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.