Økonomi & Politik

#3
Oktober 2020
93. ÅRGANG
OPEN ACCESS

TEMANUMMER

Cybersikkerhed

INDHOLD

Udgives af
Djøf Forlag

Redaktion og bestyrelse

Redaktionelt forord

MARTIN MARCUSSEN
Ansvarshavende redaktør

Center for Cybersecurity, der er placeret hos Forsvarets Efterretningstjeneste, lægger i deres årlige trusselvurdering ikke fingrene imellem: "Truslen fra cyberkriminalitet er **MEGET HØJ**", slås fast med versaler i fed skrift. Cyberkriminalitet er en samlebetegnelse for handlinger, hvor hackere bruger cyberangreb til at begå kriminalitet, der er motiveret af et ønske om økonomisk berigelse. Også truslen fra cyberspionage er **MEGET HØJ**, konkluderer centeret. Det betyder konkret, at det er meget sandsynligt, at danske myndigheder og virksomheder vil blive udsat for forsøg på cyberspionage inden for de næste to år. Truslen er især rettet mod myndigheder, som arbejder med udenrigs- og sikkerhedspolitik samt virksomheder, der besidder en viden, som andre stater har en interesse i. Helt konkret meddeler udenrigstjenesterne i Østrig, Tyskland, Italien, Kroatien og Belgien, at de har været udsat for omfattende cyberangreb på det seneste, og at statslige aktører kan have stået bag disse angreb. Særlig Rusland og Kina er således kommet i søgelyset som stater, der i særlig stor udstrækning benytter sig af cyberspionage.

Trusselsvurderingen konkluderer samtidig, at sandsynligheden for, at Danmark udsættes for destruktive cyberangreb – det vil sige angreb, der fører til omfattende datadestruktion, fysisk ødelæggelse eller ligefrem dødsfald - er **LAV**. Sådanne angreb har godt nok fundet sted i vore nærområder – på hospitaler i Storbritannien, Tv-stationer i Georgien og elselskaber i Ukraine – og godt nok måtte A.P. Møller-Mærsk tage et tab på mellem 1,6 og 1,9 milliarder kroner i 2017 og Demant et tab på op mod kr. 650 millioner i 2019 som et resultatet af destruktive cyberangreb – men alligevel identificerer Forsvarets Efterretningstjeneste kun en lav risiko på den front.

Det samme gør sig gældende for den såkaldte cyberaktivisme, hvor formålet er at gribe ind i en politisk proces eller at gøre opmærksom på en enkeltsag. Også her er trusselsvurderingen **LAV**. Cyberaktivisme kan eksempelvis tage form af kampagner, hvor der spredes falsk information og propaganda. I vore nabolande, som eksempelvis Litauen, kæmper man løbende med russiske påvirkningskampagner, der har til formål at skabe splittelse mellem befolkningsgrupper i landet og til Litauens allierede. Mest kendt er selvfølgelig den læk af informationer, bl.a. e-mails, som Demokraternes Nationale Komité blev udsat for forud for det amerikanske præsidentvalg i 2016. Men heller ikke dette synes at bekymre Center for Cybersecurity. Herhjemme blev Udenrigsministeriet udsat for en slags cyberaktivisme i 2017 da en såkaldt pro-tyrkisk gruppe

valgte at oversvømme ministeriets hjemmeside med trafik i forlængelse af endnu en debat om muhammedtegninger.

Selvom trusselsvurderingen siger tingene ligeud, er der også forhold i relation til cybersikkerhed, der ikke diskuteres så eksplicit. Dette temanummer af Økonomi & Politik, der er redigeret af Tobias Liebetrau ved Center for Militære Studier, Københavns Universitet, ønsker at kaste lys på nogle af de forhold i relation til cybersikkerhedsfænomenet, som vi enten ikke har den store viden om, eller som danske offentlige myndigheder ikke kan tale åbent om. For eksempel taler vi ofte om, at Kina og Rusland meget aktivt engagerer sig i alle former for aggressiv adfærd på cyberområdet. Vi taler knap så ofte om, at vore allertætteste allierede – som eksempelvis USA og Storbritannien – også er helt fremme på området. I både USA og Storbritannien fremfører man det synspunkt, at deres cyberadfærd har et præventivt formål og at deres gentagne forsøg på at forhindre lande som Iran, Rusland og Kina i at begå cyberspionage, -kriminalitet og –angreb kan retfærdiggøre, at man også samtidig helt eksplicit træder andre landes suverænitet under fode. Det er netop et forhold som dette, der gør, at de vestlige lande ikke virker troværdige i deres forsøg på at udvikle et fælles internationalt normsæt på området.

Vi taler også en del om, at vi som et lille land er særdeles sårbare i forhold til andre landes cyberadfærd, men vi taler ikke så meget om, at selv vore nærmeste allierede angiveligt deltager i cyberspionage på dansk grund, og da slet ikke om, at vi selv anvender cyberspionage som en del af vores generelle informationsindhentning i udlandet. Faktisk kan man sige, at cyberdomænet giver små stater som Danmark flere nye muligheder i udenrigs- og sikkerhedspolitikken. Cyberaktivitet kræver nemlig som udgangspunkt ikke dyrt materiel og koster typisk ikke menneskeliv. I dag tilbyder både universiteter og det danske forsvar unge mennesker en uddannelse i hacking – i nationens tjeneste.

Endelig gemmer der sig en vigtig diskussion, der vedrører spørgsmålet om, hvorvidt vore politikere og den brede befolkning nogensinde kan opnå en bare tilnærmelsesvis tilstrækkelig indsigt i et felt, hvor den teknologiske udvikling er kolossal hurtig med kvanteteknologien og kunstig intelligens som det næste udviklingstrin, og hvor der helt rutinemæssigt tales om ransomware-angreb, phishing-mails, VPN-løsninger og DDoS-angreb. På globalt plan er der en betydelig efterspørgsel efter eksperter, der kan hitte rede i de muligheder og gennemgribende udfordringer, der er forbundet med cybersikkerhedsfeltet. Det er eksperternes paradis – især fordi der på området endnu ikke eksisterer nogle professionsstandarder, der præciserer, hvad der er god henholdsvis dårlig praksis. I den situation er det utrygt at vide, at det er disse såkaldte eksperter, der grundlæggende definerer de præmisser som vore politikkere handler på grundlag af. Der er **MEGET HØJ** risiko for, at der styres i blinde.

TEMAREDAKTØRENS FORORD

Cybersikkerhed i perspektiv

TOBIAS LIEBETRAU
post.doc., Center for Militære Studier, Institut for Statskundskab, Københavns Universitet,
tobias.liebetrau@ifs.ku.dk

Digitaliseringen er et janushoved

Verden over gennemsyres samfund og hverdagsliv af informations- og kommunikationsteknologi. Den digitale udrulning og indrullering er normalt akkompagneret af løfter om øget vækst, velstand og velfærd. Den forjættende digitalisering går imidlertid hånd i hånd med nye risici og usikkerheder.

Det skyldes, at anvendelsen af informations- og kommunikationsteknologi er kompleks, dynamisk og diffus. Grænserne mellem det digitale og det fysiske opblødes, udviskes og forvitrer. Geografisk og tidslig bundethed omkalfatres. Desuden er størstedelen af den digitale infrastruktur privat udviklet, ejet og drevet. Ydermere indeholder den software, der understøtter digitaliseringen sårbarheder, som fjendtlige sindede aktører kan finde og udnytte. Det kan medføre, at en angriber overtager kontrollen med sårbare systemer, manipulerer data eller sætter softwaren ude af stand til at fungere efter hensigten. Derudover kan den fremtidige brug og videreudvikling af eksisterende digitale teknologier ikke sættes på formel, men forbliver åben og uforudsigelig.

> Introduktionen af nye digitale teknologier er på den ene side ledsaget af politiske, sociale og økonomiske muligheder og på den anden af nye usikkerheder og sårbarheder

Digitaliseringen af vores samfund og vores liv er derfor et janushovedet fænomen. Introduktionen af nye digitale teknologier er på den ene side ledsaget af politiske, sociale og økonomiske muligheder og på den anden af nye usikkerheder og sårbarheder. Derfor bliver cybertruslen i dag regnet for en af de – hvis ikke den – absolut største sikkerhedstrussel. Det gælder i et nationalt sikkerhedspolitisk perspektiv såvel som i erhvervslivet.

Det er karakteristisk for cybertruslen, at den både udvider og sammenkæder de sikkerhedspolitiske risici og antallet af potentielle mål – fra stater over private virksomheder til individuelle brugere. Cybertruslen og håndteringen af den udfordrer en række af de traditionelle skillelinjer, som vi normalt bruger til at indrette vores samfund og sikkerhedspolitiske tænkning efter, herunder skellene mellem nationalt og internationalt, offentligt og privat, politisk og teknologisk samt krig og fred.

Den uforudsigelighed og usikkerhed, der er forbundet med den fortsatte udvikling i og brug af informations- og kommunikationsteknologi, samt den

private sektors mellemkomst gør traditionel sikkerhedspolitisk styring, organisering og lovgivning vanskelig. Cybertruslen udfordrer dermed statens historiske monopol på at bedrive sikkerhedspolitik. Ydermere forplumrer den statslige håndtering af cybertruslen i stadigt stigende grad det klassiske skel mellem national sikkerhedshåndtering og kriminalitetsbekæmpelse, mellem intrastatslige politiopgaver og interstatslig forsvarsopgaver og mellem offentligt sikkerhedsansvar og privat sikkerhedsansvar. Vi er således vidner til et opbrud i grænserne mellem statens ansvar for nationens sikkerhed og borgerens ret til beskyttelse.

Det er derfor ikke overraskende, at cybersikkerhed er et omstridt og anfægtet begreb. Hvad der bliver kategoriseret som cybersikkerhed, og hvem der har ansvaret for at håndtere cybersikkerhed, er ikke statiske størrelser. Der findes militær-strategiske, politiske, juridiske og tekniske definitioner af cybersikkerhed, men begrebet er kontinuerligt til forhandling. Begrebsliggørelsen af cybersikkerhed konstitueres gensidigt af, hvilke typer af cybersikkerhedsudfordringer, -viden og -løsninger der vinder frem, herunder i forskningsverdenen.

I den resterende del af dette forord vil jeg derfor først præsentere et grundrids af den eksisterende cybersikkerhedslitteratur inden for forskningsfeltet International Politik. Jeg inddeler således cybersikkerhedslitteraturen i tre delvist overlappende kategorier. Derefter introducerer jeg de fem artikler, der indgår i temanummeret. De fem artikler præsenterer forskellige vinkler på cybersikkerhed. De tydeliggør, at cybersikkerhed er mangetydigt både begrebsligt og empirisk. De fem artikler tager afsat i forskellige fagdiscipliner og præsenterer en vifte af metodologiske udgangspunkter, konceptuelle tilgange og empirisk fokusområder.

Cybersikkerhedsforskningens tre ansigter

Vi kan ikke forstå vores undersøgelsesobjekter uden en forståelse for de akademiske discipliner og teorier, der konstituerer dem som sådan. En introduktion til cybersikkerhed kræver en forståelse for cybersikkerhedsforskningens historie og position inden for forskellige forskningsdipliner. I det følgende afsnit vil jeg derfor præsentere et grundrids af cybersikkerhedslitteraturen inden for International Politik og sikkerhedsstudier, herunder dens kontekst, udvikling og fortsatte forgreninger. Jeg rubricerer cybersikkerhedslitteraturen i tre kategorier: strategiske studier, governance-studier og kritiske sikkerhedsstudier.

> Jeg rubricerer cybersikkerhedslitteraturen i tre kategorier: strategiske studier, governance-studier og kritiske sikkerhedsstudier

Sondringen mellem de tre litteraturer henviser primært til forskellige teoretiske og metodologiske udgangspunkter. At fremhæve dette skel skal ikke ses som en essentialisering af de tre forskningsgrene. Snarere er der tale om forskellige videnskabelige diskurser, der har udviklet sig sideløbende, adskilt og

overlappende. Grænserne mellem dem er flydende, og de samme empiriske fænomener er ofte genstand for forskningen i alle tre litteraturer. De forskellige teoretiske og metodologiske udgangspunkter betyder imidlertid, at det er analytisk værdifuldt at behandle de tre litteraturer hver for sig.

Strategiske studier: Fra dommedagsscenarier over cyberkrig til gråzonekonflikt

Den akademiske litteratur om cybersikkerhed har sit udspring i USA. I denne litteratur bliver cyberspace betragtet som et femte militær- og krigsdomæne. Litteraturen anvender og tilpasser begreber og metodologiske tilgange, der har rod i realistisk International Politik og strategiske studier, til at foretage analyser af cyberkrig, -konflikt samt militære cybersikkerhedsstrategier (Cavelty og Wenger, 2019; Warner, 2012). Mere specifikt søger den at forstå, hvordan digitale teknologier transformerer krig og konfliktdynamikker og dermed påvirker sikkerhed og magtbalance i det internationale system. Denne tænkning trækker på og understøtter grundlæggende et neorealistisk syn på interstatslig sikkerhed og konflikt i et anarkisk system, hvor stater er black-boxes (de kan alle behandles som kompatible enheder), og det er magtbalancen, der tvinger dem til at handle på bestemte måder.

Den cybersikkerhedslitteratur, der blev udviklet i 1990'ernes og 00'ernes USA, var præget af hyperbolske dommedagsscenarier (Lawson, 2013). I forlængelse heraf opstod der i slutningen af 00'erne en konceptuel og teoretisk diskussion om anvendeligheden af cyberkrigsbegrebet (Libicki, 2007; 2009; Liff, 2012; Ridd, 2012, 2013; Stone, 2013). Thomas Ridds (2013) bog med titlen "Cyber War Will Not Take Place" er symptomatisk for denne debat. Sideløbende med den teoretiske og begrebslige litteratur om cyberkrig udviklede der sig en mere policy-orienteret diskussion om de strategiske, politiske og juridiske implikationer af brugen af militær cybermagt (Farwell og Rohozinski, 2011, 2012).

Det seneste tiår er forskning i cybersikkerhed for alvor blevet rodfæstet i den bredere realistiske og strategiske sikkerhedsdebat. Traditionel konfliktforskning er begyndt at anvende kvantitative metoder til se på effekten af digitale teknologier som værktøjer i udenrigspolitik og konfliktstyring (Valeriano og Maness, 2014; Valeriano et al., 2019). Andre har engageret sig i, hvordan og i hvilken grad cyberspace som krigsdomæne påvirker international orden (Buchanan, 2016; Kello, 2017), afskrækkelse (Godmann, 2010; Fischerkeller og Harknett, 2017; Nye, 2017; Stevens, 2012), offensiv-defensiv-balancen (Garfinkel og Dafoe, 2019; Gartzke og Lindsay, 2015; Slayton, 2017; Smeets, 2019) og tvang (Lindsay og Gartzke, 2018; Valeriano et al., 2018; Sharp, 2017).

Senest har litteraturen kastet sig over cyberangreb, der ikke enkeltstående lever op til de gængse definitioner af krig og væbnet konflikt. De udgør snarere et nyt konfliktrum, der har kilet sig ind mellem krig og fred. Her forsøger særligt stormagter som Rusland og Kina at føre en subtil form for magt- og geopolitik ved konstant at udfordre og overskride eksisterende internationale normer og regler (Breitenbauch og Byrjalsen, 2019; Harknett og Smeets, 2020; Jensen et al., 2019; Liebetrau, 2020).

Governance: Cybersikkerhedens hvem, hvad, hvor

Traditionelt har militæret, efterretningstjenester og andre nationale sikkerhedsinstitutioner været ansvarlige for national sikkerhed. På den måde har man forsøgt at bygge bro over spændingen mellem (ekstraordinær) national sikkerhedspolitik og (normal) demokratisk politik. Når cyberhændelser, der går på tværs af territorielle grænser med stor hastighed, bliver mere almindelige, så bliver de traditionelle statsbundne sikkerhedsstrukturer udfordret. Det er problematisk, da de ikke blot skal sikre samfundet og individet, men også transparens i og demokratisk kontrol med den sikkerhedspolitiske beslutningstagning. Cybersikkerhed tvinger os derfor til at genbesøge grundlæggende politiske og demokratiske spørgsmål om, hvem der skal holdes ansvarlig for hvad og af hvem.

En række forskere har derfor kastet sig over cybersikkerheds-governance det seneste årti. Det dominerende perspektiv undersøger forholdet mellem stater og virksomheder. Ofte gennem begrebet offentlige-private partnerskaber (Carr, 2016; Cavelty og Suter, 2009; Christensen og Petersen, 2017). Som følge af privatiseringen og dereguleringen af mange dele af den offentlige sektor siden 1980'erne befinder store dele af den kritiske (informations-) infrastruktur sig i dag på private hænder. Samlet set fokuserer disse studier på udfordringerne ved, at vi i stigende grad er tvunget til at fæstne lid til, at markedsdynamikker kan definere og understøtte et tilstrækkeligt højt niveau af national cybersikkerhed. Det gælder ikke kun, når vi snakker beskyttelse af kritisk infrastruktur, men også persondatabeskyttelse og beskyttelse mod cyberkriminalitet. Udgangspunktet i litteraturen er, at en grundlæggende forskel mellem økonomiske og politiske sikkerhedsinteresser hindrer de offentlige-private partnerskabers succes.

En anden del af governance-litteraturen undersøger og konceptualiserer den intrastatslige organisering af cybersikkerhedsenheder og –institutioner (Boeke, 2017; Weiss og Jankauskas, 2018). Ydermere kaster en del af litteraturen lys over private it- og cybersikkerhedsfirmaers rolle i relation til specifikke cybersikkerhedshændelser som Stuxnet (Stevens, 2019) og WannaCry (Christensen og Liebetrau, 2019).

Kritisk sikkerhedsteori: Den flygtige og flertydige cybersikkerhed

Den første bølge af forskning i cybersikkerhed inden for kritiske sikkerhedsstudier red på ryggen af sikkerhedsliggørelsesteori (Ericsson, 2001; Cavelty, 2007, 2008; Hansen og Nissenbaum, 2009). Her blev den diskursive indramning af cybersikkerhed samt brugen af metaforer og analogier studeret (Betz og Stevens, 2013; Cavelty, 2013). Første bølge af litteraturen skabte en væsentlig platform for at forstå og diskutere, hvordan forbindelser mellem cybersikkerhed og national sikkerhed bliver skabt samt en indsigt i de sikkerhedspolitiske virkninger af specifikke trusselsrepræsentationer. Som fremhævet af (Liebetrau og Christensen, 2020: 4), så er denne del af litteraturen dog begrænset af, at cybersikkerhed nemt bliver fastlåst som et spørgsmål om

national sikkerhed. Desuden bliver teknologiers politiske rolle indordnet og underlagt det diskursive udgangspunkt.

De seneste år har forskningen i cybersikkerhed inden for kritiske sikkerhedsstudier udviklet sig markant. Med inspiration fra teorier og begreber hentet i videnskabs- og teknologistudier (Cavelty, 2018; Liebetrau og Christensen, 2020: 4), Aktør-Netværk-Teori (Balzacq og Cavelty, 2016), psykoanalyse (Jacobsen, 2020a) og assemblage-teori (Collier, 2018; Stevens, 2019) har andenbølge-litteraturen rettet opmærksomhed mod, hvordan cybersikkerhed og digitalisering udfordrer og (re)konfigurerer tidslige (Stevens, 2016) rumlige (Balzacq og Cavelty, 2016), funktionelle (Christensen og Liebetrau, 2019; Jacobsen 2020; Tanzer 2019) og aktørmæssige (Liebetrau og Christensen, 2020: 4) aspekter af sikkerhed og politik.

Disse studier har bidraget til overvejelser over det epistemologiske og ontologiske grundlag for cybersikkerhed og studiet heraf. Studierne viser, at cybersikkerhed er flertydigt. At cybersikkerhed og cybersikkerhedspolitiske spørgsmål og svar bliver skabt i relationer mellem mennesker, teknologier, devices og infrastrukturer, der samtidig fastholder, unddrager og udfordrer det traditionelle nationalstatslige sikkerhedspolitiske udgangspunkt. Disse tilgange medfører en ontologisk åbenhed, idet de søger at tage højde for de foreløbige og historisk betingede forhold mellem heterogene elementer (Cavelty, 2018; Balzacq og Cavelty, 2016; Liebetrau og Christensen, under udgivelse). Det kræver en "analytisk sensibilitet for den dynamiske, heterogene og forbigående assemblage af cybersikkerhed" og understreger "behovet for situerede og kontekstuelle analyser" (Liebetrau og Christensen, 2020: 4).

Temanummerets bidrag til cybersikkerhedsforskningen

Temanummerets fem artikler tydeliggør, at cybersikkerhed er mangetydigt både begrebsligt og empirisk. De fem artikler tager afsat i forskellige fagdiscipliner og præsenterer en vifte af metodologiske udgangspunkter, konceptuelle tilgange og empirisk fokusområder.

I den første artikel undersøger Mikkel Storm Jensen muligheden for, at cybervåben giver småstater nye strategiske muligheder. Jensen gennemgår en række generelle karakteristika for cybervåben og beskriver, hvad de betyder for småstater generelt og Danmark specifikt. Han konkluderer, at cybervåben delvist ændrer balancen mellem småstater og stormagter i småstaternes favør. Han anfører dog, at der er grænser for de muligheder, våbnene åbner. Særligt for småstater, der som Danmark knytter deres sikkerhedspolitik snævert til medlemskab af en militær alliance som NATO.

Karsten Friis kaster i sin artikel lys over staters mulighed for at forsvare sig og gå til modangreb, når de bliver udsat for skadelige cyberoperationer i fredstid. Artiklen placerer sig dermed i et skæringspunkt mellem sikkerhedspolitik og folkeret. Med udgangspunkt i international ret og internationale normer undersøger Friis, hvordan toneangivende lande agerer, og han diskuterer de

sikkerhedspolitiske konsekvenser af øget brug af offensive cyberoperationer. Empirisk fokuserer artiklen på USA's nye cyberstrategi, der er baseret på vedvarende engagement og fremadrettet forsvar. Desuden undersøger Friis Norges anvendelse af offensive cyberoperationer som forsvarsmiddel, og han argumenterer for, at "Responsibility of States of International Wrongful Acts" er det mest relevante lovværk, når det kommer til offensive cyberoperationer, der falder under grænsen for væbnet konflikt.

I den tredje artikel stiller Jeppe Teglskov Jacobsen skarpt på den aktuelle status for international cybernormdannelse. Han spørger, hvorfor de internationale normforhandlinger er strandet, og hvorfor den vestlige koalitions normstrategi er fejlet? Og hvorvidt en småstat som Danmark kan være normentreprenøren, der skubber den vestlige cybernormdagsorden fremad? Jacobsens svar tager afsæt i, at kampen om internationale cybernormer er karakteriseret ved gensidige beskyldninger om hykleri og manglende anerkendelse af den efterretningsnorm, der dominerer i cyberspace. Han påpeger, at 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.

I sit bidrag undersøger Ole Willers ved hjælp af professions- og ekspertsociologi, hvem cybereksperten egentlig er. Han spørger, hvad der karakteriserer cybereksperten, og hvordan cyberekspertrollen har udviklet sig over tid? Baseret på et nyt dataset omhandlende ekspertprofiler i danske offentlige og private cybersikkerhedsråd og -udvalg argumenterer Willers for, at cybersikkerhedseksperter har bevæget sig væk fra et rent teknisk fokus og hen mod en procesorientering, som både er bredere i fokus og placeret tættere på beslutningstagere. Han argumenterer for, at denne udvikling kan styrke ekspertmagten, som nu er begrænset til få hybride aktører, der formår at bygge bro mellem tekniske, organisatoriske og økonomiske rationaliteter. Han påpeger, at en sådan udvikling kan være demokratisk betænkeligt. Samtidig understreger han, at en mindre teknifiseret cyber-diskurs åbner mulighed for at re-politisere cybersikkerhedsområdet og dermed en inklusion af langt flere aktører i den offentlige debat.

I temanummerets femte og sidste artikel zoomer Lene Wacher Lentz og Jens Myrup Pedersen ind på hacking. De peger på, at hacking både bliver forstået som en forbrydelse og en it-sikkerhedskompetence. Det kan skabe forvirring, da ikke alt er tilladt for at optimere eller teste sikkerheden ved it-systemer f.eks. gennem hacking. Lentz og Pedersen klarlægger, hvornår der bliver straffet for "hacking" efter straffeloven. Desuden undersøger de, om en it-sikkerhedsaktør må bruge "hacking" som et forsvar, når it-systemer bliver angrebet af en fjendtlig "hacker". Dermed illustrerer de, at det kan være vanskeligt at forudsige, hvor grænserne for strafansvar går for den, der vil optimere sikkerheden ved sine systemer.

Litteratur

Balzacq, Thierry og Myriam Dunn Cavelty (2016), "A theory of actor-network for cyber-security", *European Journal of International Security*, 1(2): 176-98.

Betz, David J. og Tim Stevens (2013), "Analogical Reasoning and Cybersecurity", *Security Dialogue* 44(2): 147-64.

Boeke, Sergei (2017), "National cyber crisis management: Different European approaches", *Governance*, 31(3): 449-64.

Borghard, Erica D. og Shawn W. Lonergan (2017), "The Logic of Coercion in Cyberspace", *Security Studies*, 26(3): 452-81.

Breitenbauch, Henrik og Niels Byrjalsen (2019), "Subversion, Statecraft and Liberal Democracy", *Survival*, 61(4): 31-41.

Buchanan, Ben (2016), *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, New York: Oxford University Press.

Carr, Madeline Public-private partnerships in national cyber-security strategies, *International Affairs*, 92:1

Cavelty, D. Myriam (2007) Cyber-terror: Looming threat or phantom menace? The framing of the US cyber-threat debate, *Journal of Information Technology & Politics*, 4:1. 19–36

Cavelty, D. Myriam (2008) C*yber-Security and Threat Politics: US Efforts to Secure the Information Age*. London. Routledge.

Cavelty, D. Myriam (2018), "Cybersecurity Research Meets Science and Technology Studies", *Politics and Governance*, 6(2): 22-30.

Cavelty, D. Myriam & Andreas Wenger (2020) Cyber security meets security politics: Complex technology, fragmented politics, and networked science, *Contemporary Security Policy*, 41:1, 5-32

Cavelty, D. Myriam og Florian J. Egloff (2019), "The Politics of Cybersecurity: Balancing Different Roles of the State", *St Antony's International Review*, 15(1): 37-57.

Cavelty, D. Myriam (2013), "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse", *International Studies Review*, 15(1): 105-22.

Christensen, K. Kristoffer og Tobias 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.

Christensen, K. Kristoffer & Karen L. Petersen, Public-private partnerships on cyber security: A practice of loyalty, *International Affairs*, 93:6. 1435–52.

Collier, Jamie (2018) Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision, *Politics and Governance*, 6:2. 13-21

Cormac, Rory og Richard J. Aldrich (2018), "Grey is the new black: covert action and implausible deniability", *International Affairs*, 94(3): 477–94.

Eriksson, Johan (2001) Cyberplagues, IT, and security: Threat politics in the information age, *Journal of Contingencies and Crisis Management*, 9:4. 200–10

Farwell, P. James og Rafal Rohozinksi (2011), "Stuxnet and the Future of Cyber War", *Survival,* 53(1): 23–40.

Farwell, P. James og Rafal Rohozinksi (2012), "The New Reality of Cyber War", S*urvival*, 54(4): 107–20.

Fischerkeller, Michael P. & Richard J. Harknett (2017) Deterrence is Not a Credible Strategy for Cyberspace. *Orbis*, 61: 381-393.

Garfinkel, Ben og Allan Dafoe (2019), "How does the offense-defense balance scale"?, *Journal of Strategic Studies*, 42(6): 736-63.

Gartzke, Erik Jon R. Lindsay (2015), "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace", *Security Studies*, 24(2): 316-48.

Hansen, Lene og Helen Nissenbaum (2009), "Digital Disaster, Cyber-Security, and the Copenhagen School", *International Studies Quarterly*, 53(4): 1155-75.

Harknett, J. Richard & Max Smeets (2020) Cyber campaigns and strategic outcomes, *Journal of Strategic Studies*.

Healey Jason, red. (2013), *A fierce domain: conflict in cyberspace, 1986 to 2012*, Arlington, VA: Cyber Conflict Studies Association.

Jacobsen, J.T. (2020), "Lacan in the US cyber defence: Between public discourse and transgressive practice", *Review of International Studies*, first view 20. marts, 1–19.

Jensen, Benjamin, Brandon Valeriano og Ryan Maness (2019), "Fancy bears and digital trolls: Cyber strategy with a Russian twist", *Journal of Strategic Studies*, 42(2): 212-34.

Kello, Lucas (2017), *The Virtual Weapon and International Order*, New Haven and London: Yale University Pres.

Lawson, Sean (2013), "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats", *Journal of Information Technology & Politics*, 10(1): 86-103.

Libicki, Martin C (2007), *Conquest in Cyberspace, National Security and Information Warfare*, Cambridge: Cambridge University Press.

Libicki, Martin C (2009), *Cyberdeterrence and Cyberwar*, Santa Monica: Rand Corporation.

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

Liebetrau, Tobias og Kristoffer K. Christensen (2020), "The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces, *European Journal of International Security*.

Liff, Adam P (2012), "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War", *Journal of Strategic Studies* 35(3): 401-28.

Lin, Herbet og Amy Zegart (2018), "Introduction", i Herbert Lin og Amy Zegart, red., *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, Washington D.C: Brookings Institution Press.

Lindsay, Jon R. og Erik Gartzke (2018), "Coercion Through Cyberspace: The Stability-Instability Paradox Revisited', i Kelly M. Greenhill og Peter Krause, red., *Coercion: The Power to Hurt in International Politics*, New York. Oxford University Press.

Nye, Jr., Joseph S. (2016/2017) Deterrence and Dissuasion in Cyberspace. *International Security* 41.3: 44-71.

Rid, Thomas (2012), "Cyber War Will Not Take Place", *Journal of Strategic Studies*, 35(1): 5–32.

Rid, Thomas (2013), *Cyber War Will Not Take Place*, London: Hurst.

Sharp, Travis (2017), "Theorizing cyber coercion: The 2014 North Korean operation against Sony", *Journal of Strategic Studies*, 40(7): 898-926

Slayton, Rebecca (2017) What is the Cyber Offense-Defense Balance? Conceptions, Causes and Assessment. *International Security* 41(3): 72-109

Smeets, Max (2019), "The Strategic Promise of Offensive Cyber Operations", *Strategic Studies Quarterly*, 12(3): 90-113.

Stevens, C.L. (2019). Assembling cybersecurity: The politics andmateriality of technical malware reports and the case of Stuxnet. *Contemporary Security Policy*.

Stevens, Tim (2016) *Cyber Security and the Politics of Time*. Cambridge. Cambridge University Press.

Stevens, Tim, Global cybersecurity: New directions in theory and methods, *Politics and Governance*, 6:2. 1-4

Stone, John (2013) Cyber War Will Take Place!, *Journal of Strategic Studies*, 36:1, 101-108

Tanczer, M. Leonie (2019) 50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers, *Contemporary Security Policy*.

Valeriano, Brandon & Ryan Maness (2018). How We Stopped Worrying About Cyber Doom and Started Collecting Data. *Politics and Governance*. 6(2): 49-60

Valeriano, Brandon og Ryan C. Maness (2014), "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11,' *Journal of Peace Research*, 51(3): 347–60.

Warner, Michael (2012), "Cybersecurity: A Pre-history", *Intelligence and National Security*, 27(5): 781-99.

Weiss, Moritz and Vytautas Jankauskas (2018) Securing cyberspace: How states design governance arrangements. *Governance*.

Angreb i cyberspace er en reel trussel mod Danmark

Temanummer: Cybersikkerhed

TRINE BRAMSEN
Forsvarsminister

I mange år har vi i den vestlige verden levet med et billede af en stadig mere stabil verdensorden. Vi har mere eller mindre taget fred og frihed for givet. Angreb og utryghed var noget, de fleste danskere forbandt med samfund langt fra vores.

Det billede kan vi desværre ikke holde fast i længere. De seneste år har vi set en drastisk udvikling, når det kommer til trusler rettet mod det danske samfund. Vi lever nu i en tid, hvor vi både skal have fokus på øgede fysiske trusler, men i den grad også på den nye kampplads; cyberspace.

> **Faktum er, at der stort set dagligt er konkrete trusler, forberedelser på angreb eller konkrete angreb rettet mod danske myndigheder, virksomheder eller privatpersoner.**

Også på dette område abonnerer mange desværre på den misforståelse, at cyberangreb er noget, der kan ske i en fjern fremtid. Faktum er, at der stort set dagligt er konkrete trusler, forberedelser på angreb eller konkrete angreb rettet mod danske myndigheder, virksomheder eller privatpersoner.

Det siger sig selv, at det kan have katastrofale følger, hvis kritiske dele af vores infrastruktur rammes af angreb. Det gælder eksempelvis el-nettet, transportsektoren, olie- og gasforsyningen eller sundhedssystemet. I de tilfælde kan en computervirus i yderste konsekvens koste menneskeliv.

I Danmark har vi længe haft fokus på cybersikkerhed. Det betyder også, at vi i dag har en god struktur og en stærk faglighed på området. Vi må dog aldrig tage sikkerheden for givet eller begynde at hvile på laurbærrene. Nok ses vi i dag af mange andre lande som værende stærke på feltet. Men truslerne fra cyberspace udvikler sig hver eneste dag, time og sekund. Derfor er det afgørende, at vores myndigheder har såvel muskler som ressourcer til at gøre det samme. I sidste ende er det en politisk prioritering at sikre dette. Det er også baggrunden for, at et bredt flertal af partier har afsat et stort millionbeløb, der skal udmøntes over de kommende år. For mig at se er det helt afgørende, at der er prioriteret økonomi til de trusler, vi ved vokser i fremtiden – men som vi endnu ikke ved, hvad konkret indeholder.

Center for Cybersikkerhed er den myndighed under Forsvarsministeriet, der har ansvaret for at monitorere og reagere på cybertrusler. Det giver på alle må-

der god mening. Langt hovedparten af truslerne kommer fra udlandet. Derfor er det afgørende, at der er en tæt koordination med Forsvarets Efterretningstjeneste, der jo netop rækker ud over landets grænser. Området er desuden i så kraftig udvikling, at det ikke må betragtes som drift. Det er et udviklingsområde, der kræver politisk fokus og styring.

Truslen fra cyberkriminalitet er som nævnt rettet mod alle i Danmark. Vi ser en stigende trussel fra målrettede ransomware-angreb mod danske myndigheder og virksomheder. Fremmede stater og aktører bruger cyberspionage til at indhente fortrolige oplysninger – fra myndigheder og kommercielle virksomheder. Vi ser også i disse år påvirkningskampagner med forsøg på at påvirke samfundsdebatten, så der skabes misinformation eller skabes ustabilitet.

Alt i alt står vi i en situation, hvor arbejdet for at gøre Danmark digitalt sikkert er vigtigere og mere presserende end nogensinde. Danskerne skal være trygge ved digitale tjenester og vide, hvordan man beskytter sig og færdes sikkert digitalt. Det er afgørende, at virksomheder og myndigheder har konstant fokus på cyber- og informationssikkerhed, så brugere og samarbejdspartnere bevarer tilliden til de ydelser, der leveres. Samfundsvigtige funktioner skal være beskyttet, så økonomien og samfundet ikke rammes af større forstyrrelser.

At cybersikkerhed er et komplekst felt, vidner de forskellige bidrag til dette temanummer af Økonomi og Politik om. Fra et historisk blik på cybersikkerhedseksperten over offensive cyberoperationer rundt om i verden. Herfra til normopbygning og cybersikkerhed til et udsnit af begreber og discipliner inden for området. Det er læsestof, man bliver klog af. Dette på et emne, der kun bliver stadig mere centralt, påtrængende og mere komplekst i årene, der kommer.

God læselyst.

Småstater og cybervåben – nye muligheder og nye begrænsninger

Temanummer: Cybersikkerhed

Denne artikel handler om, hvordan cybervåben giver småstater en række nye strategiske muligheder. Den forklarer først, hvorfor der ikke er megen hjælp at hente i den eksisterende forskningslitteratur. Artiklen gennemgår derefter en række generelle karakteristika for cybervåben ét ad gangen og beskrive hvad de betyder for småstater generelt og Danmark specifikt. Det konkluderes, at cybervåben delvist ændrer balancen mellem småstater og stormagter i småstaternes favør. Men der er grænser for de muligheder, våbnene åbner. Særligt for småstater, der som Danmark knytter deres sikkerhedspolitik snævert til medlemskab af en militær alliance som NATO. Cybervåben er vanskeligere at anvende i NATO end konventionelle våben både på det strategiske og operative niveau – og især hvis vi ikke er i krig. Det er derfor måske ikke overraskende, at det stadig ikke er helt klart, hvordan Danmark vil anvende disse våben – særligt i fredstid.

MIKKEL STORM JENSEN
militæranalytiker, Forsvarsakademiet, msje@fak.dk

Et uopdyrket teoretisk felt

Fra Danmarks sikkerhedspolitiske perspektiv, har den militærstrategiske forskningslitteratur to væsentlige huller: Der er meget lidt, der går i dybden med hvilke nye muligheder en småstat har med cybervåben, og der mangler noget, der beskriver, hvordan de nye våben påvirker eller fungerer i alliancer.

Strategisk teori med udgangspunkt i en realistisk[1] forståelse af forholdet mellem stater har indtil udviklingen af teknologierne bag cyberdomænet taget afsæt i staters evne til at generere fysiske midler til at påtvinge andre stater deres vilje. Derfor har staters økonomi, befolkning, størrelse og geografi været de gennemgående parametre for analyser af de kapabiliteter, som definerer stater som stormagter eller småstater.[2] Endvidere har forskningslitteraturen om strategi ofte taget udgangspunkt i stormagters strategiske valgmuligheder uden hensyntagen til småstaternes særlige begrænsninger (Bailes, Rickli og Thorhallsson, 2014: 32; Wivel et al., 2014: 7, 18; Bailes, Thayer og Thorhallsson, 2016: 10).

Men cybervåben giver småstater nye muligheder for at agere militært. Cyberdomænets egenskaber ophæver delvist de begrænsninger, som tid, rum og økonomiske forudsætninger hidtil har udgjort for småstaters militære muligheder. Kamp i cyberdomænet kræver ikke kostbar fysisk infrastruktur, men afgøres af viden og kunnen, og angreb kan ramme mål knyttet til cyberdomænet over hele kloden med lysets hastighed (Pace, 2006; Arquilla, 2012; Peterson, 2013; Bebber, 2017). Derfor kan stater, som ud fra de traditionelle parametre fremstår som småstater, nu true stormagter gennem cyberdomænet

(Clarke, 2010: 254; Rivera, 2015; Tor, 2017: 111). Den teknologiske udvikling udfordrer dermed en klassisk realistisk forståelse af forholdet mellem stater: "A great power is a state which is able to have its will against a small state [...] which in turn is not able to have its will against a great power" (Morgenthau, 1948: 129). Alligevel tager hovedparten af litteraturen om cyberstrategi implicit udgangspunkt i stormagters rationelle valgmuligheder og dilemmaer i et sikkerhedspolitisk vacuum, hvor det er de direkte effekter af statens handlinger og ikke handlingernes indirekte effekter på allierede, der er fokus for analysen (Hughes og Colarik, 2016: 19).[3] Der er kun få eksempler på specifikke småstatsvinkler på cyberstrategi: Antologien *Cyberconflicts and Small States* fra 2016 diskuterer småstaters sikkerhedspolitiske overvejelser, men fokuserer på de defensive aspekter (Janczewski og Caelli, 2016). Rivera holdt i 2015 et oplæg på en NATO-konference med titlen *Achieving cyberdeterrence and the Ability of Small States to Hold Large States at risk*. En lovende titel fra et småstatsperspektiv, men reelt handler hans artikel dog om både småstaters og stormagters evne til at afskrække modstandere i cyberdomænet, og han udfordrer ikke sine ret vidtgående antagelser om småstaters evne til at true modstanderes ømme punkter med cybermidler (Rivera, 2015). Hughes et al. analyserede året efter New Zealands teoretiske fordele og ulemper ved at udvikle offensive cyberkapabiliteter. Deres artikel udmærker sig ved at være meget konkret, men desværre undgår de alle udfordringer ved at bruge cybervåben i alliancer ved at antage, at allierede deler hemmeligheder uden problemer (Hughes og Colarik, 2016). Som det vil fremgå senere i denne artikel, vurderer jeg, at det er en forkert antagelse. Den militærstrategiske faglitteratur, der beskæftiger sig med småstaters brug af cybervåben i koalitioner, er altså meget, meget begrænset. Det er dette teoretiske hul, mit arbejde i al beskedenhed forsøger at gøre lidt mindre.

Cyberangreb: Nok se, ikke røre?

Med det på plads, så lad os betragte, hvilke nye muligheder offensive cyberkapabiliteter kan give en småstat som Danmark. I den sammenhæng kan det være nyttigt først at afklare et par terminologiske begreber om offensive og defensive militære operationer i cyberdomænet. Forsvaret offentliggjorde i 2019 den første danske doktrin for militære cyberspaceoperationer (CO). Ligesom den seneste amerikanske doktrin inddeler den danske militære doktrin cyberoperationer i to kategorier: Offensive og defensive (US Army, 2017: 1–7, 1–8; Forsvarsakademiet, 2019: 4).

Ifølge den danske doktrin er defensive operationer (DCO) "CO, der uden at anvende magt har til hensigt at bevare eller genskabe egen bevægelses- og handlefrihed i cyberspace". Det er ikke alle NATO-lande, der som Danmark doktrinært begrænser defensive cyberoperationer til operationer uden magtanvendelse. Således kunne Danmark, sådan som Holland har gjort, have valgt at åbne mulighed for at lade statsgennemførte modangreb på angribere i cyberdomænet – "hack back" – ligge inden for kategorien DCO (Hennis-Plasschaert, 2015).

Den anden kategori af militære cyberoperationer er offensive operationer (OCO): "OCO defineres som CO, der har til hensigt at anvende magt i eller gennem en modstanders del af cyberspace". Danmarks og USA's opdeling i offensive og defensive operationer udelader dog en vigtig nuance, som USA's tidligere doktriner fik med, nemlig spionage. I en ældre doktrin fra 2013 deler det amerikanske forsvar cyberoperationer op i *computer network defence* (CND), *-attacks* (CNA) og *–exploitation* (CNE) (US Joint Chiefs of Staff, 2013). Forskellen på CNA og CNE er, at i CNA ødelægger eller ændrer man data eller fysiske genstande, der er forbundet til netværket, mens CNE er spionage, hvor man skaffer sig adgang til informationer gennem modstanderens netværk, men ikke ødelægger eller ændrer noget.

Cyberspionage: Nok se, ikke røre!

For at tage de nye muligheder i CNE for et land som Danmark først åbner cyberspionage – eller indhentning, som det hedder blandt professionelle – nye strategiske perspektiver. Det er, fordi indhentningen ikke er geografisk begrænset af landets fysiske beliggenhed, men kan udstrækkes til hele internettet. Opgaven varetages i Danmark af Forsvarets Efterretningstjeneste (FE), hvis operations- og indhentningssektor har en afdeling for netværksindhentning (Forsvarets Efterretningstjeneste). Spionage via internettet byder på en række nye fordele, men indebærer også visse nye risici. De medfører dog kun marginale ændringer i Danmarks sikkerhedspolitiske situation på strategisk niveau.

> For en småstat er det derfor ikke helt risikofrit at gennemføre indhentning gennem internettet

Traditionel spionage gennemført via internettet udgør en begrænset sikkerhedspolitisk risiko: Ligesom for "gammeldags" spionage er det "flovt" for en stat, hvis man bliver afsløret i cyberspionage. Der er dog nogen former for cyberspionage, der medfører unikke ricisi: Hvis en stat opdager, at nogen forsøger at indsamle tekniske oplysninger om kritiske netværk og installationer, kan det være meget svært at vurdere, om indhentningen "bare" er indsamling af informationer, eller om det er forberedelser til et senere cyberangreb med ødelæggende effekt. For en småstat er det derfor ikke helt risikofrit at gennemføre indhentning gennem internettet, fordi erkendte forsøg kan blive misforstået som angrebsforberedelser og medføre utilsigtet eskalation fra den ramte part, måske endda uden for cyberdomænet (Cavaiola, Gomperto og Libicki, 2015: 84; Hansel, 2018: 528). Hidtil har der ikke været offentliggjort eksempler på eskalation, men risikoen er til stede, især hvor tidspres og vanskeligheder ved med sikkerhed at bestemme, hvorfra et angreb kommer, også kan spille ind. På cyberområdet er krigshistorien endnu ikke en generation gammel, så politiske og militære beslutningstagere har ikke mange erfaringer at drage på i pressede situationer. Særligt spionage mod potentielle modstanderes kommando- og kontrolsystemer for atomvåben indebærer en betydelig risiko (Klare, 2019).

Danmark kan altså – med enkelte forbehold – forsøge at benytte de nye muligheder til at styrke FE's indhentning mod traditionelle sikkerhedspolitiske mål. Teoretisk kunne Danmark også vælge at forfølge helt nye sikkerhedspolitiske mål med vores CNE-kapacitet. Vi kunne i princippet rette den mod andre landes civile virksomheder. FE kunne indhente forretningshemmeligheder og forskningsresultater med henblik på at videregive dem til danske virksomheder for at styrke Danmarks økonomiske konkurrenceevne. Det er sandsynligt, at Kina bruger dele af sine statslige indhentningskapabiliteter på den vis, både i og udenfor cyberdomænet (Jensen, Valeriano og Maness, 2019). Af mange årsager er det dog en usandsynlig udvikling for de fleste småstater. Ikke mindst på grund af deres handelspartneres sandsynlige reaktion, når den spionerende småstat en dag bliver taget i det. Fra et strategisk perspektiv er det i den sammenhæng væsentligt, at Danmark er en småstat med en åben og udadrettet økonomi. Det vil være relativt let og billigt for andre stater at straffe Danmark ved at isolere os handelsmæssigt og politisk og finde alternative handelspartnere. Her har Kina et betydeligt større spillerum som stormagt med sit enorme og købedygtige marked, som det er omkostningsfuldt at lægge på is (Harold, Libicki og Stuth Cevallos, 2016: 143–61). En sådan ændring af opgaveporteføljen ville i øvrigt kræve en ændring af loven om FE's opgaver (Forsvarsministeriet, 2017).

Offensive cyberkapabiliteter til spionage byder altså småstater på nye tekniske muligheder og større geografisk rækkevidde, men de ændrer ikke umiddelbart afgørende på Danmarks strategiske position i det internationale system.

Cyberangreb: Også røre!

Fordele ved cybervåben for småstater

Til gengæld byder cybervåben og potentialet til at kunne gennemføre CNA på mange nye strategiske muligheder og fordele, der kan virke tillokkende på en småstat, og som i nogen tilfælde kan ændre deres muligheder for at føre militær sikkerhedspolitik.

Cybervåben har en række egenskaber, der gør dem og deres effekter anerledes end konventionelle våben. Her vil jeg fokusere på dem, der har potentiale til at rokke ved de traditionelle strategiske overvejelser om, hvad småstater kan og ikke kan militært: Cybervåbens relativt lave pris, deres ubegrænsede geografiske rækkevidde, deres potentiale til strategisk effekt, deres lille logistiske fodaftryk og endelig det forhold, at det kan være meget vanskeligt eller tidskrævende at finde ud af, hvorfra et cyberangreb kommer.

Cybervåben er relativt billige. Udvikling af kapabiliteter inden for offensiv cybermagt kræver som nævnt ovenfor ikke, at en stat opbygger eller finansierer omfattende industri og forskning. Det er nødvendigt, hvis en stat vil til at bygge sine egne fly, missiler, avancerede krigsskibe eller masseødelæggelsesvåben. Selv hvis en småstat i stedet for at producere konventionelt krigsmateriel indkøber det hos større, allierede producenter (sådan som de fleste

småstater ud over Sverige og Israel gør), er moderne krigsmateriel dyrt. Omkostningerne er ikke begrænset til indkøb, for materiellet kræver også omskoling af personel, faciliteter til opbevaring og bevogtning samt ikke mindst reservedele og vedligeholdelse i al den tid, man beholder dem. Cybervåben er bestemt ikke gratis, men prisen for at opbygge et team af specialister og udruste dem med det nødvendige IT-udstyr er sandsynligvis en brøkdel af de samlede levetidsomkostninger for moderne fly eller skibe. Cybervåbens pris kan variere meget og afhænger sandsynligvis af, hvor avancerede de er, hvor målrettede de er, samt hvor megen forskning og evt. spionage der skal til for at udvikle dem (Smeets, 2016).[4] Hvis staten i forbindelse med et angreb kan nøjes med at bruge de samme cybervåben som kriminelle har til rådighed – evt. med enkelte justeringer – kan prisen være helt nede i få hundrede eller tusinde kroner for det enkelte angreb (Migliano, 2018). Hvis derimod angrebet både kræver omfattende indhentning mod målet og kræver en høj grad af specialiseret programmering for *kun* at ramme det tiltænkte mål for at undgå i "collateral damage", kan prisen løbe op i hundreder af millioner af kroner.

» **Cybervåben er bestemt ikke gratis, men prisen for at opbygge et team af specialister og udruste dem med det nødvendige IT-udstyr er sandsynligvis en brøkdel af de samlede levetidsomkostninger for moderne fly eller skibe**

Et eksempel på den første type af relativt billige cybervåben er NotPetya-angrebet i 2017. Her brugte den russiske militære efterretningstjeneste, GRU[5], modificeret kriminel software til at angribe Ukraines økonomi. Den oprindelige, kriminelle software var designet til at kryptere ofrenes data. Ofrene kunne så købe en nøgle til at dekryptere sine data for bitcoins. GRU modificerede programmet, så det bl.a. ikke bare krypterede, men komplet ødelagde data på de ramte systemer. Angrebet blev som sagt rettet mod Ukraines økonomiske infrastruktur, men softwaren havde ingen indbyggede begrænsninger, der kunne forhindre spredning til mål udenfor Ukraine. Derfor bredte angrebet sig til store dele af verden og forårsagede omkostninger for mindst 10 milliarder dollars (McAfee; Statement from the Press Secretary, 2018; Greenberg, 2018; UK Foreign Office, 2018). NotPetya var en begrænset videreudvikling af et tilgængeligt kriminelt program, og det har næppe været dyrt at anskaffe. Samtidig ramte programmet i flæng uden hensyn til, om de tilfældigt ramte mål var legitime eller en del af den konflikt, angrebet indgik i. Småstater kan altså skaffe billige cybervåben med stor effekt, hvis man ikke stiller krav om, at de kun må ramme specifikke, militære mål og ikke ødelægge i flæng. Ulempen ved den slags våben for en småstat er igen, at omkostningerne i form af omverdenens reaktioner på angrebet må forventes at være store. Og uagtet, at der ikke er international enighed om, hvordan krigens love skal fortolkes i cyberdomænet, så er det ret åbenlyst, at våben, der ikke kan rettes mod et bestemt mål, er ulovlige (Forsvarsministeriet, 2016).

I den modsatte ende af prisskalaen er STUXNET, et cyberangreb som USA og Israel angiveligt gennemførte mod Irans atomvåbenprogram i 2009-10.[6] Angrebet blev gennemført ved at udvikle og deployere software, der ændrede funktionen af de indbyggede computere i centrifugerne i det Iranske Natanz-anlæg, hvor iranerne udvandt Uran-isotoper, som kunne anvendes til fremstilling af atomvåben. Softwaren var meget avanceret og specifikt designet til ikke at påvirke andre typer computere end præcis dem i Natanz-centrifugerne og endda kun dem, der stod opstillet i præcis samme sammensætning, som i Natanz. Samtidig var softwaren konstrueret med sikkerhedsforanstaltninger, der gjorde, at den ophørte med at virke senest i 2012. Omkostningerne til konstruktionen af STUX-net er i sagens natur ikke kendt, men det er sandsynligt, at der er medgået titusinder af mandtimer og millioner af dollars til udviklingen. Det må samtidig have krævet en betydelig og sandsynligvis omkostningskrævende efterretningsindhentning at afklare den tekniske sammensætning af de hemmelige iranske atomanlæg og derefter skaffe adgang til at inficere anlæggene med softwaren, idet de angiveligt ikke var direkte sluttet til internettet (Falco, 2012: 19–20; Acton, 2017: 47).

Det er altså indimellem svært og derfor også dyrt at lave "lovlige" våben, der kan begrænses til kun at ramme bestemte mål. Omkostningerne til STUX-NET har været betydelige – men hvis man kan opnå sikkerhedspolitiske mål, som f.eks. at sinke Irans udvikling af atomvåben, er det stadig relativt billigt. Det er umuligt at lave direkte sammenligninger, men alligevel: I 2017 forventede man, at Danmarks kommende 27 F-35 jagere, der skal erstatte F-16, vil koste ca. 670 millioner kroner i indkøb og 1,8 milliarder kroner i drift pr. styk gennem deres forventede 30-årige levetid (Statsrevisorerne, 2017). Det giver en årlig omkostning i 2017-kroner på ca. 83 millioner pr. fly. For de penge som en enkelt F-35 koster at købe, vedligeholde og anvende, kan en småstat altså ansætte en hel del softwareudviklere og forsyne dem med såvel IT som den nødvendige spionage for at de kan virke.

» For de penge som en enkelt F-35 koster at købe, vedligeholde og anvende, kan en småstat altså ansætte en hel del softwareudviklere og forsyne dem med såvel IT som den nødvendige spionage for at de kan virke.

En anden fordel er cybervåbens føromtalte ubegrænsede geografiske rækkevidde. Igen har cybervåben relativt lave udviklingsomkostninger i forhold til konventionelle våben som f.eks. missiler med stor rækkevidde. Det gør det nu muligt for småstater at anskaffe våbensystemer i form af software, der kan ramme mål på den anden side af jorden – hvis målene er på nettet. Således kunne Nordkorea i 2014 ramme Sony i USA i et forsøg på at standse en film, der gjorde grin med "Den Unge Leder" og mindst 150 lande verden over i 2015 med angrebet "WannaCry", der skulle skaffe penge til Nordkoreas tomme statskasse ved at afpresse ofrene (U.S. Departement of Treasury, 2019).

Statslig cyberkriminalitet er siden blevet en særlig nordkoreansk specialitet – andre lande bruger foreløbig cybervåben til politiske formål.

Den næste fordel er cybervåbnenes potentiale til strategisk effekt – her forstået som en effekt med vidtrækkende skadelige konsekvenser. Effekterne af Not-Petya i 2017 på de ramte virksomheders logistik var voldsomme (Greenberg, 2018). Hvis Rusland rent hypotetisk (og helt bortset fra de øvrige politiske og militære konsekvenser) ville opnå samme grad af kaos, tab og forsinkelser alene på Maersk med konventionelle angreb, ville det have krævet hundredevis af luftangreb på skibe, havne og kontorer i hele verden. Cybervåben har – heldigvis – ikke haft lejlighed til at vise deres fulde, ødelæggende potentiale eller mulige mangel på samme, for der har i internettets tidsalder endnu ikke været krig mellem moderne, højtudviklede stater. De cyberangreb, stater hidtil har foretaget mod hinanden, og som er kommet til offentlighedens kendskab, har alle været led i konflikter, der har været under tærsklen for interstatslig krig, og såvel angrebene som effekterne har været begrænsede. Det gælder også de få offentliggjorte angreb med direkte kinetisk effekt på civil, kritisk infrastruktur. For eksempel lukkede et russisk angreb et ukrainsk elværk i december 2015 i seks timer, og i april 2020 forsøgte Iran muligvis at ramme dele af vandforsyningen i Israel, uden at det dog lykkedes (Buchanan og Sulmeyer, 2017: 3; Joffre, 2020; Nakashima og Warrick, 2020). Vi har derfor ikke set stater udfolde deres fulde militære cyberpotentiale, men er – igen heldigvis – begrænset i vores overvejelser af teoretiske ekstrapoleringer af den observerede, men begrænsede militære brug af cyberangreb. På samme måde som teoretiske overvejelser i 1920'erne om betydningen af strategiske bombefly gik fra, at bombefly i fremtidige konflikter ville være altafgørende, til at fly ville have en understøttende rolle i forhold til de øvrige midler til krigsførelse, varierer vurderingerne af, hvor stor en rolle cybervåben vil spille i fremtidige krige.

En yderligere fordel ved cybervåben er afledt af, at man ikke skal opbygge sværindustri eller store militære anlæg som flyvestationer, havne eller kaserner for at anskaffe dem. Det er for en udenforstående umuligt at se, om en almindelig kontorbygning med almindeligt IT-udstyr og almindelige ansatte i virkeligheden er en stats udviklings- og opbevaringscenter for cybervåben. Hvis en stat er diskret omkring sine militære cyberkapabiliteter (og de fleste stater er *meget* diskrete på det område), er der ikke mange signaturer, som en fremmed efterretningstjeneste kan se ud af satellitfotos eller spor af øvelsesaktivitet for at vurdere, hvor kapabel staten er i cyberdomænet. Det betyder, at en småstat kan udvikle disse kapabiliteter, uden at hverken fjender – eller venner – finder ud af det. Det betyder også, at småstater lettere kan overdrive deres kapabiliteter i cyberdomænet for at gøre indtryk på førnævnte fjender og venner, end de kan til lands, til vands og i luften – såkaldt strategisk *swaggering* (Art, 1980: 10; Neuman og Poznansky, 2016). Cybervåben er som skabt til swaggering: En stat kan relativt mere troværdigt signalere, at den har en offensiv cyberkapabilitet, uden at den har det, end den kan bilde omverdenen ind, at den har et hangarskib. Man skal faktisk bare sige, at man

har det, men at man er meget tilbageholdende med at bruge det. I de fysiske domæner er det muligt at vurdere småstaternes militære potentiale ud fra deres hærs, flådes og flyvevåbens tekniske og operative tilstand allerede i fredstid ved f.eks. at betragte dem på satellitfotos og følge deres træningsaktiviteter. I cyberdomænet kommer staternes militære cyberkapabiliteter først for en dag, når konflikten er i gang.

> **Cybervåben er som skabt til swaggering: En stat kan relativt mere troværdigt signalere, at den har en offensiv cyberkapabilitet, uden at den har det, end den kan bilde omverdenen ind, at den har et hangarskib**

Den sidste fordel ved cybervåben, der kan være særlig gavnlig for småstater, er, at det kan være vanskeligt og tidskrævende (men sjældent umuligt) at spore, hvor et cyberangreb kommer fra. Hvis en stat bruger konventionel vold mod eller i en anden stat, er det normalt relativt let med et fordansket engelsk udtryk at attribuere angrebet. Angrebsmidlerne, hvad enten det er en bombe, gift eller andet, efterlader fysiske spor og rester, der kan anvendes til identificere angriberen. Det samme gælder fremføringsmidlet; selv hemmelige agenter, droner og specialstyrker efterlader sig spor i form af rejseplaner, radarspor eller optagelser på sikkerhedskameraer. Cybervåben efterlader elektroniske spor, men angriberen kan gøre meget for at skjule sin identitet og sløre ophavet ved at lægge falske spor ud, der peger på andre stater eller kriminelle. Det betyder, at offeret for et velgennemført angreb sandsynligvis skal bruge en del tid på med sikkerhed at identificere angriberen. Det kan især i en krisesituation, hvor der er stort tidsmæssigt pres på beslutningstagerne, være en væsentlig faktor (Taillat, 2019: 371). I et helt hypotetisk eksempel kunne man forestille sig følgende situation: Et lille baltisk land gennemfører et cyberangreb på Rusland under en grænsestrid, hvor det føler sig meget truet. Angrebet gennemføres, så det umiddelbart ser ud som om, det kommer fra USA, i håb om at Rusland på kort sigt enten bliver skræmt og deeskalerer konflikten eller fejlagtigt "modangriber" USA, der dermed inddrages i konflikten. Eksemplet er som sagt ganske hypotetisk og forudsætter en situation, hvor det lille land virkelig er desperat af angst for at blive svigtet af sine allierede. Pointen er, at en sådan desperat handling er blevet en mere realistisk mulighed for en småstat med cyber våben.

Ulemper ved cybervåben for småstater

På baggrund af alle disse fordele kunne man forledes til at tro, at småstater med cybervåben har fået adgang til relativt billige våben med ubegrænset rækkevidde og potentiale til store ødelæggende effekter. Hvis staterne forfølger en swaggering-strategi, kan de i hvert fald lade som om, de har mere troværdighed nu end før cybervåben blev en mulighed. Hvis det er rigtigt, vender det som nævnt i indledningen op og ned på den klassiske ressourcebaserede vurdering af, hvilke stater der er stormagter, og hvilke der er småsta-

ter i det internationale system. Men cybertræerne gror ikke ind i himlen. De strategiske effekter af cybervåben er sjældent de samme som af konventionelle våben, og det påvirker, hvad stater kan bruge dem til.

For det første er effekterne af cyberangreb generelt midlertidige og reversible – dvs. skaderne kan ofte repareres, og opfølgende angreb med samme cybervåben forhindres. Da Maersk først havde identificeret NotPetya-angrebet og taget de fornødne modforholdsregler, kunne firmaet begynde at rekonstruere sine databaser og bruge sine skibe, containere og havnefaciliteter som før. Hvis skibene og havnene var blevet bombet (igen ser vi bort fra de mange andre afledte konsekvenser), havde det taget lang tid at genopbygge kapabiliteterne. Cybervåben kan heller ikke genbruges på samme måde som konventionelle våbensystemer som bombefly. De må genopfindes hver gang de systemer, de er designet til at udnytter bliver opdateret. Ofte vil selve cyberangrebet være den anledning, der udløser opdateringer og andre modforanstaltninger, som forhindrer fremtidige angreb med samme våben. For eksempel kunne Maersk ved at opdatere og omstrukturere sin IT-infrastruktur beskytte sig effektivt mod nye angreb med NotPetya. Hvis Rusland hypotetisk ville gentage effekterne af NotPetya-angrebet, ville det have været nødvendigt at tage nye cybervåben i brug. Det er, som STUXNET-angrebet på Natanz demonstrerede, naturligvis muligt i nogen tilfælde at forårsage alvorlige ødelæggelser i den fysiske verden med cyberangreb. Det vil dog sandsynligvis være vanskeligt at gennemføre så mange og så omfattende, ødelæggende cyberangreb på en anden stat, at denne ikke vil kunne slå igen i løbet af ret kort tid (Cimbala, 2014: 283).

Man kan derfor godt forestille sig, at en småstat kan gennemføre et "cyber-Pearl Harbour". Men hvis det ikke følges op af et "konventionelt Pearl Harbour", vil den angribende småstat snart blive udsat for den angrebne parts gengældelse (Junio, 2013: 131; Wirtz, 2017: 760). Derfor har cybervåben næppe samme afskrækkende effekt som store, konventionelle militære kapabiliteter eller masseødelæggelsesvåben, f.eks. atomvåben, uanset hvor meget en småstat opbygger sit cyberarsenal. Selv om det er ret usandsynligt, så lad os for eksemplets skyld antage, at Nordkorea havde udviklet cybervåben, der kunne slukke strømmen i store dele af USA. I en hypotetisk eskalerende krise truer Nordkorea først USA med at gennemføre "alle cyberangrebs moder" og fører til sidst i desperation truslen ud i livet. Strømafbrydelserne i USA medfører omfattende gener, store økonomiske tab og endda tab af flere tusinde menneskeliv. Men efter 14 dage er al strøm oppe igen i USA, og Nordkorea har ikke nye cybervåben, der kan slukke den reparerede og opdaterede infrastruktur. Til gengæld er USA nu blevet virkelig vred og gør klar til at slukke for Nordkorea permanent. I virkeligheden har Nordkorea da heller ikke opgivet sit atomarsenal eller arbejdet på at fremstille interkontinentale missiler, der kan ramme USA fysisk.

For det andet er cybervåben gode til at gennemføre planlagte angreb, men mindre gode til i defensivt regi at gennemføre improviserede modangreb.

Stater kan naturligvis udvikle og "opmagasinere" cybervåben til forudsete missioner og opgaver, men hvis et uvarslet angreb kræver improvisationer og udvikling af nye cybervåben, kan det tage uger eller måneder at indhente de fornødne informationer om de fjendtlige systemer og derpå udvikle cybervåben, der kan håndtere dem. Den nødvendige tid må skaffes ved at forsvare sig med konventionelle våben indtil da. Helt banalt kan cybervåben heller ikke fysisk beskytte statens eget territorium eller besætte modstanderens efter et vellykket angreb. Her må fysiske kapabiliteter til.

Lille stat, hvad nu?

Cybervåben er altså ikke et mirakel, der giver ambitiøse småstater som Nordkorea ubegrænset militærstrategisk spillerum eller småstater som Danmark mulighed for at undvære de allierede i NATO. Men cybervåben er et økonomisk opnåeligt supplement til småstaters konventionelle militære kapaciteter. Cybervåben kan understøtte småstaters forsvar og give dem nye muligheder for i begrænset omfang at true eller skade andre stater såvel fysisk som i cyberdomænet uden hensyn til geografiske begrænsninger og endda med en vis mulighed for at sløre, hvor angrebet kom fra. Småstater kan udvikle dem uden, at venner eller fjender ved det. Alternativt kan småstater, indtil deres bluff bliver afsløret i en konflikt, prale og overdrive deres offensive cyberkapabiliteter for at imponere samme venner og skræmme førnævnte fjender.

En række småstater har allerede kastet sig over disse muligheder. Hvis man groft betragter alle andre end USA, Kina og Rusland som småstater, så har Israel, Iran og Nordkorea brugt cybervåben mod andre stater. Storbritannien har brugt cybervåben i kampen mod ISIS i nedkæmpelsen af deres protostat (Shoorbajee, 2018). Danmark erklærede som sagt officielt i 2018, at vi har udviklet offensive cyberkapaciteter siden 2016, og at vores kapabilitet angiveligt skulle være operativ med udgangen af 2019.

> **Det er meget svært at dele viden om og koordinere brugen af cybervåben i alliancer som NATO. Cybervåben bliver af en lang række årsager holdt ekstremt hemmelige af de stater, der udvikler dem**

For småstater, der som Danmark baserer hele deres forsvar på medlemskabet af en alliance, er der dog yderligere en binding på brugen af cybervåben, som alliancefrie lande som Iran, Nordkorea og Israel ikke lider under. Det er meget svært at dele viden om og koordinere brugen af cybervåben i alliancer som NATO. Cybervåben bliver af en lang række årsager holdt ekstremt hemmelige af de stater, der udvikler dem. For eksempel bliver de uanvendelige, hvis den mindste viden om deres virkemåde eller de svagheder, de udnytter, bliver afsløret (Libicki, 2009: XIII, 18; Smith, 2013: 83). En anden grund er, at de mest avancerede cybervåben på samme måde som STUXNET sandsynligvis bliver udviklet på baggrund af sensitiv national indhentning – spionage – hvis kilder

og metoder også risikerer at blive afsløret, hvis man deler informationer om sine cyberkapabiliteter med sine allierede. Endvidere udnytter cyberangreb ofte de samme svagheder som cyberspionage. Da angrebet afslører den udnyttede svaghed, er cyberspionerne og cyberkrigerne derfor nødt til at afklare hvis mission, der er vigtigst. Nogen af de få, offentligt tilgængelige erfaringer fra USA's cyberkampagner mod ISIS tyder på, at selv intern koordination mellem forskellige amerikanske cyberrelaterede indhentnings- og kampenheder har været meget vanskelig (USCYBERCOM, 2020). Og ISIS har på cyberområdet endda ikke været en vanskelig modstander, særligt ikke hvis man sammenligner med, hvad NATO ville være oppe imod i en hypotetisk konflikt med Rusland. Det er sandsynligt, at alliancer som NATO har svært ved at dele "almindelige" hemmeligheder, og her kan man endda nøjes med at dele selve den indhentede information. Det er formentlig derfor, at NATO-landene ikke koordinerer deres forsvarspolitik og anskaffelser på cyberområdet på samme måde som med konventionelle kapaciteter. NATO har begrænset sin ambition til at give mulighed for, at de enkelte lande kan bidrage til operationer med cybervåben uden at dele viden om dem med de allierede (Rizwan og Ricks, 2017). NATO kalder dem ikke engang cybervåben, men er blevet enige om den diplomatisk spiselige, men operativt noget gumpetunge betegnelse *Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)* (Forsvarsakademiet, 2019).

Hvis man meningsfyldt skal dele viden om et cybervåben med sine allierede, vil de i mange tilfælde skulle have mange detaljer om våbnet og dets virkemåder. Nogen gange helt ned til information om selve den software, der udgør våbnet. Det er formentlig derfor, at NATO har begrænset sin ambition til at integrere effekterne af cyberangreb i sine operationer frem for at koordinere brugen af cybervåben (Rizwan og Ricks, 2017). Hertil kommer, at der ikke er nogen konsolideret international enighed om, hvordan international lov skal fortolkes i cyberdomænet, heller ikke når det gælder konflikt. Ikke engang i NATO, hvilket vil stille alliancens jurister i en udfordrende situation, hvis NATO skulle koordinere medlemmernes cyberangreb (Teglskov Jacobsen, 2017: 7). Og hvis det er svært i NATO, så er det sandsynligvis endnu vanskeligere at biddrage med cybervåben i en FN-operation – med mindre naturligvis, at vi holder det hemmeligt og dermed *ikke* koordinerer med vores koalitionspartnere.

Konklusion: Det er udfordrende for Danmark at bruge cybervåben i både krig og fred

Det ser altså ud fra de tekniske og taktiske argumenter ud til, at det er svært for en småstat at bruge avancerede cybervåben i en koalition. Enten skal man fortælle sine allierede, hvad våbnene kan og hvordan – og det er der stærke incitamenter imod. Eller også skal de allierede stole mere eller mindre blindt på, at småstatens cybervåben virker, er lovlige og ikke ødelægger noget for de allierede – og det er der også stærke incitamenter imod. Endelig kan småstaten bruge sine cybervåben uden at koordinere med sine allierede. Det gør

stormagter og småstater uden for alliancer som Israel og Nordkorea – men det vile være et brud med Danmarks brug af militær magt siden 1940. Danmark skal derfor nøje overveje, hvad man vil med sine cybervåben, og lige nu er det endnu noget uklart.

> **Cybervåben kan næppe, som foreslået af enkelte folketingspolitikere, umiddelbart anvendes unilateralt til (mod)angreb på stater, som Danmark ikke er i krig med**

På nuværende tidspunkt er der principielt klare regler for, hvordan de skal bruges i væbnet konflikt (Forsvarsudvalget, 2016). Men der mangler grundlag for at bruge dem under tærsklen for krig (Liebetrau, 2020). Cybervåben kan næppe, som foreslået af enkelte folketingspolitikere, umiddelbart anvendes unilateralt til (mod)angreb på stater, som Danmark ikke er i krig med (Lindegaard og Nielsen, 2018). Hvilke mål skulle Danmark angribe og med hvilken effekt for at afskrække fremtidige angreb? Det er for eksempel næppe sandsynligt, at Danmark selvstændigt ville gennemføre et cyberangreb på Rusland, hvis Maersk blev udsat for NotPetya 2.0, eller på Nordkorea, hvis de danske hospitaler blev lammet af Wannacry 2.0 (Jensen, 2018).

Cybervåben er altså svære for Danmark at bruge alene, især i fredstid. Kan vi så bruge dem i væbnede konflikter sammen med NATO eller andre alliancer med USA, hvor de danske kapabiliteter kan understøtte konventionelle militære operationer? Vi har meldt ud til NATO, at vi vil kunne tilbyde offensive effekter, de såkaldte SCEPVA, i NATO-operationer (Forsvarsministeriet, 2018). Men som demonstreret ovenfor er det principielt en udfordring at dele viden om sine cybervåben med allierede, selv bilateralt med USA, og det er ikke bare en operativ udfordring.

Det er en strategisk udfordring, hvis vi med vores cybervåben vil demonstrere, at vi er en lille, men kapabel militær partner. P. V. Jakobsen et al. har demonstreret, hvordan de nordiske lande gennem anvendelse af deres militære magtmidler på måder, der ikke på taktisk niveau forbedrer deres sikkerhedssituation – f.eks. ved at tage med USA til Irak og Afghanistan – søger indflydelse. Formålet er på strategisk niveau at forbedre deres sikkerhed ved at vinde prestige hos den sikkerhedsleverende alliancepartner, USA (Jakobsen, Ringsmose og Saxi, 2018). Et andet eksempel er de danske og norske effektive og omfattende bidrag med F-16 fly i Libyen 2012 (Heier, 2015). Hvis Danmark vil bruge vores cybervåben bilateralt med USA for at vinde prestige, hvad enten det sker i rammen af NATO eller i Coalitions Of the Willing, skal vi være forberedt på enten at overbevise vores allierede og især USA om, at de kan stole på effekten af vores cybervåben uden at vide mere om dem, eller at lukke op for posen og vise dem detaljerne.

Noter

1. Realistisk i IP-teoretisk forstand. Det internationale system af stater er et anarki, hvor interesser og magt er de vigtigste faktorer (Clausewitz, 1986: 29; Handel, 1990: 83; Biddle, 2006: 16; Wivel et al., 2014: 6).
2. Der er ikke en fast definition på småstater i realistisk forskningslitteratur, men de fleste tager udgangspunkt i en vurdering af staters potentiale til at generere og projicere magt (Wivel et al., 2014: 6).
3. For en omfattende gennemgang af forskningslitteratur om strategi og interstatslig cyberkonflikt frem til 2015, se Robinson et al. (Robinson, Jones og Janicke, 2015).
4. Der foreligger meget få uklassificerede oplysninger om cybervåben, herunder også hvad de har kostet at udvikle. Der er derfor tale om en vurdering af, hvad der afgør udviklingsomkostningerne (Smeets, 2016).
5. GRU (Hovedefterretningsdirektoratet) skiftede i 2010 officielt navn til GU (Hoveddirektoratet), men det nye navn blev aldrig populært. I 2018 foreslog Putin (der konsekvent har kaldt organisationen GRU), at tjenesten skulle have det gamle navn tilbage (Carroll, 2018).
6. STUX-net tilskrives i forskningslitteraturen som regel Israel og USA, men ingen af de to stater har taget ansvar for angrebet.

Litteratur

Acton, J.M. (2017), "Cyber Weapons and Precision-Guided Munitions", i G. Perkovich og A.E. Levite, red., *Understanding Cyber Conflict*, Washington, D.C.: Georgetown University Press, pp. 45–60.

Arquilla, J. (2012), *Cyberwar Is Already Upon Us*, *Foreign Policy*, https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/.

Art, R.J. (1980), »To What Ends Military Power?", *International Security*, 4(4): 3–35.

Bailes, A.J.K., J.-M. Rickli og B. Thorhallsson (2014), "Small States, Survival and Strategy", i C. Archer, A. Wivel og A.J.K. Bailes, red., *Small States and International Security: Europe and Beyond*, New York: Routledge Ltd, pp. 26–45.

Bailes, A.J.K., B.A. Thayer og B. Thorhallsson (2016), "Alliance theory and alliance "Shelter": the complexities of small state alliance behaviour", *Third World Thematics: A TWQ Journal,* 1(1): 9–26.

Bebber, R.J. (2017), "Cyber power and cyber effectiveness: An analytic framework", *Comparative Strategy*, 36(5): 426–36.

Buchanan, B. og M. Sulmeyer, M. (2017), »Russia and Cyber Opertaions: Challenges and Opportunities for the Next U.S. Administration«, Washington, D.C. https://carnegieendowment.org/files/12-16-16_Russia_and_Cyber_Operations.pdf.

Carroll, O. (2018), "Legendary GRU military intelligence agency should have historical name restored, says Putin«, *The Independent*, 2. november.

Cavaiola, L.J., D.C. Gompert og M.C. Libicki (2015), "Cyber House Rules: On War, Retaliation and Escalation", *Survival*, 57(1): 81–104.

Cimbala, S.J. (2014), "Comparative Strategy Cyber War and Deterrence Stability: Post-START Nuclear Arms Control Cyber War and Deterrence Stability: Post-START Nuclear Arms Control".

Clarke, R.A. (2010), *Cyber War: The Next Threat to National Security and what to do about it*, New York: HarperCollins Publishers.

Falco, M.D. (2012), *STUXNET Facts Report*, Tallinn, https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf.

Forsvarets Efterretningstjeneste (no date), »FE's organisation«, https://fe-ddis.dk/om-os/Organisation/Pages/Organisation.aspx.

Forsvarsakademiet (2019), "Værnsfælles Doktrin for Militære Cyberspaceoperationer". København: Forsvarsakademiet, www.fak.dk/publikationer/Documents/Værnsfælles Doktrin for Militære Cyberspaceoperationer VDMCO 2019.pdf.

Forsvarsministeriet (2016), »Militærmanual om folkeret for danske væbnede styrker i internationale militære operationer« København, www2.forsvaret.dk/nyheder/intops/Documents/Militærmanualen version 1.2 af SEPT 2016.pdf.

Forsvarsministeriet (2017), *LBK nr 1287 af 28/11/2017 (Bekendtgørelse af lov om Forsvarets Efterretningsstjeneste)*, *Retsinformation*, www.retsinformation.dk/eli/lta/2017/1287.

Forsvarsministeriet (2018), *Offensive cybereffekter*, www.fmn.dk/temaer/nato/Documents/2018/Faktaark-cyber-effekter.pdf.

Forsvarsudvalget (2016), »Redegørelse fra den tværministerielle arbejdsgruppe om Folketingets inddragelse ved anvendelse af den militære Computer Network Attack (CNA) -kapacitet«, Copenhagen, www.ft.dk/samling/20151/almdel/FOU/bilag/170/1663433.pdf.

Greenberg, A. (2018), »The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired«, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Hansel, M. (2018), "Cyber-attacks and psychological IR perspectives: Explaining misperceptions and escalation risks", *Journal of International Relations and Development*, 21(3): 523–31.

Harold, S.W., M.C. Libicki og A.Stuth Cevallos (2016), »Getting to Yes with China in Cyberspace«, Santa Monica: RAND, www.rand.org/t/rr1335.

Heier, T. (2015), "Is "out of area" also "out of control"? Small states in large operations", *RUSI Journal*, 160(1): 58–66.

Hennis-Plasschaert, J.A. (2015), »Defence Cyber Strategy, Netherlands Ministry of Defence«, Netherlands, file:///C:/Users/00182452/Downloads/PD.Defense_Cyber_Strategy_Update.pdf.

Hughes, D. og A. Colarik (2016), "Small State Acquisition of Offensive Cyberwarfare Capabilities: Towards Building an Analytical Framework", *JFQ: Joint Force Quarterly*, 83(4): 19–26.

Jakobsen, P.V., J. Ringsmose og H.L. Saxi (2018), "Prestige-seeking small states: Danish and Norwegian military contributions to US-led operations", *European Journal of International Security*, 3(02): 256–77.

Janczewski, L.J. og W. Caelli (2016), "Security of Small Countries: Summary and Model", i L.J. Janczewski og W. Caelli, red., *Cyber Conflicts and Small States*, London: Routledge.

Jensen, B., B. Valeriano og R. Maness (2019), "Fancy bears and digital trolls: Cyber strategy with a Russian twist", *Journal of Strategic Studies*, 42(2).

Jensen, M.S. (2018), »Et godt forsvar er det bedste angreb i nutidens cyberkrig«, *Information*, 9. oktober

Joffre, T. (2020), »Security cabinet: Israel didn't expect Iran cyberattack on water system«, *The Jerusalem Post*, 10. maj.

Junio, T.J. (2013), "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate", *Journal of Strategic Studies*, 36(1): 125–33.

Klare, M.T. (2019), »Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation | Arms Control Association, Arms Control Association«, www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation.

Libicki, M.C. (2009), »Cyberdeterrence and Cyberwar«, www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Liebetrau, T. (2020), *Dansk offensiv cybermagt mellem angreb, spionage og forsvar*. København.

Lindegaard, R. og Nielsen, N.S. (2018), »Naser Khader: Vi skal angribe russiske hacker-netværk«, DR.dk, 3. oktober.

McAfee (no date), *What Is Petya and NotPetya Ransomware?* www.mcafee.com/enterprise/en-us/security-awareness/ransomware/petya.html.

Migliano, S. (2018), »Dark Web Market Price Index: Hacking Tools (US Edition)«, www.top10vpn.com/research/investigations/dark-web-market-price-index-hacking-tools-us-edition/.

Morgenthau, H. (1948), *Politics among Nations: The Struggle for Power and Peace*, New York: Knopf.

Nakashima, E. og J. Warrick, J. (2020), »Foreign intelligence officials say attempted cyberattack on Israeli water utilities linked to Iran«, *The Washington Post*, 9. maj.

Neuman, C. og M. Poznansky (2016), »Swaggring in Cyberspace: Busting the Conventional Wisdom on Cyber Coercion«, https://warontherocks.com/2016/06/swaggering-in-cyberspace-busting-the-conventional-wisdom-on-cyber-coercion/.

Pace, P. (2006), "National Military Strategy for Cyberspace Operations", Washington D.C.: US Department of Defense.

Peterson, D. (2013), "Offensive Cyber Weapons: Construction, Development, and Employment", *Journal of Strategic Studies*, 36(1): 120–4.

Rivera, J. (2015), "Achieving cyberdeterrence and the Ability of Small States to Hold Large States at risk *", i 7th International Conference on Cyber Conflict: Tallinn: NATO CCD COE Publications, https://ccdcoe.org/cycon/2015/proceedings/01_rivera.pdf.

Rizwan, A. og T.E. Ricks (2017), »NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons«, https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/.

Robinson, M., K. Jones og H. Janicke (2015), "Cyber warfare: Issues and challenges", *Computers & Security*, 49: 70–94.

Shoorbajee, Z. (2018), »GCHQ head says U.K. engaged in cyberwarfare against ISIS, Cyberscoop«, www.cyberscoop.com/gchq-uk-cyberattack-isis/.

Smeets, M. (2016), »How Much Does a Cyber Weapon Cost? Nobody Knows | Council on Foreign Relations, Council on Foreign Relations«, www.cfr.org/blog/how-much-does-cyber-weapon-cost-nobody-knows.

Smith, T.E. (2013), "Cyber Warfare: A Misrepresentation of the True Cyber Threat", *American Intelligence Journal*, 31(1): 82–86.

Statement from the Press Secretary (2018), »White House Press Release«, www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.

Statsrevisorerne (2017), »Beretning om Forsvars- ministeriets beslutnings- grundlag for køb af 27 F-35 kampfly« København, www.rigsrevisionen.dk/media/2104677/sr0217.pdf.

Taillat, S. (2019), "Disrupt and restraint: The evolution of cyber conflict and the implications for collective security", *Contemporary Security Policy*, 40(3): 368–81.

Teglskov Jacobsen, J. (2017), »Danmark bør undgå en "digital Genèvekonvention", www.fak.dk/publikationer/Documents/Danmarks cyberpolitik.pdf.

Tor, U. (2017), "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence", *Journal of Strategic Studies*, 40(1–2): 92–117.

U.S. Departement of Treasury (2019), »Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups«, Press release, https://home.treasury.gov/index.php/news/press-releases/sm774.

UK Foreign Office (2018), »Foreign Office Minister condemns Russia for NotPetya attacks – GOV.UK«, Press release, www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks.

US Army (2017), "FM 3-12 Cyberspace and Electronic Warfare Ops", HQ Departement of the Army, http://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3089_FM 3-12 FINAL WEB 1.pdf.

US Joint Chiefs of Staff (2013), "US JP 3-12 Cyberspace Operations", Washington DC: US Joint Chiefs of Staff, www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf.

USCYBERCOM (2020), *USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY*, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony.

Wirtz, J. J. (2017), "The Cyber Pearl Harbor", *Intelligence and National Security*, 32(6): 758–67.

Wivel, Anders, et al. (2014), "Setting the scene: Small states and international security", i C. Archer, A Bailes og A. Wivel, red., *Small States and International Security: Europe and Beyond*, London: Routledge, pp. 3–25.

Offensive cyberoperasjoner: Den nye normalen?

Temanummer: Cybersikkerhed

Kan stater gå til motangrep om de blir angrepet digitalt i fredstid? Hva gjør toneangivende land, og hva sier internasjonal rett og normer om dette? Og hva kan de sikkerhetspolitiske konsekvensene bli av økt bruk av offensive cyberoperasjoner? Denne artikkelen diskuterer denne sikkerhetspolitiske utviklingen i kombinasjon med en analyse av det relevante internasjonale rettslige rammeverket. Artikkelen begynner med en redegjørelse av USAs nye tilnærming til offensive operasjoner, knytte til de to begrepene "persistent engagement" og "defend forward". Deretter følger en kort case-studie på Norges tilnærming til offensive cyber operasjoner, noe som bringer oss til "Responsibility of States of International Wrongful Acts"-lovverket, som er det mest relevante med tanke på offensive cyberangrep utenom væpnet konflikt. Artikkelen avsluttes med en diskusjon av dilemmaer i skjøringspunktet sikkerhetspolitikk og folkerett.

KARSTEN FRIIS
Norsk utenrikspolitisk institutt (NUPI), kf@nupi.no

Offensive cyperoperasjoner over og under radaren

Kan stater gå til motangrep om de blir angrepet digitalt i fredstid? Hva gjør toneangivende land, og hva sier internasjonal rett og normer om dette? Og hva kan de sikkerhetspolitiske konsekvensene bli av økt bruk av offensive cyberoperasjoner?[1]

Diskusjonene og trusselbildet knyttet til cybersikkerhet har lenge primært fokusert på kritisk infrastruktur som strøm, telekommunikasjon, energinett mv. Det har også vært en tendens til å legge mest vekt på mulige katastrofe-scenarier. I USA har man for eksempel brukt begreper som "digital Peal Harbor", og dermed sett for seg at cyber er et våpen på linje med strategisk bombing. Det vil si at et stort og målrettet cyberangrep vil kunne slå ut sivil og militær infrastruktur, lamme og slå ut et samfunn – i verste fall med dødelige konsekvenser. De fleste land søker å beskytte seg mot dette gjennom å bygge opp best mulig *resiliens* eller motstandsdyktighet i sine kritiske systemer, slik at effektene av et eventuelt cyberangrep blir minst mulig både i omfang og tid.

I USA har man imidlertid de siste årene begynt å se litt annerledes på det. I tillegg til å forsøke å begrense store digitale sabotasjeangrep, har man begynt å vektlegge den jevne strømmen med mindre angrep som foregår mer eller mindre kontinuerlig. Disse søker ikke nødvendigvis å slå ut store infrastruktursystemer, men snarere å undergrave USA politisk, økonomisk og sosialt. De pågående kampanjene fra primært Kina og Russland, i alt fra industrispionasje til politisk påvirkning og "fake news", sees som systematiske kampanjer for å svekke USA. I et strategi-dokument fra 2018 skriver U.S. Cybercommand (2018) at motstanderne: "exploit our dependencies and vulnerabilities in cy-

berspace and use our systems, processes, and values against us to weaken our democratic institutions and gain economic, diplomatic, and military advantages" (p. 3).

Som følge av dette, sier amerikanske myndigheter, kan ikke fokuset lenger kun være på "hack", "brudd", "hendelser" eller "angrep", men snarere på løpende, strategiske kampanjer, som bevisst ligger "under radaren" og dermed ikke forårsaker samme type respons som et spektakulært angrep på kritisk infrastruktur ville. Det er altså ikke lenger kun det store spektakulære cyberangrepet (type "Pearl Harbor") man frykter, men totaliteten av alle de mindre pågående operasjonene. Kort fortalt, USA har konkludert med at også disse pågående kampanjene har strategisk effekt (Harknett, 2018). Som respons har man konkludert med å at man bør gå mer offensivt til verks og ikke la angriperne få holde på uforstyrret. Terskelen for å respondere må altså senkes.

Folkerettsjurister har allerede diskutert disse temaene i flere år. De mye omtalte Tallinn-manualene omhandler dette. Den første diskuterte rammeverket for cyberoperasjoner under væpnet konflikt (Tallinn Manual, 2013), mens den andre tok for seg cyberoperasjoner utenfor væpnet konflikt (Tallinn Manual 2.0, 2017; Jensen, 2017). Nå ser vi imidlertid at flere vestlige land begynner å uttale seg og posisjonere seg politisk med hensyn til bruken av offensive cybervåpen utenfor væpnet konflikt (Liebetrau, 2020).

Denne artikkelen diskuterer denne sikkerhetspolitiske utviklingen i kombinasjon med en analyse av det relevante internasjonale rettslige rammeverket. Formålet er primært å bringe problemstillinger opp i dagen, ikke å argumentere sterkt i den ene eller andre retningen. Artikkelen begynner med en redegjørelse av USAs nye tilnærming til offensive cyberoperasjoner utenom væpnet konflikt. Deretter følger to seksjoner som søker å bidra til en konseptuell klargjøring av offensive cyberoperasjoner og suverenitetsbrudd. Deretter følger en kort case-studie på Norges tilnærming til offensive cyber operasjoner. Caset er valgt fordi det illustrerer en annen tilnærming enn USAs, og fordi det er tilgjengelig for en skandinavisk lesekrets. Studiet av Norge bringer oss til "Responsibility of States of International Wrongful Acts"-lovverket, som nok er det mest relevante med tanke på offensive cyberangrep utenom væpnet konflikt. Artikkelen avsluttes med en diskusjon av dilemmaer i skjæringspunktet sikkerhetspolitikk og folkerett.

USAs nye tilnærming

Flere analytikere argumenterer for at verken avskrekking eller internasjonal normbygging ser ut til å fungere når det gjelder å forhindre trusler av typen som er påpekt over (Fischerkeller og Harknett, 2017; Sulmeyer, 2018; se også Muller, 2017). Avskrekking fungerer best med kraftige våpensystemer som kjernevåpen eller konvensjonelle våpen der eventuell bruk er et drastisk skritt. Cyberangrep har vært vanskeligere å avskrekke mot fordi angrepene er mindre dramatiske og fordi man ikke har truet motstanderens systemer, men kun forsvart sine egne nettverk (Libicki, 2009; Nye 2011, 2017). Trussel om

avstraffelse har dermed begrenset effekt. Internasjonal normbygging har også vist seg krevende (Mačák, 2017; se også Jacobsen dette temanummer).

Dermed konkluderer USA, og flere andre vestlige land med at man må kunne respondere på slike pågående kampanjer ved å slå tilbake. Det er et ønske om å få et bredere sett med virkemidler for å beskytte seg. I Michael Sulmeyers (2018) ord: "In cyberwarfare, Washington should recognize that the best defense is a good offense". Om ikke, heter det, vil dagens trusselaktører fortsette sin praksis og slik aktivitet vil bli en ny "norm".

Ifølge den nye amerikanske nasjonale cyberstrategien fra i fjor høst vil USA "deter and, if necessary, punish those who use cyber tools for malicious purposes" (U.S. President, 2018). Denne avstraffelsen kan skje utenfor det digitale rom (som gjennom straffeforfølgelse), men også innenfor. I tillegg til denne strategien har det amerikanske forsvarsdepartementet (DoD) utgitt en egen cyberstrategi (som kun finnes som et sammendrag i ugradert versjon, se U.S. Department of Defense, 2018), mens U.S. Cybercommand altså utga et strategi-dokument på vårparten 2018, kalt *Vision*. I tillegg utstedte President Trump et *National Security Presidential Memorandum 13* (NSPM 13), mens Kongressen vedtok et *National Defense Authorization Act* (NDAA). Til sammen utgjør disse planene og reguleringene et sett verktøy og prosedyrer som muliggjør mer aktivitet i andre lands nettverk i fredstid (Underwood, 2019).

NSPM-13 er et gradert dokument, men de fleste analytikere antar at formålet var å forenkle de legale prosedyrene knyttet til å autorisere cyberoperasjoner utenfor det amerikanske forsvarets egne systemer. Det innebærer trolig at langt færre offentlige etater i USA må involveres før slik tillatelse kan gis (Freedberg, 2018; Chesney, 2019). I DoDs cyberstrategi heter det: "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict" (U.S. Department of Defense, 2018). Det amerikanske forsvaret skal altså enklere kunne respondere på cyberangrep i fredstid.

Det er to nøkkelbegrep som har blitt viet mye oppmerksomhet i disse strategiene, nemlig "persistent engagement" og "defend forward". "Persistent engagement"-strategien handler om å vanskeliggjøre motstanderens angrep og tvinge dem til å bruke mer ressurser på å beskytte seg selv og egne sårbarheter. Man skal altså engasjere motstanderen kontinuerlig, ikke sitte passivt og vente på å bli angrepet. "Defend forward" er et element i denne strategien og vil si å fokusere på en angripers kapasiteter ved å forsvare mot, og respondere på, strategiske angrep som ikke kvalifiserer som væpnet konflikt (Kosseff, 2019). Tanken er at det ikke lenger holder å bare forsvare egne systemer, respondere når en blir angrepet og rydde opp etterpå. I stedet skal man finne, engasjere og forpurre motstanderen, før skaden er skjedd.[2] "Defending forward" handler altså om et proaktivt forsvar som vil forstyrre angripere i en tidlig fase og i en slik grad at de må fokusere mer på forsvar enn på angrep (Harknett, 2018).

Som U.S. Cybercommand skriver i *Vision*: "Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins" (p. 6).

> **Defending forward handler altså om et proaktivt forsvar som vil forstyrre angripere i en tidlig fase og i en slik grad at de må fokusere mer på forsvar enn på angrep**

Det sentrale her er altså at USA vil gjøre cyberoperasjoner utenfor egne nettverk i fredstid (Chesney, 2018; Nakasone, 2019). Videre er ikke dette begrenset til "speiding" og etterretning, men innebærer også forstyrrende og ødeleggende aktiviteter i nettverk i andre land. Er dette slik alle aktører ser på offensive cyberoperasjoner? En viss konseptuell klargjøring kan være nyttig for den videre diskusjonen.

Hva er offensive cyberoperasjoner?

Her er det ulike tolkninger. Smeets og Lin (2018) bruker begrepet "offensive cyber capabilities" (OCC), som de definerer som "a capability designed to access a computer system or network to damage or harm living or material entities" (p. 58). NATO har ikke en klar definisjon av offensive cyberoperasjoner, i og med at alliansen kun har et defensivt mandat (Stoltenberg, 2019). Men NATO Joint Air Power Competence Centre (2017) beskriver Offensive Cyber Operations (OCO) slik: "those activities undertaken, via digital means, to infiltrate, reconnoitre, exploit, disrupt, deny access to and/or destroy the adversaries' systems and/or data." James A. Lewis (2015: 2) beskriver det slik: "offensive capabilities, unlike NATO's current defensive posture, involve deliberate intrusions into opponent networks or systems with the intention of causing disruption, damage or destruction".

NATO-senteret har altså en langt bredere definisjon enn de andre. Her inkluderes infiltrasjon, rekognosering og utnyttelse av andres nett. Dette likner på den norske definisjonen av offensive cyberoperajoner, som inkluderer både *Cyber Network Exploitation* (CNE) og *Cyber Network Attack* (CNA). Ifølge det norske Forsvarsdepartementets cyberretningslinjer (2014) er begge å anse som offensive aktiviteter, som normalt "gjennomføres […] i en motstanders nettverk". Mens CNE er informasjonsinnhenting og etterretningsvirksomhet, skal CNA "bidra til å redusere eller hindre en motstanders evne til å utnytte cyberdomenet til egne operasjoner" (s. 6). Å skille mellom CNE og CNA kan være nyttig for å spisse diskusjonen. Vi kan derfor si at det vi er opptatt av i denne konteksten ikke primært handler om spionasje (CNE), men om operasjoner som har en effekt på motstanderen, altså CNA. Selv om det i praksis til tider kan være krevende – særlig for den som blir angrepet – å skille mellom spionasje og effektoperasjoner, er det nok generelt sett mindre kontroversielt å drive CNE enn CNA. I den videre diskusjonen vil vi altså konsentrere oss om defensive CNA-operasjoner: de som skal redusere eller hindre en mot-

standers evne til å utnytte cyberdomenet til egne operasjoner. Men når kan dette gjøres?

Suverenitetsbrudd i det digitale rom?

Det er bred enighet internasjonalt om at folkerettens prinsipper om maktbruk og ikke-intervensjon også gjelder i det digitale rom (United Nations, 2015; Tallinn Manual, 2017). Imidlertid er det ingen enighet om hvor grensen skal gå (Grigsby, 2017).[3] Spørsmålet er hvilke handlinger som utløser statsansvar, hvilke handlinger som kan oppfattes som "væpnet angrep", hvilke handlinger som befinner seg under terskel for dette og dermed (ifølge noen stater, og særlig europeiske) styres av andre folkerettslige prinsipper (Hellestveit og Nystuen, 2020: 282).

Problemet fra folkerettslig hold er at så lenge man er under terskel for konflikt, er det både usikkerhet og til dels sterk stor uenighet om hvilke folkerettslige regler som gjelder for cyberoperasjoner. Det er vanskelig å se for seg folkerettslig regulering av cyberoperasjoner "utenfor konflikt" uten at det ville bringe inn omtrent samtlige kontroverser i folkeretten i våre dager knyttet til suverenitet, ikke-innblanding, og statsansvar.

USA har lenge vært svært klare på at de ikke anser at folkerettslige begrensninger på rettshåndhevelse gjelder for amerikanske operasjoner utenfor amerikansk territorium. Storbritannia ansees av og til å ligge nærmere USA i disse spørsmålene enn andre europeiske land, men også britene er bundet av flere av europeiske traktater om ekstraterritoriell anvendelse av folkerettslige regler – som USA ikke er. Frankrike med flere ser ut til å helle i retning av å hevde at også mindre digitale angrep er et brudd på suverenitetsprinsippet (Moynihan 2019: 9-10).

> Men hvor går skillet mellom vanlig diplomati, politisk press og suverenitetsbrudd?

Men hvor går skillet mellom vanlig diplomati, politisk press og suverenitetsbrudd? Det er ikke uvanlig at stater er innom hverandres nettverk, ikke nødvendigvis for å spionere, men fordi de digitale sporene og det globaliserte nettverkene gjør at datatrafikken krysser mange landegrenser. Man kan altså ikke være helt *purist* på suverenitet. Det handler om grader av suverenitet eller frihet, det er ikke absolutte termer. Ulike land ser ut til å lage ulike kriterier for å definere suverenitetsbrudd. Disse er ofte basert på de effektene en operasjon har, av både kvantitativ og kvalitativ art. Det kan altså være hvor *stor* skade et angrep påfører landet, men også *hva* som blir angrepet (Moynihan 2019: 21).

Frankrike er kanskje det landet som er mest tydelige på dette så langt. I et ferskt *White Paper* står det at landets suverenitet er brutt dersom ondsinnede cyberangrep fra andre land (og tilknyttede aktører) er rettet mot fransk infrastruktur, eller dersom det skaper effekter i Frankrike (Ministère des Armées,

2019; Schmitt, 2019; Moynihan, 2019). Frankrikes posisjon er at alvorligheten av angrepet avgjør hvilken folkerettslig norm som er brutt, det være seg prinsippene om suverenitet, ikke-intervensjon eller maktbruk. Videre pekes det ut fire vitale samfunnsområder, nemlig "fundamentale nasjonale interesser" (suverenitet, demokrati, territoriell integritet); "intern og ekstern sikkerhet"; "tilgang til grunnleggende tjenester for befolkningen" (vann, strøm, helsetjenester); og "økonomi" (Roguski, 2019). Angrep må altså treffe eller påvirke disse sektorene, og være av en viss styrke for å telle som suverenitetsbrudd.

EU har også kommet opp med en liste over hva som kan utgjøre et alvorlig cyberangrep på medlemsstatene, det vil si ha "signifikant effekt", og som kan utløse motreaksjoner ("targeted restrictive measures"). Denne er også en blanding av type angrep og graden av effekt, slik som mengde av økonomisk tap som er påført, antall medlemsland som er berørt, graden av skade påført mv. (EU Council, 2019: 9-10). Imidlertid viser ikke EU til suverenitetsprinsippet i internasjonal rett, men mer generelt til FN-charteret og UN GGE (UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security). EU snakker heller ikke om hva slags "targeted restrictive measures" det er snakk om, så det er ingen diskusjon om offensive cyberangrep som respons.

Det er med andre ord flere måter land ser ut til å definere og måle graden av et cyberangrep. Noen kaller det suverenitetsbrudd, andre ikke, men det at man ønsker å respondere på et vis er ganske utbredt. For å få bedre innsikt i hvordan slik respons kan forankres i folkeretten, vil vi i neste avsnitt kort diskutere Norges tilnærming til offensive cyberoperasjoner. Caset skiller seg ganske kraftig fra USA, og kan gi en pekepinn om hvordan andre nordiske og europeiske stater resonerer rundt dette.

Norge

I Norge er offentlige debatter om offensive cyber operasjoner mer eller mindre fraværende. Dette kan skyldes at Norge verken er eller har ambisjon om å være en ledende global aktør i det digitale rom på linje med for eksempel USA og Storbritannia. Samtidig er utfordringene like. Også norske myndigheter, institusjoner og private virksomheter utsettes for langsiktige avanserte angrep fra avanserte statlige aktører i det digitale rom. Det er ikke nødvendigvis store og spektakulære angrep (ingen "digital 9. april"), men kan være vel så krevende å håndtere for de som rammes – og slike angrep kan få strategiske konsekvenser. Samtidig er det viktig at land som tradisjonelt har vært sterke støttespillere til en internasjonal orden basert på folkerettslige regler kommer på banen og markerer hvordan man ønsker at folkerett og internasjonale normer skal gjelde i det digitale rom med tanke på offensive operasjoner eller mottiltak. Her har Norge en rolle å spille (Hellestveit og Nystuen, 2020).

Det er i dag hver enkelt virksomhet og hver sektor som har ansvaret for sin digitale sikkerhet. Kritiske samfunnsfunksjoner som omfattes av sikkerhetsloven kan få bistand fra sentrale myndigheter, slik som Nasjonal sikkerhetsmyn-

dighet (NSM) og deres samarbeidspartnere fra PST, E-tjenesten og Kripos i Felles Cyber Koordineringssenter (FCKS). Men NSM kan ikke operere i andre nett enn de som har gitt tillatelse til det eller rammes.

> I Norge er det Etterretningstjenesten som har fått "lov" til å drive såkalte offensive cyberoperasjoner utenlands

I Norge er det Etterretningstjenesten som har fått "lov" til å drive såkalte offensive cyberoperasjoner utenlands. Som det heter i Prop. 1: "Ansvaret for nettverksbaserte etterretningsoperasjoner og offensive cyberoperasjoner ligger hos Etterretningstjenesten" (Forsvarsdepartementet, 2019b: 19).

I høringsnotatet til ny Etterretningslov fra 2018 er dette beskrevet i noe mer detalj:

"*Etterretningstjenesten har det nasjonale ansvaret for å planlegge og gjennomføre offensive cyberoperasjoner, herunder cyberangrep (Computer Network Attack), samt koordinere mellom offensive og defensive cybertiltak i Forsvaret. Etterretningstjenesten har også ansvaret for å forestå etterretningsmessig attribusjon av utenlandske trusselaktører ved alvorlige cyberoperasjoner rettet mot Norge eller norske interesser*" (Forsvarsdepartementet 2018: 113).

For å få en utdyping av dette må vi imidlertid tilbake til FDs cyberretningslinjer fra 2014. Der fremgår det at offensive cyberoperasjoner som kvalifiserer som maktbruk etter FN-pakten kun kan brukes i svært begrensede tilfeller, nemlig når retten til selvforsvar i henhold til FN-pakten gjelder:

"*Et digitalt angrep kan, avhengig av omstendigheter som angrepets formål og legitimitet, styrke og konsekvenser, regnes som ulovlig maktbruk etter FN-paktens artikkel 2(4). Et angrep i cyberdomenet kan utløse en stats rett til selvforsvar etter FN-paktens artikkel 51. Terskelen er høy, og vil eksempelvis først gjelde der staten er utsatt for et omfattende angrep rettet mot kritisk infrastruktur, eller dersom cyberangrepet forårsaker betydelig tap av liv eller materiell skade*" *(Forsvars*departementet, 2014: 13–4).

Og videre:

"*Krigens folkerett kommer til anvendelse i cyberdomenet, forutsatt at terskelen for væpnet konflikt er overskredet*" *(ibid.*: 14).

I slike tilfeller kan stater respondere, også kinetisk i det ikke-digitale rom.

Men departementet skriver også: "Dersom angrepet ikke er tilstrekkelig alvorlig til å utløse selvforsvarsretten, vil den rammede stat likevel kunne iverksette andre mottiltak som ikke innebærer bruk av makt" (ibid.).

Spørsmålet er dermed hvilke regler som gjelder i tilfeller der man *ikke* er i væpnet konflikt og ikke har blitt rammet av maktbruk (dvs. at staten ikke er

"utsatt for et omfattende angrep rettet mot kritisk infrastruktur, eller dersom cyberangrepet forårsaker betydelig tap av liv eller materiell skade"). Som det står i siste setning i sitatet over er det mulig å respondere ved å iverksette "mottiltak som ikke innebærer bruk av makt."

Finnes det med andre ord offensive cyberoperasjoner som ikke kvalifiserer som maktbruk som bryter med maktforbudet? Hvordan defineres i så fall disse?

I Prop. 60S (Forsvarsdepartementet, 2019a) gjentas det at det er E-tjenesten som har ansvaret for å gjennomføre offensive cyberoperasjoner, og det begrunnes blant annet med at tjenesten har den målforståelsen og det totale etterretningsbildet som trengs. Videre står det at "Etterretningstenesta innehar i dag dei funksjonane som er naudsynte for å utøve rollen som militær cyberkommando" (p. 8). Videre fremhever Forsvarsdepartementet flere tiltak, blant annet: "Vidareutvikle Etterretningstenesta si evne i fred, krise og væpna konflikt til å følge, attribuere, varsle og aktivt motverke digitale trugslar før hendingar inntreffer" (ibid.).

E-tjenesten skal altså "aktivt motvirke" digitale trusler også i fredstid og før hendelser inntreffer. Her begynner vi å nærme oss de kapasitetene som USA legger opp til, men formuleringen er likevel såpass vag at det er vanskelig å vite hva det betyr i praksis.

Vi blir imidlertid litt klokere om vi går til det nevnte høringsnotatet til ny E-lov, hvor det står følgende om såkalte "effektoperasjoner":

"*Foruten forventningen om at Etterretningstjenesten skal bidra med informasjon, kan det være grunn til å anta at norske myndigheter vil kunne ha en forventning om at Etterretningstjenesten i enkelte tilfeller handler på bakgrunn av informasjonen den har tilegnet seg, dersom dette er nødvendig for å avverge alvorlige trusler eller utfordringer*" (Forsvarsdepartementet, 2018: 113).

Videre:

"*Gjennomføring av slike operasjoner må skje med et klart folkerettslig grunnlag og innenfor rammene av FN-pakten, humanitærretten og annen relevant internasjonal rett. Det rettslige grunnlaget vil variere etter omstendighetene, blant annet om effektoperasjoner gjennomføres i eller utenfor rammen av væpnet konflikt, om vilkårene for statlig selvforsvar er tilstede eller om tiltaket er en respons på en i fredstid folkerettsstridig handling ('international wrongful act') fra en utenlandsk statlig aktør.*" *(ibid.*, min fremhævning).

Effektoperasjoner kan tydeligvis gjennomføres i fredstid mot andre stater som har brutt folkeretten (gjort en "international wrongful act") mot Norge. Dette nyanseres og diskuteres imidlertid ikke videre i de norske dokumentene. Imidlertid er referansen "international wrongful act" viktig og trolig relevant for mange andre stater også. Neste del vil diskutere dette nærmere.

Responsibility of States for Internationally Wrongful Acts

Responsibility Of States For Internationally Wrongful Acts (United Nations, 2005) anses i det store og hele som sedvanerett, og dermed bindende folkerett (Crawford 2019).[4] I det følgende vil begrepet *statsansvar* referere til dette lovverket. I paragraf 75 står det at "In certain circumstances, the commission by one State of an internationally wrongful act may justify another State injured by that act in *taking nonforcible countermeasures in order to procure its cessation and to achieve reparation for the injury*" (min fremhævning). En angrepet stat kan altså gjøre mottiltak, under terskelen for maktbruk, for å stanse et angrep eller for å oppnå erstatning eller oppreising. Imidlertid er formuleringen "under certain circumstances" åpen for ulike tolkninger. Når er det slike "særlige forhold"?

Mottiltak kan beskrives som "acts (actions or omissions) that would violate international law but for the fact that their wrongfulness is precluded because they proportionally respond to another State's unlawful action and are designed to compel that State to desist (or to secure reparations for harm caused). Det kan også enkelt oppsummeres i begrepet "hack-back" (Schmitt, 2019).

Den nevnte *Tallinn Manual 2.0* diskuterer også dette. Manualen er utarbeidet av en gruppe eksperter på internasjonal rett og presenterer det bildet som folkerettsekspertene er enige om gjelder for cyber – eller "international law applicable to cyber operations" som det heter i tittelen. Med andre ord for operasjoner utenfor "væpnet konflikt" (som *Tallinn 1.0* fokuserte på). Manualene har blitt viktige referansepunkt for både eksperter på internasjonal rett og for myndigheter i ulike vestlige land de siste årene. Når det gjelder maktbruk står det blant annet: "An operation may be less likely to constitute a use of force if its effects have a limited 'scope, duration, and intensity'" (Tallinn Manual 2.0, 2017: 334). Å for eksempel degradere en spesifikk IP-adresse som har vært utgangspunktet for gjentatte angrep, i en begrenset periode, vil trolig ikke kalles maktbruk i internasjonal rett, ifølge *Tallinn Manual* (ibid.). Dette forutsetter selvsagt at ikke et slikt angrep får fatale konsekvenser av noe slag.

Videre sier *Tallinn Manual 2.0*. at man ikke kan utføre mottiltak mot andre angrep enn de som er rettet mot "inherently governmental functions" (Tallinn Manual 2.0, 2017: 22). Dette dreier seg om slike ting som sosiale tjenester, valg, skatteinnkreving, diplomati og forsvar. Men her er både internasjonal rett, *Tallinn Manual* og nasjonale uttalelser relativt vage. Man er kort fortalt ikke enige om når "inherently governmental functions [are] usurped or interfered with" (Schmitt, 2019).

Jeff Kosseff (2019) argumenterer for at USAs "defense forward"-konsept også kan kobles til *Responsibility Of States*-lovverket, men det er viktig å merke seg at ingen av de nevnte amerikanske dokumentene eksplisitt viser til denne delen av internasjonal rett. USA er omfattet av den same sedvaneretten, men tolkningen av når det gjelder (når er det "særlige forhold") kan alltid diskuteres. DoDs ugraderte cyberstrategi viser dog til prosessene i FN som USA støt-

ter, slik som UN GGE, og sier at: "The principles developed by the UNGGE include prohibitions against damaging civilian critical infrastructure during peacetime and against allowing national territory to be used for intentionally wrongful cyber activity" (U.S. Department of Defense, 2018: 5). Men det står ikke at strategien vil begrenses av eller knyttes til reglene om statsansvar (Schmitt, 2020).

Trusselbeskrivelsen som legitimerer "persistent engagement" i de amerikanske dokumentene handler også om mer enn vitale samfunnsfunksjoner eller "inherently governmental functions". Argumentet er at det nettopp er summen av en rekke mindre – isolert sett mindre alvorlige – angrep som utgjør trusselen. Dermed blir det vanskeligere å legitimere et motsvar på et enkelt angrep mot en ikke-vesentlig del av nasjonal infrastruktur innenfor reglene om statsansvar. Vi kan dermed anta at USA ikke vil akseptere en streng tolkning av statsansvar på dette området, men vil markere at USA ser seg bundet kun av mer fleksible regler (ibid.). Det er derfor fullt mulig at "defense forward" og "persistent engagement" går lenger enn det som reglene om statsansvar i dag klart statuerer. For skal man holde seg innenfor reglene om statsansvar legges det en god del klare begrensninger på hva man kan gjøre av offensive cyberoperasjoner.

En offensiv cyberoperasjon i fredstid kan under reglene om statsansvar kun gjøres som respons på et angrep. Det kan også kun gjøres mot stater, ikke for eksempel private foretak, med mindre disse er tydelig assosiert med staten, ifølge *Tallinn Manual 2.0* (2017: 113). Man kan altså ikke gå preventivt til verks og stanse et angrep før det er igangsatt. Imidlertid skriver DoD i sin strategi at de også skal "preempt [...] malicious cyberactivity" (U.S. Department of Defense, 2018: 2). Det er også flere observatører som tolker USAs "persistent engagement" dithen at slike forkjøpsangrep kan gjøres (Healey, 2018; Chesney, 2018). USA har også en lavere terskel enn mange andre land med hensyn til når de mener de kan respondere på angrep (Goodman, 2018).

« **Storbritannia har også lagt seg på en linje der det ikke er selve suverenitetsbruddet som er det utslagsgivende i et cyberangrep, men snarere implikasjonene. Dermed antas det at de har lagt listen relativt lavt for å kunne respondere**

Storbritannia har også lagt seg på en linje der det ikke er selve suverenitetsbruddet som er det utslagsgivende i et cyberangrep, men snarere implikasjonene. Dermed antas det at de har lagt listen relativt lavt for å kunne respondere (Schmitt, 2019). Frankrike er som sagt tydelige på at suverenitetsprinsippet gjelder, og at de kan gjøre mottiltak (med loven i hånd) nettopp av den grunn. Effekten av et strengt suverenitetsprinsipp innebærer altså også at retten til motsvar utløses på et tidligere tidspunkt.

Vi kan kanskje anta at Norge vil innta en restriktiv tilnærming, ikke ulik den franske, tett opptil reglene om statsansvar, ikke minst i og med at det eksplisitt

refereres til det i dokumentene fra FD. Vitale samfunnsfunksjoner kan trolig i praksis i stor grad sidestilles med det som omfattes av den norske sikkerhetsloven. Et angrep på slike funksjoner kan i så fall besvares i fredstid, men det må gjøres proporsjonalt. Det betyr at Norge kan gjøre offensive mottiltak for å stanse angrepet, men ikke gjennomføre et større cyberangrep mot det andre landet.

Dersom denne tolkningen av statsansvarsreglene for cyberoperasjoner er riktig, kan alle land respondere på cyberangrep mot vitale samfunnsfunksjoner i fredstid – inkludert mindre angrep som faller under terskelen for maktbruk – med proporsjonale motangrep som forpurrer eller stanser angrepet. For å gjøre det må man operere også i nettverkene til den som angriper. Men hvor grensen går for et slikt motangrep er det uenighet om, både blant folkerettsjurister og stater.

Samtidig er det ikke uvanlig at land bevisst velger å være uklare når det gjelder slike grenser, da man frykter at klarhet på dette kan invitere til angrep rett under terskelverdien. Dette gjelder særlig innenfor den delen av folkeretten som regulerer bruk av maktmidler mot andre stater. Uansett tillater reglene om statsansvar proporsjonale offensive cyberoperasjoner fra stater som blir angrepet av andre stater. Det ser ut til at en slik praksis er i ferd med også å bli forankret i ulike lands statspraksis og *opinio juris*, og dermed begynnende sedvanerettsdannelse.

Utfordringer – global eskalering av cyberkonflikter

Hva blir de praktiske og politiske konsekvensene dersom proporsjonale offensive cyberoperasjoner blir mer vanlig, eller sågar akseptert folkerettslig sedvane? I utgangspunktet ser det ut til at formålet med økt bruk av offensive cybermaktmidler skulle være å bidra til økt cybersikkerhet, ved at digital hacking og sabotasje fra stater får en økt kostnad for dem som gjør det. Det er med andre ord tenkt å endre oppførselen til dagens digitale aggressorer, og skape visse felles kjøreregler. Dermed er tanken – blant annet – at praksiser og normer også endres i retning av et fredeligere internett. Det er imidlertid flere skjær i sjøen.

En utfordring er at det kan være krevende for den som blir angrepet å skille mellom om de er utsatt for "defending forward" og "attacking forward". Om de oppfatter at de er under et offensivt angrep, øker også faren for motangrep og eskalering (Buchanan, 2018). Samtidig skal jo "defend forward" kun være mot aktører som allerede har en eller flere pågående operasjoner, så helt overraskende – og dermed eskalerende – kan det neppe være. Men her vil praksisen til ulike land med hensyn til "preventive" angrep eller forkjøps-operasjoner spille inn.

På lengre sikt er det også mulig at "persistent engagement» – og generelt mer "hack-back" – kan lede til økt aktivitet hos motstanderne, snarere enn lavere (Healey, 2018). De kan respondere på økt press ved å gjøre egne operasjoner

raskere og mer aggressive, via stadig flere aktører. Dette vil igjen kunne trigge vestlige land til å be om enda flere offensive frihetsgrader enn i dag. Dermed får vi en global eskalering av cyberkonflikter. Tilsvarende er det en fare for at raske og store motangrep vil "normalisere" cyberkonflikt i enda større grad enn i dag. Dermed kan også takten på angrep øke (Weinstein 2018).

> **«USA har allerede en gang tatt ned et IS-nettverk på en tysk server og det ble ikke godt mottatt i Tyskland. Hvordan vil USA stille seg om for eksempel Norge gikk inn i amerikanske nettverk som var proxy for angrep mot Norge?**

En annen utfordring er at de fleste cyberangrep går via en rekke internasjonale servere. På den ene siden kan aktører forsøke å fremstille det som om et annet land står bak et angrep, og dermed skape en falsk attribusjon – og respons. På den annen side kan for eksempel et russisk angrep på USA gå gjennom en rekke andre land, inkludert USAs allierte i NATO (Smeets, 2019a). Hvordan blir det om ulike NATO-land går inn i hverandres nettverk på jakt etter den som angriper dem? Særlig om det utføres effektoperasjoner i nettverk lokalisert i allierte land, er det å forvente at det kan skape bruduljer. USA har allerede en gang tatt ned et IS-nettverk på en tysk server og det ble ikke godt mottatt i Tyskland. Hvordan vil USA stille seg om for eksempel Norge gikk inn i amerikanske nettverk som var *proxy* for angrep mot Norge? Som Max Smeets argumenterer kan det bli behov for noen kjøreregler i NATO på dette (Smeets 2019b).

Folkeretten statuerer at statene har ansvar for å hindre misbruk av servere på eget territorium til "international wrongful acts" (se United Nations, 2015, para 13 (c)). Blant annet innebærer dette et ansvar om *due diligence* (Kulesza, 2016). Frankrike og en del andre land (blant annet Nederland, Estland og Finland) er tydelige på at dette bør være en bindene del av folkeretten. Michael Schmitt (2019) argumenterer for at den logiske konsekvensen av å være tydelige på dette er at den normative implikasjonen blir: Dersom en stat ikke klarer/ønsker å stanse et cyberangrep fra nettverk på eget territorium, gis den rammede staten mulighet til å respondere selv. Det vil si at politiske og diplomatiske reaksjoner kan brukes, men også at man kan gjøre mottiltak (Roguski, 2019). Det betyr at begrensede offensive operasjoner er lovlig i slike tilfeller, også i allierte nettverk. Men hvilken instans skal avgjøre om en stat har "evne og vilje" til å stanse et angrep fra eget territorium? Her vil nok de sterkeste statene ha en strengere tolkning enn mange små. Det kan medføre at spesielt svake stater og utviklingsland med dårlig kontroll over egne systemer kan bli en arena for gjentatte offensive cyberoperasjoner – samt stedfortreder-cyberoperasjoner. Dette kan svekke den internasjonale tilliten til disse statene ytterligere.

En tredje utfordring er utilsiktede effekter og målutvelgelse. Det siste er krevende i situasjoner under terskelen for væpnet konflikt. Når man er i væpnet konflikt er det tross alt visse regler for hvilke nettverk som kan rammes (mi-

litære mål, *dual-use* sivile mål osv.), men dette gjelder ikke når man er under terskelen for konflikt. Dermed er det også mer "fritt frem", og man kan få utilsiktede konsekvenser. Det er ikke sjelden at en skadevare sprer seg til andre nett enn der den opprinnelig var tenkt. Det er heller ikke alltid slik skadevare på avveie gjør noe skade, for eksempel dersom *payloaden* er svært målrettet mot en type maskin eller programvare (slik som Stuxnet). Andre ganger kan et virus spre seg globalt, slik som *NotPetya*-viruset, som opprinnelig var rettet mot Ukraina, men som spredte seg globalt. Til og med avsenderlandet kan bli rammet. Kort fortalt, økt bruk av offensive cybervåpen øker trolig også sjansen for våpen på avveie og uintenderte konsekvenser.

En siste mer generell utfordring er at dersom resultatet blir et mer "aggressivt" digitalt klima, kan det forpurre internetts kjerneverdi, nemlig å være en plattform for økonomisk utvikling, informasjonsutveksling og vekst.

Selv om både trusselbildet og regelutviklingen i folkeretten peker i retning av mulig økt bruk av offensive cyberoperasjoner, eller cyberangrep, er det imidlertid lite sannsynlig med en brå økning av slik aktivitet. Stater er fortsatt forsiktige, dels grunnet bekymringene diskutert her, dels grunnet begrensede ressurser med hensyn til attribusjon og respons. De er trolig også lite interessert i å bli eksponert internasjonalt som spesielt offensive i cyberdomenet. Om vi går mot en verden der alle er "persistent engaged" er det imidlertid lite trolig at det blir fredeligere i det digitale rom.

Med tiden vil trolig statspraksis krystallisere klarere folkerettslige kjøreregler for cyberoperasjoner. Det er positivt at land som Frankrike går tydelig ut og markerer en alternativ posisjon. Dermed kommer debatten ut av de prinsipielle juridiske kroker og kobles tettere opp mot internasjonal politikk og normbygging. Norge – og andre skandinaviske land – bør komme tydeligere på banen her.

Noter

1 Takk til Niels Nagelhus Schia, Lars Gjesvik og Erik Reichborn-Kjennerud for gode innspill og kommentarer. Takk også til redaktør og den anonyme fagfellen. En spesiell takk til Cecilie Hellestveit for god veiledning og korreks på de folkerettslige spørsmålene. Gjenværende uklarheter og unøyaktigheter står fullstendig for forfatterens regning.

2 Det er åpenbare likheter mellom dette og måten USA både politisk og juridisk har legitimert og operasjonalisert den såkalte "krigen mot terror" (se f.eks. Massumi, 2015), samt kampen mot masseødeleggelsesvåpen, men den diskusjonen er noe på siden her. Men at USA har et noe annet syn enn de fleste europeisk eland når det gjelder maktbruk utenfor konflikt er velkjent. Se for eksempel Conrad Harper (1995), som var første gang USA klargjorde sitt syn på de rettslige begrensninger som gjelder for maktbruk utenfor konflikt – altså forpliktelser under FN konvensjonen om politiske og sivile rettigheter.

3 Spørsmålet om suverenitetsbrudd I det digitale rom er en kompleks debatt i folkeretten, og det er mange nyanser jeg ikke vil komme nærmer inn på her. Se for eksempel Schmitt og Vihul (2017).

4 Se også International Law Commission (ILC): Analytical Guide to the Work of the International Law Commission: State responsibility, https://www.cfr.org/blog/implications-defending-forward-new-pentagon-cyber-strategy.

Referanser

Buchanan, Ben (2018), "The Implications of Defending Forward in the New Pentagon Cyber Strategy", *Council on Foreign Relations*, 25. september, www.cfr.org/blog/implications-defending-forward-new-pentagon-cyber-strategy

Chesney, Robert (2018), "The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes", *Lawfare*, 25. september.

Chesney, Robert (2019), "CYBERCOM's Out-of-Network Operations: What Has and Has Not Changed Over the Past Year?", *Lawfare,* 9. mai.

Crawford, James (2019), *Historical background and development of codification,* UN Audiovisual Library of International Law, https://legal.un.org/avl/ha/rsiwa/rsiwa.html

EU Council (2019), *EU Council decision (CFSP) 7299/19 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*, 14. mai, https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf.

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

Forsvarsdepartementet (2014), *FDs retningslinjer for informasjonssikkerhet og cyberoperasjoner*, Oslo: Forsvarsdepartementet.

Forsvarsdepartementet (2018), *Høringsnotat. Forslag til ny lov om Etterretningstjenesten*, 12. november, Oslo: Forsvarsdepartementet.

Forsvarsdepartementet (2019a), *Prop. 60S (2018-2019), Investeringar i Forsvaret og andre saker,* Oslo: Forsvarsdepartementet.

Forsvarsdepartementet (2019b), *Prop. 1S (2019–2020),* Oslo: Forsvarsdepartementet.

Freedberg Jr, Sydney J. (2018), "Trump Eases Cyber Ops, But Safeguards Remain: Joint Staff", *Breaking Defence,* 17. september, https://breakingdefense.com/2018/09/trump-eases-cyber-ops-but-safeguards-remain-joint-staff/

Goodman, Ryan (2018), "Cyber Operations and the U.S. Definition of 'Armed Attack'", *Just Security*, 8. mars, https://www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack/

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

Harknett, Richard J. (2018), "United States Cyber Command's New Vision: What It Entails and Why It Matters", *Lawfare,* 23. mars.

Harper, Conrad (1995), *Statement of the US Department of State*, U.N. Hum. Rts. Comm., 53rd Sess., 1405th mtg., mars 31, 20, U.N. Doc. CCPRIC/SR 1405.

Healey, Jason, (2018), "Triggering the New Forever War, in Cyberspace", *The Cipher Brief,* 1. april, www.thecipherbrief.com/triggering-new-forever-war-cyberspace

Hellestveit, Cecilie og Gro Nystuen (2020), *Krigens folkerett – Norge og vår tids kriger*, Oslo: Universitetsforlaget.

Jensen, Eric Talbot (2017), "The Tallinn Manual 2.0: Highlights And Insights", *Georgetown Journal of International Law,* 48(3): 735–78.

NATO Joint Air Power Competence Centre (JAPC) (2017), *NATO Joint Air Power and Offensive Cyber Operations*, november, www.japcc.org/wp-content/uploads/JAPCC_OCO_screen.pdf

Kosseff, Jeff (2019), "The Contours of 'Defend Forward' Under International Law", i T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga og G. Visky, red., *11th International Conference on Cyber Conflict: Silent Battle*, Tallinn: NATO CCD COE Publications, pp.1–13.

Kulesza, Joanna (2016), *Due Diligence in International Law*, Leiden: Brill.

Lewis, James A. (2015), *The role of offensive cyber operations in NATO's collective defence*, Tallinn Paper No. 8, Tallinn: NATO CCDCOE.

Libicki, Martin C. (2009), *Cyberdeterrence and Cyberwar,* Santa Monica, CA, RAND Corporation.

Liebetrau, Tobias (2020), *Dansk offensiv cybermagt mellem angreb, spionage og forsvar. En komparativ analyse på tværs av Europa,* København, Center for Militære Studier, Københavns Universitet.

Mačák, Kubo (2017), "From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers", *Leiden Journal of International Law*, 30(4): 877–99.

Massumi, Brian (2015), *Ontopower. War, Powers, and the State of Perception*, Durham, NC: Duke University Press.

Ministère des Armées (2019), *International Law Applied to Operations in Cyberspace*, Paris: Ministère des Armées.

Moynihan, Harriet (2019), *The Application of International Law to State Cyberattacks. Sovereignty and Non-intervention,* Research Paper, December, London: Chatham House.

Muller, Lilly Pijnenburg (2019), *Upholding the NATO cyber pledge Cyber Deterrence and Resilience: Dilemmas in NATO defence and security politics*¸ Policy Brief 5/2017, Oslo: NUPI.

Nakasone, Paul M. (2019), "A Cyber Force for Persistent Operations", *Joint Force Quarterly* 92(1): 10–4.

Nye, Joseph S. Jr. (2011), "Nuclear lessons for cyber security?", *Strategic Studies Quarterly*, 5(4): 18–38.

Nye, Joseph S. Jr. (2017), "Deterrence and dissuasion in cyberspace", *International Security*, 41(3): 44–71.

Roguski, Przemysław (2019), "France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I", *Opinio Juris*, 24. september, https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/

Schmitt, Michael (2020), "The Defense Department's Measured Take on International Law in Cyberspace", *Just Security*, 11. mars, www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/

Schmitt, Michael (2019), "France's Major Statement on International Law and Cyber: An Assessment", *Just Security*, 16. september, www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/

Schmitt, Michael og Vihul, Liis (2017), "Respect for Sovereignty in Cyberspace", *Texas Law Review,* 95(7); 1639–71.

Smeets, Max (2019a), "Cyber Command's Strategy Risks Friction With Allies", *Lawfare,* 28. mai.

Smeets, Max (2019b), "NATO Allies Need to Come to Terms With Offensive Cyber Operations", *Lawfare*, 14. oktober.

Smeets, Max og Herbert S. Lin (2018), "Offensive Cyber Capabilities: To What Ends?", i T. Minárik, R. Jakschis og L. Lindström, red., *CyCon X: Maximising Effects. 2018 10th International Conference on Cyber Conflict,* Tallinn: NATO CCD COE Publications, pp. 55–72.

Stoltenberg, Jens (2019), "NATO will defend itself", *Prospect*, 27. august, www.prospectmagazine.co.uk/world/nato-will-defend-itself

Sulmeyer, Michael (2018), "How the U.S. Can Play Cyber-Offense: Deterrence Isn't Enough", *Foreign Affairs,* 22. mars.

Tallinn Manual (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press.

Tallinn Manual 2.0 (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press.

Underwood, Kimberly (2019), "House-Passed NDAA Includes Key Cyber Provisions", *Signal,* 15. juli, www.afcea.org/content/house-passed-ndaa-includes-key-cyber-provisions

U.S. Cyber Command (2018), *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command,* United States Cyber Command: Washington DC.

U.S. Department of Defense (2018), *Summary Cyber Strategy 2018,* DoD: Washington DC.

U.S. President (2018), *National Cyber Strategy 2018* White House: Washington DC.

United Nations (2005), *Responsibility Of States For Internationally Wrongful Acts 2001*, United Nations: New York.

United Nations (2015), *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (GEE), 22 juli, A/70/174.

Weinstein, Dave (2018), "The Pentagon's New Cyber Strategy: Defend Forward", *Lawfare*, 21. september.

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.

Hvem er cybereksperten? Ekspertise og professioner i cybersikkerhedsfeltet

Temanummer: Cybersikkerhed

Cybersikkerhedseksperter spiller en vigtig rolle i at identificere digitale risici og at definere hensigtsmæssige løsninger. Denne artikel gør brug af professions- og ekspertsociologien til at belyse konkurrerende epistemiske rationaliteter i konstruktionen af digitale risici. På baggrund af et nyt datasæt omhandlende ekspertprofiler i offentlige og private cybersikkerhedsråd og -udvalg, argumenteres der for, at profilen af cybersikkerhedseksperter har bevæget sig væk fra et rent teknisk fokus og hen imod en procesorientering, som både er bredere i fokus og placeret tættere på beslutningstagere. Den nye ekspertprofil er positioneret i et spændingsfelt imellem tekniske, organisatoriske og økonomiske rationaliteter. I fraværet af en bred politisk debat kan denne udvikling styrke ekspertmagten, som nu er begrænset til få hybride aktører, som formår at bygge bro imellem de forskellige rationaliteter. En sådan udvikling vil være skadelig for demokratiet, men udviklingen imod en procesorienteret forståelse af cybersikkerhed åber samtidlig muligheder for at re-politisere cybersikkerhedsdiskursen igennem en mindre teknifiseret debat.

Viden om cybersikkerhed er teknisk – men også politisk

JOHANN OLE WILLERS
research fellow, Norsk Utenrispolitisk Institutt (NUPI) og ph.d.-studerende, Institut for Organisation, Copenhagen Business School, jow.ioa@cbs.dk

Cybereksperten er uden tvivl blevet en central aktør i dagens sikkerhedspolitiske debat, hvor afhængigheden af digitale ydelser og produkter i stigende grad har rettet virksomheders, politikeres og individers opmærksomhed imod digitale sårbarheder og trusler.[1] I dag er cybersikkerhed både en strategisk målsætning og en eftertragtet kompetence.

Men hvem er cybereksperten egentlig? Lene Hansen og Helen Nissenbaum konstaterede i 2009, at kombinationen af den tekniske karakter og hastigheden af forandringsprocesser indenfor cybersikkerhed cementerer ekspertens rolle som en af de centrale aktører, der konstituerer cybersikkerhed som et sikkerhedspolitisk emne (Hansen og Nissenbaum, 2009: 1166). I dag indtager cybereksperter vigtige samfundspolitiske roller gennem blandt andet offentligt-private partnerskaber (Christensen og Petersen, 2017) og i det diplomatiske felt (Segal, 2017). Samtidig er der overraskende lidt enighed om cybereksperternes færdigheder (Shires, 2018: 32). I artiklen tilnærmer jeg mig spørgsmålet, om hvad der karakteriserer cybereksperten, og hvordan cybereksperternes rolle har udviklet sig over tid. Med udgangspunkt i professions- og ekspertsociologien introducerer jeg en ny tilgang til den politiske læsning af cybersikkerhed og dets forhold til vidensdannelsen, som senest har tiltrukket akademisk interesse (Dunn Cavelty og Wenger, 2020).

Det centrale argument er, at ideer om, hvordan vi som samfund skal adressere digitale risici, ikke opstår i et institutionelt vakuum. Tværtimod bliver ideer

udviklet, testet og spredt blandt eksperter på tværs af institutionelle grænser. Om disse ideer følger en økonomisk, teknisk eller geopolitisk logik, kan have stor påvirkning på, hvordan politiske løsninger udformes (Kremer, 2014). Det er derfor nødvendigt at udvikle et analytisk apparat, der gør os i stand til at undersøge ekspertise og ekspertviden indenfor cybersikkerhed. Et forskningsfelt, hvor der historisk er blevet fokuseret på interstatslige konflikter og strategiske dimensioner (Gorwa og Smeets, 2019). Med udgangspunkt i ekspertsociologien sætter jeg fokus på ekspertvidens politiske karakter og kampen om anerkendelse (Reed, 1996; Sending, 2015). Derudover trækker jeg på Andrew Abbott's professionssociologi for at situere cybersikkerhedsarbejdet i et spændingsfelt imellem økonomiske, politiske og tekniske overvejelser (Abbott, 1988; 2005).

Jeg henter derved inspiration i senere strømninger i cybersikkerhedslitteraturen, som undersøger, hvordan cybersikkerhedsspørgsmål relaterer sig til eksisterende, og skaber nye, sociale formationer (McCarthy, 2018: 6). Actor-network-teori og science and technology studies (STS) er blevet brugt til at undersøge relationerne imellem tekniske og sociopolitiske objekter (Dunn Cavelty, 2018; Stevens, 2018). Ligeledes har assemblage teori vist sig at kunne belyse komplekse netværk af materielle og ikke-materielle aktører, som konstituerer cybersikkerhedsdebatten (Collier, 2018). Ligeledes er praksisteorien senest blevet brugt til at undersøge sociopolitiske fordelingsspørgsmål relateret til cybersikkerhedskoncepter (McCarthy, 2018). Fælles for ovenstående nye teoretiske bidrag er et analytisk udgangspunkt, som retter fokus imod, hvordan cybersikkerhed opstår igennem en sammenfletning af mennesker, objekter og ideer (Dunn Cavelty og Wenger, 2020) og hvordan de resulterende socioteknologiske processer konstituterer cybersikkerhedspraksis og -diskurs. Artiklens bidrag til denne diskussion er at udvide det teoretiske apparat ved at introducere professions- og ekspertsociologien som lovende redskaber til at undersøge den politiske karakter af vidensdannelsen i konteksten af definitionen af digitale risici og håndteringen af disse (se også T. Stevens, 2012).

Det næste afsnit introducerer litteraturen om ekspertise og giver eksempler på cybereksperters indflydelse på udformningen af regler og normer inden for cybersikkerhedsområdet. Sektionen er efterfulgt af en diskussion af professionsbegrebet i relation til cybereksperise med et fokus på, hvordan fremvæksten af nye problemstillinger har relateret sig til allerede eksisterende professionelt arbejde. Dernæst illustrerer jeg perspektivet gennem en analyse af danske eksperter i centrale offentlige og private udvalg. Jeg afslutter med en diskussion om implikationerne af en ny ekspertprofil, som både er bredere i fokus og tættere på beslutningstagere end den tidligere tekniske profil.

Ekspertise i fokus

Fra et akademisk perspektiv har vidensproduktion længe tiltrukket interesse. Her er et centralt omdrejningspunkt sammenfletningen af viden og magt (Allan, 2018; Bueger, 2014; CASE Collective, 2006). Eksperten er en person

med særlige kompetencer indenfor et defineret område. Som vi ved fra mange områder såsom økonomisk og sikkerhedspolitik er ekspertviden dog sjældent uanfægtet. Tværtimod ser vi ofte en kamp om anerkendelsen af at besidde overlegen ekspertise (Eyal, 2013a). Litteraturen opererer med udtrykket "the politics of expertise" (Reed, 1996; Sending, 2015) og refererer til "conflicts over the exclusionary jurisdictional domains arising out of the contested monopolization of abstract knowledge and technique" (Reed, 1996: 582). Med andre ord beskriver udtrykket en situation, hvor flere ekspertgrupper konkurrerer om at opnå epistemisk legitimitet til både at definere et problem samt de værktøjer og færdigheder, der skal til for at håndtere problemet. Tyskerne har et passende udtryk til at beskrive denne proces: kampen om *Deutungshoheit* – den eksklusive kapacitet til at fortolke problemer og definere hensigtsmæssige løsninger (Krentz, 2014). Epistemisk legitimitet referer derved til den nødvendige sociale anerkendelse og autoritet for at opnå "Deutungshoheit".

Men hvorfor er det vigtigt at forstå denne proces? Sikkerhed er ikke et selvforklarende koncept. Som Robert McCarthy skriver, handler det først og fremmest om spørgsmålet "sikkerhed for hvem?" (2018: 8). Cybersikkerhed er et anfægtet begreb (Smeets og Shires, 2017) og centrale aspekter såsom, hvad der kategoriseres som et sikkerhedsproblem, og hvem der har ansvaret for at håndtere problemer, forhandles kontinuerligt (Christensen og Liebetrau, 2019: 396). Hvordan sikkerhed konceptualiseres er derfor afgørende for, hvordan sikkerhedsproblemer defineres, fortolkes og håndteres. Ekspertviden står derved altid i relation til de sociale og politiske institutioner, som danner den kulturelle ramme for produktionen af viden (Slayton og Clark-Ginsberg, 2018: 117). Dette åbner op for konflikter mellem epistemer, som arbejder indenfor det samme problemfelt. Jens Kremer benytter sig af begrebet "security mindsets", der identificerer distinkte liberale og militære tænkemåder i den amerikanske tilgang til cybersikkerhed. Disse "mindsets" er afhængige af professionelle og institutionelle baggrunde, politiske overbevisninger og verdensanskuelser (Kremer, 2014). Et andet eksempel stammer ligeledes fra USA, hvor det er blevet dokumenteret, hvordan reguleringen af kritisk infrastruktur har været præget af konflikter mellem eksperter indenfor henholdsvis informationsteknologi (IT) og operationel teknologi (OT) med konsekvenser for både reguleringens form og eksperternes fremtidige profil (Slayton og Clark-Ginsberg, 2018: 124).

Muligheden for at fremme forskellige – og ofte konkurrerende – tilgange til cybersikkerhed er en af årsagerne til eksperternes betydning i feltet. Ekspertviden kan derved fungere som en legitimerende faktor i udarbejdelsen af politiske tiltag (Bueger, 2014). Der er dog også særlige strukturelle karakteristika, som kan give eksperter stor indflydelse i cybersikkerhedsfeltet. Den tekniske karakter og hastigheden af forandringsprocesser er to faktorer, som allerede blev nævnt i introduktionsafsnittet. Den globale mangel på ekspertviden er en yderligere faktor.

Tim Stevens argumenterer for, at den tekniske kompleksitet og den hurtige udvikling i cybersikkerhedsfeltet skaber et spørgsmål om, hvad der er en reel fare, og hvad der ikke er. Dette "epistemologiske problem" danner kernen af cybersikkerhedsnarrativer (T. Stevens, 2016: 155). Et sådant narrativ konstruerer, ifølge Hansen og Nissenbaum, det tekniske som "a domain requiring an expertise that the public (and most politicians) do not have and this in turn allows 'experts' to become securitizing actors [...]" (Hansen og Nissenbaum, 2009: 1167). Lignende tendenser er blevet observeret i andre felter med høj teknisk kompleksitet (Gracia og Oats, 2012; Thistlethwaite og Paterson, 2016; Tsingou, 2014).

» Mange offentlige institutioner oplever stadigvæk store problemer, når de skal hyre cybersikkerhedseksperter. I Tyskland er hver fjerde offentlig cybersikkerhedsstilling stadig ledig i 2020

Samtidig er der en markant mangel på cybereksperter på et globalt plan (Vogel, 2016). Den internationale organisation for IT-professionelle, ISACA, estimerer, at der globalt manglede to millioner cybersikkerhedseksperter i 2019 (ISACA, 2019). En konsekvens heraf er, at mange organisationer hverken har mulighed for eller råd til at ansætte kvalificerede eksperter. I starten af 2010'erne havde de amerikanske myndigheders afhængighed af private cybersikkerhedsleverandør nået et niveau, hvor flere observatører frygtede udviklingen af en strukturel ubalance, der vil muliggøre, at cybersikkerhedseksperter selv kunne definere efterspørgslen og leveringen af løsninger (Deibert, 2013; Lee og Rid, 2014). Mange offentlige institutioner oplever stadigvæk store problemer, når de skal hyre cybersikkerhedseksperter. I Tyskland er hver fjerde offentlig cybersikkerhedsstilling stadig ledig i 2020. Det gælder især stillinger i indenrigsministeriet, som snart står med ansvaret for at sikre enorme nye datamængder som konsekvens af mere offentlig og digital overvågning (Domscheit-Berg, 2020). Vi mangler tilsvarende tal fra den danske offentlige sektor, men intet tyder på en markant bedre situation. Digitaliseringsstyrelsens undersøgelse om implementeringen af internationale cybersikkerhedsstandarder konkluderer for eksempel at områderne "ressourcer, kompetencer og bevidsthed" er blandt de mest problematiske indenfor danske myndigheder (Digitaliseringsstyrelsen, 2019: 5).

Mange lande er begyndt at nævne uddannelse af cybersikkerhedseksperter som et specifikt fokusområde. I USA præsenterede Obama-administrationen den første nationale "Cybersecurity Workforce Strategy" i 2016 og afsatte 62 millioner USD årligt til at støtte uddannelsen af nye eksperter (White House, 2016). Ligeledes har Trump erklæret cybersikkerhedseksperterne "a strategic asset that protects the American people, the homeland, and the American way of life" (Trump, 2019). I Danmark er den første dedikerede kandidatuddannelse i cybersikkerhed blevet etableret på Aalborg Universitet tidligere på året (Aalborg Universitet, 2020). Den danske cyber- og informationssikkerhedsstrategi definerer ligeledes en målsætning om at etablere en bedre forståelse

for digitale risici på tværs af uddannelseskæden (Finansministeriet, 2018: 32). Storbritannien har i sin seneste nationale cyberstrategi sat et eksplicit mål om at udvikle en professionel organiseret gruppe af cybereksperter (Government of the United Kingdom, 2016; 2018).

Opsummerende kan det konstateres, at de usikkerheder der opstår som resultatet af den tekniske udvikling og en global mangel på cyberekspertise, har skabt et felt, som både privilegerer ekspertviden og underminerer muligheden for offentlig og politisk debat. Det åbner et stort spørgsmål: Hvilke metodiske værktøjer kan vi bruge til at studere, hvordan denne ekspertise er organiseret, og hvor den er placeret? I det efterfølgende afsnit introducerer jeg professionsperspektivet som et bud på en mulig tilgang.

Professioner og professionalisering

Om en professionalisering af cybersikkerhedsbranchen er en ønskelig udvikling, har længe været et omdiskuteret spørgsmål (Burley, Eisenberg og Goodman, 2014; Dawson og Thomson, 2018; National Research Council, 2013). Professionalisering bliver i denne debat konceptualiseret som en funktionel proces med formålet at sikre en minimumstandard igennem brugen af blandt andet certificeringer, licenser, fælles uddannelsesforløb og fælles etiske regler (Ford og Gibbs, 1996: 5). Debatten er da fokuseret på, om en professionalisering af cybersikkerhedsbranchen vil skabe en positiv samfundsmæssig effekt eller forværre manglen på kvalificerede eksperter. Abbotts professionssociologi, som danner baggrunden for artiklens analyse, bryder derimod med det instrumentelle fokus og retter blikket mod placeringen af ekspertviden indenfor et system af professioner, som kæmper om kontrol og anerkendelse (Abbott, 1988: 98). I de efterfølgende afsnit diskuteres den funktionelle professionsliteratur indenfor cybersikkerhed og introducerer derefter Abbotts professionssociologi.

Fra et funktionelt perspektiv kan der være klare fordele ved en professionalisering. Kunder er sikret en minimumstandard, den offentlige anerkendelse af arbejdet øges, og professionen har nemmere ved at tiltrække unge talenter gennem etableringen af klare karriereforløb og sikre arbejdsbetingelser. Der er dog også ulemper forbundet med professionalisering. Adgangsbarrierer til professionen gennem for eksempel obligatoriske uddannelsesforløb kan føre til en unødvendig reduktion af den tilgængelige arbejdskraft (Burley et al., 2014). Ligeledes konkluderede det Amerikanske National Research Council i 2013 at "some organizations may find that professionalization provides a useful degree of 'quality control' for those who work in the field, but professionalization also imposes barriers to those who wish to enter the field at a time when demand for cybersecurity workers exceeds supply" (National Research Council, 2013: 2). Professionaliseringen er derved en proces, som indebærer et afgrænsende og et homogeniserende element: en anerkendelse af at have de rigtige værktøjer til at adressere et anerkendt problem, og disse værktøjer er fælles for alle indenfor professionen (Abbott, 1988: 60). Typiske kendetegn

på modne professioner er institutionaliserede dedikerede universitetsuddannelser, professionelle organisationer, certificeringer og en fælles etiske regler (Ford og Gibbs, 1996). En organisk udvikling af disse dimensioner tager tid og professionalisering er derfor typisk en lang historisk proces (Fourcade, 2010).

Cybersikkkerhed er på mange måder en umoden profession. De første antivirusprogrammer blev udviklet i slutningen af 1980'erne, og udviklingen af det nuværende marked for cybersikkerhed skete ikke inden starten af 2010'erne, hvor angrebene blev mere ødelæggende og udbredte (Denning og Frailey, 2011). Der er mange arbejdsopgaver relateret til cybersikkerhed med ofte overlappende og løst definerede ansvarsområder (National Research Council, 2013). I 2001 identificerede Peter Denning "system security" som en af 15 discipliner indenfor IT (Denning, 2001). Begrebet "system security" refererer til en primært teknisk opgave inden for IT-afdelinger. I takt med udviklingen af et i stigende grad komplekst trusselsbillede og en kontinuerlig udvidelse af den underliggende teknologi er der opstået flere opgaver, som kræver forskellige færdigheder, viden og kompetencer (Dawson og Thomson, 2018). I 2017 udgaven af det Amerikanske Nationale Institut for Standarder og Teknologis "Cybersecurity Workforce Framework" er opgaven "system security" bare én blandt 62 "work roles" indenfor cybersikkerhedsfeltet (NIST, 2017). At anskue cybersikkerhed som en homogen profession frem for et løst sammenhængende felt er derfor problematisk. Snarere er cybersikkerhed en umoden profession, som er kendetegnet ved manglen på en fælles uddannelsesbaggrund, løs professionel organisering og eksisterende, men ikke obligatoriske certificeringer og licenser (Ford og Gibbs, 1996).

» **At anskue cybersikkerhed som en homogen profession frem for et løst sammenhængende felt er derfor problematisk. Snarere er cybersikkerhed en umoden profession, som er kendetegnet ved manglen på en fælles uddannelsesbaggrund, løs professionel organisering, og eksisterende, men ikke obligatoriske certificeringer og licenser**

Frem for at fokusere på den funktionelle professionalisering af cybersikkerhed åbner Abbotts professionssociologi for spørgsmål om, hvordan grupper kæmper om at kontrollere bestemte arbejdsopgaver i samfundet (Abbott, 1988: 98). Praktisk betyder det, at håndteringen af digitale risici foregår i et organisatorisk felt af relaterede problemstillinger (Dawson og Thomson, 2018). Er cybersikkerhed et teknisk, organisatorisk, finansielt eller kulturelt spørgsmål? Fordelen ved at bruge Abbotts perspektiv på, hvordan ekspertise organiseres socialt, er, at der tages højde for, hvordan cybersikkerhedsspørgsmål er relateret til forskellige felter: "Cybersecurity is no longer the remit only of private or corporate practitioners but has become a complex site of interaction between a very wide range of people, organizations and technologies" (C. Stevens, 2020: 133). Abbotts professionsbegreb fremhæver, at det er i relationen mellem pro-

fessioner, at kontrollen over problemer defineres. At dominere et problemfelt tillader en profession at definere problemet, at afgrænse handlingsmuligheder og, måske mest afgørende, at bestemme successkriterier (Abbott, 1988: 137).

En profession er derved kendetegnet ved at kontrollere en given opgave gennem brugen af abstrakt viden (Abbott, 1988: 8, 53). Klassiske eksempler er læger, jurister og revisorer. Nogle professioner – såsom økonomer – har markant udvidet deres magt igennem tiden ved at kontrollere flere og flere sociale problemstillinger (Fourcade, Ollion og Algan, 2015). Leonie Maria Tanczer og kollegaer dokumenterer en sådan proces, hvor cybereksperter trænger ind på jurisdiktionen af eksisterende professioner. Deres analyse viser, hvordan Cyber Security Incident Response Teams (CSIRTs) har formået at navigere geopolitiske konflikter. Ved at skabe transnationale netværk af cybersikkerhedseksperter med unikke fordele overfor klassiske politiske aktører har CSIRTs udvidet deres arbejdsfelt fra en teknisk opgave til en diplomatisk rolle (Tanczer, Brass og Carr, 2018).

Clare Stevens viser derudover, hvordan efterforskningen af cyberangreb i private sikkerhedsfirmaer placerer cybereksperten i et spændingsfelt mellem teknisk ekspertise og politiske konsekvenser. Igennem en analyse af Symantecs undersøgelse af Stuxnet-koden dokumenteres det, hvordan det tekniske arbejde blev "entangled in the politics of nuclear proliferation, diplomacy, international law, and the mechanisms of global cybersecurity governance" (C. Stevens, 2020: 130).

Ved at fokusere på professionernes konkrete arbejde frem for deres strukturelle karakteristika åbner professionssociologien en tilgang til spørgsmålet om, hvem der har autoriteten til at definere digitale risici og afgrænse håndteringen af disse. Hastigheden af forandringsprocessen i teknologien og trusselsbilledet bidrager til en afpolitisering af emnet og placerer den epistemiske autoritet fast i hænderne på eksperterne: "[T]he epistemic authority which computer and information scientists hold allow them the privileged role as those who have the authority to speak about the unknown" (Hansen og Nissenbaum, 2009: 1166-7). Offentlige og private råd og udvalg kan være en vigtig indikator på, hvilke professioner der er involveret i denne proces, fordi de fungerer som et samlingssted, hvor anerkendte eksperter samles for at diskutere presserende spørgsmål, ofte med en strukturende effekt på det videre felt (Reed, 1996; van Apeldoorn og Graaff, 2014). Det er mod dem, jeg vender mig i den følgende analyse af danske cybereksperter.

Danske cybersikkerhedeksperter

For at illustrere ovenstående teoretiske overvejelser præsenterer jeg i det følgende en analyse af danske top-cybersikkerhedeksperter. Baggrunden for analysen er en samling af nævnte eksperter i danske komitéer og råd med cybersikkerhed som det eneste fokusområde. Ekspertgrupper kan spille en strategisk rolle i strukturering af professionelt arbejde og kontrol og er derfor velegnet til professionssociologiske analyser (Reed, 1996; Seabrooke og

Tsingou, 2014). Datasættet dækker over 195 poster fordelt på 176 personer. Nogle råd er nedsat af offentlige institutioner (Cybersikkerhedsråd og Erhvervsministeriets IT Sikkerhed Virksomhedsråd). En enkelt er en uafhængig organisation, to er tilknyttet brancheorganisationer og den sidste dækker over de største danske virksomheders' ansvarlige personer for cybersikkerhed (C25-virksomheder). Rådene er blevet udvalgt igennem *purposive sampling* på baggrund af synlighed i den offentlige debat (Tansey, 2007). Analysen har et illustrerende formål og sigter ikke mod at præsentere et repræsentativt billede af alle cybersikkerhedseksperter i Danmark. Alligevel fremvises tendenser blandt Danmarks top cybersikkerhedseksperter. Det skal dog fremhæves, at datasættet har klare begrænsninger og ingen af konklusionerne, som fremgår af analysen, er definitive. Derudover er det vigtigt at understrege, at analysen udelukkende fokuserer på råd og udvalg. Faste institutioner såsom Center for Cybersikkerhed eller Digitaliseringsstyrelsens "Kontor for Cyber- og Informationssikkerhed" er derfor ikke direkte en del af datasættet. Derimod er Center for Cybersikkerhed's Cybersikkerhedsråd en del af analysen.

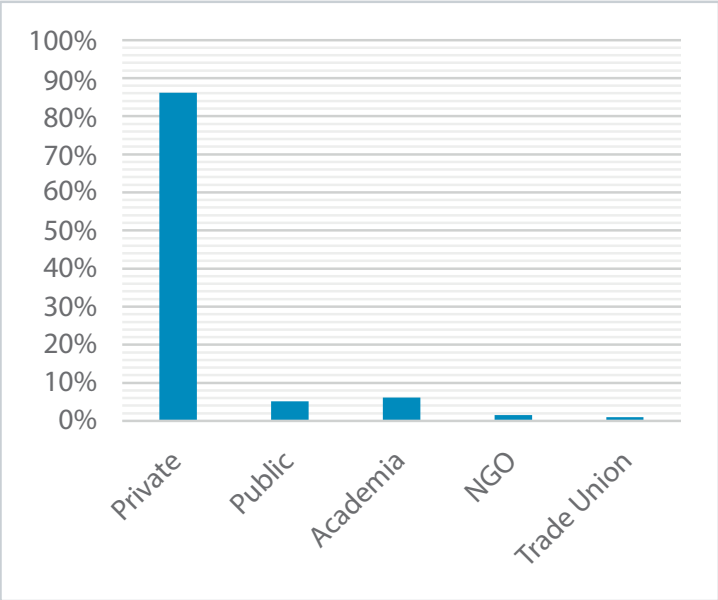
Tabel 1: Oversigt over cybersikkerhedsråd og -udvalg i analysen

Navn	Antal Medlemmer	Offentlig/Privat Styret
Cybersikkerhedsråd	19	Offentligt, Center for Cybersikkerhed
IT-Branchens Sikkerhedsudvalg	53	Privat, IT Branchen
Rådet for Digital Sikkerhed	63	Uafhængig Organisation
Erhvervsministeriets IT Sikkerhed Virksomhedsråd	14	Offentligt, Erhvervsministeriet
Dansk Industri's Udvalg for Informationssikkerhed	16	Privat, Dansk Industri
C25 Danske Virksomheder CISOs eller tilsvarende[2]	30	Privat, ikke formelt organiseret

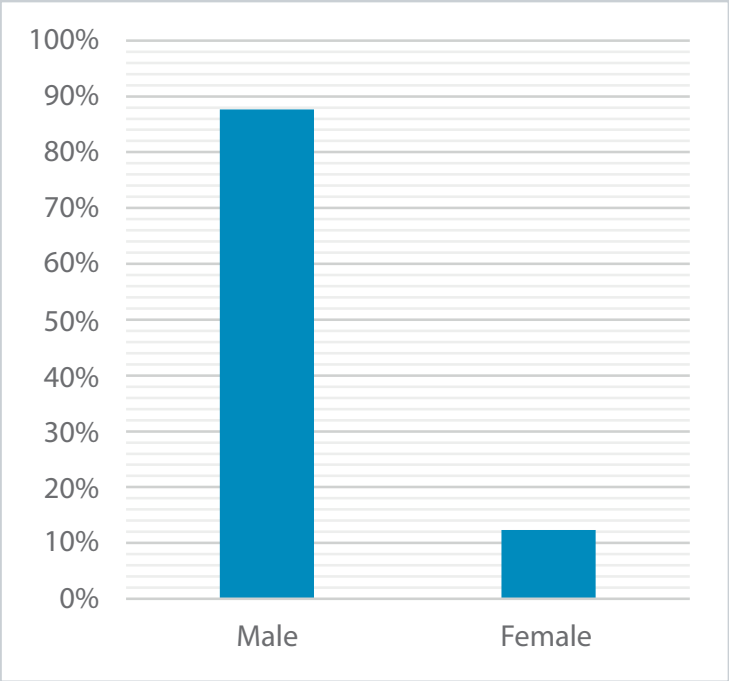
CV'er og uddannelseshistorik blev samlet fra konferencebrochurer og andre offentlige kilder såsom LinkedIn. Resultatet viser først og fremmest en heterogen gruppe af individer. To klare tendenser er, at cybereksperten arbejder i den private sektor, og langt størstedelen af dem er mænd. 86 pct. arbejder i den private sektor, mens henholdsvis 6 pct. og 5 pct. er tilknyttet forsknings- og offentlige institutioner. Kvinder udgør bare 12 pct. Der er en klar fare for "selection-bias" her, i og med at de udvalgte råd og udvalg til dels er private. Studier fra andre lande viser dog lignende resultater. Ifølge ISC²'s 2019 *Cybersecurity Workforce Survey* er 30 pct. af de adspurgte cybereksperter kvinder (ISC2, 2019). Et 2017 "*Global Information Security Workforce Study*" estimerer imidlertid, at på et globalt plan er næsten 90 pct. af cybereksperter mænd (Frost og Sullivan, 2017: 5). At finde data på andelen af offentligt ansatte cybereksperter er mere problematisk (Bate, 2018: 9). En undersøgelse fra Storbritanniens regering viser, at offentlige institutioner har 50 pct. højere sandsynlighed for at outsource cybersikkerhedsopgaver end private virksomheder (Pedley et al., 2020). Det er en indikator for, at offentlige organisationer kan have særlige

problemer med at tiltrække kvalificerede eksperter, blandt andet fordi det kan være svært at konkurrere med lønniveauet i den private sektor (Pollitt, 2010).

Figur 1: Cybereksperter fordelt på sektorer



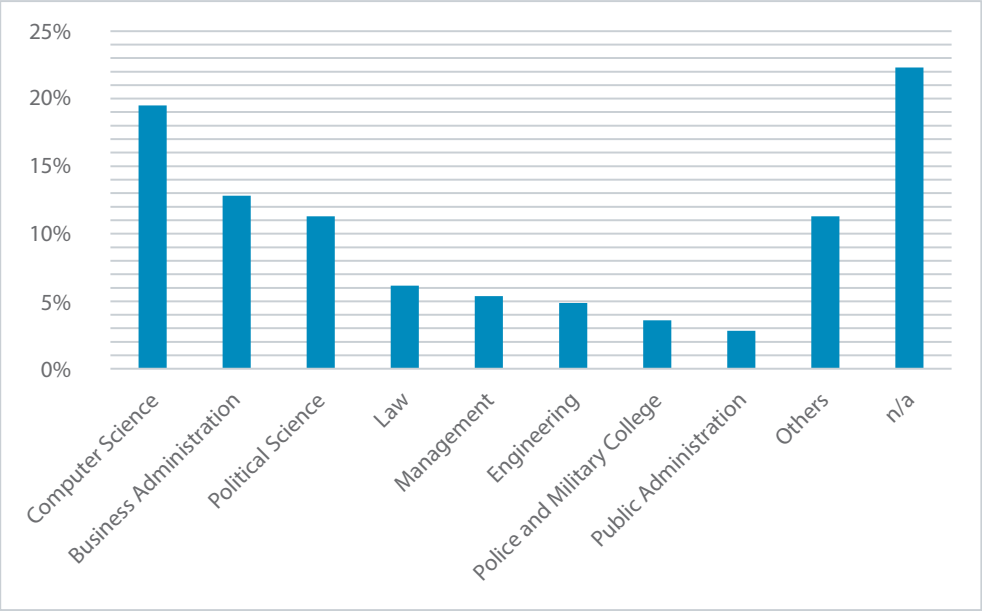
Figur 2: Cybereksperter fordelt efter køn



Uddannelsesmæssigt viser der sig derimod et blandet billede. For hver person i datasættet blev de to seneste videregående uddannelser med minimum to-årig varighed registreret. Det vil sige, at enkeltforløb ikke er blevet registreret. Formålet er at samle sammenhængende uddannelsesforløb, som blev afsluttet med et afgangsbevis. For 19 individer blev der ikke fundet uddannelsesrelate-

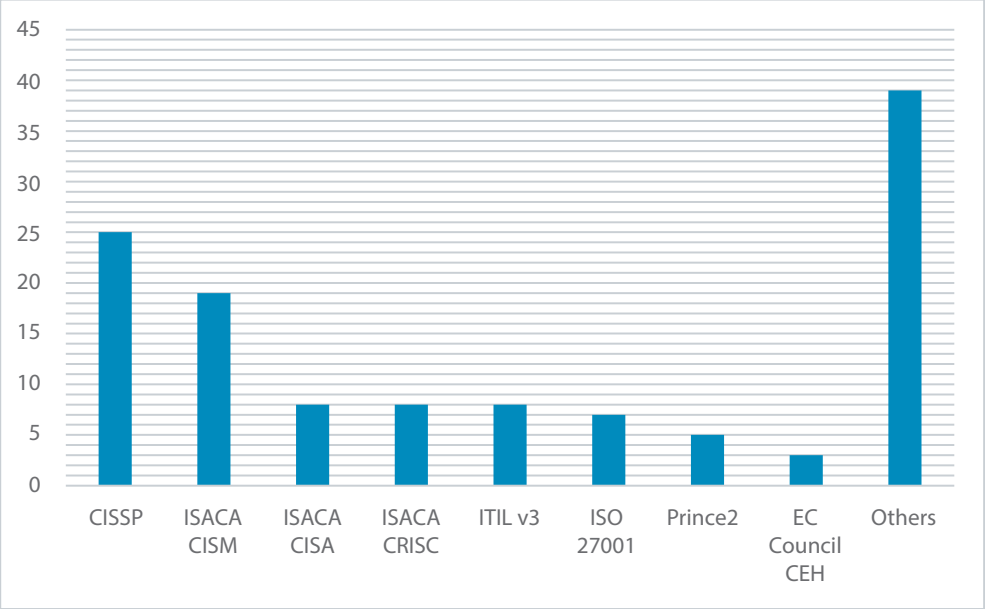
ret information. Yderlige 26 fik kun registreret én uddannelse. Tilsammen svarer de to grupper til de 22 pct. af manglende (n/a) værdier i datasættet. For at give et samlet overblik var det nødvendigt at kategorisere uddannelserne. Det var særligt vigtigt for kategorien computer science. Begrebet dækker i analysen over alle uddannelsestyper indenfor computer, IT, encryption og data science med et overvejende teknisk perspektiv. Computer engineering blev for eksempel kodet som computer science frem for engineering. Til gengæld blev "business og ICT management" kodet som management. Resultaterne skal derfor igen fortolkes som vejledende frem for definitive. Som det fremgår af figur 3 er computer science den hyppigste uddannelsestype blandt de 390 registrerede uddannelser (19 pct.). Business administration (13 pct.) og statskundskab (11 pct.) tager anden- og tredjepladserne. Det kan være overraskende, når der tages udgangspunkt i den klassiske tekniske definition af arbejdet, som diskuteret i Dennings analyse fra starten af 00'erne. En anden måde at illustrere resultatet på er, at næsten en tredjedel (32 pct.) af eksperterne har gennemført minimum én it-specifik uddannelse på universitetsniveau. Samme tendens ses i amerikanske markedsanalyser, som viser, at den hyppigste uddannelsesbaggrund for cybersikkerhedseksperter er computer science og -engineering (Frost og Sullivan, 2017: 5).

Figur 3: Cybereksperters uddannelsesbaggrund, samlede kategorier



Ligeledes er det interessant at se nærmere på de mindre klassiske uddannelser. 19 pct. af eksperterne har som minimum taget en uddannelse i business administration. Hvis vi samler business administration, statskundskab, management, økonomi og public administration i én samlet kategori, kan vi se, at næsten halvdelen (44 pct.) af eksperterne har gennemgået, hvad der kan karakteriseres som en "Djøf-uddannelse".

Figur 4: Certificeringer blandt cybereksperter[3]



Så vidt muligt blev der også taget højde for eksperternes certificeringer. Resultaterne af denne analyse skal læses med den usikkerhed in mente, at der har været et højt antal af manglende værdier (122). To tendenser står dog frem. Både "(ISC)²" CISSP (25) og ISACAs CISM-, CISA- og CRISC-certifikater (35 samlet) dominerer blandt eksperterne. CISSP-certifikatet står for Certified Information Systems Security Professional og bliver udstedt af verdens største medlemsforening af professionelle cybersikkerhedseksperter med over 150.000 certificerede medlemmer verden over (ISC², 2020). At have et CISSP-certifikat er et vigtigt signal, men det fungerer ikke i sig selv som en vej ind i branchen. Derimod er flerårig dokumenteret erfaring en nødvendig forudsætning for at kvalificere som kandidat. CISSP er ofte karakteriseret som den mest anerkendte akkreditering for cybersikkerhedseksperter og signalerer en bred viden på tværs af cybersikkerhedskategorier (Pedley et al., 2020: 14). ISACA er en bredere organisation som dækker over professionelle indenfor IT-branchen generelt og udstiller certifikater blandt andet indenfor cybersikkerhedsfeltet (ISACA, 2020).

Denne illustrerende analyse har vist, at de danske udvalg og råd for cybersikkerhed er domineret af mænd og individer fra den private sektor. Til trods for det begrænsede datagrundlag er konklusionerne på linje med undersøgelser fra USA og Storbritanien. Tekniske it-specifikke uddannelser er hyppige, og mange har også gennemført en lang videregående uddannelse inden for virksomhedsadministration og strategi eller politologi. Certifikater er primært udstedt af private transnationale organisationer med ISACA og "(ISC)²" som dominerende.

En ny ekspertprofil? Fra teknisk fokus til procesorientering

Til trods for en fortsat relativ høj varians blandt de undersøgte eksperters baggrunde ser vi mange af de samme uddannelsestyper og certificeringer. Samtidig er der en klar tendens, som placerer cybereksperten imellem eksisterende felter (Eyal, 2013b). Det tekniske fokus er suppleret med virksomhedsorganisatorisk og politologisk ekspertise. En mulig konsekvens er, at cybersikkerhed ikke længere anses som en ren teknisk kompetence, men snarere som et brobyggende led med et stærkt teknisk fundament. Fra et organisatorisk perspektiv vil en sådan udvikling tage cybersikkerhed fra at være et afgrænset led i driften af en organisation til en mere integreret rolle med en klar procesorientering (Ferdinand, 2015). Hvor den klassiske cybersikkerhedsekspert var en del af IT-afdelingen (Denning, 2001), har den nye profil både et bredere i fokus og befinder sig tættere på direktørniveauet.

Procesorienteringen reflekterer også en mere proaktiv tilgang til cybersikkerhed. I den tidlige profil som en del af IT-afdelingen var cybersikkerhed anset som en del af virksomheds*driften*. Fokus var på en effektiv forbedring af de defensive digitale kapaciteter med en prioritering af at holde omkostningerne nede. Det nye profil ser derimod ud til at være en del af organisations*udviklingen* og dermed ikke primært en omkostningsfaktor. Som en del af governance-ledet handler det om at udvikle en proces omkring organisationens digitale sikkerhed med det formål at segmentere essentielle data fra ikke-essentielle processer (EY, 2019: 7, 25).

Det kræver en ekspertprofil, som kan navigere på tværs af tre dimensioner. Som det første kræver det et intimt kendskab til organisationens opbygning og operationer. Business administration-uddannelsen kan forstås som en del af denne profil. Den anden dimension er en forståelse for det eksterne trusselsbillede. Hvem er vores modspillere, og hvad er tendenserne i den globale cybersikkerhedsarena? Politologiske og militære uddannelser kan placeres i denne type. Den tredje dimension er det tekniske fundament som oversætter operationelle og strategiske overvejelser til tekniske løsninger. Uddannelser indenfor kategorien computer-science i ovenstående analyse er relateret til denne dimension. En lignende udvikling blev dokumenteret for sikkerhedseksperter i private amerikanske virksomheder, hvor stillingen "corporate security officer" gik fra at være en teknisk til en strategisk rolle (Petersen, 2013: 225).

Samtidig kan udviklingen forstås som værende baseret på en ny sikkerhedsforståelse. Hvor den afgrænsede profil med fokus på tekniske løsninger er en refleksion af en forenklet sikkerhedsforståelse med klare linjer mellem trussel og sikkerhed, er den nye profil et tegn på anerkendelsen af, at absolut sikkerhed ikke er tilgængelig i den digitale sfære (Reichborn og Friis, 2016). I stedet er det nødvendigt at skabe processer, som sikrer organisationens modstandskraft i tilfælde af et cyberangreb. I sikkerhedspolitisk jargon kan det siges, at vi ser en udvikling fra en strategi baseret på "deterrence by denial" til en resiliensstrategi (Lasconjarias, 2017). Det vil sige, at en ren teknisk beskyttelse

ikke længere anses som hensigtsmæssigt i en verden, hvor dedikerede hackere altid vil finde en vej ind, hvis de har tilstrækkeligt med ressourcer. Resiliensstrategien prioriterer derimod identifikationen af en organisations essentielle formål – såkaldte kronjuveler – og adskiller dem enten fuldstændigt fra det resterende netværk eller bygger særlige sikkerhedsprocesser rundt om dem (ENISA, 2019: 16).

Den nye hybride profil (Petersen, 2013), som har et bredere i fokus og som er rykket tættere på beslutningstagere, styrker ekspertens rolle i relation til at definere risici og udforme hensigtsmæssige løsninger. Den professionssociologiske analyse fremhæver, hvordan cybersikkerhedsarbejdet foregår på en institutionel arena, hvor sikkerhedsforståelser kontinuerligt forhandles mellem eksperter i et spændingsfelt styret af økonomiske, politiske og tekniske overvejelser. Fra et samfundsmæssigt perspektiv rejser en sådan udvikling nye politiske, demokratiske og økonomiske spørgsmål. Det politisk-administrative system bliver udfordret til at etablere tværfagligt samarbejde både internt og med partnere fra private og civilsamfundsorganisationer (Pollitt, 2010). Fra et demokratisk perspektiv bliver det nødvendigt at skabe et grundlag for offentlig diskussion ved at styrke samfundets viden og bevidsthed om digitale risici og handlingsmuligheder. Her bliver det i stigende grad afgørende at skabe en ramme der styrker civilsamfundsorganisationers kapacitet til at formidle ekspertdreven debat til et bredt publikum. Staten kan understøtte denne proces ved at tilbyde gratis uddannelsesmuligheder indenfor cybersikkerhed. Storbritannien tilbyder for eksempel gratis kurser for unge og voksne med en interesse i cybersikkerhed (UK Cyber First, 2020; UK Cyber Skills Immediate Impact Fund, 2020). En sådan mekanisme kan også bidrage til at rette op på kønsfordelingen og motivere flere kvinder til at komme ind på cybersikkerhedsmarkedet. Målsætningen må være at løfte cybersikkerhedsdiskursen fra en teknificeret til en inkluderende debat, som anerkender den *politiske* kerne af forskellige handlingsmuligheder (Dunn Cavelty og Wenger, 2020).

Målsætningen må være at løfte cybersikkerhedsdiskursen fra en teknificeret til en inkluderende debat, som anerkender den politiske kerne af forskellige handlingsmuligheder

Fra et økonomisk perspektiv er cybersikkerhed et emne, som kun kommer til at vokse i betydning, og håndteringen af digitale risici koster penge. En succesfuld procesorientering kan minimere omkostningerne af cyberangreb betydeligt. Det kræver som diskuteret en ny ekspertprofil, som kan fungere som bindeled mellem tekniske, organisatoriske og strategiske overvejelser. Der er dog ingen tvivl om, at det tekniske element forbliver grundlaget for beslutninger. Derfor må der ydes en ekstra indsats for at øge bevidstheden om digitale trusler og sårbarheder på direktørniveauet, og en basal forståelse for cybersikkerhed bliver i stigende grad afgørende. Ligesom for den brede samfundspolitiske diskussion betyder dette ikke, at alle skal blive eksperter,

men det fordrer en bred anerkendelse af, at digitale risici er en fundamental bestanddel af det digitale samfund og økonomi.

Behov for politisk opmærksomhed og debat

Denne artikel har argumenteret for et stærkere fokus på vidensdannelsen og ekspertprofiler indenfor cybersikkerhedsforskningen. Organisationen og placeringen af ekspertviden inden for modne og umodne professioner kan være en vigtig faktor i udformningen af sikkerhedsforståelser på tværs af offentlige og private organisationer.

Der er en mangfoldighed af analyseredskaber til at analysere dynamiske processer mellem mikro- og makroniveauet. Her har jeg fokuseret på professionsbegrebet inspireret af Andrew Abbotts professionssociologi. Ved at fremhæve den politiske karakter af institutionaliseret viden har jeg rettet fokus imod placeringen af ekspertviden inden for et system af professioner, som står i et konkurrenceforhold til hinanden i kampen om at etablere en eksklusiv autoritet til at definere problemer og komme med legitime løsninger.

Analysen af danske cybereksperter indikerer, at politologisk og virksomhedsadministrativ viden er blevet vigtige referencepunkter for den ellers klassiske tekniske cybersikkerhedsprofil. Denne udvikling kan anskues som manifestationen på en ny sikkerhedsforståelse, som i større grad er fokuseret på organisationers modstandsevne i forhold til cybertrusler. Den nye arbejdsprofil ligger tættere på organisations*udvikling* med et fokus på at segmentere essentielle fra ikke-essentielle processer.

I takt med at cybereksperter udvider deres kontrol gennem en procesorienteret profil, er der brug for at supplere den teknificerede og ekspertdominerede cybersikkerhedsdiskurs med en demokratisk og inkluderende debat. En sådan form for demokratisk kontrol er afgørende i en tid, hvor cybersikkerhed vokser i betydning og er blevet en vigtig faktor i mange politiske og geopolitiske spørgsmål som for eksempel brugen af kryptering og udviklingen af offensive militære cyberkapaciteter.

Noter

1 Funding: Norwegian Research Council (#274740), 'The Market for Anarchy' Project.

2 Enkelte steder har det været nødvendigt at inkludere flere personer fra samme virksomhed.

3 Der findes en lang række certificeringer. ISC2[2]'s CISSP og ISACA's certificeringer er udstilt af den største professionelle organisation for hhv. cybersikkerhedseksperter og IT professionelle. ITIL er en "IT Service Management" certificering udstilt af Office for Government Commerce under det britiske finansministerie. ISO27001-certificeringen er en informationssikkerhedsstandard fra "International Organization for Standardization". Standarden er af stor betydning for virksomheder i forbindelse med cyberforsikringer for at dokumentere risiko managementprocesser.

Referencer

Aalborg Universitet (2020), »Danmarks første uddannelse i cybersikkerhed«, 29. januar www.nyheder.aau.dk/2019/nyhed/danmarks-foerste-uddannelse-i-cybersikkerhed.cid447828

Abbott, A. (1988), *The System of Professions – An Essay on the Division of Expert Labor*, The University of Chicago Press.

Abbott, A. (2005), "Linked ecologies: States and universities as environments for professions", *Sociological Theory*, 23(3): 245–74.

Allan, B.B. (2018), "From subjects to objects: Knowledge in International Relations theory", *European Journal of International Relations*, 24(4), 841–64.

Bate, L. (2018), "Cybersecurity Workforce Development: A Primer", https://d1y8sb8igg2f8e.cloudfront.net/documents/Cybersecurity_Workforce_Development_A_Primer_2018-10-31_175830_YMwa3ZJ.pdf

Bueger, C. (2014), "From Expert Communities to Epistemic Arrangements: Situating Expertise in International Relations", i Maximilian Mayer, Mariana Carpes og Ruth Knoblich, red., *International Relations and the Global Politics of Science and Technology*, Springer Verlag, pp. 39–54.

Burley, D.L., J. Eisenberg og S.E. Goodman (2014), "Privacy and security: Would cybersecurity professionalization help address the cybersecurity crisis"? *Communications of the ACM*, 57(2): 24–7.

CASE Collective (2006), "Critical Approaches to Security in Europe: A Networked Manifesto", *Security Dialogue*, 37(4): 443–87.

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.

Christensen, K.K. og K.L. Petersen (2017), "Public-private partnerships on cyber security: A practice of loyalty", *International Affairs*, 93(6): 1435–52.

Collier, J. (2018), "Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision", *Politics and Governance*, 6(2): 13-21.

Dawson, J. og R. Thomson (2018), "The future cybersecurity workforce: Going beyond technical skills for successful cyber performance", *Frontiers in Psychology*, 9(june): 1–12.

Deibert, R.J. (2013), *Black code: Surveillance, Privacy, and the Dark Side of the Internet*, Signal.

Denning, P.J. (2001), "Who Are We" ? *Communications of the ACM*, 44(2): 15–19.

Denning, P.J. og D.J. Frailey (2011), "The Profession of IT. Who are we – now"? *Communications of the ACM*, 54(6): 27-9.

Digitaliseringsstyrelsen (2019), »ISO 27001-modenhed i staten«. November https://digst.dk/media/21873/iso-modenhed-i-staten-nov-2019.pdf

Domscheit-Berg, A. (2020), »Bundesregierung nimmt das Problem der IT-Sicherheit nicht ernst – Anke Domscheit-Berg", https://mdb.anke.domscheit-berg.de/2020/02/bundesregierung-nimmt-das-problem-der-it-sicherheit-nicht-ernst/

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

Dunn Cavelty, M. og A. Wenger (2020), "Cyber security meets security politics: Complex technology, fragmented politics, and networked science", *Contemporary Security Policy*, 41(1): 5-32.

ENISA (2019), *Threat Landscape Report 2018 15 Top Cyberthreats and Trends*.

EY (2019), *EY Global Information Security Survey 2018–19 – Is cybersecurity about more than protection?* https://www.ey.com/en_gl/advisory/global-information-security-survey-2018-2019

Eyal, G. (2013a), "For a Sociology of Expertise: The Social Origins of the Autism Epidemic", *American Journal of Sociology*, 118(4): 863–907.

Eyal, Gil (2013b), "Spaces between fields," *Bourdieu and historical analysis*, pp. 158-82

Ferdinand, J. (2015), "Building organisational cyber resilience: A strategic knowledge-based view of cyber security management", *Journal of Business Continuity & Emergency Planning*, 9(2): 185–95.

Finansministeriet (2018), »National strategi for cyber- og informationssikerhed, https://fmn.dk/nyheder/Documents/National-strategi-for-cyber-og-informationssikkerhed-2018.pdf

Ford, G. og N.E. Gibbs (1996), *A Mature Profession of Software Engineering*, CMU/SEI-96-TR-004

Fourcade, M. (2010), *Economists and Societies*, Princeton University Press.

Fourcade, M., E. Ollion og Y. Algan (2015), "The Superiority of Economists", *Journal of Economic Perspectives*, 29(1): 89–114.

Frost og Sullivan (2017), *The 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk*.

Gorwa, R. og M. Smeets (2019), *Cyber Conflict in Political Science: A Review of Methods and Literature*.

Government of the United Kingdom (2016), "National Cyber Security Strategy 2016-2021", https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Government of the United Kingdom (2018), *Implementing the National Cyber Security Strategy – Developing the Cyber Security Profession in the Uk*. Retrieved from https://extranet.cranfield.ac.uk/government/uploads/system/uploads/attachment_data/file/767427/,DanaInfo=assets.publishing.service.gov.uk,SSL+Government_Response_to_Consultation_on_Developing_the_

Cyber_Security_Profession_in_the_UK_-_21_December_2018.pdf
Gracia, L. og L. Oats (2012), "Boundary work and tax regulation: A Bourdieusian View", *Accounting, Organizations and Society*, 37(5): 304–21.
Hansen, L. og H. Nissenbaum (2009), "Digital disaster, cyber security, and the copenhagen school", *International Studies Quarterly*, 53(4): 1155–75.
ISACA (2019), *State of Cybersecurity 2019 Part 1: Current Trends in Workforce Development*, www.isaca.org/Knowledge-Center/Research/Documents/cyber/state-of-cybersecurity-2019-part-1_res_eng_0319.pdf?regnum=500542
ISACA (2020), "IT Certification Programs | Information Technology Certifications | ISACA", www.isaca.org/credentialing
ISC² (2019), "Cybersecurity Workforce Study – Strategies for Building and Growing Strong Cybersecurity Teams".
ISC² (2020), "Cybersecurity Certification and Training | (ISC)², www.isc2.org/about
Kremer, J. (2014), "Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace", *Information and Communications Technology Law*, 23(3): 220–37.
Krentz, N. (2014), *Ritualwandel und Deutungshoheit: Die frühe Reformation in der Residenzstadt Wittenberg (1500-1533)*, Mohr Siebeck.
Lasconjarias, G. (2017), "Deterrence Through Resilience: Nato, the Nations and the Challenges of Being Prepared", i *Eisenhower Paper, Research Division*.
Lee, R.M. og T. Rid (2014), "OMG Cyber!: Thirteen Reasons Why Hype Makes for Bad Policy", *RUSI Journal*, 159(5): 4–12.
McCarthy, D.R. (2018), "Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order", *Politics and Governance*, 6(2): 5–12.
National Research Council (2013), *Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making*.
NIST (2017) *National Initiative for Cybersecurity Education (NICE) – Cybersecurity Workforce Framework*, National Institute of Standards and Technology
Pedley, D., T. Borges, A. Bollen, J.N. Shah, S. Donaldson, S. Furnell og D. Crozier (2020), *Cyber security skills in the UK labour market 2020 Findings report*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/869506/Cyber_security_skills_report_in_the_UK_labour_market_2020.pdf
Petersen, K.L. (2013), "The corporate security professional: A hybrid agent between corporate and national security", *Security Journal*, 26(3): 222–35.
Pollitt, C. (2010), "Technological Change: A Central yet Neglected Feature of Public Administration", *NISPAcee Journal of Public Administration and Policy*, 3(2): 31–53.
Reed, M.I. (1996), "Expert power and control in late modernity: An empirical review and theoretical synthesis", *Organization Studies*, 17(4): 573–97. https://doi.org/10.1177/017084069601700402
Reichborn, E. og K. Friis (2016), "From Cyber Threats to Cyber Risks", i K. Friis og J. Ringsmose, red., *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*, pp. 27–44.
Seabrooke, L. og E. Tsingou (2014), "Distinctions, affiliations, and professional knowledge in financial reform expert groups", *Journal of European Public Policy*, 21(3): 389-407.
Segal, A. (2017), "Chinese Cyber Diplomacy in a New Era of Uncertainty", *Aegis Paper Series*, 1703.
Sending, O.J. (2015), *The Politics of Expertise. Competing for Authority in Global Governance*, University of Michigan Press.
Shires, J. (2018), "Enacting Expertise: Ritual and Risk in Cybersecurity", *Politics and Governance*, 6(2): 31–40.
Shires, J. og M. Smeets (2017), "Contesting 'cyber'", *New America Foundation*.
Slayton, R. og A. Clark-Ginsberg (2018), "Beyond regulatory capture: Coproducing expertise for critical infrastructure protection", *Regulation and Governance*, 12(1): 115–30.
Stevens, C. (2020), "Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet", *Contemporary Security Policy*, 41(1): 129–52.
Stevens, T. (2016), *Cyber Security and the Politics of Time*, Cambridge University Press.
Stevens, T. (2018), "Global cybersecurity: new directions in theory and methods", *Politics and Governance*, 6(2): 1-4.
Tanczer, L.M., I. Brass og M. Carr (2018), "CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy", *Global Policy*, 9(3): 60–6.
Tansey, O. (2007), "Process tracing and elite interviewing: a case for non-probability sampling, "Political Science and Politics", 40(4): 765-72.
Thistlethwaite, J. og M. Paterson (2016), "Private governance and accounting for sustainability networks", *Environment and Planning C: Government and Policy*, 34(7): 1197–1221.
Trump, D.J. (2019), "Executive Order on America's Cybersecurity Workforce | The White House", 2. maj, www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/
Tsingou, E. (2014), "Club governance and the making of global financial rules", *Review of International Political Economy*, 22(2): 225–56.
UK Cyber First (2020), "CyberFirst overview. National Cyber Security Centre United Kingdom", www.ncsc.gov.uk/cyberfirst/overview
UK Cyber Skills Immediate Impact Fund (2020), "Cyber Skills Immediate Impact Fund (CSIIF) – Guidance for Applicants. Government of the United Kingdom",

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/825141/CSIIF_Third_Round_Guidance_for_Applicants.pdf

van Apeldoorn, B. og N. De Graaff (2014), "Corporate Elite Networks and us Post-Cold war Grand Strategies From Clinton to Obama", *European Journal of International Relations*, 20(1): 29–55.

Vogel, R. (2016), Closing the cybersecurity skills gap", *Salus Journal*, 4.

White House (2016), *Federal cybersecurity workforce strategy*, www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf

”Hacking” – forbrydelse eller digitalt selvforsvar?

Temanummer: Cybersikkerhed

Vi kender først og fremmest "hacking" som en forbrydelse. De større, opsigtsvækkende "hacking"-angreb hører vi om i nyhederne. Dog bliver "hacking"-metoden nu også italesat som en it-sikkerheds-kompetence. Således udbydes flere steder kurser i "hacking", og Forsvarets Efterretningstjeneste har oprettet et "Hackerakademi" for at rekruttere talenter til statens tjeneste. Begrebet "hacking" kan skabe forvirring, for alt er ikke tilladt for at optimere eller teste sikkerheden ved it-systemer. Denne artikel klarlægger, hvornår der straffes for "hacking" efter straffeloven. Desuden undersøges, om en it-sikkerhedsaktør må bruge "hacking" som et forsvar, når it-systemer bliver angrebet af en fjendtlig "hacker". I artiklen illustreres, at det kan være vanskeligt at forudsige, hvor grænserne for strafansvar går for den, der vil optimere sikkerheden ved sine systemer.

LENE WACHER LENTZ
adjunkt, ph.d.,
Juridisk Institut,
Aalborg Universitet,
lwle@law.aau.dk

JENS MYRUP PEDERSEN
lektor, ph.d.,
Institut for Elektroniske Systemer,
Aalborg Universitet,
jens@es.aau.dk

Gode og onde hackere

Vi tænker først og fremmest på ”hacking” af it-systemer som en forbrydelse, der håndteres af politi og retsvæsen, hvor angrebet klarlægges, og de skyldige strafforfølges. Imidlertid ses en stigende tendens til at italesætte ”hacking” som en it-sikkerhedskompetence, hvor forskellige ”hacking”-metoder anvendes for at teste sikkerheden ved it-systemer. Således udbydes flere steder kurser i ”hacking”. Desuden har Forsvarets Efterretningstjeneste oprettet et ”Hackerakademi”, under henvisning til, at en væsentlig del af opgaven med at beskytte Danmark og danske interesser ”… udføres af hackere, som er specialiseret i at indhente oplysninger ved at skabe adgang til lukkede netværk, it-systemer og computere” (Forsvarets Efterretningstjeneste, 2016).

Metoden ”hacking” af it-systemer indgår således i flere sammenhænge, og forståelsen af ”hacking” varierer betydeligt: I sociologiske kredse ses eksempler på en bredere forståelse af ”hacking”, der uafhængigt af tekniske og juridiske definitioner anskues som ”hacktivisme”, hvor en borger, der værner om sin digitale frihed, udfordrer forskellige online-overvågningsinstrumenter (Kaufmann, 2020; Hampson, 2012).

I den øgede fokus på it-sikkerhed, og generelt når vi agerer på online platforme og it-systemer, er det vigtigt at have en forståelse for, hvor grænserne går for det strafferetlige ”hacking”-ansvar. Alt må ikke gøres i den gode sags tjeneste – i optimering og test af it-sikkerhed – eller i egen oplevelse af berettigelse.

Vi vil med denne artikel klarlægge, hvad der forstås ved forbrydelsen ”hacking” af et it-system ud fra både et it-sikkerhedsperspektiv og et juridisk perspektiv.

I it-sikkerhedskredse navigeres ofte ud fra sondringen, "black-hat-hackere", som betegnelsen for de ondsindede "hackere", "white-hat-hackere", som de gode "hackere", og endelig "grey-hat-hackerne" som en gråzone derimellem. Straffelovens bestemmelse om "hacking" skal ideelt set balancere to grundlæggende hensyn over for hinanden: På den ene side står den systemejer, der investerer ressourcer i et it-system, og derfor må være den, der tillader og regulerer adgangen hertil. Heroverfor står hensynet til, at vi som brugere på internettet kan agere frit og anonymt for søge information på hjemmesider og platforme, og at det er muligt for os at påvise fejl og uhensigtsmæssigheder ved it-systemerne samt stille kritiske spørgsmål om det, man finder, uden at risikere strafansvar. Vi vil imidlertid se, at den danske straffelov er ganske klar: Man skal have lov af systemejeren for at få adgang til et it-system. Hvis man på eget initiativ og ud fra egne idealistiske eller godgørende formål tester sikkerheden ved andres systemer, risikerer man en straffesag.

» **den danske straffelov er ganske klar: Man skal have lov af systemejeren for at få adgang til et it-system. Hvis man på eget initiativ og ud fra egne idealistiske eller godgørende formål tester sikkerheden ved andres systemer, risikerer man en straffesag.**

Vi vil dernæst se på, om man må begå "hacking" som digitalt selvforsvar, hvis man selv bliver angrebet. Det følger af straffelovens bestemmelser om nødværge og nødret, at hvis man begår et strafbart forhold for at afværge et angreb eller for at redde ting i nødsituationer, kan man i visse tilfælde blive fri for straf. Der er tale om strafferetlige begreber, der er udviklet over mange år og i vidt omfang ud fra fysiske scenarier. Der ses ikke i den strafferetlige teori at være taget stilling til, hvordan man digitalt må forsvare sig selv ved angreb. Her møder de traditionelle strafferetlige begreber altså en ny teknologisk kontekst.

Vi vil illustrere "hacking"-metoden og det digitale selvforsvar ved en case om en "honeypot". En honeypot er et it-system, der er etableret med det formål at tiltrække angreb, eventuelt som afledning fra det egentlige it-system, hvor man har sine dyrebare data. Vi har valgt honeypotten som eksempel, fordi det efterhånden er et udbredt it-sikkerheds-setup, og fordi it-sikkerhedsaktøren både kan forberede honeypotten på angreb og ved monitorering af honeypotten tidsmæssigt ofte vil have mulighed for at reagere og forsvare sig, inden den fjendtlige "hacker" når til de rigtige data og systemer. Vi undersøger de retlige rammer for den situation, hvor en honeypot bliver udsat for et "hacking"-angreb, og it-sikkerhedsaktøren overvejer som selvforsvar at pacificere eller ødelægge den indtrængende software eller at iværksætte et "hacking"-angreb på den fjendtlige "hacker".

For overskuelighedens skyld bruger vi i det følgende betegnelsen "hackeren" om den fjendtlige angriber, der "hacker" et it-system, mens betegnelsen

"it-sikkerhedsaktøren" angår den aktør (en virksomhed, en ansat eller en privat borger), der måtte overveje at anvende "hacking" som digitalt selvforsvar.

Af pladsmæssige hensyn inddrages i det følgende alene straffelovens bestemmelse om "hacking", ikke det eventuelle strafansvar for uberettiget behandling af personoplysninger (GDPR).

"Hacking" som forbrydelse – de farvede hatte

Fra et it-sikkerhedsperspektiv indebærer selve metoden "hacking" blot, at man udfordrer sikkerheden ved et it-system. Det nærmere formål med "hackingen", og hvorvidt "hackingen" er lovlig, har i internationale it-sikkerhedskredse ført til den udbredte brug af sondringen "black-hat-hackere", "white-hat-hackere", og "grey-hat-hackere" (Malwarefox, 2019; Norton, 2020; Kaufmann, 2020; Kirsch, 2014). Ifølge den amerikanske softwarevirksomhed, Norton, er disse betegnelser inspireret af gamle westernfilm, hvor skurken bar sort cowboyhat og helten en hvid cowboyhat (Norton, 2020).

Den fjendtlige "hacker" kender vi: "Black-hat-hackeren", der angriber et it-system for at forvolde skade, hvorved man begår en forbrydelse og bliver strafansvarlig. Heroverfor står "white hat-hackeren", også kaldet "den etiske hacker", som betegner en person, der med et legitimt formål anvender offensive metoder til at teste sikkerheden i systemer, organisationer og virksomheder. Det centrale i forståelsen af "white-hat" er først og fremmest, at man tester systemet ud fra et klart defineret mandat fra systemejeren, som også har fastlagt, hvordan der nærmere skal afrapporteres om eventuelle sårbarheder i sikkerheden (Norton, 2020).

Imellem de to kategorier, "black-hat" og "white-hat", ses en større gråzone, hvor "grey-hat-hackeren" udfordrer sikkerheden ved it-systemer uden forudgående aftale med systemejeren. "Grey-hat-hackeren" kan agere ud fra meget forskellige motiver, eksempelvis nysgerrighed eller et ønske om at opnå anerkendelse. Der kan også være tale om et idealistisk sigte, f.eks. at man gerne vil medvirke til at opretholde en høj grad af beskyttelse ved it-systemer og personoplysninger. Der kan være stor forskel på, dels hvor langt man går for at påvise en sårbarhed, dels hvordan man kommunikerer om de sårbarheder, man finder: Om man foretager en loyal, detaljeret afrapportering til virksomheden, eller om man offentliggør sine fund gennem medierne med fuld eksponering af virksomheden (ENISA, 2016; Kirsch, 2014).

Disse farvede hatte bruges som et fingerpeg om det lovlige ved at bruge "hacking"-metoden til at udfordre sikkerheden ved et it-system. Der kan dog opstå en vis begrebsforvirring, eksempelvis hvis man – ud fra et i egen overbevisning berettiget formål – opfatter sig selv som en "white-hat-hacker", selv om man ikke har fået lov til at få adgang til systemet. Til illustration ses en omtale fra efteråret 2019 om, at en "white-hat-hacker" havde sikret 26 mio stjålne kreditkortoplysninger fra dark web ("www.pymnts.com"). Denne person, som næppe var tilladt adgang af systemejeren, må rettelig betegnes som

en "grey-hat-hacker". Uanset det anerkendelsesværdige formål det kan være at sikre stjålne kreditkortoplysninger, er en "grey-hat-hackers" adfærd problematisk. Som det vil fremgå af det følgende, vil en "grey-hat-hacker" kunne ifalde strafansvar for "hacking" efter den danske straffelov.

"Hacking" som forbrydelse efter straffeloven

Det følger af straffelovens § 263, stk. 1, at strafansvaret omfatter den, der "uberettiget skaffer sig adgang til en andens datasystem eller data, som er bestemt til at bruges i et datasystem". Ordet "datasystem" skal her forstås synonymt med it-system. Man kan straffes med fængsel indtil et år og seks måneder. Ved forskellige skærpende omstændigheder kan straffen stige til fængsel indtil seks år.

Populærbetegnelsen "hacking" antyder, at man skal forcere en sikkerhedsforanstaltning, men det er ikke et krav efter dansk ret (Lentz, 2018: 141 ff.). Adgangen skal blot være "uberettiget", hvilket helt enkelt kan bero på, at man ikke har fået lov til at få adgang af systemejeren. En "white-hat-hacker", der har samtykke og et klart mandat fra systemejeren til for eksempel en "penetration-test", hvor man simulerer et angreb med henblik på at kortlægge angrebsflader og sårbarheder, vil have en berettiget adgang og dermed ikke ifalde strafansvar for "hacking".

Man kan straffes for "hacking", hvis man har en berettiget adgang til en del af systemet, men går ud over denne adgang og tilgår andre dele, som man ikke er berettiget til at tilgå. Forbrydelsen er fuldbyrdet, når man har opnået adgang til systemet, det kræves ikke, at man har opnået kendskab til noget, ødelagt noget eller på anden vis rådet over data. Dette kan eventuelt straffes særskilt som hærværk mv.

For at straffe kræves, at den pågældende har "forsæt" til at skaffe sig uberettiget adgang, hvori ligger en vis grad af viden om eller hensigt til at begå forbrydelsen. I de tilfælde, hvor man ikke opnår adgang, vil der kunne straffes for forsøg. Dette skete i en sag, hvor den tiltalte havde forsøgt at opnå adgang til den forurettedes skattemappe ved at indtaste personens CPR-nummer, som tiltalte havde aflæst på forurettedes Facebook-profil (UfR, 2015: 345). Selv om tiltalte kunne argumentere med alene at have brugt oplysninger, der var fuldt tilgængelige for ham, og formålet alene var at se, om det kunne lade sig gøre at tilgå skattemappen og måske drille forurettede, stod det alligevel klart for ham, at han ikke var berettiget til at tilgå forurettedes skattemappe. Blot "at se om man kan" kan dermed let få én i strafferetlige problemer.

"Hacking" er underlagt "betinget offentligt påtale", hvilket betyder, at der kun bliver en straffesag, hvis forurettede anmelder forholdet til politiet eller i øvrigt tilkendegiver, at man ønsker forholdet strafforfulgt, jf. straffelovens § 275, stk. 2.

Som det ses, er "hacking"-bestemmelsen meget bred med formuleringen "uberettiget adgang", når der samtidig ikke er noget krav om, at en sikkerhedsforanstaltning skal være overvundet. Det kan være en fordel, fordi straffebestemmelsen hele tiden kan fortolkes i forhold til den teknologiske udvikling. Lovgiver skal ikke konstant omformulere teksten, efterhånden som nye "hacking"-metoder ser dagens lys. Omvendt betyder en sådan uklarhed, at det kan være svært for borgeren præcist at forudsige, hvad der er strafbart.

"Grey-hat-hackerens" test af it-systemer

"Hacking"-bestemmelsen handler om "uberettiget adgang", men hvornår kan man teknisk set siges at have opnået adgang? Ved systemer beskyttet af password vil dette være let at svare på: Når man har omgået password-beskyttelsen, eksempelvis ved at gætte password eller bruge andres password uden at have fået lov, eller man har måske fundet en bagdør til at få adgang til systemet udenom password-beskyttelsen. Ved andre it-systemer kan det være sværere at fastlægge, hvornår der er opnået "adgang". Problematikken er særlig relevant for de it-kyndige: Hvor meget må man undersøge sikkerheden på andres systemer, før man kan siges at have fået "uberettiget adgang" til datasystemet?

Spørgsmålet var relevant i en ankedom afsagt af Østre Landsret den 7. marts 2017, hvor en far havde opdaget en sikkerhedsbrist i et it-system, som blev brugt som kommunikationsplatform mellem forældre og børnehave. Sårbarheden bestod i, at det var muligt at skrive programkode i et beskedfelt, der ellers normalt er rensede for programkode. Ved at udnytte denne sårbarhed, lavede faren et popup-vindue, som fremkom hos brugerne med teksten: "Ring til [systemudbyderen] og sig, at jeres nye intranet-løsning er blevet hacket". Byretten dømte for "hacking" under henvisning til, at adgangen var uberettiget, idet adgangen gik ud over den adgang, som forældre, der benytter tjenesten, normalt har, hvilket tiltalte havde indset. Retten lagde navnlig vægt på, at tiltalte skrev beskeden i et beskedfelt på en måde, så den blev vist som et popup-vindue, dog fandt retten det ikke bevist, at tiltalte havde haft til hensigt, at popup-vinduet skulle vises hvert tiende sekund. Den omstændighed, at tiltaltes gerning kun var mulig på grund af en sikkerhedsbrist, kunne ikke føre til et andet resultat. Straffen blev fastsat til 10 dagbøder a 500 kr. under henvisning til den begrænsede skade, og til at tiltalte ikke derved fik adgang til personfølsomme oplysninger, samt at formålet med handlingen var at påpege et sikkerhedsproblem (Lentz, 2018: 149).

Landsrettens flertal frifandt for "hacking" og lagde vægt på, at et vidne fra Rigspolitiet havde udtalt, at den tiltalte ikke havde fået adgang til serveren "i den forstand, at han havde adgang til oplysninger eller ændrede noget på denne". På den baggrund blev det konkluderet, at tiltalte ikke havde "skaffet sig adgang til oplysninger fra [systemudbyderens] informationssystem eller adgang til programmer, han ikke var berettiget til at tilgå", eller at tiltalte i øvrigt havde "foretaget ændringer i de oplysninger og/eller programmer, han

var berettiget til at tilgå." Landsrettens mindretal på én voterende ville dømme for "hacking" (Lentz, 2018: 149).

Uanset at tiltalte ikke havde fået adgang til oplysninger om andre brugere, er det dog ganske klart, at han var gået ud over sin berettigede brugeradgang som forælder og var tilgået området for administrators tekniske opsætning af siden, når han tilmed var i stand til at "låse" brugerfladen af med et popup-vindue og hindre andre i at bruge systemet (Lentz, 2018: 149).

Dommen er desværre ikke trykt i de juridiske tidsskrifter, men sagen opnåede en del medieopmærksomhed (Version2, 2016). Umiddelbart kan frifindelsen måske opfattes som et carte blanche til, at man godt må undersøge og udfordre sikkerheden ved it-systemer ved at lave popup-vinduer. Nogen vil måske også kunne få tanken, at det er tilladt at udfordre sikkerheden, hvis man selv eller ens nærmeste pårørende har personfølsomme oplysninger liggende i systemet. Dette vil være en forkert udlægning af dommen. Som nævnt afhænger det strafferetlige ansvar af, om man har fået samtykke af systemejeren og dernæst af, om man er gået ud over samtykket til at tilgå en del af datasystemet, som man ikke har haft berettiget adgang til. Popup-vinduer må således vurderes helt konkret. Derudover har det ingen betydning, om ens egne data er lagret i it-systemet.

IT-Branchen udgav i 2018 på baggrund af denne og andre lignende sager en vejledning om, hvordan man skal forholde sig, hvis man opdager en sikkerhedsbrist med samtidig opfordring til virksomheder om ikke at anmelde dem, der indrapporter fejl og sårbarheder (IT-Branchen, 2018; Version2, 2018). En række virksomheder har tilsluttet sig dette samarbejde, "Kodeks for Indrapportering af Sikkerhedsbrister". Initiativet skal ses som en håndsrækning til de "grey-hat-hackere", der ikke har intention om at gøre skade, og som en erkendelse af, at hvis sikkerheden ved it og data generelt skal forbedres, så må man komme sådanne personer i møde.

Systemejeren har rådigheden over, om der bliver en straffesag mod "greyhat-hackeren". Straffelovens "hacking"-bestemmelse aktualiseres kun, hvis forurettede anmelder forholdet til politiet eller i øvrigt tilkendegiver, at man ønsker forholdet strafforfulgt. I en anerkendelse af "greyhat-hackerens" gode intentioner, kan systemejeren blot lade være med at indgive en anmeldelse om "hacking".

Hvis systemejeren anmelder forholdet, er straffeloven restriktiv: Det gælder helt grundlæggende inden for strafferetten, at det ikke fritager for straf, hvis man med en strafbar handling ønsker at sætte fokus på en problemstilling og skabe samfundsdebat. Således vil det heller ikke være en undskyldning for straf, hvis man skaffer sig uberettiget adgang til et it-system, fordi man er bekymret over it-sikkerheden og opbevaringen af ens egne eller nære pårørendes data. Dog kan et sådant formål i sammenhæng med en begrænset skade være en omstændighed, der konkret kan begrunde, at man idømmes en mildere straf (Lentz, 2018: 150).

» enten har man samtykke og dermed lovlig adgang til et system, eller også har man ikke, og adgangen vil være uberettiget og strafbar. Kun 'white-hat-hackeren' med det klare mandat fra systemejeren vil gå fri, 'grey-hat-hackeren', der på egen hånd 'hacker' systemer vil være strafansvarlig

Konklusionen er derfor, at hvis man opdager sårbarheder ved et it-system, må dette blot konstateres. Man skal tage kontakt til systemudbyderen for at informere om sårbarhederne og få det nødvendige samtykke, hvis man vil tilbyde at teste yderligere. I fortsættelse af diskussionen om "white-hat-hacking"-begrebet gælder der derfor ikke i strafferetlig henseende nogen farvet hat: enten har man samtykke og dermed lovlig adgang til et system, eller også har man ikke, og adgangen vil være uberettiget og strafbar. Kun "white-hat-hackeren" med det klare mandat fra systemejeren vil gå fri, "grey-hat-hackeren", der på egen hånd "hacker" systemer vil være strafansvarlig. Sådan må det nødvendigvis være. Alternativet er meget vanskeligt: Hvem skulle bestemme, hvad der er anerkendelsesværdigt formål, der berettiger til, at man uden tilladelse bryder sikkerheden ved andres it-systemer? Man kan tilmed spørge, hvorfor skulle borgeren have adgang til på egen hånd at "hacke" – og måske ødelægge – andres systemer for at "sætte fokus på sårbarheder", når der er offentlige myndigheder som Datatilsynet og politiet til at håndhæve sikkerheden ved it-systemer. Sat på spidsen ville alle "hackere" kunne undskylde sig i retten med, at de blot testede sikkerheden ved andres systemer.

Selv om en "grey-hat-hacker" måske tør gøre det, som politiet ikke har kompetencer eller ressourcer til, som f.eks. den person, der sikrede 26 mio. stjålne kreditkortoplysninger fra dark web, er der tale om en glidebane af selvtægt. Hvem er de gode? Den person, der tror, han gør noget godt ved at "hacke" en "hacker", har måske misforstået noget, så han "hacker" nogle helt andre. At der ikke ville blive noget strafferetligt efterspil mod den "grey-hat-hacker", der sikrede stjålne kortoplysninger fra dark web, beror i en dansk kontekst på, at et sådant forhold naturligvis ikke ville blive anmeldt til politiet af den systemejer på dark web, som opbevarede de stjålne kortoplysninger. Han har jo selv et forklaringsproblem og risikerer et strafansvar. Pragmatisk set bliver der således ikke danske straffesager mod de "grey-hat-hackere", der rammer plet mod kriminelle. Disse sager bliver ikke anmeldt. Men det er på eget ansvar og egen risiko at ramme plet.

"Hacking" som digitalt selvforsvar

I det følgende vil vi undersøge, om man for at beskytte sine systemer mod et "hacking"-angreb, selv må "hacke" tilbage for at forsvare sig. Ved vurderingen af denne form for digitalt selvforsvar må vi se på, hvad straffeloven egentlig forstår ved selvforsvar.

Hvis man begår et strafbart forhold for at forsvare sig, kan man blive straffri, hvis man opfylder betingelserne for "nødværge" i straffelovens § 13. Betingelserne er restriktive: Handlingen skal være nødvendig for at modstå eller afværge et påbegyndt eller overhængende uretmæssigt angreb. Desuden må handlingen ikke åbenbart gå ud over, hvad der under hensyn til angrebets farlighed, angriberens person og det angrebne godes betydning er forsvarligt.

Som det ses, skal angrebet være aktuelt, og man skal forsvare sig direkte over for angrebet. Hverken i tiden før et angreb bliver aktuelt, eller efterfølgende når angrebet er slut, er det tilladt at gøre noget strafbart for at forsvare sig. Man må gøre det "nødvendige" og "forsvarlige" for at forsvare sig, men hvad ligger der nærmere i det?

Nødværge er ofte relevant i forbindelse med fysiske angreb på personer, hvor det nødvendige og forsvarlige vil være at afværge et voldeligt angreb med samme form for vold, hvorimod det almindeligvis ikke vil være forsvarligt at afværge et knytnæveslag med et knivsstik. Nødværgebestemmelsen angår dog også afværgelse af angreb på ting mv. Skulle det ske, at selvforsvaret går ud over det tilladelige, er der alligevel en vis mulighed for at gå fri efter straffelovens § 13, hvis selvforsvaret "ikke åbenbart går ud over" det forsvarlige, hvor der altså gives et lille spillerum. I øvrigt er der mulighed for straffrihed, hvis selvforsvaret var "rimeligt begrundet i den skræk eller ophidselse", man har oplevet ved at blive angrebet, jf. § 13, stk. 2.

Nødværgebestemmelsen suppleres af straffelovens § 14, der angår "nødret": En handling straffes ikke, hvis den var nødvendig til at afværge truende skade på person eller gods, og lovovertrædelsen må anses for at være af forholdsvis underordnet betydning. Her er det altså tilladt at ofre et mindre gode for at redde personer eller ting fra skade, eksempelvis hvis man bruger andres ting til at slukke en ildebrand med.

For det digitale selvforsvar er det navnlig nødværge-bestemmelsen, der er relevant: Må man begå et strafbart forhold mod angriberen for at stoppe et digitalt angreb? Kernen i nødværge-bestemmelsen er, at man må afværge et aktuelt angreb med det nødvendige, forsvarlige middel. Det oplagte for it-sikkerhedsaktøren ville først være at overveje, om det er muligt midlertidigt at lukke ned for de systemer eller servere, der er angrebet. Ellers vil det måske være muligt at stoppe et igangværende "hacking"-angreb ved at pacificere de fjendtlige systemer. Er der tale om egentlig ødelæggelse af software eller hardware, vil dette som udgangspunkt være hærværk efter straffeloven. Dette kan dog være berettiget som nødværge for at afværge et "hacking"-angreb, uanset om det giver visse dønninger eller ulemper tilbage i det system, der bruges til at styre angrebet.

Til spørgsmålet om it-sikkerhedsaktøren må begå decideret "hacking" ved at skaffe sig adgang til et andet it-system for at forsvare sig mod et påbegyndt eller overhængende "hacking"-angreb, vil svaret formentlig være et nej.

Dette vil næppe være det nødvendige og forsvarlige at gøre for at afværge det "hacking"-angreb, man selv er udsat for.

Man kunne forestille sig, at it-sikkerhedsaktøren overvejer at forsvare sig med metoden, man kender fra DDoS-angreb, hvor man overbelaster angriberens server med forespørgsler, hvilket måske kan stoppe det fjendtlige "hacking"-angreb. Her får it-sikkerhedsaktøren ikke "adgang" til et andet it-system, men afbryder så at sige udefra aktiviteten fra det angribende system. Forsætligt at overbelaste andres servere og dermed hindre ejerens rådighed er som udgangspunkt strafbart efter straffelovens § 293, stk. 2, men det er ikke utænkeligt, at en sådan handling kan være straffri som nødværge for at afværge et "hacking"-angreb. Uanset berettigelsen som nødværge er der dog den usikkerhed ved metoden, at man ikke kan være sikker på at ramme den fjendtlige angriber, idet angrebet kan komme fra systemer og servere, der uforvarende er blevet involveret (se nedenfor om proxy-servere).

Grænsen for nødværge går ved det afsluttede angreb. Man kan dog diskutere, hvornår et angreb er helt afsluttet. Således er det den traditionelle antagelse ved tyveri, at det vil være lovlig nødværge at løbe efter tyven for at fratage ham den genstand, han netop har stjålet fra én (Toftegaard, 2019: 130; Langsted og Waaben, 2015: 140). Er der ikke tale om en sådan umiddelbar reaktion på tyveriet, er der ikke tale om nødværge. I stedet betragtes handlingen som selvtægt, der alene har et genoprettende sigte og således som udgangspunkt ikke fritager for strafansvar for den strafbare handling, man måtte udføre f.eks. for at skaffe sine ting tilbage. Begår man indbrud i tyvens hjem for at få sine ting tilbage, begår man en strafbar handling i form af husfredskrænkelse, der som udgangspunkt vil blive straffet, dog vil der måske i forhold til strafudmålingen være tale om formildende omstændigheder (Langsted og Waaben, 2015: 139).

Indenfor strafferetten har Waaben argumenteret for, at der kan være et område – om end begrænset – for lovlig selvtægt. Dette illustreres med, at hvis man har fået stjålet sin cykel, må man straffrit kunne tage cyklen tilbage, hvis man ser den parkeret på offentlig vej, idet man ikke ved denne handling vil krænke andres interesser (Langsted og Waaben, 2015: 140, se endvidere Langsted, 2020: 19). Ligeledes argumenteres for, at det vil være lovlig selvtægt at gå ind i tyvens forhave, hvor man kan se ens stjålne cykel stå, og formentlig vil man også kunne opnå straffrihed for at ødelægge en lås, som gerningsmanden efterfølgende har forsynet cyklen med (Langsted og Waaben, 2015: 140).

Disse cykel-eksempler fra den strafferetlige teori angår en genstand, som tyven har borttaget fra ejeren, og som nu er i tyvens besiddelse, og som ejeren nu med sikkerhed identificerer som sin egen. Eksemplerne er vanskelige at omsætte til en digital kontekst, hvor man udsættes for et "hacking"-angreb. Først og fremmest kan det diskuteres, hvor længe et "hacking"-angreb er i gang, og hvornår det egentlig kan siges at være afsluttet. Man kan godt forestille sig, at "hacking"-angrebet bliver en tilstand, hvor malware forbliver i systemet, og angrebet ikke endeligt er stoppet, og angriberen ikke endeligt er

lukket ude. Så længe der er et igangværende angreb, må der være adgang til forsvarlig og nødvendig nødværge. Når angrebet er afsluttet, kan man ikke begå en strafbar handling og opnå straffrihed som nødværge. Her er det også vanskeligt at omsætte cykel-eksemplet ovenfor til en digital kontekst, da det næppe giver mening at "løbe efter 'hackeren' for at få sine data tilbage". Her må man henvises til at indgive anmeldelse til politiet om dét, man har været udsat for og overlade håndhævelsen til myndighederne.

At begå præventiv nødværge

Det ligger i nødværgereguleringen, at man skal reagere på et "påbegyndt eller overhængende angreb" og i relation til den nødretlige straffrihed, at man skal afværge "truende skade på person eller gods" ved at ofre ting af mindre værdi for at redde et større gode. I begge situationer reagerer man på en pludseligt opstået situation. Det forudsættes her, at har man mere tid, eller kan angrebet eller faresituationen forudses, så er der ikke adgang til nødværge eller nødret, som fritager én for straf for det strafbare forhold, man har begået. Så må man i stedet for planlægge efter det, tage sine forholdsregler eller kontakte politiet, hvis man føler sig truet og frygter at blive angrebet, eller tilkalde beredskabsmyndighederne ved fare, brand etc.

Må man begå et strafbart forhold som præventiv nødværge, hvis et angreb fremstår sandsynligt for én, men angrebet ikke er påbegyndt eller overhængende? Som udgangspunkt vil svaret være nej, fordi det ikke opfylder betingelserne for nødværge efter straffelovens § 13. Denne problematik har navnlig været aktuel i sager om familiedrab, til eksempel, UfR 1993.193 V, hvor den tiltalte havde dræbt sin storebror med to skud, da han lå og sov på sofaen. Den dræbte havde terroriseret hjemmet og mishandlet familiemedlemmerne i årevis. I sådanne situationer får man ikke straffrihed som følge af nødværge, fordi der ikke er et påbegyndt eller overhængende angreb, som man forsvarer sig imod. Dog kan sådanne forhold indgå som formildende omstændigheder, når straffen skal fastsættes.

Hvordan forholder det sig med andre former for forberedelse af nødværge? Det er klart, at man må have en kniv liggende på sit natbord for at være forberedt på at forsvare sig, hvis der kommer en indbrudstyv, eller man bliver udsat for et overfald. Ved blot at lægge kniven frem har man ikke begået et strafbart forhold, og nødværge-bestemmelsen bliver ikke aktuel. Skulle der opstå en situation, hvor man faktisk bruger kniven til at forsvare sig med, skal det selvfølgelig vurderes, om denne handling er straffri som nødværge.

I den strafferetlige teori tales desuden om at etablere generelle afværgeforanstaltninger, f.eks. at anbringe en glubsk hund for at forhindre, at tyve trænger ind på en byggeplads om natten. Her er der ikke tale om, at man forsvarer sig mod et påbegyndt eller overhængende angreb, og situationen falder derfor uden for nødværge-bestemmelsen (Toftegaard, 2019: 130). I en sag fra 1973 havde ejeren forbundet sin bil, der var parkeret på gaden, med lysnettet for at forhindre tyveri af bilen. Installationen blev opdaget ved, at en forbipasseren-

des hund fik stød, da den lod sit vand op ad bilen. Retten vurderede, at installationen ikke var straffri som nødværge, og tiltalte blev dømt for overtrædelse af stærkstrømsreglementet (sagen er omtalt i Kommenteret straffelov, s. 188, med henvisning til TFDP 1973.401, hvor sagen er refereret).

Hvorvidt sådanne "faretilstande", man måtte etablere for at forsvare sig mod et eventuelle angreb, kan tillades, afhænger af en helt konkret vurdering, hvori indgår, om en lovregulering er overtrådt, og hvad der findes af advarsler til beskyttelse både af tilfældigt forbipasserende og af de ulovligt indtrængende, dette eksempelvis i relation til "glubske pladshunde" (Kommenteret straffelov, s. 188). Desuden må lovligheden bero på en almindelig forsvarlighedsvurdering (Baumbach, 2014: 435).

Som ovenfor nævnt vil det næppe være straffrit som nødværge, hvis it-sikkerhedsaktøren begår "hacking" af et andet it-system for at forsvare sig mod et aktuelt angreb. Skulle man vælge at sætte sine systemer op til et automatisk "hack-back", kommer nødværge slet ikke på tale, fordi der ikke er et aktuelt angreb, man forsvarer sig imod. En sådan automatisk opsætning skal vurderes som en generel afværgeforanstaltning, hvis tilladelighed skal vurderes helt konkret, se videre nedenfor i honeypot-eksemplet.

Skulle it-sikkerhedsaktøren alligevel vælge at lave et "hack-back" eller at sætte systemet op til at foretage en sådan handling, er det langt fra sikkert, der bliver et strafferetligt efterspil mod den pågældende. Hvis man har ramt plet mod den fjendtlige "hacker", vil denne næppe anmelde it-sikkerhedsaktøren til politiet. Men it-sikkerhedsaktøren bør være klar over, at denne fremgangsmåde er problematisk i forhold til straffeloven, og som nævnt ovenfor vil det også her være på eget ansvar og egen risiko at ramme plet.

Honeypot som digitalt selvforsvar

Vi vil illustrere "hacking" som digitalt selvforsvar ved en case om en "honeypot". En "honeypot" er betegnelsen for et it-system, der er etableret med det formål at blive angrebet. Typisk vil det være en selvstændig form for digital kopi eller "dobbeltgænger" af et kørende system eller service, som ligner det rigtige system udefra, hvorved it-sikkerhedsaktøren får mulighed for at se, hvilke angreb der foretages mod systemet. Man kan forestille sig en producent, der etablerer en honeypot af et af sine produkter for at kunne følge med i, hvordan produktet angribes, hvis det eksponeres direkte mod internettet. En anden variant er at bruge en honeypot som afledning. Man kan forestille sig, at en "hacker", der forsøger at angribe et universitet, i sin indledende søgen kommer til at betræde den etablerede honeypot, hvorved der genereres en alarm, fordi man ved, at der under normale omstændigheder ikke skal være aktivitet omkring honeypotten.

» En "honeypot" er betegnelsen for et it-system, der er etableret med det formål at blive angrebet

Strafferetligt er der intet til hinder for, at man etablerer en honeypot for på denne måde at optimere sin sikkerhedsindsats ved at sætte et falsk offer frem, som kan blive udsat for ondsindede angreb. Honeypotten skal her ses som en sikkerhedsforanstaltning, hvor man så at sige befinder sig på sin egen banehalvdel. Det aktualiserer ikke noget strafansvar for ejeren af honeypotten. Tværtimod vil man være berettiget til at anmelde de angreb, som honeypotten udsættes for, som "hacking" eller forsøg på "hacking". Hvis man konstaterer aktivitet på sin honeypot, som tolkes som et angreb, hvor "hackeren" forsøger at få uberettiget adgang til det it-system, hvor ens data er beskyttet, må it-sikkerhedsaktøren afværge angrebet. Det nødvendige og forsvarlige kan være at ødelægge den indtrængende software, selvom det kan give visse dønninger tilbage i hackerens system. Dog vil det umiddelbart ikke være tilladt som nødværge at lave et "hacking"-angreb på et andet it-system.

Spørgsmålet er, om en honeypot må programmeres til som en generel afværgeforanstaltning at pacificere eller ødelægge den indtrængende software. Også her er det vanskeligt at omsætte de strafferetlige eksempler til en digital kontekst. I det øjeblik installationen laves, overtræder man umiddelbart ikke nogen regulering, i modsætning til bilejeren, der havde overtrådt stærkstrømsreguleringen ved at sætte strøm til sin bil for at forhindre tyveri. Det er dog ligeså klart, at hvis man programmerer honeypotten til at ødelægge eventuel, senere indtrængende software, har man forberedt en automatisk hærværkshandling. Da der på tidspunktet for programmeringen ikke er et aktuelt angreb, er vi uden for nødværge-bestemmelsen. Hvorvidt en sådan automatisk hærværks-installation er tilladelig, vil afhænge af en konkret vurdering af, hvordan det er sikret, at den ikke rammer nogen, der uforvarende har bevæget sig ind på honeypotten, og hvorvidt installationen i det hele vurderes at være forsvarlig. Selvsagt er det, vi kender fra den fysiske verden, hvor man advares om en bidsk hund på den afspærrede byggeplads i aftentimerne, vanskeligt at overføre til den digitale kontekst. Det er domstolene, der i sidste ende vil vurdere tilladeligheden af sådanne generelle afværgeforanstaltninger, og spørgsmålet bliver først aktuelt, hvis nogen eller noget er blevet påvirket negativt af foranstaltningerne, og et eventuelt strafansvar skal afgøres.

Uanset hvordan it-sikkerhedsaktøren vælger at afværge et angreb, er det tilladt at indsamle oplysninger om den fjendtlige "hacker". Man kan måske forestille sig, at det med forskellige tracking-teknologier vil være muligt at skaffe sig oplysninger om "hackerens" IP-adresse (der identificerer en computers eller anden enheds globale adresse på internettet, og som tildeles af internetudbyderen), land, browserversion mv. Her får man ikke uberettiget adgang til noget it-system, men man sikrer sig vigtige identifikationsoplysninger, som vil kunne videreformidles til politiet i forbindelse med anmeldelse af det angreb, man har været udsat for.

Dog knytter der sig en stor usikkerhed til en sådan identifikation af den formodede angriber. Dette skyldes, at den globale IP-adresse, der identificeres, kan være delt mellem flere computere og brugere. Desuden kan angriberen

meget vel være gået gennem en eller flere proxy-maskiner i sit angreb og dermed have camoufleret sin egen IP-adresse. Sådanne proxy-maskiner kan være intetanende borgeres computere eller netværk med dårlig sikkerhed, som bliver brugt af kriminelle til "gennemgang" for at skjule, hvem der egentlig står bag forbrydelsen. Skulle en it-sikkerhedsaktør i en sådan situation ty til et "hack-back", vil den computer eller server, man umiddelbart kan se, at angrebet kommer fra, ikke være forbryderens computer. Derimod er ejeren i denne sammenhæng en intetanende borger eller virksomhed, der nu oplever et "hacking"-angreb med mulig ødelæggelse af udstyr, software og kompromittering af data til følge. Situationen illustrerer fint, hvorfor "hack-back" og anden digital selvtægt i egen oplevelse af berettigelse generelt ikke er nogen farbar vej.

Teknologi og strafferet

Vi har i denne artikel klarlagt, hvad der forstås ved "hacking" som forbrydelse efter straffeloven, hvor det afgørende er, om der er samtykke fra systemejeren til, at man får adgang. I forhold til den internationalt anvendte terminologi om de farvede hatte, vil ikke bare den ondsindede "black-hat-hacker" blive straffet efter straffeloven. "Grey-hat-hackeren", der i egen opfattelse af berettigelse tilgår it-systemer uden systemejerens samtykke, vil også få problemer med den danske straffelov.

Stadig har vi brug for som samfund at få alle gode kræfter i spil, når det gælder konstant fokus og optimering af it-sikkerhed til gavn for os alle. Det er et tiltrængt initiativ, at IT-Branchen har udarbejdet et kodeks for fair behandling af de "grey-hat-hackere", der loyalt indrapporterer sikkerhedsbrister ved it-systemer. Det er ikke hensigtsmæssigt, hvis strafferetten skal løse situationer med dårlig dialog mellem sådanne whistleblowere med gode intentioner og den systemejer, der nu får chancen for at rette op på sikkerheden ved sine systemer. I nogle tilfælde vil systemejeren derved undgå at få en bøde fra Datatilsynet for dårlig sikkerhed ved opbevaring af personoplysninger.

» Den traditionelle strafferetlige tankegang om nødværge, hvor man forsvarer sig mod angreb, er vanskelig at anvende i en digital sammenhæng. Eksemplet om at løbe efter tyven, der har stjålet ens cykel for at få cyklen tilbage, er meget vanskeligt at omsætte til en digital virkelighed

Den traditionelle strafferetlige tankegang om nødværge, hvor man forsvarer sig mod angreb, er vanskelig at anvende i en digital sammenhæng. Eksemplet om at løbe efter tyven, der har stjålet ens cykel for at få cyklen tilbage, er meget vanskeligt at omsætte til en digital virkelighed, hvor man gerne vil forsvare sine systemer mod angreb, måske undersøge et igangværende "hacking"-angreb og forsøge at opspore "hackeren" og klarlægge, hvad der er sket med ens data og forhindre fortsat uberettiget brug af data. Det man må gøre, hvis man

er udsat for et "hacking"-angreb, er som udgangspunkt kun det nødvendige og forsvarlige for at afværge dét angreb, men giver ikke adgang til hævn eller "hack-back" af gerningsmandens systemer. Når man i sit digitale selvforsvar selv bliver "hacker", kan man blive strafansvarlig.

Har man mulighed for at tilvejebringe identifikationsoplysninger om "hackeren", vil dette uden tvivl være værdifuld viden, som skal angives i anmeldelsen til politiet, eksempelvis om den IP-adresse, angrebet er sket fra, hidrører fra dansk territorium. Der er ingen tvivl om, at den første indledningsvise screening for politiets efterforskning vil være at klarlægge, om der er danske efterforskningsmuligheder, og om angrebet ser ud til at være begået af en gerningsmand i Danmark. Dansk politi har kun kompetence til at efterforske i Danmark, og efterforskning i udlandet, f.eks. ved at opspore, hvem der har anvendt en bestemt udenlandsk IP-adresse, kræver det andet lands retshjælp. Resultatet vil være en mere kompliceret og langvarig efterforskning på tværs af landegrænser, og dette vil formentlig kun iværksættes i sager af en vis grovhed, eksempelvis hvor der er sket en større økonomisk skade.

I den fortsatte optimering af it-sikkerhed ved danske it-systemer og udvikling af nye teknologiske værktøjer til digitalt selvforsvar, er det vigtigt konstant at være opmærksom på strafferettens grænser for, hvad man må foretage sig. Den strafferetlige lovgivning, man skal orientere sig i, bygger i vidt omfang på brede formuleringer, hvor tanken har været, at også nye teknologiske muligheder skulle rummes heri. Vi så det ved "hacking"-bestemmelsen, hvor den meget brede formulering "uberettiget adgang" til datasystemer dog kan give anledning til tvivl om, hvor meget man må undersøge andres systemer, og hvornår der teknisk set kan siges at være opnået adgang. Hvad angår det digitale selvforsvar, og hvad man må gøre, når man udsættes for et "hacking"-angreb, er det straffelovens nødværge-begreb, der er det centrale omdrejningspunkt. Igen er der tale om en meget bred bestemmelse. Her må man ty til fysiske eksempler om drab i familieforhold, cykeltyveri, biler tilsat strøm samt bidske hunde på byggepladser for at skitsere, hvordan nødværge-begrebet skal forstås i en ny digital kontekst. For lovgiver kan sådanne brede formuleringer være en fordel, for så kan man lade området udvikle sig i retspraksis, når domstolene tager stilling til konkrete sager med nye teknologiske metoder. Ulempen er for den enkelte borger, at det er svært at forudsige præcist, hvad man må foretage sig, og hvornår man kan rammes af et strafansvar. Der er ingen tvivl om, at it-sikkerhedsaktøren sættes på en vanskelig opgave.

Litteratur

Baumbach, Trine (2014), "Strafferet og menneskeret", København: Karnovgroup.

ENISA, European Union Agency for Cybersecurity (2016), "Good Practice Guide on Vulnerability Disclosure. From challenges to recommedations", www.enisa.europa.eu/publications/vulnerability-disclosure

Forsvarets Efterretningstjeneste (2016), "FE opretter hackerakademi", pressemeddelelse, 16. marts, https://fe-ddis.dk/Nyheder/nyhedsarkiv/2016/Pages/Hackerakademi.aspx

Hampson, Noah C. (2012), "Hacktivism: A New Breed of Protest in a Networked World", *Boston College International and Comparative Law Review*, 35(2): 511-42.

IT-Branchen (2018), "Kodeks for Indrapportering af Sikkerhedsbrister", https://itb.dk/raadgivning/kodeks-for-indrapportering-af-sikkerhedsbrister/laes-kodekset/

Kaufmann, M. (2020), "Hacking surveillance", *First Monday*, 25(5), https://doi.org/10.5210/fm.v25i5.10006

Kirsch, Cassandra (2014), "The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law", *Northern Kentucky Law Review*, 41(3): 383-403.

Langsted, Lars Bo (2020), "Ulovlig selvtægt. En analyse af straffelovens § 294", *Juristen*, 1, pp. 16-21.

Langsted, Lars Bo og Knud Waaben (2015), *Strafferettens almindelige del*, København: Karnovgroup.

Lentz, Lene Wacher (2018), "'Hacking' og det digitale privatliv", *Juristen*, 4, pp. 141-53.

Madsen, Lasse Lund, Thomas Elholm og Morten Niels Jakobsen (2019), *Kommenteret straffelov, almindelig del*, København: Jurist- og Økonomforbundets Forlag.

Malwarefox (2019), "10 Types of Hackers You Should Know", https://www.malwarefox.com/types-of-hackers/

Norton (2020), "What is the Difference Between Black, White and Grey Hat Hackers?", https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html

Symantec (2019), "Internet Security Threat Report", volume 24, www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Tidsskrift for Dansk Politi (1973), s. 401, København: Dansk Politiforbund.

Toftegaard Nielsen, Gorm (2019), *Strafferet 1. Ansvaret*, på grundlag af Lasse Lund Madsen, København: Djøf Forlag.

Version 2 (2018), "Sikkerhedsbrister: Længe ventet vejledning til whistleblowing udgivet", 15. juni, www.version2.dk/artikel/sikkerhedsbrister-laenge-ventet-vejledning-whisteblowing-udgivet-1085420

Version2 (2016), "Dom faldet i kontroversiel hackersag", 15. april, www.version2.dk/artikel/dom-faldet-i-kontroversiel-boernehave-hackersag-709985

www.pymnts.com (2019), "White-Hat Hacker Swipes 26M Stolen Credit Cards From Dark Web", 15. oktober, www.pymnts.com/news/security-and-risk/2019/white-hat-hacker-swipes-stolen-credit-cards-from-dark-web/

Domme

UfR (Ugeskrift for Retsvæsen), 2017 p. 247 V.

UfR 2015, p. 345 Ø.

UfR 1998, p. 1769/2 Ø.

TfK (Tidsskrift for Kriminalret), 2008, p. 745/2 V.

Østre Landsrets utrykte ankedom af 7. marts 2017 (S-2696-16)

Love

Straffeloven (lovbekendtgørelse nr. 976 af 17. september 2019)

Stærkstrømsreguleringen, den nugældende elsikkerhedslov, lovbekendtgørelse nr. 26 af 10. januar 2019 med tilhørende bekendtgørelser.

Moderne tider. Aktiv krisestyring – er Keynes tilbage?

Temanummer: Cybersikkerhed

På sin vis har forskningen i Keynes' forfatterskab vist sig at være særdeles sejlivet. Således dannede dette baggrunden for den keynesianske æra og gav nogen inspiration til den ny-keynesianske teoridannelse. Der forskes også stadigvæk aktivt i forfatterskabet især inden for post keynesianske kredse. Om end i perioder under pres forsvandt keynesianismen dog aldrig helt, og efter The Great Recession og Covid-19-pandemien er keynesianismen så aktivt tilbage i makroteorien? Og hvad med den post keynesianske tænkning? Vinder denne også øget anerkendelse? Om især disse aspekter handler nærværende artikel.

Om Keynes, keynesianisme og moderne tider

FINN OLESEN
Professor, Institut for Økonomi og Ledelse, Aalborg Universitet, finn@business.aau.dk

På sin vis har forskningen i Keynes' forfatterskab vist sig at være særdeles sejlivet. Af helt naturlige årsager beskæftigede mange sig med hans tanker i forbindelse med keynesianismens gennembrud, som for alvor tog fart efter 2. Verdenskrig. I en Kuhnsk terminologi var der en del paradigmatisk normalvidenskabelig forskning, som skulle på plads.

Med *The General Theory* var rammerne for det nye paradigme givet. Og med Keynes' tidlige død allerede i april 1946 var det især op til andre end ham selv at udfylde, hvad der nu skulle til for at gøre *The General Theory* til et egentlig makroøkonomisk paradigme.[1] Som eksempelvis beskrevet i Olesen (2008) blev den dominerende fortolkning af *The General Theory* hurtigt forankret i, hvad der benævnes for den neoklassiske syntese; blandt andet på baggrund af fremstillingen i Modigliani, (1944). I denne forståelse var Keynes' tankegang ikke generel. Han beskrev i stedet for et specielt tilfælde. Nemlig, hvordan en økonomi kan låses fast i en lavkonjunktur, når især løndannelsen er infleksibel. Keynes var altså lig med kriseteori i en situation, hvor markedskræfterne var sat afgørende ud af kraft.

Med et sådant perspektiv kom keynesianismen hurtigt til at fokusere på det kortere sigt i den økonomiske analyse. Det grundlæggende problem var, hvorledes et makroøkonomisk udfald fastholdes så tæt på fuld beskæftigelsessituationen som overhovedet muligt. Midlet til at opnå den størst mulige minimering af konjunkturudsvingene blev den efterspørgselsregulerende økonomiske politik – ofte benævnt for "stop-and-go"-politikken. På sigt tog markedsmekanismen over. På sigt sikrede ændringer i de relevante relative prisforhold, at det aktuelle outputniveau var maksimeret. På sigt tog altså mere klassiske teoretiske dyder over.

Men nogle makroøkonomer var ikke tilfredse med denne fortolkning af Keynes' teoretiske univers. Set i deres perspektiv var fortolkningen ganske forkert. Keynes' forståelsesramme var virkelig en *generel* teoridannelse, som kunne forholde sig til, hvad der skete i monetære produktionsøkonomier, uanset om disse befandt sig i en økonomisk krise, i fuld beskæftigelse eller i en boom-like situation. Og så gjorde Keynes brug af en fundamental set anden metodologi end den, som den keynesianske mainstream (den neoklassiske syntese) og andre mere klassisk orienterede økonomer anvendte. Og disse post keynesianske ryster gentog deres kritik ofte og tit med en vedvarende intensitet, der ikke så ud til at kunne aves, selv når de talte for døve ører. Hvorfor dog gå op i tilsyneladende teoretiske spidsfindigheder, når nu der stort set var en bred tilslutning til, hvordan økonomierne skulle forsøges styret mest hensigtsmæssigt gennem økonomisk politik? Med Richard Nixon så var 1960'erne en tid, hvor "we are all Keynesians now".

Og senere fulgte som bekendt en periode præget af den monetaristiske tankegang. Ofte sættes startskuddet for denne revolte i makroteorien til Milton Friedmans Presidential Address fra december 1967 (jf. eksempelvis Olesen, 2019). Som bekendt kom denne tænkning efterfølgende til at bane vejen frem mod den ny-klassiske teoris indtog, hvor især Robert E. Lucas indtager den ledende rolle. Sammen med den ny-keynesianske tankegang skabte disse to forståelsesrammer basis for den nuværende moderne makroøkonomiske mainstream. Dermed holdt en ny syntese – New Neoclassical Synthesis (NNS) (jf. Goodfriend, 2004) – med sine DSGE-modeller sit indtog på den makroøkonomiske scene, som den hurtigt kom til at dominere.[2]

På det kortere sigt kan moderne økonomier godt være kendetegnet ved trægheder og imperfektioner, som kan fremkalde et inoptimalt makroøkonomisk udfald – hvorfor også en aktiv økonomisk politisk indsats måske kan gøre en positiv forskel – men på længere sigt sejrer markedsmekanismen. Denne er på sigt så effektiv, at økonomien bringes tilbage på sin ligevægtssti, hvor en intertemporal optimal forbrugsplanlægning realiseres; for en kritik af tankegangen kan der henvises til Byrialsen og Olesen (2014). Også derfor var det ved anvendelse af denne tankegang f.eks. nødvendigt at foretage en deregulering af den finansielle sektor, som det faktisk skete i såvel USA som i EU med den hensigt at fremkalde en større mængde likviditet til en lavere pris (rente). Og faktisk var det forbavsende få, som kritiserede denne tænkning for at være ude af trit med virkelighedens kompleksitet. Og endnu færre stillede spørgsmålstegn ved tankegangen metodologi.[3]

Men er teori og metodologi nu uden betydning?

> **korrekt teoretisk forankring og anvendelse af den rigtige metodologi er begge kommet for at blive i økonomi; også selv om nogle måtte have sværere end andre ved at erkende og anerkende dette.**

Nej, selvfølgelig ikke (se f.eks. Olesen 2012, 2010, 2009 og 2007). Med en forkert teori (og metodologi) kan man jo analysere virkelighedens kompleksitet forkert. Og finder man i denne problematiske forhold af en sådan størrelsesorden, at man vælger at gribe ind gennem konkrete økonomisk politiske tiltag, kan man jo komme til at dreje på de forkerte håndtag med uønskede ex post konsekvenser til følge. Så jo; korrekt teoretisk forankring og anvendelse af den rigtige metodologi er begge kommet for at blive i økonomi; også selv om nogle måtte have sværere end andre ved at erkende og anerkende dette.

Og netop også derfor er den post keynesianske sang blevet sunget så længe, som tilfældet er. Gennem tiderne selvfølgeligt mere eller mindre kraftigt alt efter, hvordan de faktiske vilkår nu engang var – både konjunkturmæssigt og hvad angik indholdet i den herskende makroøkonomiske mainstream.

Om netop keynesianismens nuværende status som relevant makroøkonomisk forståelsesramme og bestandigheden i den post keynesianske fastholdenhed og de ovenfor nævnte forhold handler dette essay. I de efterfølgende afsnit vil forskellige aspekter derfor blive taget op til nærmere behandling.

Vejres der morgenluft hos non-mainstream makroøkonomer?

Makroøkonomisk set var tiden før The Great Recession som ovenfor beskrevet i al væsentlighed præget af en mainstream konsensus. TINA-princippet syntes at have været gældende (som Margaret Thatcher ofte udtrykte sig: There Is No Alternative). Men med den globale finansielle krises indtog fra 2008 – se Bork (2019) for en god og kort belysning af den globale finanskrise – der efterfølgende slog over i en egentlig realøkonomisk recession, kom mainstream tankegangen under pres. Hvorfor forudså mainstream slet ikke dette omfattende tilbageslag i den globale økonomi? Hvor var forståelsen af finansielle forholds afgørende betydning for, hvorledes de økonomiske processer forløber i moderne globalt interagerende økonomier? Og hvad var det relevante policy-svar på krisen, når nu der hos mainstream var en så ensidig markant fokusering på udformningen af en optimal pengepolitik, og virkeligheden tilsagde, at "facts of life" var et rentemæssigt zero-bound-scenario?

Flere kritiske ryster – især selvfølgelig, men ikke udelukkende, af en heterodoks observans – råbte op om behovet for forandring. Og også fra mange økonomistuderende kom spørgsmålet: lærer vi om økonomi på den rette måde? Således opstod eksempelvis i UK the "post-crash economics society", hvor de studerende efterlyste mere pluralisme gennem f.eks. en introduktion til alternative tilgange til økonomi, kendskab til økonomis udviklingshistorie og et bedre samspil mellem lærebøgernes teoretiske udsagn og virkelighedens realiteter (jf. Taylor, 2016). Hos nogle non-mainstreamere vejredes endda så megen morgenluft, at de ligefrem anså et egentlig paradigmeskift i makroteori for muligt. Og rigtigt er det da også, at alvorlige økonomiske kriser kan sætte den herskende tænkning under pres (se f.eks. Olesen, 2014). Det ved vi fra den økonomiske teoris udviklingshistorie. Men et egentligt paradigmeskifte som konsekvens af The Great Recession? Næppe. Men forandring – helt sik-

kert. Således har flere toneangivende mainstreamere antydet mulige udviklingsspor – for nu blot at nævne et par klassiske referencer: se Galí (2018) og Christiano o.a. (2018). Hvor meget teoretisk forandring, der faktisk kommer til at blive realiseret, må fremtiden vise.

Økonomisk-politisk synes konklusionen derimod at være den, at der også blandt mainstreamerne har været en ganske betydelig lydhørhed overfor ønskerne om at bruge den økonomisk politik aktivt i den udstrækning, som det måtte være muligt. Dette er læren af, hvad der skete efter udbruddet af The Great Recession i mange lande. Den pengepolitiske indsats blev fornyet gennem indførsel af såkaldte ukonventionelle tiltag (Q.E.-aktiviteter); jf. erfaringerne fra FED og ECB: massiv indsats for at stille en tilstrækkelig likviditet til rådighed for den finansielle sektor og et forsøg gennem opkøb af lange papirer på at presse den lange rente ned. Begge med den primære hensigt at forsøge at stimulere aktiviteten i den private sektor. Og sekundært vel også med den hensigt at gøre livet lidt lettere for flere finansministre, når de skulle ud og finansiere deres voksende offentlige budgetunderskud gennem lånoptagelse. Samtidig blev også finanspolitikken i et vist omfang revitaliseret. I netop et "zero-bound-scenario" syntes denne at virke bedre, end mainstream traditionelt tidligere havde vurderet (jf. Blanchard og Leigh, 2013). Ekspansive tiltag blev derfor gennemført – i nogle lande mere markant end i andre.[4] I bund og grund altså en art konjunkturstabiliserende efterspørgselsrettet økonomisk-politisk strategi med keynesianske kendetegn.

» **Hjælpepakker af en historisk set ukendt størrelser er blevet – og bliver – gennemført i de forskellige lande. Så talrige er disse tiltag, også i Danmark, at næppe nogen længere har styr på dem alle og deres konkrete indhold. Har man nogensinde før i moderne tid set mage til gennemført renlivet keynesianisme?**

Og nu, hvor den globale verden er sendt til tælling på grund af Covid-19-virussen, er strategien endnu klarere. Økonomierne må understøttes aktivt finansielt som også realøkonomisk. Hjælpepakker af en historisk set ukendt størrelser er blevet – og bliver – gennemført i de forskellige lande. Så talrige er disse tiltag, også i Danmark, at næppe nogen længere har styr på dem alle og deres konkrete indhold. Har man nogensinde før i moderne tid set mage til gennemført renlivet keynesianisme?

Udsagnet om vejringen af morgenluft har dermed lige nu en hel del for sig, når udformningen af den praktiske økonomiske politik skal vurderes. I koret af økonomer, som anbefaler en aktiv økonomisk politisk strategi i de nuværende Covid-19-tider, ses nu ikke længere blot heterodokse ryster, men også en ganske udbredt skare af mainstream teoritro væbnere.

Er keynesianismen død?

På denne baggrund kan man spørge sig selv: er keynesianismen død? Svaret herpå er både ja og nej. Det er afhængigt af, dels hvad man definerer som keynesianisme, dels perspektivet: død eller levende i henseende til hvad?

På sin vis har den form for keynesianisme, der tager sit udgangspunkt i den neoklassiske syntese på baggrund af bl.a. Modigliani (1944), været til stede i den makroøkonomiske tænkning lige siden sin fødsel. Fokus på imperfektioner og stive priser på kort sigt, som kunne fremkalde inoptimale makroøkonomiske situationer, der sommetider er af en sådan størrelsesorden, at markedsmekanismens styrke og effektivitet må understøttes af økonomisk-politiske tiltag, har været effektivt til stede i den økonomisk politiske planlægning i de fleste lande siden, det keynesianske paradigme slog igennem efter den 2. Verdenskrig. I gamle dage naturligvis med et fokus på at opnå den størst mulige konjunkturstabilisering, mens der i mere moderne tid har været fokuseret især på en nødvendig strukturtilpasning af de enkelte økonomier (en udbudsorienteret forankret økonomisk politik), men også i nogle situationer som tidligere nævnt ved at holde hånden under niveauet for den aggregerede efterspørgsel i samfundet, når økonomierne virkelig blev slået ud af kurs.

I denne henseende har megen af den praktiske udformning af økonomisk politik i mange lande haft et keynesiansk skær. Nogle gange selvfølgelig med et klarere lys end andre gange. Og i visse situationer havde udformning af den økonomiske politik en helt anden teoretisk forankring. Men alligevel synes det rimeligt at konkludere, at med et økonomisk politisk perspektiv har keynesianismen været til stede ganske længe. I et temanummer fra foråret 2020 i tidsskriftet *Review of Keynesian Economics* beskæftiger flere bidrag sig således med den aktuelle status af den keynesianske teori, og her er den generelle konklusion netop den, at økonomisk politisk set er keynesianismen stadigvæk levende og aktivt til stede i "real life". Og som sådan kom The Great Recession for mange til at virke som et "wake-up-call"; det styrkede klart forståelsen for både det brugbare og det nødvendige i af forfølge en keynesiansk økonomisk politisk strategi (se f.eks. Eichengreen, 2020; Fazzari, 2020 og Rowthorn, 2020).

Makroteoretisk set er svaret mere valent. Siden 2. Verdenskrig var der jo en periode med både monetarisme som ny-klassisk tænkning, som satte den keynesianske teoriforståelse i skammekrogen. Men i moderne tid, hvor den New Neoclassical Synthesis (NNS) har været totalt dominerende, er der sket en tilbagevenden til en tankegang, der igen fokuserer afgørende på imperfektioner og fleksibilitetsproblemer i løn- og prisdannelsen – dette er det klare ny-keynesianske element i NNS (men selvfølgelig på en anderledes og ganske mere raffineret måde end, hvad der kendetegnede den oprindelige neoklassiske syntese). Først på sigt virker markedsmekanismen optimalt. Her bringes økonomierne tilbage på deres optimale ligevægtstrend. Og undervejs kan der selvfølgelig være brug for at justere økonomierne gennem en ændring i den økonomiske politik, hvis denne kan gøre en positiv forskel.

Men for nogle er det ovenstående ikke udtryk for, at keynesianismen er levende. For nogle af disse har keynesianismen været død siden makroteorien med den oprindelige neoklassiske syntese fejlfortolkede og forlod de guidelines, som Keynes med sin *General Theory* gav teoretisk som også metodologisk. Og disse post keynesianske økonomer har lige siden da forfægtet, hvad de mener er den rette fortolkning af Keynes: hans teoridannelse er ikke et specialtilfælde om en økonomi i krise kendetegnet ved infleksibilitet i især løndannelsen; det er en generel teoridannelse, som kan analysere makroøkonomiske udfald med fuld beskæftigelse såvel som situationer med krise og depression som overophede forløb. Man bør derfor skelne mellem "Keynesian economis" og "the economics of Keynes" for nu at henvise til en berømt bogtitel fra 1968 (skrevet af Axel Leijonhufvud).

Er den post keynesianske tænkning marginaliseret?

Hvis post keynesianerne har ret i deres fortolkning af Keynes, hvorfor har disse så ikke haft mere gennemslagskraft på den makroøkonomiske tænkning efter 2. Verdenskrig, end tilfældet har været? Et entydigt svar herpå gives næppe, men nedenfor påpeges en række forhold, som måske giver nogle flige af sandheden.

For det første har der sjældent været megen dialog mellem mainstreamerne og de mere heterodokse økonomer (jf. eksempelvis Olesen, 2012a). Årsagerne hertil er givetvis flere.

Dels fremstår den post keynesianske tænkning ikke så formaliseret og helstøbt på samme vis, som tilfældet er for NNS; det var jo netop Keynes' pointe, at der ikke gives "one model for all seasons".

Dels udtrykker ikke alle post keynesianske makroøkonomer sig altid på matematisk formelsprog, når de fremsætter teoretiske udsagn – ofte er de af indlysende årsager mere kvalitativt formuleret. Tænk blot på forventningernes centrale betydning som styrende element for agenternes adfærd – med en usikker fremtid, ontologisk som epistemologisk, så giver det næppe megen mening at forsøge at formulere disse præcist matematisk; og den rationelle forventningsdannelse har aldrig virket dragende på post keynesianere. Og som bekendt betragter post keynesianere virkeligheden som en foranderlig størrelse. Det økonomiske system er derfor at betragte som et åbent, socialt og sti-afhængigt system indeholdende mange kvalitative aspekter, der netop ikke alle lader sig beskrive præcist korrekt med en matematisk "sprogbrug" (jf. Chick og Dow, 2005). På andre stræk er formelle matematiske modeller klart mere anvendelige (og brugbare), når teoriudsagn skal modelleres og et givet problem analyseres; tænk eksempelvis på post keynesiansk vækstteori. Og empirisk set har mange post keynesianere intet besvær eller problemer med at anvende en økonometrisk belysning – i denne henseende er de meget mainstream-like i deres anvendte approach. Tænk blot på alle de Stock Flow Consistent, SFC, modelarbejder der løbende publiceres.[5]

Dels har mange mainstreamere nok opfattet kritikken fra flere post keynesianere som en forældet kritik rettende sig imod en makroøkonomisk tænkning, der er ældre og anderledes end det, der i dag repræsenteres af den moderne makroøkonomiske mainstream. Kritikken har derfor for dem virket irrelevant. Og rigtigt er det da også, at mainstream har udviklet sig siden de første benchmark DSGE-modeller så dagens lys. Og rigtigt er det også, at nogle af de heterodokse økonomer har haft svært ved at erkende disse forandringstiltag og give mainstream anerkendelse herfor. Og så dog alligevel; det er tvivlsomt, om den makroøkonomiske mainstream fortælling nogensinde kommer til at bortkaste sin klassisk orienterede ligevægtsdragt. For mange non-mainstreamere er det netop dette aspekt, som gør grundlæggende ondt. Med en klassisk teoretisk klædedragt kan visdommen fra det keyneske univers ikke forstås korrekt; jf. eksempelvis fremstillingen hos Jespersen (2009). Eller som Pernecky og Wojick (2019: 769 og 770) udtrykker sig: "Det keyneske paradigme og den generelle ligevægtsteori er fundamentalt set forskellige. At forsøge at inkorporere Keynes' tænkning ind i en generel ligevægtsramme giver blot anledning til misforståelser og fejlfortolkninger … hvorfor få (om overhovedet nogle) af de teoretiske kerneelementer i *General Theory* ikke rigtig har fundet indpas i den moderne makroøkonomiske mainstream" (oversat af forfatter).

For det andet er der måske en ideologisk dimension, som gør sig gældende. Grundlæggende har økonomi at gøre med markedsdirigerede økonomier. Det var netop gennem et sådant institutionelt set up, at økonomis far Adam Smith forudså, at et sådant system kunne levere den ønskede vare: mere velstand til de mange, uden at det sker på nogens bekostning; se eksempelvis (Olesen og Pedersen, 2002: kapitel 3). Og som bekendt er Adam Smith også en af fædrene til liberalismen. Så økonomer, som de er flest, har vel næppe svært ved at få sympati for en sådan politisk tankegang. I moderne tid har der tilsvarende længe blæst neoliberale vinde over mange af de vestlige lande. Og dette har naturligvis også påvirket den økonomiske tænkning, og den måde, hvorpå økonomi som fag doseres på uddannelsesinstitutionerne (se eksempelvis Ngulube, 2018). Og det har også haft konsekvenser for synet på, hvilken form for økonomisk politik det var acceptabelt at føre. I en europæisk kontekst skal den førte austerity-politik således måske også begrundes i en "en konservativ modstand mod 'big government' og dermed kan forsvaret for nødvendigheden af austerity vise sig at være en bekvem undskyldning for at få skåret i de offentlige udgifter og gjort den offentlige sektor mindre" (oversat af forfatter) (jf. Rowthorn, 2020: 7). Og gav keynesianismen ikke netop baggrunden for, at der efter den 2. Verdenskrig kunne opbygges betydelig omfattende velfærdssystemer i mange lande med store offentlige sektorer og en væsentlig beskatning til følge? Så vejrer der ikke et rødt skær over både Keynes[6] og de heterodokse post keynesianske økonomer? Og inden for økonomi er det sjældent sådan, at modsætninger mødes og harmoniske forhold opstår.

For det tredje er megen af den post keynesianske økonomisk-politisk forståelse forankret i en opfattelse af, at den samlede efterspørgsel bør gives en

afgørende betydning. Med en kendt parafrase: hold øje med beskæftigelsen – underforstået den fulde beskæftigelse – så vil mange af de andre potentielle økonomiske problemer forsvinde af sig selv (f.eks. frygten for kraftige offentlige budgetunderskud). Og siden monetarismen og den ny-klassiske forståelse brød igennem i 1970'erne, har megen økonomisk politisk forståelse været centreret omkring udbudsforhold: fokuser på den nødvendige strukturtilpasning, så klarer på sigt markedsmekanismen eventuelle problemer med beskæftigelsen. Et egentligt efterspørgselsfokus er sjældent hverken særligt nødvendigt eller interessant. Et sådant synspunkt ligger dog mere underdrejet efter årene med The Great Recession og den nuværende Covid-19-pandemi. Det er efterhånden gået op for de fleste, at efterspørgselsforhold ikke generelt kan negligeres. I hvert tilfælde ikke på det kortere sigt. Efterspørgslens betydning også på lang advokeres som regel alene af post keynesianske økonomer (se f.eks. Skott, 2016).

Eksempelvis har økonomistuderende herhjemme som også internationalt efterlyst en bredere tilgang til økonomi som fag betragtet. Eller alternativt formuleret: de har efterlyst mere pluralisme

Som belyst i det forrige afsnit, så er det især, hvad angår økonomisk politik, at også mainstream nu udviser en eller anden form for keynesiansk forståelse. Og når netop The Great Recession dokumenterede, at også moderne globalt forankrede økonomier ikke er krisefrie, så burde også heterodokse økonomiteorier have fået en bedre mulighed for at etablere sig. Eksempelvis har økonomistuderende herhjemme som også internationalt efterlyst en bredere tilgang til økonomi som fag betragtet. Eller alternativt formuleret: de har efterlyst mere pluralisme. Så er der håb forude for post keynesianerne? Måske. Det får tiden vise. Nogle udtrykker sig klarere og med færre forbehold. Således fremhæver Guizzo (2020: 119): "Den post keynesianske tradition har pådraget sig en større opmærksomhed de seneste år især efter The Great recession i de akademiske miljøer og fremstår nu som en veldefineret forskningstradition" (oversat af forfatter). Om dette så også indebærer evnen til at få hul igennem til de mere mainstream-like miljøer, er noget ganske andet. Men kan den post keynesianske skole tiltrække unge og moderne uddannede økonomer med en større eller mindre bagage af makroøkonomisk mainstream teoriforståelse, der nu skal sættes i perspektiv, er der nok en bedre mulighed for kommunikation og måske endda en vis form for indflydelse, end hvad "gamle" post keynesianske økonomer har oplevet. De unge har måske ikke så meget fokus rettet mod kritik af mainstream som det væsentligste, men snarere det at fokusere på, hvorledes makroteorien fremadrettet kan udformes mere hensigtsmæssigt (og pluralistisk) afspejlende fænomener fra "real life" på bedre vis, end hvad der har været gældende for den hidtidige mainstream forståelse. Teoretisk indflydelse og gennemslagskraft kan måske bedst opnås ved en "step by step"-strategi – eksempelvis ved at forskellige teoriretninger

på forskellige områder forsøger at komplementere hinanden – snarere end at vente på et egentlig paradigmeskift?

Unge økonomer må først som sidst følge deres overbevisning

Hvorom alting er, så har heterodokse økonomer haft det svært længe. Makroøkonomisk set har disse rejst megen kritik mod mainstream, men egentlig uden den store gennemslagskraft. Lydhørheden hos mainstreamerne og lysten til at deltage i en respektfuld gensidig berigende teoretisk dialog har været begrænset. Om det også vil fortsætte sådan fremadrettet, får tiden vise. Givet er det dog, at den post keynesianske røst ikke forstummer. Selv om et liv som måske marginaliseret økonom kan have sine besværligheder, så vil der forhåbentlig alligevel blive ved med at komme nye unge økonomer til denne tænkning. Hvis ikke uddør skolen selvfølgelig af sig selv med tiden. Lad nogle spørgsmål fra Marc Lavoie til Victoria Chick – begge ledende post keynesianske økonomer – afslutte denne artikel.

I interviewet spørges der (Lavoie, 2020: 7-8): ”Der er et spørgsmål, som vi altid stiller – har du nogle råd til unge økonomer, som finder den post keynesianske tænkning interessant og inspirerende? Jeg ville egentlig hade at være i deres situation; i moderne tid er strukturen indenfor den akademiske verden noget ondskabsfuld – der er kun plads til mainstream-fortællingen; heterodokse alternativer er der ikke rigtig rum til; så de unge, der er tilhængere af en sådan opfattelse, får det svært – det bliver vanskeligt for dem at gøre en videnskabelig karriere indenfor den universitære verden. – Men er der intet positivt at fremhæve? – joh, hvis du virkelig mener, at den post keynesianske måde at forstå økonomi på er den rigtige måde, så kan du selvfølgelig kun gå videre ad dette spor. Hvad ellers skulle du gøre? Jeg var så lykkelig i min tid at komme ind i den akademiske verden, hvor også anderledes opfattelser end den herskende var tilladte – dengang var der også rum for heterodokse alternativer – du er nødt til at følge den retning, som du mener, er den rigtige. Hvad ellers skal du gøre? Det er den eneste måde, som grundlæggende kan give dig ro og gøre dig tilfreds” (oversat af forfatter).

Noter

1. Som sådan bidrog Keynes selv med især to væsentlige bidrag: hans forsøg på en opsamling af debatten efter udgivelsen af *The General Theory* fra 1936 i Keynes (1937) og hans bidrag "How to Pay for the War" fra 1939/40.
2. Således påpegede en af de førende økonomer indenfor tankegangen, (Woodford, 2009: 268 og 274), at: "mens godt nok ikke alle problemer inden for makroteorien er løste, så er der blandt ledende makroøkonomer ikke længere nogen fundamental uenighed om, hvilke spørgsmål man ønsker svar på og ej heller ved hjælp af hvilken teoretisk forståelsesramme og hvilke empiriske metoder man skal forsøge at øge det makroøkonomiske vidensniveau … [og dette sker konkret ved netop at anvende NNS-tankegangen og DSGE-modellerne, idet] … der er i realiteten ingen andre relevante og brugbare alternativer hertil" (oversat af forfatter).
3. I en dansk kontekst har Jesper Jespersen været en af de få, som igen og igen har rejst sin kritiske røst mod den moderne makroøkonomiske mainstream. Eksempelvis ved hans disputats fra 2007, der især fokuserede på metodologiske spørgsmål (jf. Jespersen, 2009).
4. I en EU-sammenhæng blev der dog også forfulgt en "austerity"-strategi. Med denne forarmelsens politik – selv ikke så skarpe 1. semester-studerende i økonomi kan forklare, hvorfor sådanne indgreb gennem også effekten fra de automatiske stabilisatorer ikke får et aktuelt offentligt budgetproblem til at forsvinde, men tværtimod har en indbygget tendens til at forværre budgetproblemerne i de kommende år – blev det lavkonjunkturelle forløb i EU forlænget i et unødigt omfang.
5. I en dansk sammenhæng kan der eksempelvis henvises til det modelarbejde, der foretages på Aalborg Universitet af makrogruppen. Der er således udarbejdet en empirisk "state of the art"-model for dansk økonomi (jf. Byrialsen og Raza, 2019), der danner basis for flere analyser af forskellige makro tiltag.
6. Om end f.eks. (Fuller, 2019) forsøger at argumentere for den opfattelse, at Keynes faktisk var socialist, så er det helt dominerende synspunkt i Keynes-forskningen i overensstemmelse med Robert Skidelskys fortolkning, når han ofte har påpeget, at Keynes i sin grundholdning var liberal igennem hele sit liv.

Litteratur

Blanchard, Olivier og Leigh, Daniel (2013), "Growth Forecast Errors and Fiscal Multipliers", *IMF Working Paper – WP/13/1*, International Monetary Fund 2013.

Bork, Lasse (2019), "Et tilbageblik på den globale finanskrise et årti senere" i Finn Olesen og Mogens Ove Madsen, red., *Mod strømmen – en stridsmand fylder 70 – et festskrift til Jespersen*, Aalborg: Aalborg Universitetsforlag, pp. 65-81.

Byrialsen, Mikael Randrup og Finn Olesen (2014), "DSGE: den makroøkonomiske baseline model – en introduktion og en kritik", *Ekonomiska Samfundets Tidskrift*, 2: 74-89.

Byrialsen, Mikael Randrup og Raza, Hamid (2019), "An empirical stock-flow consistent macroeconomic model for Denmark", *Annandale-on-Hudson, NY: Levy Economics Institute of Bard College*, Working Paper Collection No. 942.

Chick, Victoria og Sheila Dow (2005), "The meaning of open systems", *Journal of Economic Methodology*, 12(3): 363-81.

Christiano, Lawrence o.a. (2018), "On DSGE Models", *Journal of Economic Perspectives*, 32(3): 113-40.

Eichengreen, Barry (2020), "Keynesian economics: can it return if it never died?", *Review of Keynesian Economics*, 8(1): 23-35.

Fazzari, Steven (2020), "Was Keynesian economics ever dead? Is so, has it been resurrected?", *Review of Keynesian Economics*, 8(1): 46-60.

Fuller, Edward (2019), "Was Keynes a socialist?", *Cambridge Journal of Economics*, 43(6): 1653-82.

Galí, Jordi (2018), "The State of New Keynesian Economics: A Partial Assessment", *Journal of Economic Perspectives*, 32(3): 87-112.

Goodfriend, Marvin (2004), "Monetary Policy in the New Neoclassical Synthesis: A Primer", *Federal Reserve Bank of Richmond Economic Quarterly*, Summer: 21-45.

Guizzo, Danielle (2020), "Why does the history of economic thought neglect Post-Keynesian economics?", *Review of Keynesian Economics*, 8(1): 119-37.

Jespersen, Jesper (2009), *Macroeconomic Methodology: A Post-Keynesian Perspective*, Edward Elgar.

Keynes, John Maynard (1936), *The General Theory of Employment, Interest and Money*, The Collected Writings of John Maynard Keynes Vol. VII, The Macmillan Press 1973.

Keynes, John Maynard (1937), "The General Theory of Employment", her fra *The Collected Writings of John Maynard Keynes, Vol. XIV*, Macmillan, Cambridge University Press 1973: 109-23.

Keynes, John Maynard (1940), "How to Pay for the War", *The Collected Writings of John Maynard Keynes Vol. IX*, Macmillan & St. Martin's Press 1972: 367-439.

Lavoie, Marc (2020), "'If you are convinced that post-Keynesian economics is a good way of thinking, get on with it' – Interview with Victoria Chick", *Euro-*

pean Journal of Economics and Economic Policies: Intervention, 17(1): 1-8.

Modigliani, Franco (1944), "Liquidity Preference and the Theory of Interest and Money", *Econometrica*, January: 45-88.

Olesen, Finn (2007), "Kritisk realisme og post keynesianisme – et alternativ til mainstream", *Ekonomiska Samfundets Tidskrift*, 3: 129-38.

Olesen, Finn (2008), "Keynes' metodologi og makroøkonomisk forskning – et bud på en belysning", Økonomi & Politik, 81(1): 46-65.

Olesen, Finn (2009), "Idealiseret økonomisk adfærd – nogle metodologiske refleksioner, *Tidsskrift for Samfunnsforskning*, 3: 349-66.

Olesen, Finn (2010), "Uncertainty, bounded rationality and post-Keynesian Macroeconomics", *European Journal of Economics and Economic Policies – Intervention*, 7(1): 109-24.

Olesen, Finn (2012), "Makroøkonomisk tænkning og kravet om realisme", *Ekonomiska Samfundets Tidskrift*, 3: 143-56.

Olesen, Finn (2012a), "Om den gode videnskabelige dialog – en kommentar", *Erhvervshistorisk Årbog*, 1: 1-8.

Olesen, Finn (2014), "Sætter kriser mainstream tænkningen under pres?", *Erhvervshistorisk Årbog*, 1: 1-9.

Olesen, Finn (2019), "Milton Friedman om pengepolitik – En skelsættende Presidential Address fra 1967", *Erhvervshistorisk Årbog*, 1: 1-12.

Olesen, Finn og Kurt Pedersen (2002), *Den økonomiske teoris rødder – fra Aristoteles til Lucas*, Systime Academic.

Pernecky, Mark og Paul Wojick (2019), "The problematic nature and consequences of the effort to force Keynes into the conceptual cul-de-sac of Walrasian economics", *Cambridge Journal of Economics*, 43(3): 769-84.

Rowthorn, Robert (2020), "The Godley-Tobin Lecture: Keynesian economics – back from the dead?", *Review of Keynesian Economics*, 8(1): 1-20.

Skott, Peter (2016), "Public debt, secular stagnation and functional finance" i Mogens Ove Madsen og Finn Olesen, red., *Macroeconomics After the Financial Crisis – A Post-Keynesian perspective*, London: Routledge, pp. 20-37.

Taylor, Gareth (2015), "Economics: A subject in crisis?", *Teaching Business & Economics*, 19(1): 15-8.

Woodford, Michael (2009), "Convergence in Macroeconomics: Elements of the New Synthesis", *American Economics Journal: Macroeconomics*, 1(1): 267-79.

Håndteringen af coronakrisen – offentlig-privat interaktion som løsningsmodel

Temanummer: Cybersikkerhed

Den første kritiske fase af coronakrisen handlede i høj grad om at ruste sundhedsvæsenet til at håndtere sygdommen. Det krævede store mængder medicinsk udstyr, herunder masker, visirer, tests, respiratorer og andet kritisk udstyr. Disse typer udstyr leveres af den private sektor og indkøbes primært af den offentlige sektor. Under coronakrisen blev der brudt med denne opdeling. I stedet blev interaktionen i langt højere grad præget af et løbende samarbejde, som i høj grad kan forstås med klassisk rationalistisk teori. Her viste fleksible samarbejdsformer sig at komme hurtigt i gang, så industrien og den offentlige sektor løbende kunne udvikle løsninger. Med det udgangspunkt kan der udledes en række spørgsmål til, hvordan den fremtidige organisering af indsatsen kan organiseres, samt hvordan den offentlige sektors indblanding i markedet i forbindelse med coronakrisen kan påvirke innovationen i den private industri på længere sigt.

MINA ERBAS
Konsulent, KPMG,
Studerende ved
Institut for Statskundskab,
Københavns Universitet,
mina_erbas@hotmail.com

EMIL LOBE WELLINGTON SUENSON
Politisk chef,
Medicoindustrien,
Ekstern lektor ved
Institut for Statskundskab,
Københavns Universitet,
lobe_suenson@hotmail.com

Omdrejningspunktet for denne artikel er, hvordan Danmark håndterede forsyningssituationen af værnemidler, tests og andet kritisk medicinsk udstyr til coronahåndtering under coronakrisen, og hvordan den offentlige sektors indblanding i markedet under krisen kan have påvirket innovationen i life science-industrien på længere sigt. For at belyse emnet vil der blive trukket på tre klassiske teorier om interaktion mellem aktører, hvor aktørcentreret spilteori, selvstyrende institutioner og credible commitment (troværdige forpligtelser) vil blive præsenteret. Herefter benyttes teorierne til at analysere, hvordan den danske offentlige sektor og industrien samarbejdede under krisen.

Grundlæggende kan forløbet beskrives således: Tidligt i coronakrisen afgiver staten et credible commitment med et lovindgreb vedrørende bl.a. priser på medicinsk udstyr. Dette indgreb ændrer ligevægten i spillet mellem den offentlige sektor (køberen) og den private sektor (sælgeren), så sektorerne begynder at samarbejde. Samarbejdet kan i første omgang forstås som en selvstyrende institution, men ændrer senere form, da regeringen tager initiativ til at oprette en ny styrelse, som bl.a. skal håndtere indkøb af medicinsk udstyr til håndtering af corona og lignende situationer i fremtiden. Med dette afsæt diskuteres konsekvenserne af den offentlige sektors indblanding i markedet ift., hvordan innovationen i industrien påvirkes på længere sigt. Vi finder, at det kan have skabt et stærkere samarbejde mellem det offentlige og private – hvilket særligt kan have betydning for innovationen. Dog kan man argumentere for, at statslige indgreb i markedet kan give usikkerhed om fremtidigt afkast og kan mindske investeringslysten samt tilliden mellem sektorerne, hvilket kan føre til mindre innovation.

Interaktion mellem aktører – det rationalistiske teoretiske udgangspunkt

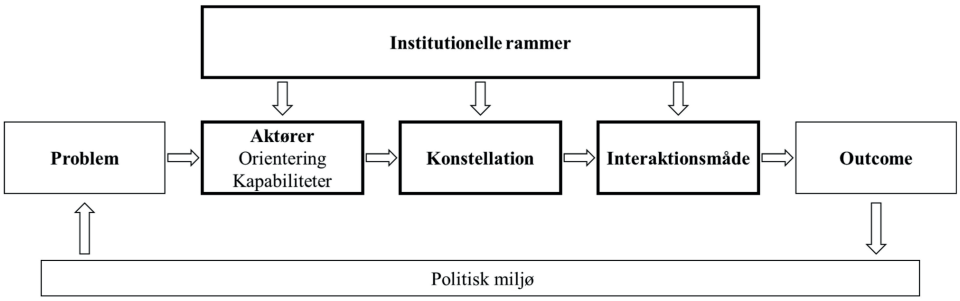
For at kunne betragte interaktionen mellem den offentlige og den private sektor, vil der i dette afsnit blive trukket på tre klassiske værker af de rationalistiske teoretikere Fritz Scharpf (1997), Elinor Ostrom (1990) og Douglas North (1993). De beskæftiger sig med henholdsvis aktørcentreret spilteori, selvstyrende institutioner og credible commitment, som på forskellige måder beskriver interaktion mellem aktører. Alle teorierne har et rationalistisk udgangspunkt, hvor aktørerne forstås som egennyttemaksimerende aktører, der påvirkes af de institutionelle rammer, som de befinder sig i.

Spillet mellem aktørerne

Institutionelle rammer forstås som det system af regler, der er med til at styre aktørernes handlinger, hvilket både kan være formelle regler, såsom lovgivning, og uformelle regler, som kultur og sociale normer (Scharpf, 1997: 38).

Figur 1 illustrerer, hvordan et spil overordnet set kan se ud iflg. Scharpf (1997). Frameworket kaldes aktørcentreret institutionalisme og består af aktører, deres konstellation og interaktionsmåde, som påvirkes af de institutionelle rammer, hvilket påvirker resultatet i et spil. Aktørerne har specifikke kapabiliteter og orienteringer, hvilket fx kan være deres forudsætninger/evner til at udføre en opgave. Interaktionsmåden kan være samarbejdende eller ikke-samarbejdende, og der skelnes mellem simultane og sekventielle spil og mellem plus-, nul- og variable-sums-spil (Scharpf, 1997: 43-5 og 73). Interaktionsmåden vil have betydning for aktørernes præferencer. Spillet kan opstilles i en matrix, hvor aktørernes præferencer kan rangordnes, og spillerne kan på den baggrund vælge at defekte (optimere eget udfald på bekostning af den anden) eller samarbejde (Scharpf, 1997: 73). Spillene mellem aktørkonstellationer kan bindes sammen med narrativer, hvilket kan være nødvendigt, da aktørerne i et spil i virkeligheden kan bestå af mere komplekse konstellationer og beslutningsniveauer, hvor der kan være tale om flere spil på forskellige niveauer – ofte kaldet two-level games (Scharpf, 1997: 30). I en række situationer kan der opstå kollektive handlingsproblemer, som ofte eksemplificeres med det klassiske prisoners dilemma (PD)-spil, hvor begge aktører defekter og dermed opnås et suboptimalt resultat.

Figur 1: Aktør-centreret institutionalisme



Note: Scharpf (1997: 44).

Selvstyrende institutioner

Ostrom (1990) fokuserer på, hvordan man kan løse kollektive handlingsproblemer med udgangspunkt i »common pool resources« (CPR), som er en fælles mængde ressourcer. De inddeles i ressourcesystemet (beholdningen) og ressourceenheder (forbruget) (Ostrom, 1990: 30-1), og der skelnes mellem open- og limited-access CPR's (Ostrom, 1990: 23). Når et CPR findes i begrænsede mængder, kan »Tragedy of the Commons« opstå, fordi aktører handler som i PD-spillet (Ostrom, 1990: 3-5). Ostrom foreslår derfor, at problemet kan løses ved at ændre de institutionelle rammer og aktørernes kapabiliteter, hvilket kan ske gennem selvstyrende institutioner, som styres og finansieres af aktørerne selv (Ostrom, 1990: 15-6). Det sænker omkostninger for staten, giver medbestemmelse til aktørerne og sikrer bedre information, fordi aktørerne selv er inkluderet i reguleringen og monitoreringen (Ostrom, 1990: 17 og 27). Løsningen er et alternativ til ren centralisering eller privatisering. Det private marked og/eller staten kan tage rollen som koordinator i samarbejdet, men håndteringen varetages af aktørerne selv. Fordelen ved at inkludere staten i et givet omfang kan være, at staten lettere kan afgive et credible commitment, som kan få aktørerne til at overholde reglerne (Ostrom, 1990: 40-1). Tillid, forudsigelighed og information er afgørende for samarbejdet, da det kan gøre aktørerne villige til at samarbejde, fordi de føler sig sikre på fremtidige afkast. Over tid kan samarbejdet danne normer og føre til en fælles forståelse af, hvordan aktørerne interagerer med hinanden (Ostrom, 1990: 25-6 og 35-6).

Credible commitment

North (1993) beskæftiger sig med problematikken med manglende credible commitment, der kan føre til suboptimale resultater (North, 1993: 6-7). Et commitment kan fx særligt forstås som credible, hvis aktørers handlemuligheder begrænses ved lov. Dermed ændres den institutionelle ramme om samarbejdet, og aftalen vil være mere troværdig (North, 1993: 8-9). Et eksempel er den private ejendomsret, som er statens credible commitment for, at den ikke eksproprierer befolkningens ejendom. Dette stimulerer økonomisk udvikling, da det giver aktørerne incitament til at investere i deres ejendom og dermed opnå fremtidige afkast (North, 1993: 8).

Håndteringen af forsyningerne af medicinsk udstyr under coronakrisen

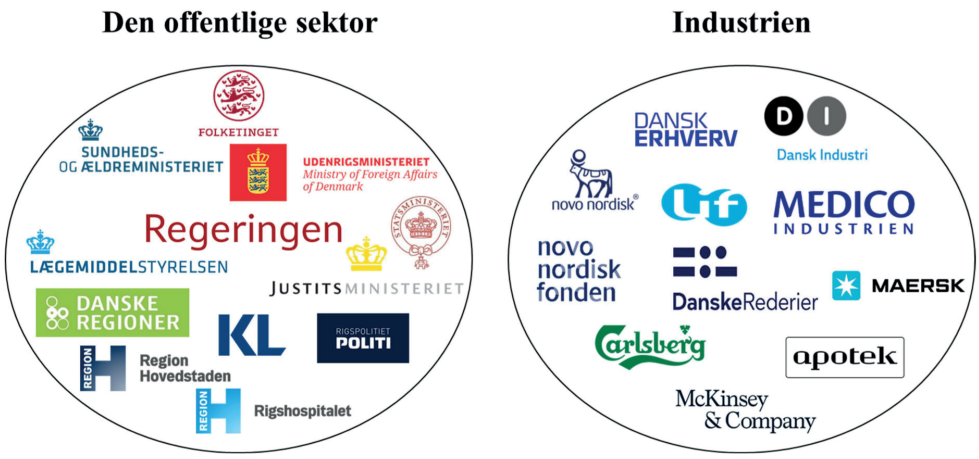
Med udgangspunkt i teorierne om interaktion mellem aktørerne vil der i dette afsnit være fokus på at forstå, hvordan man i Danmark har håndteret forsyningssituationen af kritisk medicinsk udstyr i coronakrisens akutte fase.

Modspil – rammerne for spillet ridses hårdt op

Coronakrisen medførte at der kom et stort pres på sundhedsvæsnet, som dermed skulle bruge flere ressourcer til håndteringen af krisen (Lægemiddelstyrelsen, 2020). Kritisk medicinsk udstyr blev med Ostroms begreber en limi-

ted-access ressource, hvor den offentlige sektor i et vist omfang kunne styre forbruget, men ikke styre beholdningen, der produceres og sælges af en række private aktører, som vi i artiklen vil referere til som "industrien". Den offentlige sektor og industrien kan her forstås som alle de involverede offentlige og private aktører. Hovedaktørerne i forbindelse med corona-håndteringen er skitseret i figur 2. Her ses det, at både den offentlige sektor og industrien består af en række forskellige aktører. Den offentlige sektor består her af de statslige myndigheder, regionerne og kommunerne. Industrien består bl.a. af nogle af de største medico-, pharma-, produktions- og fragtvirksomheder samt organisationer, som repræsenterer de forskellige områder i industrien. Derudover har der under coronakrisen været en lang række nye aktører, som har forsøgt at udnytte situationen ved at producere og sælge fx tests, mundmind og masker af en tvivlsom kvalitet til meget høje priser – et problem, som har været globalt (Lægemiddelstyrelsen, 2020b; Haahr Lund 2020). Disse aktører er meget forskellige fra den traditionelle industri, som udvikler, producerer og sælger medicinsk udstyr i Danmark. Dog vil industrien i den følgende analyse blive behandlet som en samlet aktør, da analysen omhandler markedsvilkårene for alle private leverandører.

Figur 2: Aktørkonstellation – den offentlige sektor og industrien som aktører



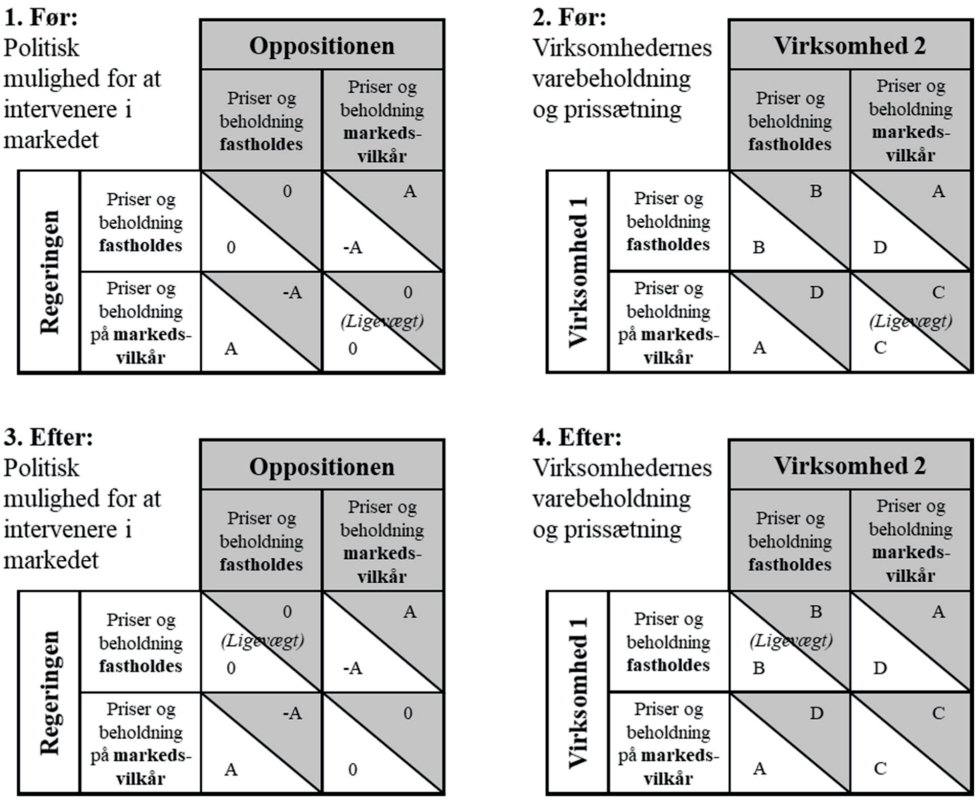
Håndteringen af krisen i forhold til forsyningen af kritisk medicinsk udstyr kan beskrives som to sammenhængende PD-spil, hvor alle aktører forsøger at handle rationelt givet de institutionelle rammer. Virksomheder kan normalt justere deres udbud og deres priser efter efterspørgslen på markedet, og politikere vil normalt ikke blande sig i markedsvilkårene og prisdannelsen. Denne normale situation kunne dog have medført voldsomme prisstigninger og mangel på medicinsk udstyr under coronakrisen, da der som nævnt ovenfor var en række nye aktører udenfor den traditionelle medicoindustri, som forsøgte at udnytte situationen ved bl.a. at tage meget høje priser. Det skyldes, at efterspørgslen steg voldsomt uden at udbuddet af medicinsk udstyr kunne øges i samme tempo. Derfor vedtog man politisk at give nye muligheder ift. at påvirke bl.a. priserne på markedet. Spillene illustreres med trin 1-4 i figur 3 nedenfor.

Figuren er inspireret af Suenson et al. (2016), som beskriver, hvordan vedtagelsen af budgetloven i 2012, der bl.a. skulle sikre overholdelsen af de kommunale og regionale budgetter, blev muliggjort af finanskrisen. Krisen ændrede holdningen i befolkningen og i Folketinget, hvilket gjorde det muligt for de politiske aktører at vedtage loven (Suenson et al., 2016: 10). Dette forklares med et nul-sums-spil om pladserne i Folketinget, hvor de politiske aktører før finanskrisen kunne risikere at miste deres mandater i Folketinget og derfor ikke valgte at samarbejde om at begrænse kommunernes og regionernes økonomi. Krisen førte til et præferenceskift i befolkningen, der brød den sædvanlige konkurrence mellem regeringen og oppositionen og i stedet muliggjorde samarbejde (Suenson et al., 2016: 9 og 12). Dette præferenceskift kan også ses i de første faser af coronakrisen, hvor oppositionen samarbejdede med regeringen og dermed uden tøven gav regeringen en række meget vidtgående beføjelser ift. coronahåndtering (Jensen, 2020).

Da den stigende efterspørgsel på medicinsk udstyr betød, at der flere steder i sundhedssektoren manglede nødvendigt udstyr (Lægemiddelstyrelsen, 2020a), valgte regeringen at udnytte den nye forhandlingsposition, hvor der kunne findes opbakning i Folketinget, og pålagde gennem Lægemiddelstyrelsen, at regioner, kommuner og private virksomheder med medicinsk udstyr skulle indsende oplysninger om lagerbeholdning og opbygge lagre. For de private aktører gjaldt det videre, at Lægemiddelstyrelsen kunne kontrollere salget og priserne på produkterne (Retsinformation, 2020). Dermed har et enigt folketing givet Lægemiddelstyrelsen mulighed for at gribe direkte ind i markedet. Herved får regeringen demonstreret et credible commitment – og givet et utvetydigt signal. Man vil ikke fra det offentliges side acceptere store prisstigninger, hvilket giver industrien en ny institutionel ramme. Nu er der endnu større incitament til at samarbejde med det offentlige, for at sikre at virksomhederne fortsat har mulighed for at styre deres egne priser igennem krisen – dette var naturligvis særligt relevant ift. de aktører, som ifølge Lægemiddelstyrelsen forsøgte at slå plat på situationen (Lægemiddelstyrelsen, 2020b).

Regeringen og oppositionen vælger at samarbejde om hastelovgivningen, som bl.a. giver mulighed for at intervenere direkte i markedet. Hastelovgivningen medfører, at industrien naturligt foretrækker at samarbejde om coronahåndteringen for bl.a. at bevare muligheden for selv at prissætte og styre varebeholdningen. Lovindgrebet betyder altså, i tråd med Scharpf (1997), Ostrom (1990) og North (1993), at når spillets institutionelle rammer ændres for industrien, så skifter aktørernes adfærd, hvilket fører til en ny ligevægt. Figur 3 viser spillet mellem aktørkonstellationer i den offentlige sektor og i industrien, hvor det ses, at ligevægten efter corona skifter i konstellationerne, hvilket gør statens lovindgreb muligt og giver industrien incitament til at samarbejde. Det er samtidig et eksempel på, hvordan der foregår spil på forskellige niveauer, som har betydning for andre spil.

Figur 3: Ligevægten før og efter corona



Note: Egen illustration inspireret af Scharpf (1997: 75) og Suenson et al. (2016: 8).

Samspil – stærkere sammen end hver for sig

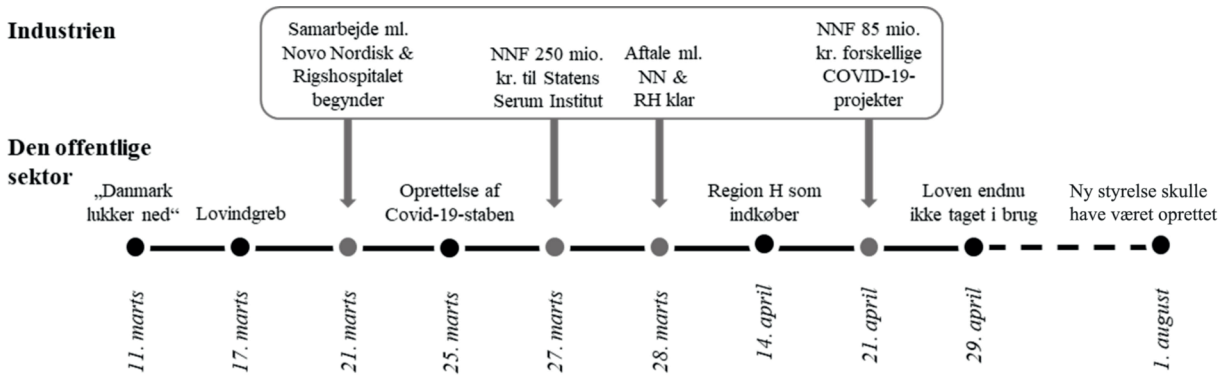
Efter vedtagelsen af hastelovgivningen viser forløbet, hvordan aktørerne foretrækker at samarbejde. En lang række private og offentlige aktører begynder at etablere hidtil usete samarbejdskonstruktioner. Der oprettes en særlig Covid-19-stab, som både består af staten og industrien under Den Nationale Operative Stab (NOST), Novo Nordisk og Rigshospitalet udvikler et tæt samarbejde om at udvidelse af testkapaciteten, og Novo Nordisk Fonden (NNF) bevilliger store beløb til Statens Serum Institut og til forskellige Covid-19-projekter (Region H, 2020a; Kjær og Kjeldtoft, 2020; NNF, 2020). Lars Rebien Sørensen, bestyrelsesformand i NNF, udtaler i den forbindelse, at samarbejdet er med til at forbedre deres evne til at tackle lignende udfordringer i fremtiden (NNF, 2020). Udtalelsen indikerer, at lovindgrebet har ført til samarbejde mellem aktørerne i Covid-19-staben, der fungerer som en selvstyrende institution (jf. Ostrom), hvor de involverede parter selv tager ansvar og står for organisering og monitorering, hvilket kan have den fordel at gøre processen mere effektiv. Erhvervsministeren, Simon Kollerup, fremhæver også industriens afgørende rolle under coronakrisen og udtaler i juli 2020, at da »coronapandemien var på sit højeste, var [industrien] med til at sikre, at hospitaler og apoteker havde adgang til livsvigtig medicin og medicinsk udstyr« (Kollerup, 2020). Videre fremhæves det, at indsatsen understreger en dansk tradition for at finde fælles løsninger på fælles problemer (Ibid.). I skrivende stund er lovindgrebet ikke taget i brug (Folketinget, Sundheds- og Ældreudvalg, 2020). Det kan skyldes,

at samarbejdet har fungeret, og at det derfor ikke har været nødvendigt, eller fordi vedtagelsen primært var et strategisk træk for at give industrien incitament til at samarbejde.

I den forbindelse er det interessant, at man fra offentlig side har brugt mere almindelige metoder til at holde priserne nede. Eksempelvis fik Region Hovedstaden ansvaret for det samlede danske indkøb af værnemidler på verdensmarkedet (Region H, 2020b). Stigende centralisering af indkøb var allerede en tendens i Europa før coronakrisen (Crea et al., 2019: 576 og 595). Coronakrisen har altså ikke – i hvert fald endnu ikke – ført til større ændringer af indkøbspraksissen i Danmark.

Regeringen har planlagt at oprette en ny styrelse til at håndtere denne og lignende situationer i fremtiden ved bl.a. at skulle stå for indkøb af udstyr (Regeringen, 2020). Det oplyses, at styrelsen skal videreudvikle og opruste arbejdet, der er foregået i NOST. Der kan med udgangspunkt i Ostroms tanker om selvstyrende institutioners effektivitet være en frygt for, at det vil være en mindre effektiv måde at organisere samarbejdet på, hvis det formaliseres som en selvstændig offentlig myndighed, hvor industriens aktører kan være mere afskåret fra at bidrage til processen. Figur 4 illustrerer forløbet og viser, hvordan samarbejdet er forløbet med sekventielle valg mellem aktørerne.

Figur 4: Samarbejdet mellem den offentlige sektor og industrien ved sekventielle valg



Note: Egen illustration baseret på offentligt tilgængeligt materiale (se litteraturliste for kildehenvisninger).

Det kan bestemt ikke udelukkes, at særligt den etablerede industri på eget initiativ af pragmatiske grunde valgte at samarbejde, da nogle problemer kan anses for at være så store, at de kun kan løses af flere store aktører samtidig (Greve, 2019: 20). Det kan derfor sagtens være, at industrien – i hvert fald den etablerede medico- og medicinalindustri – med eller uden lovindgrebet havde valgt at indgå i samarbejdet med den offentlige sektor. Uden lovindgrebet kan staten i lignende fremtidige situationer muligvis opnå samme samarbejdende tilgang fra industriens side uden først at skulle afgive et credible commitment om at ville intervenere i markedet ved behov. Dette skyldes, at virksomhederne – og i særdeleshed de aktører, som forsøgte at udnytte situationen – har

prøvet det før og derfor ved, hvad de kan forvente, hvorfor de institutionelle rammer kan være sat på forhånd. Det kan både forstås ud fra Ostroms fokus på normer og tillidsopbygning over tid, men også med fx Robert Axelrods arbejde om gentagne spil. Axelrod (1990) viser, hvordan aktører i PD-situationer vil samarbejde over tid, særligt når de ved, hvad de kan forvente af de andre aktører hvilket også gælder for rationelle egennyttemaksimerende aktører, som private virksomheder (Axelrod, 1990: 24). Ulempen ved statens lovindgreb kan dog være, at det kan forstås som en ikke-samarbejdende strategi i første omgang, hvilket kan have skabt mistillid mellem aktørerne.

Ovenstående gennemgang af forløbet viser, at statens lovindgreb kan have fået ligevægten til at skifte og aktørerne til at samarbejde, ved at regeringen og oppositionen tidligt i forløbet etablerer en forpligtelse ift. industriens prissætning og forsyning. Yderligere viser analysen, at samarbejdet til at starte med ligner en selvstyrende institution, som kan være effektiv, men senere ændres til at skulle være en ny statslig styrelse, som potentielt kan være mindre effektiv og fleksibel end en selvstyrende institutionel ramme.

Betydningen af den offentlige sektors indblanding for innovationen

I forbindelse med coronakrisen er der lavet betydelige ændringer i indretningen af sundhedsvæsenet, og der er afsat betydelige ressourcer til sundhedsvidenskabelig forskning. Derudover har den offentlige sektor interveneret i markedet på en række områder. Derfor kan det være relevant at belyse, hvordan den offentlige sektors håndtering af coronakrisen kan påvirke innovationen i life science-industrien – på kort og på lang sigt.

Traditionelt betragtes styringen af de offentlige velfærdsområder og rammevilkårene for erhvervslivet som to adskilte politiske og forvaltningsmæssige discipliner. På sundhedsområdet er de private og offentlige aktører dog meget afhængige af hinanden, hvilket har væsentlige konsekvenser for, hvordan styringen af området tilrettelægges. Danmark har et næsten udelukkende offentligt finansieret sundhedsvæsen, hvor alene forbrugsudgifterne hertil udgør over 160 mia. kr. årligt. Den danske industri inden for udvikling og salg af lægemidler og medicinsk udstyr (life science-industrien) er blandt de største erhvervsområder i Danmark og omsætter for ca. 210 mia. kr. om året (Damvad Analytics, 2018). De private virksomheder trækker på forskning udført på offentlige universiteter, der laves offentlige-private innovationspartnerskaber (OPI'er) på offentlige hospitaler, og den offentlige sektor er den primære aftager af industriens produkter (Regeringens vækstteam for life science, 2017: 51-4). Omfanget og karakteren af de offentlige indkøb har derfor stor betydning for produktudviklingen, og innovationen i industrien og indretningen af den offentlige sektor er afgørende for virksomhedernes udviklingsmuligheder.

På langt sigt – potentiale for innovation pga. store investeringer på sundhedsområdet

Da en stor del af forskningen på sundhedsområdet foregår på tværs af det offentlige og private, kan en fordel ved det udvidede samarbejde under coronakrisen være, at de offentlige og private aktører har kunnet udvikle deres kendskab og tillid til hinanden, hvilket kan have stor betydning for udviklingen af OPI'er (Vallgårda og Krasnik, 2016: 185; Brogaard, 2015: 553). En udfordring, der ofte ses ved offentligt-privat-samarbejde, er, at der kan være for langt mellem dem, der udvikler innovative løsninger, og dem, der skal anvende løsningerne i praksis (Omachonu og Einspruch, 2010: 11). Det tættere samarbejde under corona kan have ført til en bedre forståelse af hinandens processer og dermed en bedre forståelse af barrierer for produktimplementering. Mazzucato (2015), der særligt stiller sig kritisk over for industriens udnyttelse af offentlig forskning til kommercielle hensyn, fremhæver, at økonomisk udvikling og innovation i industrien skabes af samarbejde, netværk og vidensdeling mellem aktørerne pga. feedback-mekanismer (Mazzucato, 2015: 43). Det større samarbejde kan have givet dem et bedre netværk på tværs af sektorerne og lettet adgangen for vidensdeling. Samlet set kan det vise sig, at det større samarbejde under corona kan have ført til et stærkere fremtidigt samarbejde med mere tillid mellem aktørerne, en bedre forståelse af hinandens processer, bedre netværk og vidensdeling – alle elementer, som er vigtige for OPI'er og dermed innovationen i fremtiden.

Life science-industrien indeholder to hovedgrene: 1) medico (medicinsk udstyr) og 2) pharma (lægemidler), hvor særligt udbud og efterspørgsel af medicinsk udstyr har været påvirket under corona. Indkøb af medicinsk udstyr sker som udgangspunkt via offentlige udbud, hvorved prissætningen er underlagt fri konkurrence mellem leverandører (Regeringens vækstteam for life science, 2017: 54). På det private marked ville større efterspørgsel derfor normalt kunne føre til mere innovation, da der ville allokeres mere kapital til de efterspurgte områder. Statens indblanding, i hvert fald som set i Danmark, har betydet, at prisniveauet kunne kontrolleres ved lov. Derfor kan det forventes, at industrien ikke har sat priserne markant op, og at de økonomiske gevinster ved større efterspørgsel derfor ikke er fuldt udnyttet. Sammenlignet med en situation uden statslig indblanding kan det betyde, at færre midler end under normale vilkår allokeres, hvilket kan føre til mindre innovation end ellers.

Den offentlige sektors særlige fokus på et område fører typisk til, at flere midler tilføres (Vallgårda og Krasnik, 2016: 171). For både de offentlige og private investeringer gælder det, at det større fokus vil betyde, at investeringer og forskning skubbes i den retning, og dermed at kommende innovationer i industrien kan forventes at udspringe af sundhedsindustrien. North (1993) eksemplificerer dette: Hvis det største afkast i en økonomi kommer fra pirateri, så kan det forventes, at organisationer vil investere i færdigheder, der vil gøre dem til bedre pirater (egen oversættelse, North, 1993: 14). Innovationer inden for informationsteknologi er et område med stort potentiale for innovationer, hvor bl.a. løsninger der anvender tracking devices tidligere er fremhævet

(Omachonu og Einspruch, 2010: 5-7). Et corona-relateret eksempel på dette er, at potentialet kombineret med efterspørgslen førte til, at flere forskellige smittesporingsløsninger blev udviklet af forskellige udbydere (Lund, 2020). Selvom der på nuværende tidspunkt ses forskellige udfordringer med de første smittesporingsløsninger, kan coronakrisen muligvis blive katalysatoren på dette område.

Innovation i sundhedssektoren bygger på godt samarbejde mellem aktørerne, og godt samarbejde bygger i høj grad på tillid mellem dem. Det potentielle statslige indgreb i ejendomsretten og prisdannelsen kan give usikkerhed om fremtidige afkast i industrien og kan mindske investeringslysten. Som fremhævet af North så har politikere tidligere fralagt sig muligheden for at gribe ind i den private ejendomsret for at få større økonomisk vækst til gengæld. Det betyder, at det risikeres, at der vil blive investeret mindre, og udbuddet vil falde, hvis det frygtes, at den offentlige sektor vil inddrage produktionen (North, 1993: 7), hvilket derfor kan betyde mindre innovation i industrien, fordi det sænker investeringslysten, når fremtidigt afkast er usikkert. Omvendt fremhæves det af Mazzucato (2015), at den vigtigste form for innovation er grundforskning, som i overvejende grad er drevet af den offentlige sektor. Det skyldes, at afkast på investeringerne kan ligge meget langt ude i fremtiden og være meget usikre (Mazzucato, 2015).

På kort sigt – behov for et effektivt governance set-up til håndteringen

På kort sigt vil der være behov for flere forskellige former for innovationer – herunder bl.a. institutionel innovation til at håndtere en eventuel anden bølge i efteråret og vinteren 2020/2021. Her vil der være behov for at lave et effektivt set-up, som ikke er for tungt. Stiafhængighed vil i den forbindelse være relevant at være opmærksom på. Stiafhængighed beskrives både af North, Scharpf og Ostrom, men begrebet beskrives mest udførligt af Pierson (2004), der blander rational choice-teorien med historisk institutionalisme (Pierson, 2004: 8). Stiafhængighed beskrives her som sociale processer, der udviser positiv feedback og dermed genererer forgreningsmønstre i den historiske udvikling (Pierson, 2004: 21). Historien, der ligger før aktørernes handlinger, har stor betydning for de valg, der senere tages og kan tages, hvilket forklares med institutionernes træghed (stickiness) (Pierson, 2004: 8). Positiv feedback karakteriseres ved at være uforudsigelig, ufleksibel og svær at ændre. Potentielt kan positiv feedback lede til sti-ineffektivitet, hvilket betyder, at timing og tidspunkt er afgørende for bl.a. implementering (Pierson, 2004: 18-9).

Pierson er særligt interessant, når man ser på den danske case, hvor der allerede på baggrund af arbejdet i NOST er planlagt at oprette en ny styrelse. Stiafhængighed kan føre til inefficiente udfald, hvilket der ifølge Ostrom også kan være sandsynlighed for her, hvor en ny styrelse kan ende med at være mere omkostningstung og ufleksibel. Institutionel innovation kunne her være at videreføre arbejdet, der er foregået i Covid-19-staben og decentralt i regionerne, som rammerne for samarbejdet som en selvstyrende institution, hvilket kan være mere effektivt, da håndteringen i højere grad styres af aktørerne

sammen. En sådan institution vil være en ny slags offentlig institution og måde at drive samarbejdet mellem det offentlige og private, hvor erhvervslivet er mere direkte involveret i en offentlig myndighed. Det vil kunne være en ny kategori i de forskellige former for markedsgørelse, som allerede ses på sundhedsområdet (Petersen og Suenson, 2013: 101-2). Da den nye styrelse placeres under Justitsministeriet med det formål, at sundhedsmyndighederne skal kunne fokusere på sundhedsfaglige kerneopgaver (Regeringen, 2020), er det imidlertid mere sandsynligt, at den nye styrelse vil have en mere normal struktur ift. håndteringen af denne og lignende situationer fremover. Det kan dog være en mindre effektiv styringsform og være mindre gavnligt for samarbejdet og innovationen i sektoren.

Samarbejde er vejen frem

Coronakrisen er ikke slut – og den vil med sikkerhed have langstrakte konsekvenser, som ligger langt ud over de rent sundhedsmæssige. Denne artikel har beskæftiget sig med krisens akutte fase og forsyningen af medicinsk udstyr samt de politiske og institutionelle dynamikker, som muliggjorde det samarbejde med industrien, der var medvirkende til at fremskaffe tests, værnemidler og andet medicinsk udstyr i de kritiske forårsmåneder i 2020.

Ud fra en teoretisk tilgang er det interessant, at forsyningen af medicinsk udstyr kunne betragtes som et klassisk kollektivt handlingsdilemma, samt at løsningen på dette netop blev forsøgt etableret med en blanding af de tilgange, som man kender i litteraturen – credible commitments og selvstyrende institutioner. Først anvendte regeringen den politiske situation med massiv krisebevidsthed til at indføre hastelovgivning, som sendte et klart signal til de nye aktører udenfor den traditionelle medicoindustri, der forsøgte at udnytte situationen ved bl.a. at tage meget høje priser. Dernæst begyndte en lang række private og offentlige aktører at etablere hidtil usete samarbejdskonstruktioner, hvilket gav samarbejdet karakter af en selvstyrende institution. Dermed tog de involverede parter selv ansvar for organisering og monitorering, hvilket kan have gjort processen mere effektiv.

Forløbet i foråret viser, at det kan lade sig gøre at have et fleksibelt samarbejde på tværs af den offentlige og den private sektor, samtidig med at man fra statens side har mulighed for at gribe ind overfor aktører, som forsøger at udnytte situationen.

Fremadrettet er det interessant, om man formår at høste gevinsterne ved det fleksible samarbejde og mobilisere ressourcer på tværs af den offentlige og private sektor, hvor den etablerede industri er afgørende for at levere bl.a. de produkter, som efterspørges. Omvendt er det klart, at en nyoprettet styrelse er nemmere at håndtere ift. de styringslogikker, som præger det politiske system. Der er dog en risiko for, at man kan få en mere rigid styring med en styrelse under Justitsministeriet, som ikke har nærheden til de kliniske miljøer eller industrien.

Mere generelt kan man spørge, om det i mange sammenhænge ikke ville være fordelagtigt i en dansk kontekst at udnytte det høje tillidsniveau på tværs af den offentlige og den private sektor til at opbygge mere fleksible og effektive samarbejdskonstruktioner, som i mindre grad er baseret på kontrol. Om man vil det, er i høj grad et spørgsmål om politisk risikovillighed.

I valget mellem kontrol og tillid skal der også tages højde for, at innovation – særligt på sundhedsområdet – kræver samarbejde mellem den offentlige og private sektor, da bl.a. udstyr og løsninger skal udvikles i samspil med de offentlige kliniske miljøer. Dette taler for, at håndteringen af coronakrisen fortsat baseres på nært og fleksibelt samarbejde mellem den offentlige og den private sektor.

Litteratur

Axelrod, R. (1990), *The Evolution of Co-operation*, New York: Penguin Books.

Brogaard, L. (2015), "Drivkræfter og barrierer i offentlige-private innovationspartnerskaber (OPI) på sundheds- og ældreområdet i Danmark", *Politica*, 47(4): 541-60.

Crea, G., A. Cavaliere og A. Cozzi (2019), "Price discrimination in the Italian medical device industry: An empirical analysis", *Economia Politica*, 36(2): 571-608.

Damvad Analytics (2018), "Life-science-industriens fodaftryk på dansk økonomi", 15. januar, hentet fra: https://em.dk/media/12998/lifescience-industriens-fodaftrykpaadanskoekonomi_damvad.pdf.

Folketinget, Sundheds- og Ældreudvalg (2020), Sundheds- og Ældreudvalget 2019-20: SUU Alm.del – endeligt svar på spørgsmål 801, 29. april (Doc. no.: 1166861), København.

Greve, C. (2019), *Løsninger i partnerskab, offentlig-privat samarbejde*, København: Gyldendal A/S.

Haahr Lund, M. (2020), "Verdens største netbutik slår ned på grådige ansigtsmaske-sælgere", 26. februar, hentet fra: https://finans.dk/erhverv/ECE11969082/verdens-stoerste-netbutik-slaar-ned-paa-graadige-ansigtsmaske saelgere/?ctxref=ext.

Jensen, T.K. (2020), "Folketinget har vedtaget vidtgående hastelov mod corona", DR.dk, 12. marts, hentet fra: https://www.dr.dk/nyheder/politik/folketinget-har-vedtaget-vidtgaaende-hastelov-mod-corona.

Kjær, J.S., og S.S. Kjeldtoft (2020), "Helt usædvanligt: Industrien har fået fast sæde i regeringens kontroltårn under krisen", Politiken.dk, 2. april, hentet fra: https://politiken.dk/indland/art7738392/Industrien-har-f%C3%A5et-fast-s%C3%A6de-i-regeringens-kontrolt%C3%A5rn-under-krisen.

Kollerup, S. (2020), "Debat: Simon Kollerup: Life science er én af nøglerne til en genrejsning efter corona", Børsen, 9. juli, hentet fra: https://borsen.dk/nyheder/opinion/life-science-er-nogle-til-genrejsning.

Lægemiddelstyrelsen (2020a), "Lægemiddelstyrelsen får flere beføjelser til at modvirke forsyningsproblemer", 24. marts, hentet fra: https://laegemiddelstyrelsen.dk/da/nyheder/2020/laegemiddelstyrelsen-faar-flere-befoejelser-til-at-modvirke-forsyningsproblemer/#.

Lægemiddelstyrelsen (2020b), "COVID-19: Lægemiddelstyrelsen advarer mod ulovlige forhandlere", 25. marts, hentet fra: https://laegemiddelstyrelsen.dk/da/nyheder/2020/covid-19-laegemiddelstyrelsen-advarer-mod-ulovlige-forhandlere/.

Lund, J. (2020), "Google og Apple slår ny dansk corona-app i privatlivsbeskyttelse", Prosa, 27. april, hentet fra: https://www.prosa.dk/artikel/google-og-apple-slaar-ny-dansk-corona-app-i-privatlivsbeskyttelse/.

Mankiw, N.G. (2017), *The Economics of Healthcare*, E-booklet, Harvard University.

Mazzucato, M. (2015), *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*, Great Britain: Anthem Press.

NNF, Novo Nordisk Fonden (2020), "Novo Nordisk Fonden har bevilget op til 250 mio. kr. til Statens Serum Institut i forbindelse med etableringen af et nationalt testcenter for den ny coronavirus", 21. april, hentet fra: https://novonordiskfonden.dk/da/nyheder/novo-nordisk-fonden-har-bevilget-op-til-250-mio-kr-til-statens-serum-institut-i-forbindelse-med-etableringen-af-et-nationalt-testcenter-for-den-ny-coronavirus/.

North, D.C. (1993), "Institutions and Credible Commitment. *Journal of Institutional and Theoretical Economics*", 149(4): 1-22.

Omachonu, V.K., og N.G. Einspruch (2010), "Innovation in Healthcare Delivery Systems: A Conceptual Framework", *The Innovation Journal: The Public Sector Innovation Journal*, 15(1): 2-20.

Ostrom, E. (1990), *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge: Cambridge University Press.

Petersen, O.H., og E.L. Suenson (2013), "Markedsgørelse i den offentlige sektor: Private løsninger på offentlige problemer"? i K. Kosiara-Pedersen, G. Nedergaard og E.L. Suenson, red., *Statskundskab i praksis: Klassiske teorier og moderne problemer*, København: Karnov Group Denmark A/S, pp. 101-18.

Pierson, P. (2004), *Politics in time: History, institutions, and social analysis*, New Jersey: Princeton University Press.

Regeringen (2020), "Styrket samfundsmæssigt beredskab / Pressemøde: Ny styrelse og teststrategi", 12. maj, hentet fra: https://www.regeringen.dk/nyheder/2020/pressemoede-i-spejlsalen-om-covid-19-i-danmark/.

Regeringens vækstteam for life science (2017), *Life science i verdensklasse: Anbefalinger fra regeringens vækstteam for life science*, København, pp. 1-10 + 51-6.

Region H, Region Hovedstaden (2020a), "Novo Nordisk klar til at hjælpe med at teste for COVID19", 28. marts, hentet fra: https://www.regionh.dk/presse-og-nyt/pressemeddelelser-og-nyheder/Sider/Novo-Nordisk-klar-til-at-hj%E6lpe-med-at-teste-for-COVID19.aspx.

Region H, Region Hovedstaden (2020b), "Region H påtager sig opgaven med at indkøbe værnemidler til hele landet", 14. april, hentet fra: https://www.regionh.dk/presse-og-nyt/pressemeddelelser-og-nyheder/Sider/Region-Hovedstand-stiller-sig-i-front-for-indk%C3%B8b-af-varnemidler-til-det-danske-sundhedsvaesen.aspx.

Retsinformation (2020), "Bekendtgørelse om særlige foranstaltninger vedrørende forsyning af medicinsk udstyr og personlige værnemidler i forbindelse med håndtering af Coronavirussygdom 2019 (COVID-19)", 22. marts, hentet fra: https://www.retsinformation.dk/eli/lta/2020/253.

Scharpf, F. (1997), *Games Real Actors Play: Actor-Centered Institutionalism in Policy Research*, Colorado: Westview Press.

Suenson, E.L., P. Nedergaard og P. M. Christiansen (2016), "Why lash yourself to the mast? The case of the Danish Budget Law", *Journal of Public Budgeting and Finance*, 36(1): 3-19.

Vallgårda, S. og A. Krasnik (2016), "Det danske sundhedsvæsen", i S. Vallgårda og A. Krasnik, red., *Sundhedsvæsen og sundhedspolitik*, København: Munksgaard, pp. 155-214.

Mere moralisering end analyse i et biased kampskrift for DR

Temanummer: Cybersikkerhed

Denne artikel analyserer en bog om Danmarks Radio skrevet af Christian S. Nissen, tidligere generaldirektør for DR. Han argumenterer for, at danske politikere i deres styring af DR ikke har magtet at modvirke truslerne fra internationale medier som YouTube og Netflix, som ifølge ham vinder frem med unfair metoder. Dette mener han vil svække dansk sammenhold og kultur. I artiklen her argumenteres for, at hans bog er et biased partsindlæg for det gamle DR, som ikke selv har formået at komme ind i en ny medieverden. Selvom Nissen præsenterer sig som tidligere forsker og henviser til forskning, er hans brug heraf overfladisk eller forkert.

BØJE LARSEN[1]
professor emeritus, ph.d, Copenhagen Business School, bl.om@cbs.dk

I foråret 2020 udkom bogen "Politik mellem følelser og fornuft. Spillet om danske mediers fremtid" (Nissen, 2020).[2] Bogen analyserer det såkaldte medieforlig 2019, der i den offentlige opfattelse og i denne artikel mest angik og angår Danmarks Radio (DR). Deltagerne i medieforliget var de daværende regeringspartier Venstre, Liberal Alliance og Konservative samt regeringens støtteparti, Dansk Folkeparti. Socialdemokratiet og venstrefløjspartierne forlod forhandlingerne på et sent tidspunkt vist bl.a. i håb om et snarligt regeringsskifte, som også kom i form af Mette Frederiksen-regeringen, som lagde forliget på is (Altinget 10.9.20). Bogens forfatter er Christian S. Nissen (fremover Nissen), der har haft ledende stillinger i det offentlige og var generaldirektør i Danmarks Radio 1994-2004.

Nissen belyser medieforliget ved at fortælle om de forhold, der efter hans mening satte scenen for medieforhandlingerne, både i dansk debat og politik og mht. den teknologiske udvikling. Nissen argumenterer i denne beskrivelse for, at DR var udsat for negativ "framing" i pressen, og at de globale mediemastodonter, f.eks. Google, YouTube og Netflix, vinder frem via urimelige forretningsmetoder. Dernæst beskriver Nissen selve forhandlingerne ud fra interviews med deltagerne. Resultatet af forhandlingerne ser Nissen som utilfredsstillende. DR taber og derved svækkes dansk sammenhængskraft. »Politikerne magtede ikke at løfte deres mediepolitiske ansvar«, sammenfatter Nissen sit budskab i Jyllands-Posten 2.2.20.

I denne artikel vil jeg kritisk undersøge Nissens analyse af de nævnte forudgående forhold, der satte scenen for forhandlingerne, herunder argumentationen om DRs betydning for dansk sammenhængskraft. Jeg ser også kritisk på hans teoretiske analyse af forhandlingerne, herunder ordene i bogens titel "Følelser og fornuft", som han begrunder hos sociologen/politologen Max Weber.

Min kritiske analyse skal ses i forhold til, at Nissen præsenterer sig og bogen som seriøs analyse og nærmest videnskab (henvisning til egen uddannelse, tidligere lektor, videnskabelige referencer, f.eks. s. 10). Ikke "blot" som en debatbog eller som et "vredt læserbrev" eller "Twitterbesked", som præsidenter og andre skriver. Men selv en debatbog og et læserbrev kan analyseres for kvaliteten af sine argumenter.

Anmeldelserne af Nissens bog

Nissens bog blev ved sin udgivelse omtalt i pressen på fremtrædende plads og af kvalificerede anmeldere. Anmeldelserne giver inspiration til nogle af de punkter, jeg tager op i denne artikel. Derfor giver jeg dem omtale.

Generelt er anmeldelserne positive, men få er uden kritiske kommentarer. En enkelt er nærmest fuldstændig negativ:

Altinget.dk bringer (4.2.20) en anmeldelse af bogen af *Lisbeth Knudsen*, der har haft en mediekarriere omfattende både A-pressen, Berlingske Media, DR (som nyhedsdirektør) og Mandag Morgen/Altinget.dk. Hun læser bogen således, at medieforliget var uden nytænkning. Forklaringen på forliget er "[f]lere års vrede og gammelt nag hos primært Venstre og Dansk Folkeparti" og en kampagne fra Danske Medier. Knudsen nævner "følelser og fornuft" fra titlen og forstår Nissen derhen, at public service kun kan opretholdes gennem værdibaserede holdninger og idepolitik.

Journalist *Kurt Strand*, der også har en baggrund i DR, skriver i sin anmeldelse i Information (3.2.20), at bogen bør være "pligtlæsning" for medieinteresserede. Nissen leverer "en overbevisende sammenhæng og analyse, skrevet med et kvart århundredes uundgåelig, mediepolitisk indsigt". Strand ser specielt Venstres finansminister Claus Hjorth Frederiksens fjendtlighed for årsagen til beskæringen af DR. Strand tolker, i modsætning til Knudsen, Nissens bog således, at den viser, at "politikere lader følelser og det letfattelige overtrumfe fornuft."

I Kristeligt Dagblads anmeldelse (7.2.20) er politologi-professor emeritus *Tim Knudsen* også positiv: "Den tidligere generaldirektørs kombination af medieindsigt og godt politologisk håndværk overbeviser […] om, at dansk mediepolitik er beskæmmende provinsiel, kortsynet og savner forståelse for, at medieområdet er afgørende for dansk kultur, sammenhængskraft og demokrati."

I Berlingske Tidende (19.2.20) kalder en anden politologi-professor, *Peter Nedergaard*, bogen "god og vigtig". Også han understreger det nationale. DR kan være et af de "mest solide forsvarsværker for dansk kultur". Ud fra Nissens opfattelse, at DR-nedskæringerne i medieforliget er et resultat af et følelsesmæssigt hævntogt fra bl.a. Claus Hjorth Frederiksen og Dansk Folkeparti, kommer bogen dog til at virke som "ét langt forsvar for DR." Nedergaard mener endelig, at følelses-fornuft-argumentationen bedre havde været udeladt. Den kaster for lidt af sig.

I Politiken anmeldes bogen af chefredaktør *Christian Jensen* (3.2.20) noget mere kritisk. Nissen roses for sin minutiøse gennemgang, inklusive interviews med politikere. Jensen ser, som Nissen, medieforliget som en falliterklæring, der fokuserede på Radio24syv snarere end det globale medieopbrud. I en "værdibaseret sognerådspolitik faldt især de borgerlige partier igennem som udsynsløse og hårflækkende småstatspolitikere". "[Forløbet viser] medie-politikere, der – som titlen svagt antyder – er styret af værdipolitiske følelser, frem for det, forfatteren anser og patenterer som rationel fornuft." Bogen er "et slet skjult forsvarsskrift" for DR, hvad Jensen dog finder ok, men "det havde været mere klædeligt at tone rent flag". Når bogen således "er yderst interessant læsning, skyldes det, at den giver et sjældent indblik i den særlige offerpsykologi, der tilsyneladende har sat sig i toppen af DR-organisationen. […Nissen] sympatiserer blindt med DR-toppens offerfortælling."

Jyllands-Postens anmelder er *Mikael Jalving* (9.2.20), som jeg ser beskrevet som borgerlig historiker og debattør med en ph.d. Jalving har enkelte positive bemærkninger: "[Nissen] formår at gennemgå handlingsforløbet kronologisk og redeligt" og har "udmærkede og troværdige indsigter". Jalving læser bogen således, at forklaringen på den økonomiske beskæring af DR var den politiske utilfredshed med DR, som han ikke dog ikke ser noget usagligt i. Jalvings konklusion er: "[Bogen] kunne have været et nydeligt universitetsspeciale, men som bog skrevet af en voksen og erfaren mand udviser [den] en overraskende mangel på sproglig, kompositorisk og intellektuel modenhed. Særligt hans betragtninger om politik mellem følelser og fornuft virker underligt påhæftede og juvenile, manden er trods alt over 70."

Med anmeldelsernes kommentarer som inspiration vil jeg i det følgende undersøge to spørgsmål:

1. Er bogen biased, og hvis ja – hvordan?
2. Er bogen godt politologisk håndværk eller et "nydeligt", men ikke tilfredsstillende universitetsspeciale? Her ser jeg især på Nissens brug af teori og principielle tolkninger af medieforhandlingerne.

Er bogen biased, og hvis ja – hvordan?

Det engelske ord "biased" har sneget sig ind i det danske sprog. Den Danske Ordbog (internettet 24.4.20) definerer det således: "Forvrængning af undersøgelsesresultater, målelige størrelser el.lign., som især skyldes forudindtagethed eller metodiske fejl." Jeg bruger det i denne betydning, men dog også i betydningen "forvrænget fremstilling af samfundsmæssige og mediemæssige forhold, der skyldes forudindtagethed eller metodiske fejl", også uden at der er tale om talmæssige størrelser.

Bias i beskrivelse af rammebetingelserne for medieforhandlingerne

Nissen beskriver i bogen som nævnt den forhistorie, som satte dagsordenen for de konkrete forhandlinger. Det sker i kapitel 2 til og med 6. I det følgende

beskriver jeg seks eksempler på bias i disse. Afsnitsoverskrifterne afspejler Nissens teser.

- DRs møgsager er ødelæggende. Manglende presseberedskab
- Negative ord i pressen framer DR negativt
- Lobbyaktivitet mod DR
- De udenlandske mediegiganter bruger unfair forretningsmetoder
- Kuratering – snæver eller bred. DR gør det rigtige
- DR bidrager til dansk sammenhold

DRs møgsager er ødelæggende. Manglende presseberedskab

I kapitel 2 beskriver Nissen en række "møgsager" for DR i årene, fra han forlod DR (2004). Disse sager gav iflg. Nissen i disse år DR et dårligt ry i pressen. Møgsagerne omfattede kritik af DRs hævdede høje direktørlønninger og fratrædelsesordninger, nyhedsdirektørens mange arbejdsgiverbetalte rejser mellem bolig og arbejde, "sagen" om DRs USA-korrespondents hustrus hest, der på husets regning blev flytransporteret til USA, og "sagen" om en mediedirektørs overgang til at være mangfoldighedskonsulent, men med uændret løn. Til disse overvejende økonomiske møgsager kan også føjes "sagen" om den fhv. dramachef, der på forsiden af Politiken udtalte, at en DR-serie om 1864-krigen var tilsigtet at være et "slag mod DF" (s. 33, 134) samt nedlæggelsen af Underholdningsorkesteret i 2014 (s. 42ff). (Når jeg her og i det følgende giver sidetal i en parentes eller i teksten uden nærmere angivelse, er det altid til Nissens bog.)

Nissen lægger ikke fingrene imellem i beskrivelsen af møgsagerne og skriver, at DR var blevet noget "tonedøv" over for kritik. DR havde også kun et svagt presseberedskab (s. 39).

Han giver forklaringer, som er fair nok i sammenhængen, men som ved nærmere eftertanke peger på, at tonedøvhed kan smitte. Han beskriver f.eks., hvordan Rigsrevisionen, statsrevisorerne og to konsulentfirmaer ikke havde indvendinger i forskellige af sagerne. Men ulovligheden var ikke kritikernes hovedpointe (selvom de sikkert ville have nydt den), men vel en form for "moralsk" forargelse eller blot en forestillet sådan. Hvis private virksomheder, f.eks. banker kritiseres for at udbetale store bonusser i krisetider, så vil fornuftige PR-folk nok forklare dem, at det er en tynd undskyldning at pege på, at det er lovligt. De pågældende havde et valg inden for rammerne af det lovlige, og det er det valg, der kritiseres. Og uanset at man som offentlig virksomhed kan klage over manglende armslængde og for meget detailstyring i resultatkontrakter, så har også de, inkl. DR i de nævnte sager, et råderum, og det er adfærden inden for det, der kritiseres (om end måske med håb om, at det råderum lovgivningsmæssigt indskrænkes).

Argumentationen om det manglende presseberedskab ligner den, man ser på valgaftener, når tabende partier ikke kritiserer egen politik og fremfærd, men siger "at vi skal lære at kommunikere den bedre til vælgerne". Kritisér aldrig

dig selv, accepter ingen indrømmelse, hyr kommunikationsfolk, synes parolen at være.

Denne parole kan man måske også ane, når Nissen får givet den i øvrigt respekterede fhv. departementschef, Michael Christiansen, der nu var bestyrelsesformand i DR, medansvaret for den dårlige pressehåndtering. Nissen nævner flere fejltrin. Bl.a. gik det "[h]elt galt" (s. 40), da Christiansen åbnede for besparelser hos DR.

Måske mener Nissen, at en forhandler generelt aldrig må gøre det. Eller måske med sin baggrund, at offentlige ledere/bestyrelsesformænd i hvert fald ikke må gøre det.

Negative ord i pressen framer DR negativt

Nissen nævner (s. 51) en bog, der beskriver "framing" som at sætte et budskab ind "i en særlig (begrebs)ramme, f.eks. ved at bruge særlige ord og vendinger, så modtagerens opfattelse påvirkes i en bestemt retning – uden at hun/han selv er opmærksom på det." Det kan ifølge bogen, Nissen henviser til, bruges som et manipulatorisk redskab.

Mht. debatten om DR forud for medieforhandlingerne hævder Nissen (s. 52), at ordene "tvangslicens", "statsmedier" og "mediemastodonten" er sådanne negative framing ord, der blev anvendt af mange aktører omkring DR. Han argumenterer rimeligt for, at dette er negativt ladede ord, også selvom de har et beskrivende indhold. Han kortlægger ikke det faktiske omfang af denne framing i medierne.

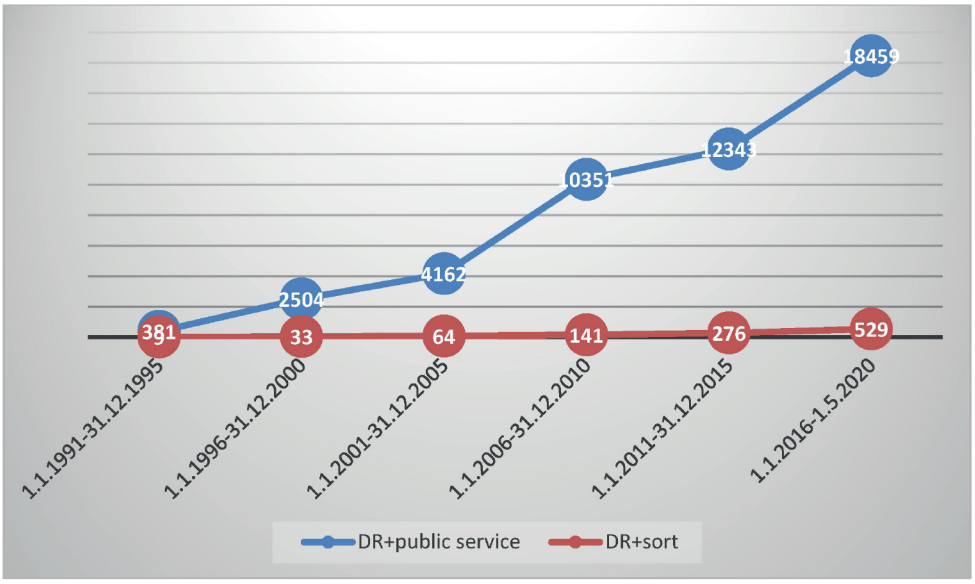
Han overvejer heller ikke, om DR er omgivet af og/eller selv aktivt bruger "positive" ord til framing. To grupper af udtryk ville det være nærliggende at undersøge. Først "Danmarks Radio". "Danmark" men også ord som "dansk", "folke-", "national". "Nationalmuseet" har vel, ud over ordenes deskriptive indhold, for mange en positiv klang. Private enheder er heller ikke kede af disse ord. "Danske Bank", "Den Store Danske Encyklopædi", også markedsført som "det danske nationalleksikon", "Dansk Industri", "Dansk Metal".

Et andet plusord, der ofte knyttes til Danmarks Radio, er "public service". Den Danske Ordbog beskriver det som en "virksomhed som en (ikkekommerciel) radio- eller tv-kanal yder i offentlighedens interesse, især i form af et alsidigt og afbalanceret programudbud" (internettet 13.5.20). Det positive i udtrykket ses nok lettest ved at spørge sig selv: Hvem vil ikke gerne betegnes om én, der arbejder i offentlighedens interesse? Som lønmodtager, som selvstændig?

Jeg har i mediedatabasen Infomedia.dk, der omfatter alle danske nyhedsmedier inklusive netmedier, undersøgt forekomsten af de tre sorte, dvs. negative ord, som Nissen nævner (i formen "tvangslicens", "statsmedie" og "mediemastodont", der også fanger ordene i flertal og i ordforbindelser) sammen med udtrykket "Danmarks Radio" eller "DR". Samt artikler "public service" sam-

men med "DR" eller "Danmarks Radio. Dataene er opgjort i fem-årsperioder, fra 1991 til 1.5.20 (opgørelsestidspunktet). Resultaterne ses i figur 1.

Figur 1: Positiv og Negativ Framing af DR



Tallene angiver antallet af artikler med det søgte indhold. Den øverste kurve viser antallet af artikler med "DR" eller "Danmarks Radio" *og* "public service" over årene. Den beskedne kurve forneden viser antallet af artikler om DR mm. samt et af de sorte, dvs. negative ord. Den forveksles let med X-aksen. For den seneste periode er antallet af artikler med DR og »public service« 35 gange så høj som dem med de sorte ord. Når kurven for begge typer af artikler er stigende over årene, synes det i en separat analyse, der ikke er vist her, ikke i væsentlig grad at være den relative andel af artikler med disse ord, der stiger, men at Infomedia.dk omfatter flere og flere medier over årene. Mange af artiklerne med "public service" nævner kun begrebet deskriptivt. Nogle få bruger det som et ideal i forbindelse med kritik af DR – f.eks. at "tant og fjas"-materiale om udskæring af mango-frugter og bagedyst ikke hører under public service.

» **Antallet af artikler i pressen med DR og "public service" er 35 gange så højt som artikler med negative ord**

Disse tal kan ikke bekræfte Nissens påstand om dominansen af de negative ord i pressen.

Lobbyaktivitet mod DR

Anvendelsen af det pæne ord "presseberedskab" i forhold til DRs beskyttelse af sig selv står i kontrast til Nissens beskrivelse af andres indsats for at tjene deres interesser. Når producenter af nyheder og underholdning uden for DR gør det, omtaler Nissen det normalt som "lobbyaktivitet", og han har i især

et godt øje til interesseorganisationen Danske Medier, der omfatter private medier (s. 57).

Nissen indleder sin beskrivelse af Danske Medier med at citere, hvad man kunne kalde en DR-offer-udtalelse fra tidligere DR nyhedsdirektør Ulrik Haagerup (Altinget.dk 16.5.17): "[D]en kollektive, kommercielle mediestrategi forklædt som journalistik, som handler om at gøde jorden for politikerne, der helst skal påvirkes til at tro, at det vil løse dagbladenes uomtvistelige problemer, hvis heller ikke DR i fremtiden vil være i stand til at levere et ordentligt indhold til hele befolkningen og binde Danmark sammen." (s. 56). Dagen efter citeres nyhedsdirektøren for, at der er tale om en "meget koordineret […] lobbykampagne" (s. 57).

Den Danske Ordbog (internettet, 13.5.20) definerer lobbyisme som "påvirkning af fx embedsmænd eller politikere til at tage bestemte hensyn i forbindelse med udarbejdelse og vedtagelse af love, planer osv. især en organiseret påvirkning iværksat af en bestemt interessegruppe eller -organisation." Som et eksempel på sprogbrugen nævnes: "Lobbyismen i amerikansk politik har skabt et system, der minder om en karikatur af europæisk demokrati." I hvert fald eksemplet antyder noget af den negative framing, ordet kan skabe. I Nissens bog er denne tone – karikatur af demokrati – ikke fjern, når lobbybegrebet bruges.

Nissen tager således tråden op fra Haagerups nævnte udtalelse ved at beskrive den fjende, han åbenbart mener DR står overfor, nemlig en af formændene for Danske Medier. Han er "kendt som hardliner." "Han fulgte i sporet af sin mentor, den hårdtslående Jørgen Ejbøl (med tilnavnet Pansergeneralen efter Ejbøls store forbillede, den amerikanske general George Patton)" (s. 57).

Senere dannes en udvidet gruppe omkring Danske Medier med andre private aktører på medieområdet. Nissen fortæller, at gruppen omtalte sig selv som Pippigruppen med henvisning til Pippi Langstrømpes udsagn om, at man som stor og stærk (vel mønted på DR) skal være særlig flink ved de små.

Denne framing (lobby, Patton, Pippi) af modstandere gør Nissens tekst sjovere at læse end hans omtale af DRs situation (svagt presseberedskab, pengeforbrug er inden for det lovlige). Men forskellen viser en vis bias.

Fremstillingen af Pippi-gruppens aktiviteter er stort set uden kildeangivelse, også når man forstår, at der er tale om oplysninger fra gruppens interne møder.

De udenlandske mediegiganter bruger unfair metoder

I kapitel 3 beskriver Nissen opbruddet i det danske mediemarked. Her er interessante oplysninger, men også en stærk framing i DRs favør. Den er især synlig, når Nissen omtaler Facebook, Google, Netflix og Apple. De udøver "dominans", betaler ikke skat i Danmark, er del af overvågningskapitalismen og lænser det danske mediemarked for penge. Sidstnævnte argumentation kunne frihandelsmodstandere også anføre på andre områder. Hvorfor franske

oste og vine? Vi har danske oste. Hvorfor tyske biler, vi har danske cykler? Hvorfor tager vi ikke masseproduktion tilbage fra Kina og Bangladesh? Kritikpunkterne mod de udenlandske udbydere er valide, men ikke alt.

» Kritikpunkterne mod de udenlandske udbydere af TV er valide, men ikke alt

Nissens framing omfatter nemlig ikke en forklaring på, hvorfor forbrugerne mon ofte ser fjernsyn hos især Netflix og Google (YouTube). Skulle der være noget for DR at lære heraf? Måske endda noget, de kunne gøre uden en besked fra politikerne?

Her kunne man f.eks. mht. Netflix og YouTube nævne, at alt deres materiale er tilgængeligt, når man vil, nat og dag (on demand), og hvor i verden man er. For DR er det kun en megen beskeden del, der er tilgængeligt. Mht. den tilgængelige del må man vente til DR enten sender det på deres tider (flow) og/eller gør det tilgængeligt fra deres arkiver. Man betaler for Netflix, men kan opsige det, hvad man ikke kan med DR, også selvom man ikke kan modtage deres tilbud. YouTube er grundlæggende gratis, selvom det i stigende grad kræver betaling for hele film.

DR har (optalt 14.5.20 på dr.dk/drtv/a-aa) ca. 1.700 on demand-tilbud. Skønsmæssigt 1/3 kan ikke ses i udlandet. Nexflix har mindst 3.000-4.000 titler, sandsynligvis mange flere, i form af film, serier og tv-shows (se f.eks. usikre kilder som flexable.com og flixfilm.dk). YouTube har sandsynligvis flere millioner (jeg har heller ikke her et pålideligt tal, langt større tal nævnes på internettet, f.eks. https://www.quora.com/How-many-videos-are-on-YouTube?)

YouTube har været og er for mange stadig associeret med søde kattevideoer. Og der er meget stof, hvis gennemsnitlige kvalitet er langt under DRs gennemsnitlige kvalitet. Men ser man på programfladen som helhed, er kattevideo-opfattelsen ikke dækkende. Der er en stor gruppe programmer om, hvordan man gør ting, man ikke har prøvet før, f.eks. reparation mm. af hus, bil, pc, mobiltelefon, hvordan man laver mad, passer dyr, sundhedsrådgivning, både fra det autoriserede lægevæsen og andre, madlavning, lære sprog. Disse how-to-programmer er ifølge https://www.brandwatch.com/blog/youtube-stats/ det vigtigste motiv i USA for at bruge YouTube.

Mht. sundhedsrådgivning ser jeg artikler, som analyserer YouTubes tilbud fra det autoriserede lægevæsen. Det handler bl.a. om instruktionsvideoer fra operationer, som vel er lettere at forstå end ord om dem (Farag, Bolton and Lawrentschuk, 2020). Det er en review-artikel, der har set på 37 artikler om emnet. De skriver, at disse videoer ofte bruges i undervisning og ses af studerende. De nævner artikler, der ser positive virkninger, men de foreslår også en slags peer-review af dem. Dette er naturligvis ikke noget for Danmarks Radio.

Et andet større område på YouTube er musikvideoer og film. F.eks. pop, gammel som ny. Som et tilfældigt eksempel på det gamle – og danske – kan nævnes Raquel Rastenni: YouTube har over 100 videoer, mest sange, ingen hos DR. Kim Larsen: YouTube har over 200 indslag heraf mange af hans sange, 11 hos DR. Men også klassisk musik: Rued Langgaard: YouTube over 70, mange af hans symfonier. DR: 1. Seriøse film: Bille August: Netflix: 4, DR og YouTube: 0. Ingmar Bergman: YouTube: >100, flere af hans film. DR og Netflix: 0. Tager man kunstnere fra fjernere lande, bliver forskellen mere kras.

Universiteter som Harvard og Yale tilbyder mange hundrede videoer fra deres undervisning på YouTube. Hvor er DR?

Er man interesseret i historisk stof, er DR sjældent vinder. Tunge temaer som f.eks. Buchenwald og Gulag giver 0 resultater på DR, men begge over 50 på YouTube. Og der er rigelige videoer om de fleste store hændelser i verdenshistorien. Universiteter som Harvard og Yale tilbyder mange hundrede videoer fra deres undervisning (hvor er DR mht. danske universiteter?). Politik og religion er også godt dækket og med et meget bredere spektrum end hos DR. YouTube er efter kritik dog begyndt at slette indhold med useriøse sundhedsråd og ekstreme politiske og religiøse videoer, men de oplyser, at de ønsker at opretholde en åben platform (Frankfurter Allgemeine Zeitung, 16.5.20: 3).

Til sidst et træk, der sætter YouTube i en særlig god konkurrencesituation i forhold til institutioner som DR: DR må producere og købe det materiale, de sender. YouTube får det meste foræret af brugerne.

Når seertallet hos DR falder, og især unge falder fra (DR, 2018), kan der altså være tale om, at DR har konkurrenter, som har flere og bedre tilbud. Ikke blot at disse udenlandske udbydere er mastodonter, der arbejder med unfair metoder, som er den dominerende vinkel for Nissen.

Kuratering – snæver eller bred? DR gør det rigtige

Med udtrykket "kuratering" henviser Nissen til en interessant problemstilling i den nye medie-verden med de beskrevne mange tilbud. Nemlig hvordan dette udvalg præsenteres for brugeren. I en figur s. 129 sætter han sit synspunkt på spidsen og hævder, at de nye medier anvender en snæver kuratering, illustreret i figuren med en snæver lyskegle på mulighederne, mens en bred kuratering giver flere og bredere tilbud. Læseren kender sikkert disse henvisninger i form af udtryk som "her er noget, der sikkert vil interessere dig, baseret på hvad du tidligere har købt/set." Nissen mener, uden nærmere argumentation eller kilde, at DRs flow-tilbud anvender en bred kuratering, fordi en levende redaktør sammensætter programfladen, dvs. hvad kommer efter hvad. Dette afhænger dog naturligvis af, om den pågældende levende "kurator" (redaktør) har en smal eller bred horisont og viden, om det er den samme person fra dag til dag, og hvis han/hun skifter, om han/hun så kommer fra den samme, forenklet sagt for argumentationen, énsidige pool eller åndsret-

ning, f.eks. som nogle DR-kritikere nærmest mener (f.eks. "røde lejesvende" eller københavnere).

Der er næppe tvivl om, at f.eks. YouTube repræsenterer større alsidighed og variationsrigdom, også i en grad, så de som nævnt har fået kritik herfor. Ser man på DRs søgemaskine for det stof, de tilbyder on-demand, er resultatet også nedslående. Søger man Carl Nielsen, får man to på DR. Ingen supplerende forslag. Netflix: 0. YouTube giver over 100 og flere symfonier i fuld længde, nogle sikkert fra DR, som de ikke vil vise frem. Der gives forslag til andre komponister, fra Wagner til Vivaldi og flere. Samt kommentarer fra brugere, der f.eks. fortæller om deres følelser ved at høre musikken eller erindringer om, at de i deres ungdom mødte en af musikerne. Laver man en stavefejl i Carl Nielsens navn hos DR, f.eks. skriver Caro, får man intet. YouTube finder ham.

Hos YouTube er der et yderligere tilbud, der gør det muligt at finde rundt, uden at det sker efter kun ét princip. Forskellige YouTubere kan lægge deres lister af udsendelser, egne eller andres på sitet, og man kan abonnere på dem gratis. På den måde kan man følge forskellige "kuratorer" og deres forslag, ikke blot den autoriserede som hos DRs flow-TV eller ingen som på DR on demand. Endelig kan nævnes, at man til sin Android telefon kan få et antal apps, der hjælper med søgningen på YouTube.

En supplerende mekanisme i et nogenlunde liberalt samfund er, at venner og medier omtaler nye eller interessante tilbud hos Netflix etc. Endda DRs internet-avis er begyndt at gøre det i en form for anerkendelse af den situation, DR lever i, som ikke er nået frem til DRs serviceredegørelse, jf. nedenfor.

Alt i alt: Nissen framer DRs personbårne udvalgsmetoder som "kuratering", der klinger smukt af kunstudstillinger. Det tilsvarende negative ord, "algoritmer" bruges i den danske debat i dag om de onde internationale udbydere, der må ty til it-løsninger for at hjælpe med udvælgelsen. Det havde været godt, hvis Nissen havde fundet empiri om kvaliteten af disse udvalgsmetoder hos DR og andre. Ikke blot givet løse påstande. Det er en forskningsopgave, som andre med fordel kan tage op.

DR bidrager til nationalt sammenhold

Nissen og nogle af anmelderne af hans bog mener, at DR styrker det danske sammenhold, måske er det det eneste der gør det. F.eks. skriver Nissen (s. 297): "Mener man […], at internationalisering af medieudbud og -forbrug risikerer at undergrave national identitet, kultur og sammenhæng, vil løsningen snarere være en videreudvikling af public service-medierne, som er et af de få midler til opretholdelse af et nationalt samfund i global verden." Tanken fyres hos ham og nogle af anmelderne ofte af i en kort sætning. Det virker som en automatargumentation. Der er ingen nærmere oplysninger eller kilder.

Nissen og andre nævner også i forbindelse med det nationalistiske argument (f.eks. s. 127), at DR er nødt til at sende populært stof, dvs. det "tant og fjas", som nogle borgerlige kritikere er skeptiske overfor, for at fastholde seerne for

det seriøse og vigtige stof. En skribent skærer dette synspunkt klart ud i pap sådan her: "Det er naivt at tro, at den generelle befolkning frivilligt vil opsøge samfundsoplysende programmer" (Jyllandsposten 28.4.18).

» Nissen og anmelderne argumenterer ikke for, hvorfor det netop er den danske nationalstat, der skal styrkes. Ikke f.eks. Skandinavien eller Europa

Nissen og anmelderne argumenterer ikke for, hvorfor det netop er den danske nationalstat, der skal styrkes. Ikke f.eks. Skandinavien eller Europa. Her stiller man sig på linje med DF, som ellers ofte fremstilles som fjenden.

Uden at være medieforsker ser jeg, at der i den videnskabelige litteratur er artikler, der benytter opbruddet i Østeuropa og andre steder til – i en form for naturligt eksperiment – at undersøge, hvad radio og TV kan betyde. Jeg har identificeret tre teser, men andre findes utvivlsomt, De tre er:

Påvirknings-tesen
TV (fra udlandet) *kan* påvirke borgernes synspunkter, herunder politiske synspunkter. Her findes især undersøgelser af f.eks. USA's indflydelse på Nazi-tyskland, senere Sovjetunionen og DDR (Nye, 2008). Med nogen forsigtighed kan det måske overføres til, hvilke påvirkningsmuligheder eller virkninger, DR har f.eks. politisk og mht. holdninger til sammenhold og den danske nationalstat. I hvert fald er der inspiration til hypoteser og metoder, hvis man seriøst ønsker at undersøge det.

Escapisme-tesen
Her er opfattelsen tværtimod, at vesttysk TV *styrkede* DDR. De to forfattere (Kern and Hainmueller, 2009) har produceret en overbevisende artikel, der bl.a. bruger interne DDR-undersøgelser, som beskriver, hvor i DDR, man kunne og ikke kunne modtage vesttysk TV. F.eks. kunne man ikke i Dresden, som i DDR jargon derfor kaldtes "de uvidendes dal". Og samtidig har forfatterne tal for, hvor mange ansøgninger om udrejse, der var, og data fra dengang hemmelige holdningsmålinger hos (i det konkrete tilfælde) yngre DDR-seere. Dér, hvor folk *ikke* kunne se vesttysk TV, var seerne mere pro-DDR.

Forfatterne tolker det på den måde, at seerne *ikke* primært valgte vest-TV pga. politiske udsendelser og nyheder, som i øvrigt også viste, at der var problemer og konflikter i Vesttyskland. Heller ikke for at beundre forbrugsgoderne, som det ellers har været peget på fra modstandere af genforeningen af Øst og Vest. Nej, de så underholdningsudsendelser, der kunne aflede dem fra en grå hverdag. Det er derfor også logisk, at DDR-fjernsynet i 70'erne og fremefter producerede og sendte meget underholdningsstof og -shows, ikke sjældent inspireret af tilsvarende i vesttysk fjernsyn, som man ønskede at overgå for at fastholde øst-seerne. Østtysk TV tilbød også klip fra gamle film fra nazi-tiden med stadig kendte og elskede kunstnere (nazi-styret forfulgte i øvrigt også denne underholdningsstrategi mht. filmproduktionen). Hertil kom i DDR de

daglige strengt politisk styrede og formmæssigt dødkedelige nyhedsudsendelser og lignende, som mange lukkede af for.

> **Netflix, HBO, YouTube etc. vokser måske frem, fordi nogle, når de kommer fra arbejde, ønsker underholdning, ikke politik eller "københavneri"**

Overført til DK: Netflix, HBO, YouTube etc. vokser måske frem, fordi nogle, når de kommer fra arbejde, ønsker underholdning, ikke politik eller »københavneri«. Ungdommen vælger så måske af tilsvarende grunde YouTube's musiktilbud. Særligt tændte med specialinteresser, uden for DR-universet, i politik, religion og sundhed, søger måske også YouTube.

Nostalgi-tesen
Jeg har ikke set dette udtryk anvendt, men fænomenet omtales, f.eks. (Lüthi, 2015: 84): »*Brutal historical reality had suddenly become sweet memory*«. DDR-underholdningsudsendelser har mange ældre østtyskere i dag et nostalgisk forhold til f.eks. godnat-udsendelsen for børn, "Unser Sandmännchen". Men også indkøbt materiale som f.eks. Olsenbanden med tysk tale. Når sådanne østtyskere opdager, at jeg er dansk, kan de også finde på at nævne "Die Olsenbande" og sige „Mächtig gewaltig", som er den skæve tyske oversættelse af Bennys "skidegodt". Måske smitter denne nostalgi af på disse seeres syn på DDR og deres ungdom der.

Overført til DK kan det måske betyde, at uanset om seere forlader DR, så vender de måske tilbage til Matador, Borgen, Bagedysten, Bamse og Kylling ved fester og vemodige lejligheder. Men det er næppe denne nostalgivirkning, som DR-fortalerne tænker på. Eller er det?

Jeg overlader til læserne at søge videre i den omfattende medielitteratur. Min pointe er, at sagen ikke er så klar, som Nissen og anmelderne formoder. Også selvom DDR heldigvis ikke er/var Danmark.

Dette hovedafsnit mener at have dokumenteret varierende grad af bias og/eller manglende argumentation i Nissens beskrivelse af de mediemæssige vilkår for DR. Mht. disse afsnit må jeg erklære mig enig med de anmeldere af bogen, der mest ser bogen som et ret udokumenteret forsvarsskrift for DR.

Hvad kan være Nissens motiv til at være biased?

Hermed mener jeg, som i krimi-film, at vi som detektiver må spørge, hvilket motiv skulle Nissen (dog) have for at skrive biased om DR og andre mediespørgsmål.

Mit svar er her, at Nissens motiv til "forbrydelsen" kan være, at han i 2004 blev fyret som generaldirektør for DR. Fyringen skete under stor offentlighed opmærksomhed og med hårde anklager mod ham. Han nævner ikke sin fyring

i sin bog om medieforliget, men nævner mange andre hæderværdige hændelser i sin karriere. Det er menneskeligt forståeligt, men styrker en mistanke.

> En leders fyring nogle få gange i karrieren er ikke tegn på, at han/hun er mindre dygtig

Nærværende forfatters vurdering er, at en leders fyring nogle få gange i karrieren ikke er et tegn på, at han/hun er mindre dygtig. Det er nogle gange et tegn på vovemod og vilje, som få frakender Nissen. Men det sætter også ofte spor og lyst til at komme igen, ja måske ligefrem hævnlyst hos offeret.

I det år (2004), hvor Nissen i oktober måned måtte forlade DR som fyret med øjeblikkeligt varsel, registrerer mediedatabasen Infomedia.dk godt 400 artikler med DR og hans navn. En stor del af artiklerne handler om ham som person, hans fyring og mediernes forklaringerne og teorier herfor. De omfatter oplysninger/påstande/udsagn om en udsultning af DRs Århusafdeling, konflikter med medarbejderne i øvrigt, en formodet benhård ledelsesstil, umulig at samarbejde med og en 300 mio. kr. budgetoverskridelse på DR-byggeriet i Ørestaden. På det politiske plan beskrives en nedbrudt tillid mellem Nissen og DR-bestyrelsesformand Jørgen Kleener, V, som satte sin stilling ind på, at Nissen blev fyret. Alle medlemmer af bestyrelsen, på nær SFs medlem, støttede fyringen.

Rolf Bagger, forfatter, der dengang var medlem af bestyrelsen udpeget af kulturministeren (K), hælder i en kronik i Jyllands-Posten (5.4.2007) salt i såret og hævder, at Nissen "i dag [sikkert] priser sig lykkelig over, at han dengang insisterede på en bestemmelse om, at årsagen til fyringen ikke måtte omtales." Hans kronik har titlen "En rigtig beslutning at fyre Chr. S. Nissen."

Nissen, på sin side, citeres i forbindelsen med afskedigelsen (BT 11.11.04) for at have set "tydelige tegn på mere politisk indblanding i DRs arbejde… Jeg kan huske, hvor vrede en række politikere var over DR-dækningen af Irak-krigen." Nissen taler, som andre, om Claus Hjort Frederiksen, V, som den egentlige hovedmand bag sin fyring (se også Arbejderen.dk 6.10.04). Alt i alt konkluderer denne forfatter, at Nissen havde et (forståeligt) had til VLAK-regeringen, der også stod for medieforliget. Dette (med)forklarer hans angreb på politikere, der "ikke magtede".

> Nissen havde et forståeligt had til VLAK-regeringen, der stod for medieforliget

Godt politologisk håndværk eller nydelig/mådelig studenteropgave?

I den foregående diskussion af bias så jeg især på første del af Nissens bog (kapitel 2-6). I dette hovedafsnit vil jeg især se på Nissens kapitel 8, der angår selve forhandlingerne.

Kapitlet hører ifølge anmelderne til bogens bedste i den forstand, at den bias som præger første del – som beskrevet ovenfor – er mindre tydelig, ligesom Nissen bidrager med data om forhandlingerne ud fra de interviews, han har ført med ni deltagere over flere omgange (s. 23).

Side 202-3, dvs. ét opslag, er det, der i studenteropgaver hedder teoriafsnittet, som jeg vil se på i dette hovedafsnit. Senere, i kapitel 7 og senere i kapitel 10 beskriver han sit følelser-fornuft begrebspar og søger at forankre det hos Max Weber. Det tager jeg op i næste hovedafsnit.

Lindblom: Muddling Through

På s. 202-3 skriver Nissen om sin første teoretiske vinkel: "I praktisk politik drejer beslutningerne sig snarere om med små, korrigerende skridt at undgå et umiddelbart problem end at forfølge en bevidst kurs mod et højere eller mere fjerntliggende mål som beskrevet af den amerikanske politolog Charles E. Lindberg [sic] i artiklen 'The Science of Muddling Through'." Den lille skrivefejl i navnet – som er Lindblom – er en sjælden smutter i en ellers i denne henseende fejlfri bog fra det professionelle Gyldendal. Men at Nissen ikke har fanget dette i korrekturen, hvor hans opgave er at dække sådanne faglige ord ind, ikke skole-stavefejl i dansk, ser jeg som et lille udtryk for hans manglende fortrolighed med og kærlighed til det og den, han citerer. Det kommer også til udtryk i hans meget knappe beskrivelse, der kun omfatter det, som her er citeret.

Lindblom (1917-2018) var ung lektor i økonomi på Yale University, da han skrev den nævnte artikel (Lindblom, 1959). Han blev en af verdens mest kendte og citerede politologer. I artiklen sætter han to beslutningsforståelser op overfor hinanden: "The root method" og "the branch method". "The root method" svarer til det, som Nissen og mange andre kalder den "rationelle model" eller "fornuft" (s. 197). Ordet "rationelle model" framer denne forståelse meget positivt i forhold til de komplekse problemstillinger (om medier i moderne samfund), som Nissen undersøger, men da denne model har været genstand for en næsten enslydende kritik i litteraturen, kalder jeg den her og fremover den "pseudo-rationelle model".

Kritikken mod "the root method" (alias den pseudo-rationelle model) går på, at der i komplekse situationer normalt er mange mål. De er sjældent klare eller overensstemmende. Man kender heller ikke alle handlemuligheder/midler og deres potentielle konsekvenser. Overfor dette stiller Lindblom "the branch method", hvor man sammenligner løsninger i nærheden af det kendte. Hvilke repræsenterer en forbedring? Derved og samtidig vælger man også mål. Et succeskriterie her er ikke den ideale løsning, men netop at man er enige, om det så er ud fra forskellige målforestillinger.

» **Nissens data viser os, at målene for medieforliget ikke lever op til det rationelle pseudoideal – det ville i øvrigt være en sensation**

Nissens data viser os, at målene for medieforliget ikke lever op til det rationelle pseudoideal – det ville i øvrigt være en sensation: Det dominerende mål-plusord er "public service". Nissen udreder, at det i sin engelske oprindelse betyder, at noget er statsbetalt og -udbudt (s. 117), men det giver jo ikke meget retning. Nogle i den danske debat mener, at DR skal være et smalt fyrtårn med kvalitetsstof, mens andre igen mener, at uden "tant og fjas" vender brugerne deres "antenner" mod f.eks. Netflix og YouTube. Andre igen mener, at public service betyder mere stof fra Jylland. Eller måske skandinavisk eller europæisk stof. Der er simpelt uenighed om målene.

Lindbloms provokerende synspunkt er, at ikke alene er "the root method" ikke realistisk, men "the branch method" er *bedre*. Set i et større perspektiv, argumenterer Lindblom for, at de skyklapper, som de løbende sammenligninger i nærheden af det kendte medfører, kan afbødes, hvis det politiske system tillader forskellige aktører og interesser at præge beslutningsprocessen, dvs. hvis forskellige interesser har deres "watchdog" (Lindblom, 1959: 85). Det giver et andet perspektiv på "lobbyister" – de er samfundsmæssigt set nyttige parter – end det, Nissen har på Danske Medier. Lindblom udvikler senere dette perspektiv på demokratiet (Lindblom, 1965). Selvom han personligt også blev mere skeptisk med årene overfor lobbyisme fra det store erhvervsliv i USA, så står hans skarpe principræsonnement stadig som et brugbart måleinstrument.

Man kunne videre argumentere, at politikere *foretrækker* "the branch method". Nissen fortæller, at kulturminister Mette Bock, måske en af de sidste troende, eller med det ord, jeg bruger i næste afsnit "idepolitikere", tilrettelagde en proces forud for de konkrete beslutninger, hvor forskellige emner og spørgsmål blev diskuteret. Det kalder nogle af Nissens interviewpersoner (overvejende mediepolitikere) for "studiekredsen" (s. 222 f). Tilsyneladende ville de garvede politikere hellere gå til stålet og diskutere løsninger, enighed og uenighed. En anden interessant serie af oplysninger fra Nissen går på, at politikerne fortæller, at når de læser ekspertredegørelser (f.eks. fra Kulturministeriet, 2016; Kulturstyrelsen, 2019) læser de dem "overfladisk", i betydningen snupper det, de kan bruge i deres argumentation. De søger ikke overblik, men argumenter i en "branch method"-forhandling (s. 200-201).

Hvis man skulle bruge Lindbloms ræsonnement til vejledning i mediesituationen, der ikke blot kritiserer politikerne, så kunne man sige, at der måske på DRs område mangler nogle interesseorganisationer og lobbygrupper, der tager forsømte interesser op. Tidligere var der Erhards Jacobsens Aktive Seere og Lyttere, der måske burde genopstå med kontor i Jylland. Danske Medier kan med stolthed arbejde videre. Vi mangler måske også en lobby-gruppe,

der kæmper for et smallere og skarpere public service-ideal. Kunne det være en del af Arbejdernes Erhvervsråd eller Cepos.dk? Måske nogle der kæmper for uden for DK boende danskere, som betaler licens/skat, men som ikke har adgang til udsendelser.

Nissen bruger Lindblom overfladisk. Efter at have nævnt ham, nærmest rituelt, fortsætter han andre steder i bogen i den pseudo-rationelle forestillings- og drømmeverden. Og nogle af anmelderne af bogen læser det som hans hovedsynspunkt.

Allison: Standardrutiner mm. i Finansministeriet og DR

Et andet klassisk navn i politologien er Graham Allison (1940 –). Hans berømte artikel fra The American Political Science Review 1969 har titlen "Conceptual models and the Cuban missile Crisis" (1969). Her præsenterer han tre modeller til forståelse af den amerikanske regerings beslutninger under Cuba-krisen, hvor præsident Kennedy stoppede Sovjetunionens opstilling af raketter på Cuba ved en blokade af de sovjetiske skibe, der var på vej med raketter. Nissen anvender ikke Allisons modeller, men de ligger lige for.

Allisons tre modeller er: *Rational Policy*, *Organizational Process* og *Bureaucratic Politics.*

Rational Policy svarer til "den pseudo-rationelle model", jeg har talt om. Også Allison kritiserer den ad de linjer, jeg har nævnt. Den kan heller ikke bruges til noget i den situation, Allison vil forklare.

Allisons anden model *Organizational Process* peger på det, som Allison kalder "Standard Operation Procedures" (SOP). I Cuba-caset: Flyvevåbnet er dygtigt og vant til at bombe, så de foreslår at bombe de opstillede raketter på Cuba. Flåden kan stoppe skibe, så det foreslår de. Hæren foreslår invasion. Allison citerer nogle sørgmuntre udtalelser herom. Flåden bliver spurgt af forsvarsminister McNamara, om de har check på det med at stoppe skibene, f.eks. om de havde russiske tolke ombord. Flåden svarer nærmest "fuck off" og svinger med deres manual. Kennedy kalder Udenrigsministeriet "en skål grød" (Allison, 1969: 702), som man må forstå, man ikke, i Kennedys optik, kan få et "klart svar" fra for andet end sædvanligt diplomatisk snak.

Nissen har data, der også peger på SOP-adfærd, men han samler dem ikke systematisk: Ser vi på aktørerne i en udvidet forstand: DR har sine standardmåder at reagere på: Mere af det samme mht. formidlingsmåde (flow-tv), afvisning af kritik (offerfortælling). DRs eller i alt fald forfatternes implicitte tænkning kan man få et billede af ved at læse DRs "Service-redegørelse" for 2018 (den seneste) (DR), som også Nissen refererer til. Udsendelser, der kan ses/høres på et andet tidspunkt end det normale programsatte tidspunkt, kaldes "tidsforskudt", dvs. referencen er flow-tv og dets fastdagsprogram. Man tilbyder seerne at "indhente" det, hvis man ikke har været der til den tid, som DR definerer som den rigtige tid at se udsendelserne på. "Liggetiderne" (der berettes som forøgede) er den tid, DR tillader deres udsendelser at være til-

gængelige, som kan ses som byggende på et principsyn om, at ikke alt i DRs store bestand af materialer kan eller bør være tilgængelige eller være genstand for "tilrådighedsstillelse" (s. 7). Et sådant ejerskabs-syn præger ikke udbydere som YouTube og Netflix.

SOP-tankegangen ligner udbredte tanker i organisationsteorien: At organisationer (virksomheder, offentlige og private, foreninger etc.) har en tendens til at stivne over tiden. At gentage sig selv, ikke vise den fornyelse, i produkter og struktur, der skal til på markeder, der ændrer sig. Bernt Bresemann har på dansk udgivet en bog, der beskriver nogle af disse tanker og erfaringer (Bresemann, 2014), såvel fra forskere som fra erfarne konsulenter.

Ofte skal der en ganske sjælden og stærk ledelsesindsats til for at bryde denne organisationsinerti. Helst kombineret med en chokerende udefrakommende hændelse. DR havde sådanne skelsættende oplevelser med Radio Mercur, der sprængte DRs sippede tilgang til ungdommens musik, som den kunne høres i Radio Luxemburg. Og TV2s oprettelse 1987 fik for en tid DR til at oppe sig mht. nyhedsformidlingen. Radio24syv viste i en kort periode, hvordan radio også kan laves.

En løsning, der følger af SOP-tænkningen, kunne være, at der nu igen må etableres en eller flere danske, konkurrerende udbydere af det, som DR nu leverer. Det kan være, at der ikke lige nu er et politisk flertal for det, men det er stadig en principiel mulighed.

Allisons tredje model er *Bureaucratic Politics*. Den har lighed med den forrige derved, at den også ser beslutningstageren som typisk bestående af flere enheder/personer. Men her ses de ikke blot som bærere af enheders standardløsninger (SOP) som i den forrige model, men som konkurrenter om indflydelse og om at få deres egne løsninger igennem. Både på tværs af apparaterne/ministerierne og indenfor disse. Man manøvrerer mod hinanden. Kun i journalistsladder og memoirer kommer oplysninger om denne magtkamp i korridorerne nogle gange frem, skriver Allison. Det kræver, at man dykker ned i forløbet. På side 155-159 har Nissen, ud fra sine interviews, en opstilling af de forskellige politikeres holdning til DR, fordelt efter disses placering til højre eller venstre i politik. Og pengene passer sådan ca. Til venstre vil man styrke DR. Til højre vil man tæmme dem. Men ifølge bureaukratisk kamp perspektivet er højre og venstre ikke det eneste perspektiv, måske slet ikke det væsentligste. Der er også gamle venner og fjender, potentielle partnere.

Allison beskriver også disse bureaukratiske aktører som omgivet af og nærmest stressede af de mange forskellige beslutninger, der skal træffes, og problemer der skal løses. Den enkelte beslutningssituation står sjældent alene og er for den enkelte aktør ikke blot afgrænset til det "store" problem, som skal løses (hos Allison: Sovjets raketter, i denne artikel: Et nyt medieforlig), men også morgendagens møde kl. 8.00, og det man ikke har nået. Der er også andre problemer, der kalder på opmærksomhed. Måske nærmest latterlige delproblemer af det store problem, men med en tidsfrist NU. Alle kæmper deres

små kampe for at komme frem og vise, at de kan. Om ikke andet så ved at stå i vejen for konkurrenten, som man hader af et godt eller mindre godt hjerte.

Nissen kunne have brugt Allisons bureaukrati-perspektiv til at fortælle mere systematisk om Claus Hjorth Frederiksen og hans frustration over DR, om en Jørgen Kleener i klemme. Om Brian Mikkelsen og hans lille strid med den dygtige Lisbeth Knudsen, der har, måske mere eller mindre elsket, været alle prominente steder i medie-Danmark. Og om Brian Mikkelsens og Bertels Haarders mere positive syn på DR. Han kunne have inddraget sig selv, for Nissen skriver ikke blot, hævder jeg, for at forsvare DR, men også for *sin* ære efter fyringen. Nu har han tiden og friheden til at gøre det. Det ville også have givet et bedre metode-perspektiv end den flade tilståelse, at han er "public service biased" (s. 13). Nissen kunne i denne beskrivelse have taget inspiration fra DRs roste serie Borgen, der dækker både den store politik og det personlige element.

James March – Garbage Can og Technology of Foolishness

På bogens "teoriopslag" s. 202-3 nævner Nissen en anden kendt forsker, som bl.a. har beskæftiget sig med beslutninger, James March (1928-2018). Nissen henviser til en til samling af hans artikler (March og Kreiner, 1995), der er oversat til dansk.

Også March har grundigt kritiseret den pseudo-rationelle model, ad de samme linjer, som jeg omtalte ovenfor. Hvad Nissen ikke nævner fra artikelsamlingen, er March's kendte, overvejende deskriptive beslutningsmodel, Garbage Can-modellen, som March blev inspireret til via sit arbejde (og frustration) som ung akademisk leder ved University of California ca. 1968-70 (March og Kreiner, 1995: 87–117).

Skraldespanden (Garbage Can'en) er en beslutningsanledning, noget der sætter beslutninger i gang. Det kan være et møde, et forhandlingsforløb etc. Modellen beskriver et nærmest tilfældigt og anarkisk forløb, hvor beslutninger er resultat af fire delvis uafhængige strømme til den pågældende skraldespand: Indkommende problemer, løsningsideer, deltagere og deres tid og energi. Disse strømme kobles så. Det første problem på dagsordenen, hvor der endnu er tid og energi, kobles måske med det problem, der har domineret i de sidste dage eller år. Og 2/3 af tiden går med det. Måske bliver "problemet" faldende annonceindtægter i de private medier på den måde koblet med DRs størrelse og ekspansion på det private område. Er der aktører til stede, der har tid og energi til at forfølge sagen, kan det føre til en "beslutning" eller snarere et "outcome", som March foretrækker at kalde det. Beslutningen om at flytte Radio24syvs redaktion til Aarhus var vist et sådant, nærmest tilfældigt outcome i sidste øjeblik af forhandlingerne. Sidst i møderne og forhandlingerne, hvor alle er kørt trætte, kan de mærkeligste beslutninger komme igennem. Nu vil man bare hjem.

Ifølge March er der normalt flere skraldespande aktive på én gang (andre forhandlinger etc.), som deltagere, problemer og løsninger kan flygte til, hvis de ikke er "tilfredse" i den første spand. De praktiske råd til beslutningstagere efter denne model er vedholdenhed og energi. Tag din sag op i alle sammenhænge og spande, uanset om de hedder noget andet. Hævd uden blusel, at din løsning også er relevant her.

Nissen kunne også have ladet sig inspirere af March artikel om The Technology of Foolishness, der bygger på den grundantagelse, at vore formodede mål og standardløsninger (SOP!) ofte er del af problemet (March og Kreiner, 1995: 71–85, her er Marchs begreb oversat til »fjolleriets teknik«). Vi undersøger dem ikke. Vi har brug for at lære nye mål at kende gennem eksperimenter eller tilfældige valg.

Skulle man drage nogle praktiske råd fra Technology of Foolishness, kunne det være et forslag om, at man skal give en klatskilling til hver højskole, så de kunne "lege radio eller tv". Måske skulle DR af egen drift, som YouTube, åbne for, at man modtog "hjemmelavede" videos fra brugere, måske kun fra danske skattebetalere, og efter en vis selektion, men ikke *for* tæt, for det skal ikke alt være "normalt" DR-stof og "kvalitet", der tilbydes gennem dette særlige mediatek. Det meste ville sikkert være vrøvl og amatørisme, men hvem ved, hvad seerne ville mene? En mulighed var også at åbne for skriftlige kommentarer fra brugerne til bestående mediatek-tilbud. Igen redigeret, måske af eksterne tillidspersoner, for at undgå de ofte meget hadske kommentarer dette kan medføre.

Socialkonstruktivistisk beslutningstagen

En sidste, endnu mere anarkistisk og nærmest dystopisk beslutningsforståelse, kunne man kalde "socialkonstruktivistisk beslutningstagen". Nissen anvender ikke begrebet, og det findes ikke i litteraturen. Men for mig synes det en oplagt (om end ekstrem) forståelse af forhandlingsforløbet, som Nissen beskriver i kapitel 8:

Målene er uklare, men til fri anvendelse og fortolkning. Positive mål er noget, man hæfter på beslutninger, man kan lide. Og hvis vi mere med Lindblom og March ser "problemer" som igangsættere af beslutningsprocesser, så er også disse socialt konstruerede. Hvad er egentlig et problem andet end, at det står i omtalt avisen eller hos DR som et sådant? Tilsvarende med data og facts f.eks. fra undersøgelser etc. I hvert fald bruges de selektivt af beslutningstagerne, der piller det ud, der passer i deres argumentation. Administrationen svarer med henholdende tågesnak, når politikere på den forkerte side spørger.

Resultaterne af beslutningerne, her det besluttede medieforlig, er heller ikke noget givet, men er også til fri fortolkning – giver det det ene eller andet? – mere marked, mere demokrati, mere plads til de private, styrker eller fastholder det danskheden, som både DF, flere anmeldere og Nissen mener. Ingen anfægter det. Eventuelle beslutninger og forlig holder ikke sæsonen ud. Nu er

gevinsterne om nogle høstet. Implementeringen er noget andre må tage sig af og høste æren eller bebrejdelser for. Medieforliget blev delvis skrottet af en ny regering. Så kan maskinen køre igen, måske med de gamle problemstillinger, måske med helt nye, som er varme på det nye tidspunkt, måske med gamle eller nye løsninger og deltagere.

Hvis politik er eller opleves på denne dystopiske måde, kan det føre til fremmedgørelse over for det politiske. Måske er det særligt sandsynligt i diktaturer. Man trækker sig tilbage til det private, til glæden ved fuglenes sang, kærligheden til og fra de nærmeste og underholdningsudsendelser i TV. De politiske er for nedtrykkende.

Jeg har svært ved at foreslå konstruktive forbedringer ud fra dette.

Dog ser det ud til, at samfund sommetider eller ofte overlever sådanne dystopiske systemer. Måske bekymres vi blot, fordi vi deler vestlige samfunds overdrevne tro på, at uden ledelse og styring går det hele galt. I Middelalderen overlevede man, vel uden nogen større samlet styring, mens man i enkelte klostre dyrkede skrivekunst og den klassiske litteratur, som derved blev tilgængelig for os. Man kan også notere, at Mette Frederiksen-regeringen vist ikke har lavet et nyt medieforlig eller resultatkontrakt, men verden forsætter, og DR sender.

Nogle gange er de problemer, som det politiske er brændende optaget af, nogle, som forsvinder igen. Enten var de forkerte, eller andre og større problemer tager over, og selvom vi ikke har "løst" de gamle problemer, glemmer vi dem.

Som et eksempel på problemstillinger, der på et tidspunkt optog den nationale politik glødende, er dansk forsvarspolitik i 1930'erne. Hvis vi holdt lav profil og ikke provokerede Hitler, regnede nogle med, at vi ikke ville blive udsat for aggression fra Hitler, mens andre mente, at vi kunne afværge Hitler med oprustning. I dag mener jeg, at historieforskningen fortæller os, at det var ret ligegyldige problemstillinger, fordi Danmark blev besat af andre grunde: Hitler ville sikre sig Norge for at undgå en søblokade som i Første Verdenskrig. Først ville han kun besætte Ålborg flyveplads og omgivelser, men kort før besættelsen ændrede man det til hele Danmark, da man vist mente, at det var for bøvlet at have et frit Danmark og et besat. Tilsvarende med de mange blodige diskussioner og krige om Sønderjylland. I dag kan vi se, at det heldigvis også er en ubetydelig problemstilling, hvis et EU udvikler sig som en ny identitet og system, hvor det er ret ligegyldigt, hvor man bor, og hvilket sprog man taler (og for resten: hvilket TV man ser).

Nissen henviser overfladisk til to teoretikere (Lindblom og March). Jeg har føjet nogle til for at vise, at der ville have været flere muligheder. Det er ikke min ide, at Nissen skulle have anvendt flere, men at han havde valgt nogle, gerne andre, og var gået i dybden med dem. Der kunne på den måde, mener jeg, være kommet en mere spændende og holdbar bog ud af det.

Max Weber – politik mellem følelser og fornuft – den høje teoriklinge

Nissen skriver i bogens konkluderende kapitel s. 296f: "Bogens analytiske vinkel på politikdannelse "mellem følelser og fornuft" har forhåbentligt bidraget til en forståelse af disse afgørende svagheder [ved medieforliget]."

For de boganmeldere, jeg citerede i denne artikels begyndelse, er dette håb ikke gået i opfyldelse. De har forskellige opfattelser af nytten ved begreberne og også af, hvad Nissen vil sige med dem. Én mener, at begreberne ikke kaster noget af sig. En anden, at de er påhæftede hans argumentation. To mener, at de skal forstås sådan, at politikerne er for følelsesstyrede og ignorerer facts og rationel fornuft. Kun en enkelt synes at nævne det, som Nissen vist mener. Dette sørgelige resultat kan have flere årsager. Måske har disse dygtige anmelderne haft for travlt. Måske er Nissen flertydig ved, at han i sin beskrivelse af forhandlingsforløbet tit henviser til (se ovenfor, samlet under min model "socialkonstruktivistisk beslutningstagen"), hvordan politikerne kun læste og brugte de elementer i sagkyndige rapporter mm., som passede ind i deres kram. (Også selvom Nissen selvegen har været med til at præge en af dem). Hans tydelige frustration herover i nogle passager af bogen kan have fået nogle anmeldere, jf. ovenfor, til at tro, at mere fornuft og saglige undersøgelse er Nissens hovedbudskab.

Hvad mener så Max Weber?

S. 195ff søger Nissen at forankre følelser-fornuft begreberne hos den tyske sociolog/politolog Max Weber (1864-1920).

Forenklet sagt er Nissens udsagn, at *både* følelser og fornuft er nødvendige i politiske spørgsmål som f.eks. omkring medieforliget. Specielt manglede forhandlerne følelser i betydningen visioner. S. 197 citerer Nissen følgende fra Max Weber:

»Problemet er, hvordan varme, lidenskab og fornuft kan smedes sammen i en og samme sjæl. Politik skabes med hovedet, ikke med andre dele af kroppen eller sjælen. Og alligevel kan engagement i politik, hvis det ikke blot skal være en letfærdig intellektuel leg, men snarere virkelig menneskelig adfærd, alene fødes og næres af lidenskab.«

Kilden er en anerkendt amerikansk oversættelse fra Webers original på tysk, som Nissen så oversætter til dansk. Den originale version af udtalelsen findes i artiklen Politik als Beruf (Weber, 1971b: 546). Jeg bruger i det følgende forkortelsen PaB som henvisning til denne tyske original. Nissen har ikke været opmærksom på den udmærkede danske oversættelse af Webers foredrag (Kaspersen m.fl., 2003). Den afgørende mangel ved Nissens oversættelse er, at Weber, hverken i originalen eller i den danske oversættelse, anvender ordet "fornuft", altså et af Nissens nøgleord.

I en figur på samme side som Weber-citatet (s. 197) beskriver Nissen sin opfattelse af begrebet "fornuft" som "rationelle valg", dvs. den beslutningsmodel, som jeg tidligere kaldte "den pseudo-rationelle model". På den følgende side giver han et eksempel på sådan fornuft, nemlig Finansministeriets Adam-model.

Her tager Nissen inspireret af sin fejloversættelse fejl: Weber tænker i PaB *ikke* på "den pseudo-rationelle beslutningsmodel" a la Adam-modellen. Weber beskriver ganske vist andetsteds, at kapitalismen udvikler en rationaliserings- og planlægningskultur, hvor mange ting sættes på tal. Næsten som i vore dages kritik af djøffere og vores formodede afhængighed af tal og Excel-ark (Larsen, 1979). Men dette Weberske rationalitetsbegreb er højst en meget fjern fætter til det fornuftsbegreb, Weber benytter i PaB. I den tyske original anvender Weber ordet "Augenmaß". I den nævnte danske oversættelse "øjemål" i betydningen hensyn til fremtiden, "balance" eller "ikke-ekstremisme" jf. nedenfor.

PaB-teksten bygger på en tale, Weber holdt i München 28.1.1920 (Kaesler, 2014: 28), altså ret kort efter afslutningen af Første Verdenskrig. Tilhørerne var en gruppe venstreorienterede studerende. En revolution var som i andre dele af Tyskland i gang uden for foredragssalen. Da Webers noter til talen for nogle år siden dukkede op på en auktion, blev det hævdet, at Weber oprindeligt ikke ville deltage, men da studenterne så truede med at invitere lederen af revolutionsregeringen i München, Kurt Eisner, som Weber opfattede som en useriøs politiker (Kaesler, 2014: 892), stillede Weber op. Eisner blev mindre end en måned efter foredraget myrdet af en 22-årig højreorienteret aktivist (Seibt, 2010). Rosa Luxemburg, der kritiserede socialdemokratiet fra venstre, var i Berlin blevet myrdet 13 dage før. (Politik var på den tid andet end 5 procents-besparelser). Noterne bestod i øvrigt kun af otte uordentlige stikordssedler. Den senere udgivne tekst er baseret på et stenografisk referat, som Weber før publiceringen redigerede, men som dog stadig er ret rodet og præget af sted og situation. Den udgivne længde er på 55 tættrykte sider, så studerende må have været hårdføre i disse pre-Power Point tider.

Weber var ved Første Verdenskrigs udbrud i 1914 begejstret for krigen som den overvejende del af befolkningen i Tyskland. Under krigen blev han mere skeptisk og advarede mod handlinger, der kunne gøre krigen svær at slutte på en værdig måde og på en måde, der ville være fremmende for et samarbejde med de tidligere fjender. F.eks. argumenterede han – uden held – imod den totale U-bådskrig i Atlanten, der bl.a. førte til sænkning af passagerskibet Lutisania, der igen førte til USA's indtræden i krigen og derved gjorde det vanskeligt for Tyskland at få en mild fred, hvad de som bekendt heller ikke fik.

Politik – leve af eller leve for?

"Beruf" har på tysk to betydninger, som inspirerer Webers artikel. Beruf betyder erhverv, job = noget, man lever *af* (nok den dominerende betydning i dag). Men Beruf betyder også = noget man lever *for*, føler sig kaldet til, både i

religiøs betydning, men også i betydningen noget, man ønsker at udføre, kan identificere sig med.

De første 40 sider af PaB giver et overblik over politik-erhvervets udvikling med eksempler fra Tyskland, USA, UK og Frankrig. Det var nok noget, Weber havde "på lager". En *meget* kortfattet opsummering kan lyde: "Politikere" var først fyrster, jordbesiddere, rige og veluddannede, dvs. overklassen og derved også ret uafhængige. De var der måske i et parlament eller lignende for at kontrollere en konge. Senere blev politiker-job en vej til at skaffe goder til familien, klanen, partiet, egen religiøse gruppe eller regionen, der valgte ham eller hende. På dansk har jeg for nylig set udtrykket "klanpolitiker", som i mange udviklingslande er dominerende, og som der i Danmark stadig er få spor af (stikord: jysk motorvejsmafia). En senere tid (i vestlige lande) bød på en underordnet rolle som stemmekvæg. Jeg har set ord på dansk som "levebrødpolitiker" og "karrierepolitiker" om disse politikere.

Selvom Weber bruger mange sider på dette og er ganske kritisk, også over for den tyske situation før krigen, hvor parlamentarikerne efter hans mening generelt var for tamme, er det ikke job-siden af politik i sig selv, som bringer hans blod i kog i foredraget og situationen.

Det, der bekymrer ham, er afvigelser fra den gyldne midte især mht. politik som kald. Weber forklarer denne bekymring ved hjælp af udtrykkene a) *Verantwortungsethik*, som man kan fordanske som *ansvarlighedsetik* eller *realpolitik* (mit ord) og b) *Gesinnungsethik*, som man kan fordanske som *sindelagsetik* eller *idepolitik* (mit ord). Weber ser disse begreber som klare idealtyper, der teoretisk udelukker hinanden, men i praksis kan og bør gode politikere, i hvert fald i parlamenterne, have træk af begge. Men det kan være svært, for de kan være under tæt kontrol af indpiskere og gruppeformænd. Weber mener derfor også, at der sommetider kan formuleres mere visionær politik udenfor end i parlamenterne. Journalister kan f.eks. gøre det, og det skriver Weber anerkendende om. Samt f.eks. ansatte i interesseorganisationer. Eller forskere, der som Weber selv optræder i debatten, f.eks. med PaB-foredraget.

Ansvarlighedsetik, som Weber i foredraget og mht. situationen uden for foredragssalen nok foretrækker, bygger på overvejelser om, om noget er realistisk, kan lade sig gøre, har negative sidevirkninger. En ansvarlighedsorienteret politiker ved, at verden ikke altid er, som vi håber. Der er bivirkninger af den ideale politik. Der er fjender og modstandere. Der er aktører, og de eksisterer måske også efter beslutningen. Det kalder Weber for at have "øjemål" i politik. Ansvarlighedsetik er også at blive ved, kæmpe videre, acceptere nederlag, når nødvendigt – politik er som at bore i hårdt træ. Man skal kunne tåle, når man kritiseres for ikke at have nået mere (PaB: 560, artiklens afsluttende sætninger).

Sindelagsetik betyder, at politikeren tager udgangspunkt i mål og visioner. Det er nødvendigt med mål og visioner, men Weber vil understrege, at i sin *ukonstruktive* form kan det blive til: Målet helliger midlet. Alt der ikke fører

til målet og som ikke realiserer målet fuldt ud på Thunbergs vis af den ukonstruktive, idepolitiker. Her er parallellen til hans kritik af den uindskrænkede U-bådskrig.

Fra begyndelsen af PaB understreger Weber, at han med sine definitioner ikke søger at beskrive, hvilken indholdsmæssig politik der er tale om (PaB: 505). Også morderen Hitler må efter denne opfattelse klassificeres som (en ukonstruktiv) sindelagspolitiker, der krævede alt eller intet og rev sig selv, millioner af mennesker og nationen med i ødelæggelsen. Weber kendte vist ikke Hitler, som dog på dette tidspunkt allerede var i München og ved at gøre karriere i DNSAP, og som nogle få år senere sad i byens fængsel og skrev "Mein Kampf". Weber kendte selvfølgelig Eisner og regnede ham med til de ukonstruktive og ikke få af de tilsvarende og samtidige revolutionære i Berlin og i Rusland, kommunister, anarkister og voldsfanatikere.

Weber citerer til beskrivelse af ukonstruktiv sindelagspolitik/idepolitik sociologen Simmel (PaB: 545) for udtrykket "steril ophidselse". Og føjer ord (PaB: 547) som "selvberuselse", "usaglighed", "ansvarsløshed" (her: min oversættelse) og "letfærdig intellektuel leg" (i det citat Nissen anfører) til. Det er folk, der brokker sig "på gammel kvindevis" over tab f.eks. i krigen, og som er optaget af skyld, helst hos andre, men også hos sig selv, snarere end at tage fat på: Hvad gør vi nu for at komme videre? (PaB: 549).

Dansk politik har været i stand til tidligere at vise dette Weberske øjemål. F.eks. ved efter begge verdenskrige ikke at kræve for meget mht. Sønderjylland/Slesvig. Også selvom der var vilde idepolitikere, der ønskede det. At Danmark og Tyskland er og forbliver naboer, må konstruktive idepolitikere tage hensyn til.

I tabel 1 nedenfor har jeg sammenfattet Webers hovedargumentation, som jeg har ridset den op her i teksten plus et par fabuleringer ud fra Webers tankegang.

Tabel 1: Øjemålet: Den gyldne midte i politik

Politik = job, lever *af*	**Politik = kald, lever *for***	
Ukonstruktiv job-politiker	Øjemålet. Den gyldne midte	Ukonstruktiv idepolitiker
Jobbet bruges til at skaffe fordele til sig selv, familien, klanen, partiet, egen religiøse gruppe, hjemregionen.	Kombination: At man i jobbet også ser et kald. At man i kaldet ser problemerne. Kombination af ansvarlighedsetik (realpolitik) og sindelagsetik (idepolitik). Dvs. en sindelagsetik, der er tæmmet af ansvarlighed.	Målet helliger midlet. Ædel hensigt antages altid at føre til noget godt. Alt eller intet-holdning. Steril ophidselse. Letfærdig intellektuel leg.
I øvrigt stemmekvæg, der gør som gruppeformand og indpisker kræver.	Øje for afbalancering af muligheder *og* konsekvenser. Der er en dag efter denne.	Fremtidige magtkonstellationer og konsekvenser ignoreres.
Spørger andre: Hvad skal jeg gøre nu?	Spørger sig selv: Hvad skal vi gøre nu for at komme videre?	Klager. Anklager sig selv og andre. Går af, hvis det ikke lykkes. "Så kan det være det samme."
Kræver evne til at tåle at være usynlig, undtagen over for de få, man leverer goder til.	Kræver evne til at leve med kritik fra ukonstruktive idepolitikere, der kræver alt eller intet. Men også en forståelse for, at det kan være farligt at demonstrere sit idepolitiske talent for meget.	Kræver evne til at overleve efter en mulig succes(bog), når den overhales af nye bøger, ideer og situationer.

Alt i alt er det Webers opfattelse, at »fornuft« er et »*øjemål*«, en balance mellem det ideelle og det mulige, ikke pseudo-rationel beslutningstagen.

»*Følelser*», som Nissen i positiv forstand *gør central i sin analyse,* bruger Weber *næsten udelukkende i PaB og* i hans andre politiske tekster i en negativ betydning om farlige ekstremister og ukonstruktive idepolitikere (Weber, 1971a: 122, 149, 159, 170, 457).

Kan vi forbedre det politiske system?

Problemet med idepolitikken i et demokrati er måske ikke de individuelle politikere, men at der (som Weber antyder i sin historiske analyse) i forholdstalsvalgsystemer kombineret med en lav spærregrænse er "for mange" partier og "for mange ideer". Kun i nødsituationer og ved udefrakommende pres, en besættelse eller farlig epidemi finder man ud af at stå sammen om nogle næsten fælles mål.

Man kunne derfor også – ud over at beklage sig over de politikere, vi har – undersøge de, mener jeg, ret mange tilfælde, hvor danske politikere med et idepolitisk temperament og realpolitisk erfaring forlader politik eller måske direkte drives ud. Er det deres partiorganisationer og disses pampere, som driver dem ud? Er det de rammevilkår, disse politikere må arbejde under, de roller, de tilbydes, der får dem til at føle, at det er for småt, det her? Er det den kritik udefra, de får? Fra Danmark kunne man måske nævne skikkelser som Søren Pind og Uffe Elbæk (to nævnt, mange glemt). Mette Bock, der har været hos Kaospiloterne, i DR og andre interessante steder (s. 170), og som

nu fortælles at ville være præst, kunne være et supplerende eksempel. Men man måtte også forholde sig til, hvorfor og hvordan en Bertel Haarder har overlevet så længe.

Konklusion om Nissens brug af Weber: Nissens brug af ordene følelser og fornuft svarer ikke til Webers brug af disse ord, selvom den har mindelser herom. Det er i sig selv ok. Nissen kan naturligvis analysere sine data ud fra *sit* begrebspar, som han vil. Men heller ikke det lykkes, hverken i mine eller de fleste anmelderes øjne, så det giver mening. Og han kan ikke smykke sig med, at hans begreber stammer fra Max Weber. Man kan man med et udtryk fra litteraturen kalde Nissens henvisning til Weber for *ceremoniel* (Lounsbury and Carberry, 2005), dvs. henvisning til en klassiker, uden at denne kendes eller bruges. Man kunne også bruge værre ord.

» Man kan man med et ord fra litteraturen kalde Nissens henvisning til Weber for ceremoniel

Konklusion – interessant bog med bias, overfladisk teoribrug og moralisering

Nissens bog er velskrevet, med mange gode problemstillinger og data. Desværre er den også et ensidigt forsvarsskrift for det gamle DR, præget af hans utilfredshed med en regering, der fyrede ham. Ensidigheden består i en biased beskrivelse af vilkårene omkring DR og af DR. Den teoretiske analyse, som Nissen lover os via sin baggrund, er overfladisk. Hans brug af Weber er forkert. Han moraliserer over politikerne i forliget, men spørger ikke, hvad vi mere systematisk kunne gøre ved det.

Noter

1 Bøje Larsen skriver om sig selv: Jeg er organisationssociolog og historiker. Mere på min hjemmeside www.kbl.dk. Bor nu i Berlin, og selvom jeg har nostalgiske følelser for dk, har jeg udviklet en vis skepsis overfor for stærke dansk-nationalistiske ideer, som forekommer i DK og i Nissens bog. En anden bias fra min side kan hænge sammen med, at Nissen viste mig den tillid at sende dele af sit manus til sin bog til mig for kommentarer, hvor jeg nævnte nogle af de vinkler, denne artikel tager op. Det blev ikke til en konstruktiv idémæssig dialog, hverken for ham eller mig. Desværre.

2 Tak til Torsten Skov og Peter Aagaard for kommentarer til tidligere versioner af denne artikel.

Litteratur

Allison, G.T. (1969), 'Conceptual Models and the Cuban Missile Crisis', *American Political Science Review*, 63(3): 689–718.

Bresemann, B. (2014), *Turnaound Management. Fra ledelsessvigt til genopretning*, København: Bernt Bresemann.

DR (2018), 'DR's Public Service-Redegørelse'. Tilgængelig på: https://www.dr.dk/om-dr/fakta-om-dr/publikationer.

Farag, M., Bolton, D. og Lawrentschuk, N. (2020), 'Use of YouTube as a Resource for Surgical Education – Clarity or Confusion', *European Urology Focus*, 6(3), pp. 445–9.

Kaesler, D. (2014), *Max Weber. Eine Biographie*, München: C.H Beck.

Kaspersen, L.B., Andersen, H., og Bruun, H.H. (red.) (2003), *Max Weber: Udvalgte tekster*, bind 1, København: Hans Reitzels Forlag.

Kern, H.L. og J. Hainmueller (2009), 'Opium for the Masses: How Foreign Media Can Stabilize Authoritarian Regimes', *Political Analysis*, 17(4): 377–99.

Kulturministeriet (2016), 'Public Service – De næste ti år', *Rapport fra Public Service udvalget*, pp. 1–5.

Larsen, B. (1979), 'Max Webers bureaukratianalyse: Misforståelse og muligheder', *Økonomi & Politik*, 52(1): 36-64

Lindblom, C.E. (1959), 'The Science of "Muddling Through"', *Public Administration Review*, 19(2): 79–88.

Lindblom, C.E. (1965), *The intelligence of democracy: Decisionmaking through mutual adjustment*, New York: Free Press.

Lounsbury, M. og E.J. Carberry (2005), 'From king to court jester? Weber's fall from grace in organizational theory', *Organization Studies*, 26(4): 504–25.

Lüthi, L.M. (2015), 'How Udo wanted to save the world in "Erich's lamp shop": Lindenberg's concert in Honecker's East Berlin, the NATO Double-Track Decision and Communist Economic Woes', *Contemporary European History*, 24(1): 83–103.

March, J.G. og K. Kreiner (1995), *Fornuft og forandring – Ledelse i en verden beriget med uklarhed*, København: Samfundslitteratur.

Nissen, C.S. (2007), *Generalens veje og vildveje – 10 år i Danmarks Radio*, København: Gyldendal.

Nissen, C.S. (2020), *Politik mellem følelser og fornuft. Spillet om danske mediers fremtid*, København: Gyldendal.

Nye, J.S. (2008), 'Public diplomacy and soft power', *Annals of the American Academy of Political and Social Science*, 616(1): 94–109.

Seibt, G. (2010), 'Max Webers "Politik als Beruf". "Ich kann nicht anders."', *Süddeutsche Zeitung*, 17. maj.

Slots- og Kulturstyrelsen (2019), *Mediernes udvikling i Danmark*, København.

Weber, M. (1971a), *Gesammelte Politische Schriften*, Tübingen: J.C.B. Mohr (Paul Siebeck).

Weber, M. (1971b), 'Politik als Beruf', i *Gesammelte Politische Schriften*. Tübingen: J.C.B. Mohr (Paul Siebeck), pp. 505–60.

Det internationale Folketing og muligheden for diplomatisk koordination

Temanummer: Cybersikkerhed

Som så mange andre parlamenter har Folketinget gjort sig bemærket som en aktiv international aktør. Selvom udenrigspolitik formelt er et regeringsanliggende, er kontakten til udlandet en fast del af arbejdet i Folketingets udvalg, delegationer, partier og Præsidium. Dette "parlamentariske diplomati" opererer til tider uafhængigt af, men oftest i koordination med Udenrigsministeriet, der bl.a. bistår i planlægningen af udvalgsrejser. I denne kronik diskuteres, hvorvidt et mere strategisk samarbejde kan føre til en bedre udnyttelse af den diplomatiske kapacitet. Historien viser, at samarbejde mellem det ministerielle og det parlamentariske diplomati kan fungere godt, men at en balancegang kræves for at sikre, at hverken Folketingets autonomi eller regeringens udenrigspolitiske prærogativ sættes over styr. Tilrettelægges det ordentligt, kan et samarbejde dog være fordelagtigt for såvel Folketinget som for regeringen og Udenrigsministeriet.

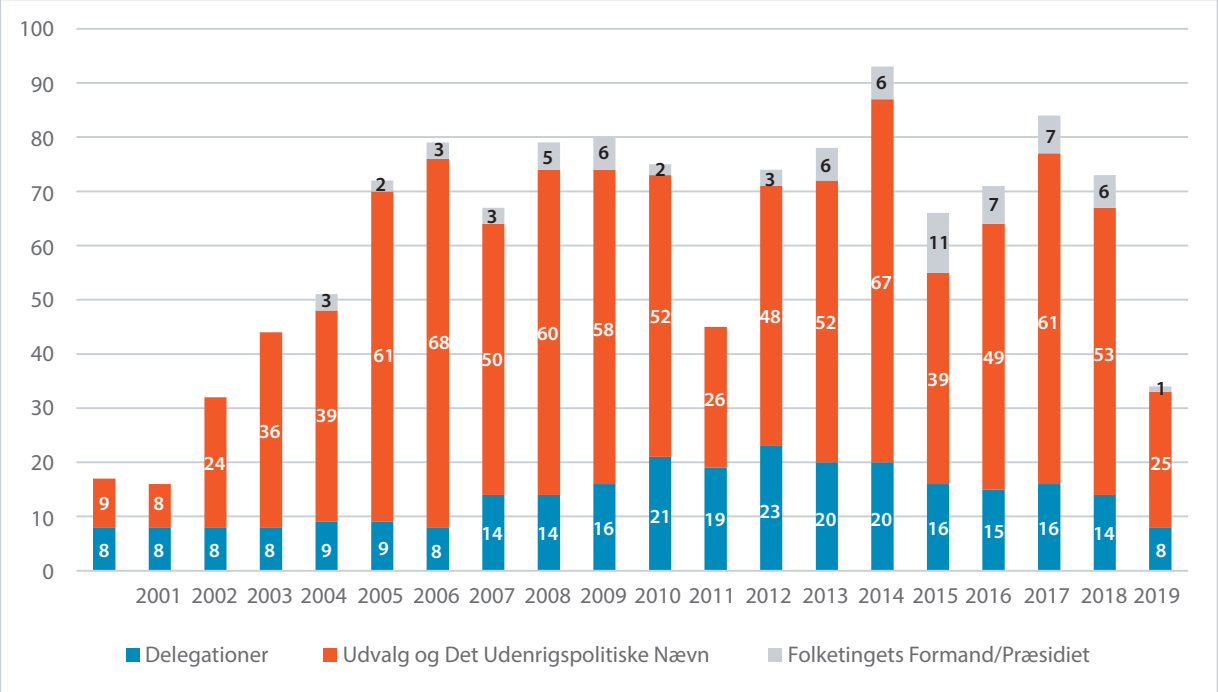
VIKTOR LERCHE-JØRGENSEN LASSEN
cand.scient.pol.,
viktorlassen@hotmail.com

I takt med at skellet mellem indenrigs- og udenrigspolitik udviskes, flere beslutninger tages i internationale institutioner og private aktører i visse tilfælde overgår stater i økonomisk betydning og realpolitisk indflydelse, mister Udenrigsministeriet sin traditionelle rolle som gatekeeper mellem ind- og udland. Diplomatiets funktioner "siver ud af udenrigsministerierne" og overtages af andre ministerier, såvel som ikke-statslige aktører, herunder byer, virksomheder og NGO'er (Marcussen, 2013).

I Danmark er en del af diplomatiet også sivet ind i Folketinget. Ifølge Grundloven repræsenterer regeringen riget i mellemfolkelige anliggender. Folketingets samtykke er påkrævet i visse udenrigspolitiske spørgsmål, og det Udenrigspolitiske Nævn har krav på at blive konsulteret "forud for enhver beslutning af større udenrigspolitisk rækkevidde". I udgangspunktet er mellemfolkelige anliggender dog regeringsanliggender, der i henhold til Udenrigsloven varetages af udenrigstjenesten.

Ikke desto mindre har også Folketinget taget en del af den diplomatiske métier til sig og praktiserer såkaldt parlamentarisk diplomati (Stavridis og Jančić, 2016). Det er ikke et nyt fænomen. Allerede i 1889 var Frederik Bajer (V) sammen med parlamentarikere fra otte andre lande med til at stifte Den Interparlamentariske Union (IPU) som et tværnationalt forum, hvor parlamentarikere kunne arbejde for dialog og fredelig bilæggelse af internationale konflikter. Det var bl.a. med til at sikre ham Nobels Fredspris i 1908.

Figur 1: Årligt antal udlandsrejser foretaget af Folketingets delegationer, udvalg (inkl. Det Udenrigspolitiske Nævn) og Formanden/Præsidiet



Kilde: Lassen (2020).

I dag er en stor del af Folketingets arbejde orienteret mod udlandet. I perioden fra år 2000 til og med 2019 er der registreret mere end 1.200 udlandsrejser i Folketingets rejsekalender (figur 1). Siden Radioudvalget foretog Rigsdagens første udenlandske udvalgsrejse i 1925 (dog ikke længere end til Malmö), er studieture blevet en fast del af udvalgsarbejdet. Men rejser er mere end blot en mulighed for at indhente inspiration og erfaringer til brug i det parlamentariske arbejde på Christiansborg. Det er også en mulighed for at repræsentere folkestyret udadtil.

Det sker især i de interparlamentariske forsamlinger, hvor Folketinget er repræsenteret, som typisk træder sammen et par gange om året. IPU er siden Frederik Bajers tid vokset til at omfatte 179 nationale parlamenter, hvorfor forsamlingen til tider omtales som en parlamentarisk pendant til FN's Generalforsamling. Siden 1952 har medlemmer af Folketinget og de øvrige nordiske parlamenter arbejdet for regionalt samarbejde i Nordisk Råd. Folketinget er også repræsenteret i Europarådets, NATO's og OSCE's respektive parlamentariske forsamlinger, der i sin tid blev oprettet for at sikre, at bl.a. det menneskerets- og sikkerhedspolitiske samarbejde ikke kun foregik på regeringsniveau. I EU har Lissabontraktaten givet de nationale parlamenter nye muligheder for at samarbejde med hinanden og med Europa-Parlamentet, hvor Folketingets sekretariat har en medarbejder fast udstationeret. Folketinget er desuden repræsenteret i det arktiske parlamentssamarbejde og har efter seneste valg derudover fået en fast arktisk delegation.

Folketinget og dets organer repræsenterer ikke i formel forstand Danmark under udlandsbesøg. Men interessen for at møde de parlamentariske repræsentanter er stor, når eksempelvis Folketingets Formand eller Det Udenrigspolitiske Nævn kommer på besøg. Efter regenten er Formanden den næstøverst rangerende i Danmark, og selv om der til daglig ikke følger stor politisk magt med posten, tæller den slags i diplomatiets verden. Det så man især, da Mogens Lykketoft (S) nærmest omdannede formandsposten til en parlamentarisk udenrigsministerpost og mødtes med en talløs række af repræsentanter – fra statsledere til menneskeretsaktivister – på Formandskontoret og på besøg rundt om i verden. Det Udenrigspolitiske Nævn bliver jævnligt taget imod af beslutningstagere på regeringsniveau, der dermed ofte får mulighed for at møde forhenværende såvel som mulige fremtidige danske stats- og udenrigsministre.

Desuden opretholder også de enkelte partier hver især forbindelser, f.eks. til søsterpartier i udlandet. Udenlandske diplomater i København har nogle gange fundet det svært at få folketingsmedlemmerne i tale (Marcussen og Nielsen, 2019). Men ved at invitere individuelle folketingsmedlemmer på besøg i de respektive lande, er det lykkedes bl.a. det amerikanske, franske og taiwanske udenrigsministerium at skabe kontakt.

Koordination mellem klassisk og parlamentarisk diplomati?

Udenrigsministeriet har altså ikke monopol på kontakten til udlandet. I stedet forsøger ministeriet i dag at koordinere internationale aktiviteter, både på tværs af ministerier og sammen med kommuner, erhvervsliv og NGO'er.

Også det parlamentariske diplomati udøves i mange henseender i koordination med Udenrigsministeriet. Ambassaderne bidrager til planlægningen og afviklingen af udvalgsrejser. Ambassaderne har til gengæld mulighed for at bede udvalgene om at tage konkrete problemstillinger op på vegne af danske virksomheder (ERU, 2013). Ministre inviterer udvalg med på eksportfremstød og på besigtigelsesture af Danmarks bistandsindsats. Folketinget er hvert år repræsenteret i den danske delegation til FN's Generalforsamling og ved FN's Klimatopmøder.

For at få det fulde diplomatiske udbytte ud af Folketingets rolle som international aktør har flere foreslået at opgradere koordinationen mellem det klassisk ministerielle diplomati og det parlamentariske diplomati til et mere strategisk niveau. Ambassadør Peter Taksøe-Jensen forslår i sin udredning af dansk udenrigspolitik, at Folketinget kan "koordinere sine internationale aktiviteter, herunder udvalgsrejser, mere aktivt med elementerne i den nationale udenrigs- og sikkerhedspolitiske strategi og med timingen for eventuelle danske indsatser" (Taksøe-Jensen, 2016: 89).

Forhenværende udenrigsminister og medlem af Folketinget Holger K. Nielsen har efterspurgt større vidensdeling og opfordret Udenrigsministeriet til aktivt at bruge Folketinget dér, "hvor den diplomatiske etikette gør det vanskeligt for

regeringen at operere. Det gælder f.eks. i kontakten til oppositionsbevægelser, menneskerettighedsforkæmpere, nationale mindretal m.v." (Nielsen, 2020: 173). Nielsen nævner selv som eksempler Folketingets modtagelse af Dalai Lama og et besøg i Tyrkiet i forbindelse med fængslingen af kurdiske parlamentarikere. Også i EU og de øvrige medlemsstater diskuteres potentialet for en synergieffekt ved at forbinde diplomatiske indsatser på parlaments- og regeringssiden (Zamfir, 2019).

I Danmark er den slags ikke uden fortilfælde. Selvom udenrigspolitik alle dage har været et regeringsanliggende, er der tradition for, at det parlamentariske og det ministerielle diplomati væves sammen. Allerede i 1918 blev Rigsdagens partier inviteret til at deltage i den delegation til Reykjavik, der på Danmarks vegne skulle forhandle om Islands selvstændighed. Konservative afstod, men både Socialdemokratiet og Venstre sendte delegerede, der sammen med handelsminister Hage (R) hver især fik betydelig direkte indflydelse under forhandlingerne (Duedahl, 2006). Året efter var alle Rigsdagens partier repræsenteret, da vilkårene for Sønderjyllands genforening skulle fastlægges på Versailleskonferencen. Udenrigsminister Scavenius (R) var gået med til at lade hvert parti udpege en delegeret, efter det trods uenigheder var lykkedes partierne og de sønderjyske repræsentanter at formulere en fælles forhandlingsposition (Jørgensen, 1970: 254).

I 20'erne og 30'erne blev Danmark et foregangsland for parlamentarisk deltagelse i Folkeforbundet. Sammen med Schweiz var Danmark det eneste land, der havde parlamentarikere med til samtlige regulære sessioner (Götz, 2016: 266) og traditionen fortsatte i FN efter Anden Verdenskrig. Hvor mange lande udelukkende lader sig repræsentere af deres regering og karrierediplomater, har Folketinget fra starten været repræsenteret i den danske delegation til FN's Generalforsamling, hvor de i mange år havde stor direkte indflydelse.

I 60'erne førte den parlamentariske indflydelse til debat. Da SF udpegede Kai Moltke som sin delegerede, fik det eksempelvis Dagbladet Information til at spørge, "om det kan være formaalstjenstligt at lade en overbevist modstander af den hidtidige danske udenrigspolitik repræsentere den danske regering. Kai Moltke vil givetvis ikke føle sig forpligtet til at undlade at give udtryk for sine meninger i udvalgene" (Information, 1961). Man var med andre ord blevet bevidst om, at Folketingets suverænitet risikerede at støde sammen med det udenrigspolitiske regeringsprærogativ.

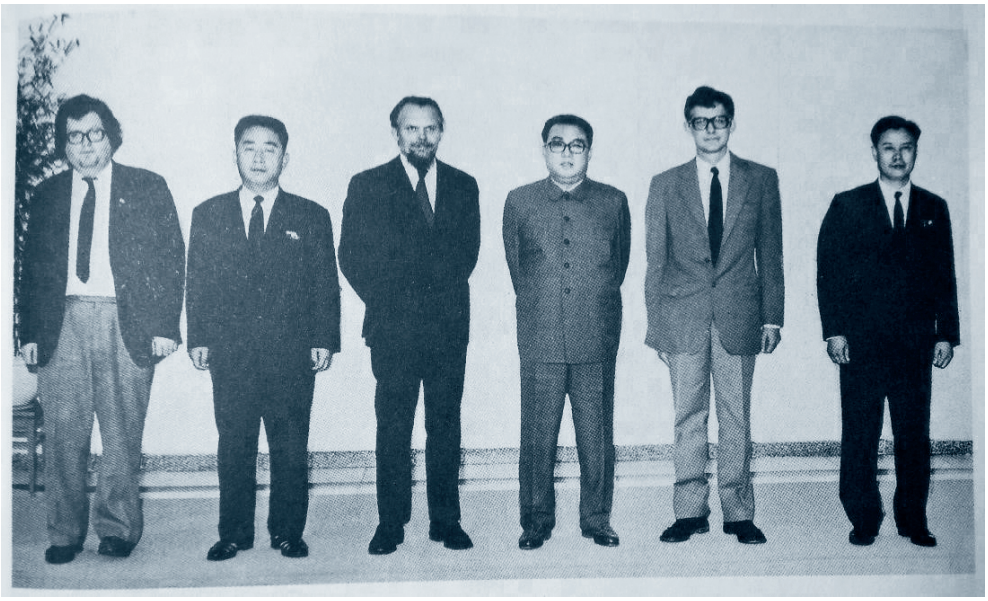
I 1965 udbrød der magtkamp i FN-delegationen. Delegationsformand og medlem af Folketinget Frode Jakobsen (S) havde i praksis taget styringen i delegationen og dermed i dansk FN-politik. Det huede ikke hans partifælle, udenrigsminister Per Hækkerup (S), der var uenig med Jakobsen i mange udenrigspolitiske spørgsmål. Jakobsen blev tilbudt den til lejligheden opfundne stilling som nedrustningsambassadør for at skabe "et mere logisk hierarki i den danske FN-repræsentation" (oversat af forfatter), som det blev

omtalt fra amerikansk side (Midtgaard, 2005: 270). Jakobsen afslog tilbuddet, men fratrådte efterfølgende delegationsformandsposten.

Siden da blev folketingsrepræsentanterne i FN-delegationen degraderet fra at være officielle repræsentanter og har siden haft officiel status som suppleanter eller rådgivere. Nogle var utilfredse, mens andre satte pris på ikke at skulle optræde som repræsentanter for udenrigspolitikker, de ikke altid selv var enige i (Petersen, 1998: 120).

Note: Rigsdagens kloakudvalg på studietur til England i 1936. Det Kgl. Biblioteks Billedsamling.

Note: Rigsdagens repræsentant Hartvig Frisch (S) underskriver FN-pagten ved San Francisco-konferencen i 1945. I baggrunden ses de øvrige danske delegationsmedlemmer: legationsråd Povl Bang Jensen, professor og repræsentant for Frihedsrådet Erik Husfeldt og gesandt Henrik Kauffmann. Politikens Pressefoto.



Note: Formand for venskabsforeningen Danmark-Nordkorea Christen Amby samt folketingsmedlemmerne Gert Petersen (SF) og Svend Auken (S) på besøg hos Kim Il-Sung i 1973. Den 1,92 m høje Svend Auken er angiveligt redigeret lavere på billedet for ikke at rage for meget op over Den store leder (Petersen, 1998: 271).

Koordinationens begrænsninger og muligheder

En øget koordination mellem det klassiske og det parlamentariske diplomati i dag må ikke skabe tvivl om Folketingets autonomi. Regeringen kan selvsagt ikke pålægge medlemmer af Folketinget, hvad de skal gøre og sige, eller hvem de skal mødes med. Koordination må heller ikke skabe tvivl om regeringens udenrigspolitiske prærogativ. Skal Danmark fortsat have én og ikke 179 udenrigspolitikker, bør der fortsat være en vis armslængde, så folketingsmedlemmer ikke fejlagtigt opfattes som repræsentanter for officiel dansk udenrigspolitik. Der er også grænser for, hvilken diplomatisk rolle Folketinget kan tiltænkes. Størstedelen af udenrigstjenestens arbejde er "rugbrødsarbejde", og mange opgaver kræver ubetinget den ekspertise og erfaring med det diplomatiske håndværk, som kun en professionel udenrigstjeneste kan levere.

Men en højere grad af koordination kan også medføre betydelige fordele for Folketinget såvel som for regeringen og Udenrigsministeriet. Folketingsmedlemmerne kan få mulighed for at opbygge værdifulde internationale netværk, få del i af noget af al den viden, der eksisterer i Udenrigsministeriet, og styrke den parlamentariske kontrol.

Regeringen kan ved at inddrage Folketinget få større sikkerhed omkring den parlamentariske opbakning. Det er især relevant i spørgsmål, hvor Grundloven kræver Folketingets samtykke. Men Folketingets deltagelse i FN-delegationen er igen også et godt eksempel. I 80'erne fik det alternative sikkerhedspolitiske flertals dominans i udenrigspolitikken regeringen til at genoverveje Danmarks kandidatur til FN's Sikkerhedsråd. Folketinget blev dog fortsat inviteret med i delegationerne til FN's Generalforsamling, og daværende FN-ambassadør Ole Bierring forklarede efterfølgende, at det netop var ved at inkludere Folketinget, at man fik skabt en fælles forståelse af Danmarks

muligheder og begrænsninger i FN. Mens der var stor politisk kontrovers om Danmarks forhold til NATO, sikrede regeringen sig parlamentarisk ro på bagsmækken hvad angik FN, mens Danmark havde plads i Sikkerhedsrådet 1985-86 (Götz, 2011: 195).

Også i Udenrigsministeriet kan man have en interesse i et tættere samarbejde med Folketinget. Omkring århundredskiftet udtalte Frederik Bajer fra Folketingets talerstol: "Jeg beklager, at vor udenrigspolitik er sejlet ind i et så tavst tidsrum, at vi i modsætning til andre stater lever i en næsten fuldstændig uvidenhed om, hvilke opgaver særlig Udenrigsministeriet lever for" (citeret i Larsen, 1986: 11). Samme uvished plager Udenrigsministeriet i dag, og folketingsmedlemmernes opfattelse af, at ministeriet lukker sig om sig selv (Tjalve og Henriksen, 2008) har givetvis bidraget til dets svækkede position på Slotsholmen (Andersen, 2020) og dalende bevillinger gennem mange år. Et tættere samarbejde med Folketinget kunne give folketingsmedlemmerne bedre blik for diplomatiets betydning og dets udfordringer. Med deres synlighed i offentligheden kan folketingsmedlemmerne også give Udenrigsministeriets offentlighedsdiplomatiske indsats et boost, både i udlandet og i Danmark.

Tages der højde for det parlamentariske diplomatis styrker og begrænsninger, kan øget samarbejde med det klassiske diplomati være fordelagtigt for alle parter og styrke Danmarks samlede stemme udadtil. Samarbejdet kan tilrettelægges på mange måder. Her følger til sidst et par idéer til, hvor man kunne starte.

- Udenrigsministeriets Trade Council (tidligere Eksportrådet) modtager allerede i dag Folketingets rejsekalender og fordeler den rundt til eksportmedarbejdere på ambassaderne, der har mulighed for at bede tilrejsende udvalg om at tage bestemte problemstillinger op med myndigheder i landet af interesse for danske virksomheder. Det er oplagt at overveje, om der også er andre diplomatiske dagsordner, parlamentarikerne kan rekrutteres til, f.eks. demokratiindsatser rundt omkring i verden.
- Folketinget har for nylig fået både en arktisk delegation og et tværpolitisk netværk for FN's verdensmål. Både Arktis og Verdensmålene er vigtige elementer i dansk udenrigspolitik og nyder bred interesse i Folketinget. Det er derfor oplagt at overveje, hvordan disse nye formater for folketingsarbejdet kan indtænkes i Danmarks samlede udenrigspolitik.
- Et andet muligt format er parlamentariske venskabsgrupper. Et bredt flertal i Folketinget støttede i 2004 op om oprettelsen af en parlamentarisk venskabsgruppe i solidaritet med Taiwan. Derudover har Folketinget ikke haft andre venskabsgrupper. I mange andre parlamenter er de ellers udbredte, f.eks. har den svenske Rigsdag omkring 40 bilaterale og regionale venskabsgrupper, og det franske Senat har 80 (Zamfir, 2019: 9). Flere parlamenter, bl.a. det estiske, har desuden venskabsgrupper til Danmark. Venskabsgrupper i Folketinget ville kunne fungere som fora for udvidet dialog og vidensdeling med Udenrigsministeriet, som kontaktpunkter for det diplomatiske korps i København og som repræsentanter for Folketinget ved indkommende besøg.

Litteratur

Andersen, Louise Riis (2020), "På tværs – om Udenrigsministeriets position på Slotsholmen", *Økonomi & Politik*, 93(1): 143-55.

ERU (2013), "Forslag om at tænke erhvervslivet ind i studierejser", Erhvervs-, Vækst- og Eksportudvalget 2012-13 Alm.del, Bilag 200.

Götz, Norbert (2011), *Deliberative Diplomacy: The Nordic Approach to Global Governance and Societal Representation at the United Nations*, Dordrecht: Republic of Letters Publishing.

Götz, Norbert (2016), "Parliamentarian Democracy Going Global: The Fading Nordic Model", Jussi Kurunmäki og Johan Strang, red., *Rhetorics of Nordic Democracy*, Helsinki: Finnish Literature Society, pp. 262-89.

Information (1961), "SF's FN-delegerede maa stemme mod sin overbevisning", 8. august.

Jørgensen, Harald (1970), *Genforeningens statspolitiske baggrund*, Historisk Samfund for Sønderjylland.

Larsen, Knud (1986), "Lovgivningsmagten og udenrigspolitikken – historisk set", i Niels Jørgen Haagerup og Kristian Thune, red., *Folketinget og udenrigspolitikken*, København: Dansk Udenrigspolitisk Institut/Jurist og Økonomforbundets Forlag.

Lassen, Viktor Lerche-Jørgensen (2020), *Parlamentarisk diplomati – Folketinget som international aktør*, speciale, Institut for Statskundskab, Københavns Universitet.

Marcussen, Martin og Svend Roed Nielsen (2019), *På mission i Danmark. Diplomatisk tiltrækningskraft til debat*, København: DJØF-Forlag.

Marcussen, Martin (2013), "Det klassiske diplomati fragmenteres og hybriddiplomatiet opstår". *Samfundsøkonomen*, juni, no. 2, pp. 5-11.

Midtgaard, Kristine (2005), *Småstat, magt og sikkerhed. Danmark og FN 1949-65*, Odense: Syddansk Universitetsforlag.

Nielsen, Holger K. (2020), "Folketinget og Udenrigsministeriet". Økonomi *&* *Politik*, 93(1): 165-74.

Petersen, Gert (1998), *Inden for systemet – og udenfor*, København: Lindhardt og Ringhof.

Stavridis, Stelios og Davor Jančić (2016), "The Rise of Parliamentary Diplomacy in International Politics", *The Hague Journal of Diplomacy*, 11(2-3): 105-20.

Taksøe-Jensen, Peter (2016), *Dansk diplomati og forsvar i en brydningstid. Udredning om dansk udenrigs- og sikkerhedspolitik*, Udenrigsministeriet.

Tjalve, Vibeke Schou og Anders Henriksen (2008), *'Vi diskuterer jo ikke politik på den måde'. Regeringen, Folketinget og sikkerhedspolitikken,* København: Dansk Institut for Militære Studier.

Zamfir, Ionel (2019), "Connecting parliamentary and executive diplomacy at EU and Member State level", European Parliamentary Research Service.

One-size does not fit all – En undersøgelse af danske diplomatiske repræsentationers brug af sociale medier til offentlighedsdiplomati

Temanummer: Cybersikkerhed

Hvordan anvender danske diplomatiske repræsentationer sociale medier så forskellige steder som Rom, Riyadh og Reykjavik? Der findes ikke en one-size-fits-all, når det gælder offentlighedsdiplomati på sociale medier. Variationen i både outreach, indhold og engagement på repræsentationernes sociale medier viser, at der ikke findes én samlet forklaring på brugen af SoMe til offentlighedsdiplomati. Snarere bliver tilstedeværelse og aktivitet på SoMe bestemt af den lokale kontekst, de ressourcer, de enkelte repræsentationer har til rådighed i hverdagen, samt den enkeltes forståelse af, hvad en moderne diplomat er og skal være i fremtiden.

SIGNE RÁZGA AGNILD
cand.scient.pol,
Institut for Statskundskab,
Københavns Universitet,
signe.agnild@gmail.com

FRANCISKA KIRKEGAARD FLUGT
cand.scient.pol.,
Institut for Statskundskab,
Københavns Universitet,
franciskaflugt@gmail.com

Sociale medier er blevet en del af hverdagen for mennesker i hele verden. Det er her, man vedligeholder kontakten til sine netværk, skaber nye forbindelser, og endda her mange får nyheder. Sociale medier (SoMe) kan bruges til at bekæmpe autoritære regimer, som under det arabiske forår eller til at føre valgkampe i demokratiske samfund. De kan selvfølgelig også bruges til at sprede fake news om politiske modstandere. Sociale medier er med andre ord blevet direkte kanaler mellem beslutningstagere, virksomheder og ganske almindelige mennesker.

Udenrigstjenesternes brug af sociale medier afspejler den nye virkelighed. Det er ikke længere nok blot at udføre diplomati i den traditionelle forstand – bag lukkede døre, med hemmelige møder og fast protokol. Man kan ikke nøjes med at være en diplomat, som lever i det skjulte – man skal kunne diskutere og fremme sit lands interesser offentligt, ude såvel som hjemme. Offentlighedsdiplomatiet har bevæget sig væk fra periferien af den diplomatiske praksis og er i højere grad blevet integreret i de mere etablerede diplomatiske aktiviteter (Melissen, 2005). I den moderne verden fylder offentlighedsdiplomatiet således mere og mere, og det er særligt gjort muligt ved hjælp af sociale medier (Marcussen og Nielsen, 2019: 175).

Denne kronik er resultatet af forskning, der for første gang systematisk studerer, hvilket outreachpotentiale, hvilket indhold og hvilket engagement den danske udetjeneste skaber med sine SoMe-profiler (Agnild og Flugt, 2020). Kronikken afsluttes med en række konkrete anbefalinger til, hvordan man på de enkelte repræsentationer kan forbedre sin strategiske brug af sociale medier. Studiet bygger dels på en kvantitativ kortlægning af de danske repræsentationers brug af sociale medier og dels på interviews med en række am-

bassadører og kommunikationsansvarlige fra danske repræsentationer over hele verden.

Lokal kontekst, ressourcer og personlige erfaringer

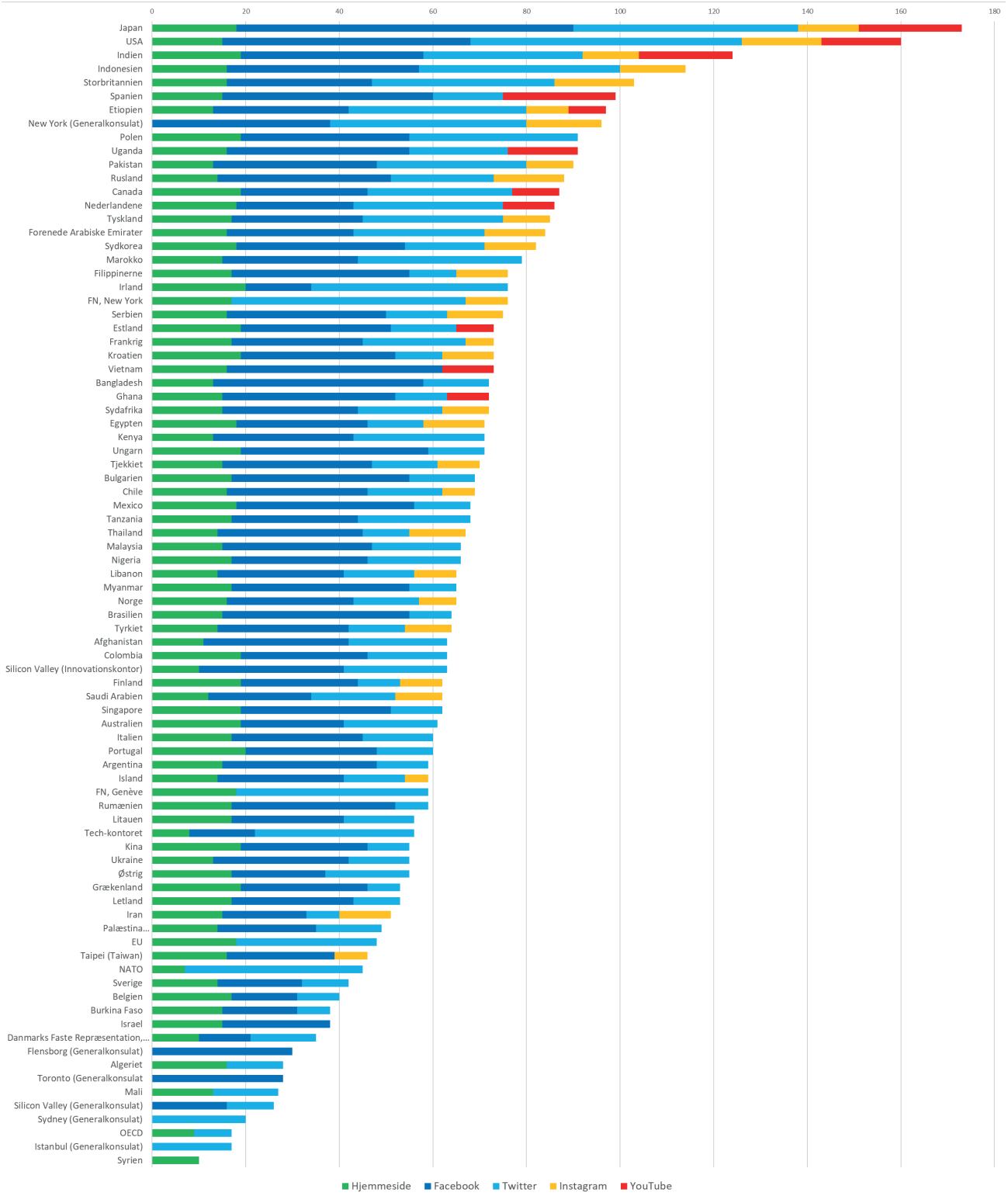
Studiet har først og fremmest vist, at der er stor variation i det outreach, danske repræsentationer har på sociale medier. Mens ambassaderne både benytter sig af Facebook og Twitter, kommunikerer de multilaterale repræsentationer primært på Twitter. Generelt har de multilaterale repræsentationer en høj tilstedeværelse på Twitter i forhold til ambassaderne. Twitter ses af mange som et politisk medie, og anvendelsen af denne platform skal netop ses i lyset af, at de multilaterale repræsentationer primært forsøger at ramme beslutningstagere, mens ambassaderne tillige forsøger at ramme den bredere offentlighed.

Indekset i figur 1 nedenfor viser noget om, hvor omfattende de danske diplomatiske repræsentationers SoMe beredskab er, og dermed hvor stort et SoMe-potentiale repræsentationerne har hver især. Det er vigtigt at understrege, at et stort SoMe-beredskab – et stort outreach som eksempelvis hos ambassaderne i Tokyo og Washington – ikke nødvendigvis er ensbetydende med et tilsvarende stort antal følgere på de sociale medier, eller at ambassaden når ud til sine følgere på en effektiv måde.

Der er stor variation i både brugen af Facebook og Twitter blandt alle repræsentationerne. Ligeledes er der ikke noget mønster i, hvilke repræsentationer der er til stede på hhv. Instagram og YouTube. Dette indikerer, at SoMe-indsatsen i Udenrigsministeriet er decentraliseret og i høj grad op til den enkelte repræsentation selv.

Der er kun lille variation i, hvilket indhold de enkelte repræsentationer kommunikerer på sociale medier. Mens det klassiske diplomati med billeder af eksempelvis møder, håndtryk og officielle besøg stadig bliver prioriteret højt blandt alle repræsentationer, prioriterer særligt ambassaderne også opslag om Danmark og dansk mentalitet. Her bliver især Udenrigsministeriets nyhedsbrev Denmark Daily benyttet som afsæt for historierne.

Figur 1: Danske repræsentationers SoMe-potentiale



Note: De danske repræsentationers outreach er baseret på en gennemgående analyse af deres hjemmesider, samt profiler på Facebook, Twitter, Instagram og YouTube. Jo mere information, jo bedre opdateret og jo flere sprog, etc.; jo højere score. Generalkonsulater og innovationscentre har ikke egne hjemmesider og har derfor ikke fået en score i denne kategori.

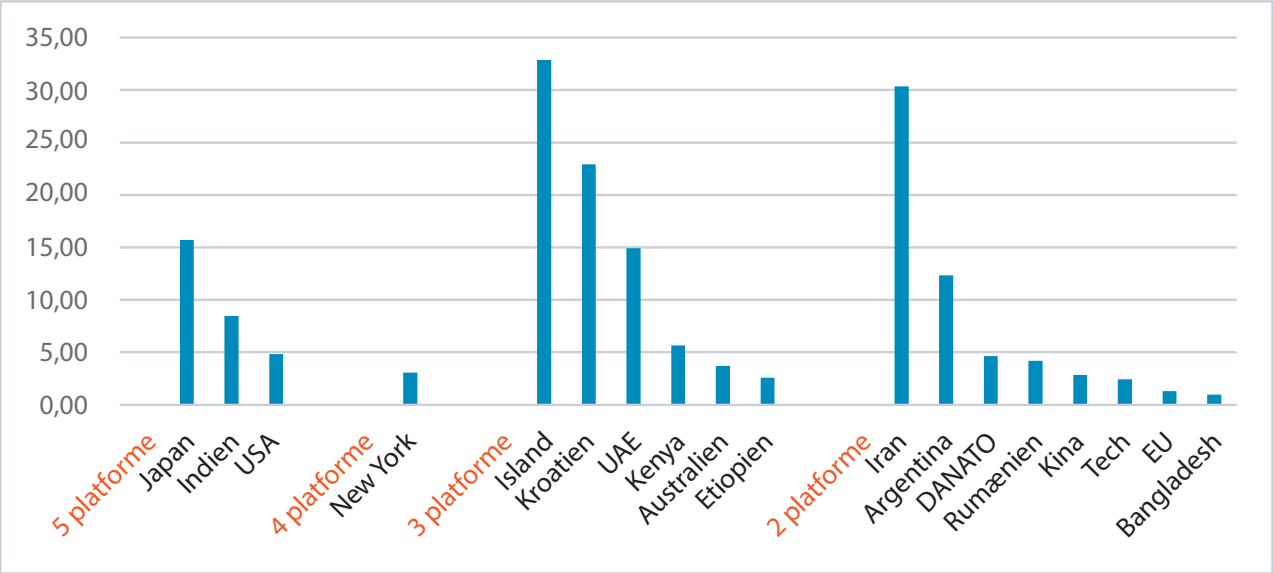
Det er dog i høj grad den lokale kontekst, som har indflydelse på, om man vælger at skrive om f.eks. cykelmentalitet eller danske klimaløsninger jf. eksemplerne i figur 2.

Figur 2: Cykelmentalitet på generalkonsulatet i New York, danske klimaløsninger på ambassaden i Kenya og klassisk diplomati på ambassaden i Kuala Lumpur.

Ét er antallet af følgere, noget andet er, om repræsentationerne formår at engagere sine følgere på de sociale medier. Kommentarer og likes, også kaldet engagement, påvirker rækkevidden på ens opslag. Mens nogle er bredt til stede på flere platforme, har andre prioriteret en mere dybdegående og smal tilstedeværelse på få platforme. Repræsentationernes engagement beregnes på IPM – interaktioner pr. tusind brugere, som beregnes ud fra en måneds aktivitet – i dette tilfælde februar 2020 (Haug, 2014: 31). Ser man på det engagement, de danske repræsentationer skaber, kan man se, at der ikke er én repræsentation, som generelt skaber meget engagement på tværs af sine plat-

forme. Tillige er det ikke nødvendigvis en fordel at prioritere hverken bredere eller smallere tilstedeværelse – forklaringen på variationen skal derfor findes andre steder.

Figur 3: Engagement fordelt på antal SoMe-platforme



Note: Gennemsnitligt engagement på tværs af platform for udvalgte diplomatiske repræsentationer fordelt på antallet af platforme (Facebook, Twitter, Instagram og YouTube. Ved fem platforme har repræsentationen mere end én profil på et af medierne). Som det kan ses, er det ikke nødvendigvis en fordel for engagementet at have flere eller færre SoMe-platforme.

Variationen i brugen af sociale medier kan overordnet forklares af tre ting: Lokal kontekst, ressourcer og personlige erfaringer med sociale medier. Flere af de danske repræsentationer ønsker at skille sig ud med deres indhold for at blive bemærket. Måden repræsentationerne varierer deres indhold, er i høj grad præget af, hvilken kontekst de befinder sig i – det handler om at finde den lokale krog. Kommunikationen på sociale medier skal altså udvikles decentralt og ikke bare fra et kontor på Asiatisk Plads. De begrænsede ressourcer på repræsentationerne betyder dog, at det kan være en udfordring for repræsentationerne at producere indhold, som kan skabe engagement hos deres følgere. Derfor bliver også diplomaternes personlige erfaringer med sociale medier vigtige for måden at være til stede på.

Anbefalinger til danske repræsentationer

Studiet har ført til en række anbefalinger til de diplomatiske repræsentationer i deres strategiske brug af sociale medier. Anbefalingerne skal ses i den kontekst, den enkelte repræsentation befinder sig i og tager udgangspunkt i, hvad repræsentationerne kan gøre for at optimere tilstedeværelsen på sociale medier.

1. Kend dit publikum
2. Dialog frem for monolog
3. Samarbejd med andre repræsentationer i modtagerlandet
4. Bliv personlig
5. Få de "rigtige" engageret
6. Prioritér sociale medier i hverdagen

Kend dit publikum

Den lokale kontekst spiller ind, når det handler om brugen af SoMe. Der er altså ikke en "one-size-fits-all"-model, der kan anvendes overalt i verden. Hvad der virker i Berlin, virker ikke nødvendigvis i Bamako. Første anbefaling er således, at repræsentationerne lærer deres publikum at kende. Dette gælder for de platforme repræsentationerne anvender, men også for ambassadørernes egne SoMe-profiler – særligt for dem, som tager deres private profiler med videre til nye stillinger.

Det handler med andre ord om at identificere, hvordan man finder en lokal krog, som kan tiltrække og interessere sin målgruppe. Følges ambassadens Facebookside primært af danskere i modtagerlandet, bliver informationer om dansk mentalitet irrelevante, og det falder måske ikke i god jord blandt saudi-arabiske følgere, hvis man deler billeder med folk i badetøj.

Det kan derfor lyde simpelt, men det er essentielt for kommunikation på sociale medier, at man identificerer sine følgere – hvilken aldersgruppe befinder ens følgere sig i? Hvor kommer de fra? Hvilke(t) sprog bør man kommunikere på? Dette betyder naturligvis ikke, at Udenrigsministeriets centrale SoMe-enhed bliver irrelevant. Den bør fortsætte med at levere indhold og information, og den kan nemt anvendes hvis og når ambassaderne har brug for teknisk assistance.

Dialog fremfor monolog

Sociale medier er betinget af interaktion mellem brugerne (Boyd og Ellison, 2007: 11). Flere af de danske diplomatiske repræsentationer anvender SoMe til blot at pushe informationer om Danmark – at "Danmarksplaine". Man bør i stedet på de enkelte repræsentationer fokusere på interaktion med sine følgere og basere sin SoMe-indsats på dialog fremfor monolog.

Det er ikke nok blot at lægge opslag op, som stiller spørgsmål, hvis man ikke også følger op på den dialog, man selv har startet. De danske repræsentationer bør derfor prioritere tovejskommunikation på SoMe. Dette kan dog være svært og nogle gange umuligt at gøre i praksis. Sagen er jo den, at det kræver ressourcer at holde en dialog kørende på sociale medier. Dette leder til tredje anbefaling.

Samarbejd med andre repræsentationer i modtagerlandet

Har man ikke ressourcer til at have en ansat til at facilitere dialog med repræsentationens følgere, kan man samarbejde med andre udenlandske repræsentationer for at øge sit outreach. Hvis andre udenlandske repræsentationer, med egne følgere, deler, kommenterer eller liker en dansk repræsentations opslag, øges rækkevidden markant. Man kan altså ved hjælp af samarbejde med andre repræsentationer i modtagerlandet få en større platform at formidle sit budskab på.

De danske repræsentationer rundt om i verden samarbejder allerede med andre repræsentationer i modtagerlandet, når de holder EU-møder, filmfestivaler eller lignende. De diplomatiske forbindelser eksisterer altså allerede, og dette samarbejde kunne naturligt udstrække sig til også at involvere SoMe.

Bliv personlig

"Denmark Daily"-nyhedsbrevet er et glimrende værktøj til at formidle nyheder om Danmark. Nyhedsbrevet bruges aktivt af flere af de danske repræsentationer, når der skal deles indhold på deres SoMe-sider. De præfabrikerede historier kan repræsentationerne plukke fra, når man finder noget, som er relevant eller interessant for følgerskaren. Det er dog vigtigt – ja helt afgørende – at indholdet tilpasses den lokale kontekst og ikke bare anvendes ukritisk. Kommunikation på SoMe virker kun, når det er i øjenhøjde med modtageren, og når der bliver delt billeder og videoer fra hverdagen: Det virker at blive personlig. Et eksempel herpå kan ses på den danske ambassade i Indien, hvor ambassadør Freddy Svane under de seneste måneders CoVid-19-lockdown har sendt videoer ud til danskere i Indien og på Sri Lanka, hvor han giver en kort update på situationen i landene. Videoerne er optaget på hans iPhone og er i en uformel og personlig tone, men opretholder den professionalisme, som en repræsentant fra en offentlig myndighed skal have.

Få de "rigtige" engageret

På de sociale medier handler det også om at få de "rigtige" engageret. Hvem de rigtige er, afhænger af budskabet. For the Trade Council kan der være tale om beslutningstagere i virksomheder, mens det for ambassadører kan være andre ambassadører eller beslutningstagere i modtagerlandet. En ting er, hvem ens nuværende følgere er. En anden er, hvem man kunne tænke sig at ramme. Hvis ønsket er at nå ud til beslutningstagere i modtagerlandet, nytter det ikke noget at "Danmarksplaine", eller at gøre opmærksom på, at vi i Danmark endnu engang er kåret som et af de lykkeligste lande i verden – hvilket ellers kan være et glimrende budskab til den brede offentlighed. På den danske ambassade i Rumænien har man erfaring med at få beslutningstagere engageret ved at være en lille smule provokerende. Ambassaden delte et opslag i maj 2019 med følgende tekst: "'*Hvad er prognosen?*' '*weekenden bliver varm*' '*Og derefter?*' '*derefter køligt – i skyggen*'" (oversat af forfatter). Opslaget blev lagt på Facebook, da man samme weekend skulle have en folkeafstemning om

korruption. Om mandagen skulle lederen af det rumænske socialistparti for domstolen og have en afgørelse i en sag om netop korruption. Opslaget blev delt næsten 2.000 gange, fik mere end 900 kommentarer og skabte i den grad opmærksomhed i Rumænien. Det var nok ikke noget, som var gået i et mere autoritært styre, og kunne måske endda nogle steder i verden resultere i en "persona non grata"-situation. Men i Rumænien udnyttede den danske ambassade den mere uformelle kontekst, hvilket ikke alene blev populært i befolkningen, men også skabte opmærksomhed blandt lokale beslutningstagere.

Prioritér sociale medier i hverdagen

De ovenstående anbefalinger leder til en naturlig sidste anbefaling: prioritér sociale medier i hverdagen. (Offentligheds)kommunikation har stadig en tendens til at være det sidste, man prioriterer på den enkelte repræsentation. Dette synes at være en massiv fejlprioritering. Sociale medier kan være en vigtig del af diplomati-værktøjskassen, særligt for en småstat som Danmark, som ikke nødvendigvis har den naturlige opmærksomhed fra modtagerlandet. Det er i høj grad op til ambassadøren – som leder af repræsentationen – at skabe et rum, hvor SoMe bliver en naturlig del af hverdagen. Er ambassadøren ikke med på SoMe-bølgen, får repræsentationen svært ved at lave et effektivt digitalt offentlighedsdiplomati. Asiatisk Plads kan gøre meget for at fremme brugen af SoMe, ved f.eks. at hjælpe med indhold gennem Denmark Daily, eller at skabe incitamentsstrukturer, men hvis ikke den enkelte ambassadør i sin egen lokale kontekst, ser fordelene ved at benytte sig af SoMe, er der langt igen.

Kilder

Agnild, S.R. Og F.K. Flugt, (2020), *SoMe – Diplomatiets nye, og ikke så hemmelige våben*, speciale, Institut for Statskundskab, Københavns Universitet.

Boyd, D.M. og N.B Ellison, (2007), "Social Network Sites: Definition, History, and Scholarship", *Journal of ComputerMediated Communication*, 13(1): 210–30.

Haug, A. (2014). *Sig du kan li' mig: Indholdsstrategi for sociale medier*, København: Gyldendal Business.

Marcussen, M. og S.R. Nielsen (2019), *På mission i Danmark: Diplomatisk tiltrækningskraft til debat*, København: Djøf Forlag.

Melissen, J. (2005), "The New Public Diplomacy: Between Theory and Practice", i J. Melissen, red., *The New Public Diplomacy: Soft Power in International Relations*, Basingstoke & New York: Palgrave MacMillan, pp. 3-27.

Abstracts

Small states and cyber weapons – new opportunities within limits

Mikkel Storm Jensen, Military Analysts, Royal Danish Defence College, msje@fak.dk

This article seeks to partially fill a gap in the literature on military strategy by describing how cyber weapons provide small states with an array of new military opportunities that they will likely find it difficult to take advantage of if they are part of an alliance. It does so by describing technical and tactical reasons why the emergence of cyber weapons has potential to influence the military balance between small and large states in favour of the small states, but also how the technical and tactical characteristics particular to cyber weapons encumber their use in alliances and hence may limit their usefulness for said small states.

Offensive Cyber Operations: The New Normal?

Karsten Friis, senior researcher, Norwegain Institute of International Aaffairs (NUPI), kf@nupi.no

Can states retaliate if they are being digitally attacked in peacetime? What are major states doing, and what do international law and norms stipulate on this? What can the international security policy implications be with increased use of offensive cyber operations? This article discusses this development in international security policy in combination with an assessment of the relevant international legal framework. It starts off with a discussion of US' new approach to offensive operations related to the two concepts "persistent engagement" and "defend forward". A brief case study of Norway's approach to offensive cyber operations follows next, which again leads to the legal framework called "Responsibility of States of International Wrongful Acts". This is the most relevant international legal framework related to offensive cyber operations outside armed conflict. The article concludes with a discussion of dilemmas in the intersection between security policy and international law.

International Promotion of Cyber Norms. How to Resolve the Deadlock?

Jeppe Teglskov Jacobsen, Assistant professor, Royal Danish Defence Aacademy, jeja@fak.dk

The current expectations of progress in the on-going global debates on the norms for responsible state behavior in cyberspace are low. But why have the international norm negotiations come to a stand-still and the Western coalition's norm promotion strategy failed? And can a small state like Denmark become the norm entrepreneur that pushes the Western norm agenda ahead? Drawing on the norms literature in International Relations, the article locates a key obstacle to progress in the mutual accusation of hypocrisy, which – when directed towards the US and its allies – needs to be understood in the context of the Snowden revelations and the lack of acknowledgement of the intelligence norm that dominates in cyberspace. An emerging Western openness about and nuance in states' use of cyber capabilities provides countries such as Denmark with the opportunity to become the pioneer that develops political clarifications and shares the best practices, and thereby contribute with important and much-needed reference points for

other countries. But it requires that the Danish authorities are willing to invest resources in the cyber diplomacy while simultaneously addressing the internal disagreements head-on regarding e.g. how much hackers should be used in the Danish foreign and security policy.

Who is the Cyber Expert? Expertise and Professions in the Cyber Security Field

Johann Ole Willers, research fellow, Norwegian Institute of International Affairs and ph.d-student, Department of Organization, Copenhagen Business School, jow.ioa@cbs.dk

Cybersecurity experts play an important role in identifying and managing digital risks. This article employs insights from the sociology of professions and the sociology of expertise to highlight competing epistemic rationalities in the constitution of cyber risk. Drawing on a novel dataset of expert profiles in public and private Danish cybersecurity expert groups and committees, it is argued that the profile of cybersecurity experts has moved away from a purely technical focus to a process orientation which is both broader in scope and closer to the decision-making level. The new expert profile is positioned at the intersection of technical, organizational and economic rationality. In the absence of public scrutiny, this development could reinforce expert power and undermine democratic practices. It offers, however, also an opportunity to re-politicize the public cybersecurity discourse.

Hacking – crime or digital self-defense?

Lene Wacher Lentz, assistant professor, ph.d., Department of Law, University of Aalborg, lwle@law.aau.dk
Jens Myrup Pedersen, associate professor, ph.d., Departmnt of Electronic Systems, University of Aalborg, jens@es.aau.dk

Traditionally, we understand "hacking" as a crime, and we hear about the most notorious hacking attacks in the media. However, hacking is also being articulated as a specific cybersecurity skill: Courses in hacking are available and the Danish Defence Intelligence Service has established a "Hacking Academy" with the purpose of recruiting talented "hackers" to government services. The concept of hacking might be confusing, as there will be limitations to which methods can be applied with the purpose of optimizing or testing cybersecurity. In this article, we clarify to what extent the hacking-provision in the Danish Criminal Code applies. Furthermore, we clarify whether the method "hacking back" can be legitimately used as cyber defense, if you experience your systems being attacked by a hacker. It is illustrated how the criminal liability often will appear unpredictable for those working to improve the security of IT-systems.

Review Article – Modern Times: Active Crisis Management – the Return of Keynes?

Finn Olesen, Professor, Aalborg University Business School, University of Aalborg, finn@business.aau.dk

Somehow, Keynesianism never disappeared totally from the scene of macroeconomics. And now, after The Great Recession and the Covid-19 virus, is Keynesianism back for good? Is it now time to go back to a more fundamental Keynes-like macroeconomic understanding? And what about the post Keynesians? Do they have a chance of gaining territory?

Review Article: Handling the Coronavirus – Public-Private Interaction as the solution

Mina Erbas, Consultant, KPMG, Student, Department of Political Science, University of Copenhagen, mina_erbas@hotmail.com
Emil Lobe Wellington Suenson, Head of Government Affairs, Danish Medical Device Association, External Lecturer, Department

of Political Science, University of Copenhagen, lobe_suenson@hotmail.com

The first critical phase of the corona crisis required a massive effort to prepare the health care system to deal with the virus. It required large amounts of medical devices, including masks, visors, tests etc. These devices are usually supplied by the private sector and procured by the public sector in Denmark. During the corona crisis, this division was changed. Instead, the interaction was to a much greater extent characterized by an ongoing and flexible collaboration between the private industry and the public sector. This process can to a large extent be understood with classical rationalist theory. On that basis, a number of questions can be deduced as to how the future organization of the effort should be organized, as well as how the public sector's intervention in the market in connection with the corona crisis can affect innovation in the private industry in the long run.

Review Article: Moralizing in a biased defense for the Danish State Television and Radio Company (DR)

Bøje Larsen, professor emeritus, ph.d, Copenhagen Business School, bl.om@cbs.dk

This article discusses a book about the Danish State Television and Radio Company, DR. The author of the book, Christian S. Nissen, former director of DR, argues that Danish politicians have not been mature enough to let DR adopt to the threats from big international media like YouTube and Netflix. Such companies are conquering the Danish market with unfair methods and thereby, according to Nissen, weakening Danish society. In this article, it is argued that Nissen's book is a biased defense for DR that is steeped in the old world of flow TV. Despite presenting himself as a former researcher and referring to research literature, Nissen's use of such literature is superficial or wrong.