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.