på, hvad der kommer til at ske på området for cybernormer og staters adfærd i cyberspace, må Udenrigsministeriet, som det skete i Estland efter 2007, nødvendigvis tilføres økonomiske ressourcer, så Danmarks techambassadør kan omfavne hele spektret af cyberpolitiske problemstillinger. En sådan udvidelse kan blandt andet indbefatte:

1. en EU-cyberattaché i Bruxelles, der kan sætte sit præg på det cyberdiplomatiske spil i EU, som først er ved at tage form.
2. en medarbejder eventuelt knyttet til FN-missionen i New York med særligt fokus på at få danske eksperter og diplomater i fremtidige UNGGE-lignende forhandlingsgrupper.
3. et tværfagligt team i København med fod i Udenrigsministeriets juridiske, sikkerheds- og handelspolitiske kontorer med ansvar for – og råderum til – at udvikle og koordinere den juridiske og sikkerhedspolitiske linje på området.

## Bedre regulering af it-sektoren

De seneste danske regeringer har ikke taget initiativ til at investere i udviklingen af regulering af og standarder for det danske marked for it-produkter. I udgangspunktet er en småstat som Danmark udfordret af ikke at have mange muligheder for at stille krav til og regulere store multinationale it-virksomheder. Men i en tid, hvor behovet for statslig intervention i markedet for it-produkter bliver tydeligere og tydeligere, har den danske regering sammen med de øvrige EU-lande et ansvar for, at der bliver udviklet klare rammer, som virksomhederne skal holde sig inden for. I USA, som ellers generelt er tilbageholdende med enhver form for regulering, fremlagde Det Hvide Hus' Kommission for Forbedring af National Cybersikkerhed, med højtstående deltagere fra det amerikanske erhvervsliv, en rapport i december 2016. Rapportens forfattere anbefaler flere it-sikkerhedsstandarder samt regulering, hvis disse ikke bliver fulgt (Donilon & Palmisano 2016).

En lignende udvikling vil efter alt at dømme også finde sted i EU. EU har i andre sammenhæng netop udvist tilstrækkelig styrke til at få techgiganter til at ændre praksis. Jo hurtigere Erhvervsstyrelsen og Erhvervsministeriet anerkender behovet for regulering, desto hurtigere kan de høste frugterne af det gode renommé som digital nation, som Danmark har, og i samarbejde med danske virksomheder udvikle brugbare standarder samt licens-, bøde- og incitamentsordninger. Det vil gøre Danmark til en politikmager (og ikke blot en "politiktager") i EU, hvilket i sidste ende giver danske virksomheder en konkurrencefordel.

## Et styrket cyberforsvar

Det danske forsvar har fået midler til både at bruge cyberspace til indhentning og som en del af fremtidige militære operationer. Som nævnt tidligere indeholder disse aktiviteter ofte et dilemma. De sårbarheder i fjendens it-systemer, som udnyttes, er nogle gange sårbarheder i kommercielle it-produkter, som også bruges i Danmark og i resten af verden. Det danske forsvar kan med fordel ligesom USA udvikle en procedure for, hvornår disse sårbarheder gemmes, og hvornår og hvordan de deles med henblik på udbedring. En sådan procedure balancerer hensynet til it-sikkerhed med behovet for indhentning med henblik på varetagelsen af Danmarks sikkerhed. Klare standarder og krav til virksomheder, der udvikler, sælger eller implementerer it-produkter, kan hjælpe forsvaret med at lægge det rette snit.

En procedure for vurdering af it-sårbarheder kan dernæst søges drøftet med Danmarks allierede i NATO med henblik på at skabe fælles overordnede retningslinjer. Godt nok er en deling af information omkring konkrete offensive cyberkapabiliteter landene imellem usandsynlig, men det ændrer ikke ved, at det ikke er i Danmarks interesse, at allierede udvikler militære kapabiliteter uden hensyntagen til de konsekvenser, udnyttelsen af it-sårbarheder eventuelt kan have på tværs af alliancen. Forslag til fælles retningslinjer og konkrete initiativer til samarbejde og informationsdeling udvikles oftest i samspil mellem akademiske fora og interstatslige organisationer. Derfor kan Forsvarsministeriet med fordel sekundere cybermedarbejdere til NATO Cooporative Cyber Defence Centre of Excellence i Tallinn og NATOs hovedkvarter.

Derudover er der både i Danmark og på tværs af alliancen stadig en betragtelig videnskløft mellem de it-eksperter, som sikrer vores systemer og netværk, og de militære og politiske beslutningstagere, der allokerer midler og udstikker de strategiske retningslinjer. En måde at skabe synlighed for Danmark på det cyberpolitiske område er at deltage i og måske endda arrangere internationale cyberberedskabsøvelser, hvor det politiske og strategisk niveau også er repræsenteret. På den måde opbygges en større bevidsthed blandt beslutningstagere omkring de muligheder og ikke mindst risici, der er forbundet med at være en førende digital nation.

## Konklusion

Microsofts forslag om en digital Genèvekonvention er en attraktiv idé: Klare juridiske retningslinjer, der begrænser statslig cyberoprustning og cyberangreb på kritisk

infrastruktur, samt mere statsligt samarbejde med teknologiindustrien om at identificere og udbedre sårbarheder er vigtige tiltag. I denne artikel har jeg imidlertid opstillet en række argumenter for, at en åbning af forhandlinger om en konvention for statslig adfærd i cyberspace ikke nødvendigvis er så attraktiv for de stater, der ellers normalt søger international juridisk klarhed. Ikke nok med at Microsofts forslag ikke tager hånd om de it-sårbarheder, der eksisterer i cyberspace, og som fortsat vil blive produceret af de tech-virksomheder, der agerer heri, men en storstilet digital konvention for statslig adfærd i cyberspace er dødsdømt allerede, inden den kommer til forhandlingsbordet. Det skyldes, at forslaget ikke har taget højde for det faktum, at enhver konventionsforhandling er en del af den politisk-diplomatisk virkelighed med interesser, der går udover cyberspace. Åbner man forhandlingerne, åbner man også for drøftelser, som USA og de fleste vesteuropæiske stater ikke ønsker genåbnet, og man underminerer de igangværende uformelle drøftelser om internationale cybernormer i diverse fora. Derudover udnytter efterretningstjenester de it-sårbarheder, som eksisterer i cyberspace, til at efterforske og retsforfølge kriminelle og øge egne forhandlingspositioner internationalt. Dette prærogativ ønsker ingen stat at afgive. Sidst er håndhævelsen af en konvention vanskeliggjort af, at stater af frygt for at miste indhentningskapacitet ikke altid ønsker at fremlægge de tekniske beviser, som faktisk attribuerer et cyberangreb.

Hvis en småstat som Danmark imidlertid opprioriterer andre indsatser, er der stadig god mulighed for at få indflydelse på det cyberpolitiske område. I stedet for at presse på for en højpolitisk "digital Genèvekonvention" kan Danmark udnytte, at cyberpolitikken internationalt stadig er ved at finde sine fødder. Med en opprioritering af det cyberdiplomatiske område, en udnyttelse af Danmarks gode renommé som digital frontløber og gode forhold til den private sektor samt mere forsvarspolitisk initiativ internationalt kan Danmark som småstat "punch above their weight."

## Om forfatteren

Jeppe T. Jacobsen er Ph.d.-studerende på Dansk Institut for Internationale Studier og på Center for War Studies, Syddansk Universitet. Jeppe beskæftiger sig primært med amerikansk cyberforsvarspolitik, samt med betydningen af cybermilitære kapabiliteter for international sikkerhed. Tidligere arbejdede han med cyber diplomati i det danske Udenrigsministerium.

## Litteratur

Austin, Greg (2014) «Small States Need Cyber Diplomacy.» *neweurope.eu*. Tilgængelig på: http://www.neweurope.eu/article/small-states-need-cyber-diplomacy

Carr, Madeline (2016) «Public–private partnerships in national cyber-security strategies», *International Affairs*, 92 (1): 43–62.

Crandall, Matthew & Collin Allan (2015) «Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms». *Contemporary Security Policy*, 36 (2): 346–368.

Donilon, Tom & Palmisano, Sam (2016) «Commission on Enhancing National Cybersecurity. Report on Securing and Growing the Digital Economy.» Tilgængelig på: https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecuritycommission-report-final-post.pdf

EU Commission (2017) «How digital is your country? Europe improves but still needs to close digital gap.» European Commission – Press Release. 03.03.2017. Tilgængelig på: http://europa.eu/rapid/press-release_IP-17-347_en.htm

Finnemore, Martha & Duncan B. Hollis (2016) «Constructing Norms for Global Cybersecurity.» *The American Journal of International Law,* 110 (3): 425–479.

FN's Generalforsamling (2015a) «*Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.*» Tilgængelig på: http://undocs.org/A/69/723

FN's Generalforsamling (2015b) «*Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.*» 70. session, dagsordenspunkt 93. Tilgængelig på: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

Goertzel, Karen M. (2016). «Legal Liability for Bad Software.» Tilgængelig på: http://static1.1.sqspcdn.com/static/f/702523/27213494/1472233517737/201609-Goertzel.pdf?token=xi3hJI%2Btv66tqXCQp5LTh4veBQc%3D

Guardian Staff (2017) «Ransomware attack 'like having a Tomahawk missile stolen', says Microsoft boss. *The Guardian*. 15.05.2017. Tilgængelig på: https://www.theguardian.com/technology/2017/may/15/ransomware-attack-like-having-a-tomahawk-missilestolen-says-microsoft-boss

Henriksen, Anders (2012) «*Cyberkrig. Folkeretten og computer network operations.*» København: Center for Militære Studier. Rapport.

Henriksen, Anders (2017) «Politics and the development of legal norms in cyber space.» i Karsten Friis & Jens Ringsmose (Red.) *Conflict in Cyberspace. Theoretical, strategic and legal perspectives.* London: Routledge (s. 151–164).

Jacobsen, Jeppe T. & Jens Ringsmose (2017) «Cyber-bombing ISIS: why disclose what is better kept secret?» *Global Affairs,* 3 (2): 125–137.

Kaspersky, Eugene (2017) «A Digital Geneva Convention? A Great Idea.» *Forbes*. 15.02.2017. Tilgængelig på: https://www.forbes.com/sites/eugenekaspersky/2017/02/15/a-digital-geneva-convention-a-great-idea/#13dd85b11e6e

Knake, Robert K. (2017) «Don't Blame the NSA for WannaCry.» 16.05.2017. Tilgængelig på https://www.cfr.org/blog-post/dont-blame-nsa-wannacry

Meyer, Paul & Daniel Stauffacher (2017) «WannaCry, the Digital Geneva Convention and the urgent need for Cyber Peace.» ICT4Peace commentary. Juni. Tilgængelig på: http://ict4peace.org/wannacry-the-urgent-need-for-cyber-peace/

Microsoft (2017) «A Digital Geneva Convention to protect cyberspace» Microsoft Policy Papers. Tilgængelig på: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH

Minárik, Tomáš & Kris van der Meij, K. (2017) «Geneva Conventions Apply to Cyberspace: No Need for a 'Digital Geneva Convention'». 18.06.2017. Tilgængelig på https://www.ccdcoe.org/geneva-conventions-apply-cyberspace-no-need-digital-geneva-convention.html

Morozov, Evgeny (2017) «Why do we need 'accidental heroes' to deal with global cyber-attacks?» *The Guardian.* 20.05.2017. Tilgængelig på https://www.theguardian.com/commentisfree/2017/may/20/cyber-attack-ransomware-microsoft-tech-giants-are-only-winners

Muller, Lilly P. (2016) «Makt og avmakt i cyberspace: hvordan styre det digitale rom?» *Internasjonal Politikk*, 74 (4): 1–23.

Neumann, Iver B. & Sieglinde Gstöhl (2006) «Lilliputians in Gulliver's World?» i C. Ingebritsen, I. Neumann & S. Gstöhl, *Small States in International Relations.* Washington, WA: University of Washington Press.

Neutze, Jan (2017) «The need for a «Digital Geneva Convention» in Times of Cyber(In)Security». European Commission High Level Meeting, Brussels, October 3, 2017. Tilgængelig på: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=36025&no=4

Nye, Joseph S. (2010) «Cyber Power.» Belfer Center for Science and International Affairs, Harvard Kennedy School. Tilgængelig på: http://belfercenter.ksg.harvard.edu/publication/20162/cyber_power.html.

Nye Jr., Joseph S. (2014) «The Regime Complex for Managing Global Cyber Activities.» Waterloo, ON & London: Centre for International Governance Innovation and the Royal Institute for International Affairs. Global Commission on Internet Governance Paper Series no. 1.

Reus-Smit, Christian (red.) (2004) *The Politics of International Law*. Cambridge: Cambridge University Press.
Schmitt, Michael N. (red.) (2017) *Tallinn Manual 2.0. On the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.
Schmitt, Michael N. & Liis Vihul (2014) «The Nature of International Law Cyber Norms.» i Liis Vihul (Red.) *The Tallinn Papers. A NATO CCD COE Publication on Strategic Cyber Security*. Tallinn: CCDCOE (55–86).
Schneier, Bruce (2017) «Schneier Brings Campaign for IoT Regulation to RSA.» 14.02.2017. Tilgængelig på https://www.schneier.com/news/archives/2017/02/schneier_brings_camp.html
Schwartz, Ari. & Robert K. Knake (2016) «Government's Role in Vulnerability Disclosure – Creating a Permanent and Accountable Vulnerability Equities Process.» Cambridge, MA: The Cyber Security Project. Discussion Paper 2016-04. Harvard Kennedy School, Belfer Center for Science and International Affairs.
Smith, Brad (2017) «The Need for a Digital Geneva Convention.» 14.02.2017. Tilgængelig på: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digitalgeneva-convention/#sm.001hyuheo1049czppep2qitwbu5q3
Starks, Tim (2017) «Spying tool reauthorization hits Senate calendar, but not without objections». Morning Cybersecurity – Politico. 18.10.2017. Tilgængelig på: http://www.politico.com/tipsheets/morning-cybersecurity/2017/10/18/spying-tool-reauthorization-hits-senate-calendar-but-not-without-objections-222866
Steinmetz, Robert & Anders Wivel (red.) (2010) *Small States in Europe. Challenges and Opportunities*. London & New York: Routledge.
Tarp, Maria Nilaus & Jens Ole Bach Hansen (2013) «Size and Influence. How small states influence policy making in multilateral arenas.» DIIS Working Paper 2013:11.
Tikk-Ringas, Eneken (2016) «International Cyber Norms Dialogue as an Exercise of Normative Power.» *Georgetown Journal of International Affairs,* 17 (3): 47–59.
UNOG (2017) «Current Internet Governance Challenges; what's next?» UNITAR Seminars – Geneva Lecture Series. 09.11.2017. Tilgængelig på: https://www.unog.ch/unog/website/dg.nsf/(httpPages)/3A579B24BAEBFB55C1257E3B004BD723?OpenDocument

**Abstract in English**

Although Denmark, as a small-state actor, has an interest in global IT security and clarity of international norms in cyber space, this article argues that it is not in Denmark's interest to pursue a "Digital Geneva Convention," the proposal currently being put forward by Microsoft. Starting negotiations on a comprehensive digital convention would risk reopening already concluded international agreements and undermining on-going, non-binding negotiations. It also overlooks the gains that states' security apparatuses legitimately pursue in cyberspace. This, however, does not mean that a small state like Denmark should stay passive in the field of international cyber politics. On the contrary, the continuing political uncertainty in cyberspace provides small states with the possibility of "punching above their weight". Prioritizing Danish cyber engagements in the EU, NATO, the UN and in non-governmental fora as well as enhancing cooperation with the private sector in both Denmark and internationally, would strengthen Denmark's political profile internationally and security in cyberspace more generally.

**Keywords:** cyberspace; Microsoft; cyber diplomacy; international law; small states