Røde Kors

Forsvarets høgskole

DET KONGELIGE FORSVARSDEPARTEMENT

Folkerettskonferansen 2021

Hybride trusler og cyberoperasjoner

Produsert ved Forsvarets høgskole (2021)

Redaksjon: Førsteamanuensis Camilla G. Cooper og løytnant Emilie Aasheim

ISBN: 978-82-93958-00-0

Henvendelser om denne utgivelsen kan rettes til:

Forsvarets høgskole

v/Stabsskolen

Postboks 1550 Sentrum

0015 Oslo

Epost: fhs.kontakt@mil.no

Forsidefoto: Cybersikkerhetssenteret (CSS), Cyberforsvaret på Jørstadmoen (Anette Ask/Forsvaret)

Folkerettskonferansen 2021

Hybride trusler og cyberoperasjoner

Forord

Camilla G. Cooper (PhD), redaktør

Folkerettskonferansen er en videreføring av et fagseminar på dagsaktuelle temaer knyttet til krigens folkerett/internasjonal humanitær rett arrangert i samarbeid mellom Norges Røde Kors, tidligere Forsvarets Stabsskole (nå Forsvarets høgskole, avdeling Stabsskolen) og det Kongelige Norske Forsvarsdepartement. Samarbeidsseminaret ble arrangert første gang i 2006, og i anledning 15-årsjubileet har det fått en mer moderne form og nytt navn: Folkerettskonferansen.

Tema for Folkerettskonferansen 2021, som ble avholdt den 14. oktober på Akershus Festning, var hybride trusler og cyberoperasjoner. Temaene er nært knyttet til hverandre og begge har resultert i behov for ny kunnskap for å sikre at Forsvaret ivaretar sin rolle som beskytter av norske interesser på best mulig måte, og for at sivilsamfunnet skal kunne bidra til et tryggere samfunn generelt.

Hybrid krigføring innebærer at krigen kan utkjempes og avgjøres på et politisk og diplomatisk plan, i informasjonssfæren, innenfor økonomi og finans, i cyberrommet og andre områder enn det tradisjonelle. I tillegg kan det være uklart hvem de hybride aktørene er og hvem som har ansvaret for å håndtere de hybride truslene. Skillet mellom kriminalitet eller utenlandske trusler er ofte uklart, og det er heller ikke like klart om truslene er så alvorlig at Forsvaret skal involveres eller om de skal håndteres med mer diplomatiske verktøy. Når vil hybride trusler utgjøre et væpnet angrep og når krysses terskelen til en væpnet konflikt slik at krigens folkerett kommer til anvendelse? Hybride virkemidler er ofte designet for å skape tvil nettopp om krigens folkerett får anvendelse, og når trusselaktørene opererer uten tydelig å tilkjennegi hvem de er eller opererer på vegne av, er det vanskelig å opprettholde et tydelig skille mellom det sivile og militære slik at de sivile i størst mulig grad kan beskyttes.

Hybridkrigføring utfordrer derfor både det norske sektorprinsippet og folkeretten. Det krever godt samarbeid og tydelig arbeidsfordeling mellom justis- og forsvarssektoren, og det krever meget god kunnskap både om hva som foregår og hvem som står bak, og hvordan de rettslige rammene skal anvendes i slike situasjoner. Slik kunnskap er med andre ord viktig for Norges sikkerhet, og vi håper denne konferansen har bidratt til å belyse disse problemstillingene.

Cybervirkemidler utløser også særlige spørsmål. Krigens folkerett skiller mellom militære og sivile, og mellom personer og gjenstander. Sivile personer og gjenstander skal ikke være

mål for angrep. Men hva er en gjenstand i cyberdomenet? Og hvordan skiller man mellom sivile og militære når mye av infrastrukturen er delt? Både det å gjennomføre militære operasjoner på en god måte også i cyberdomenet og samtidig jobbe for å unngå at militære operasjoner forårsaker skade og lidelse for sivile og sivilbefolkningen, byr på både praktiske og rettslige problemstillinger.

Dette er et område hvor det fremdeles er noe uklart hvordan folkeretten skal komme til anvendelse. Samtidig tilsier moderne samfunn med stor og økende avhengighet av digital infrastruktur at vi trenger tydelig regulering av krigføring også i cyberdomenet. Når stater ikke klarer å komme til internasjonal enighet om hvordan nye domener skal reguleres, må stater bidra til utviklingen ved å regulere egen adferd og dele sin oppfatning av hvordan aktivitetene bør reguleres. Et slikt eksempel er nasjonale manualer i krigens folkerett, og den norske versjonen fra 2013 har blant annet vært tydelig på at også data kan utgjøre et objekt slik at angrep på data må gjøres i tråd med reglene i krigens folkerett.

For å belyse de utfordringene hybride trusler og cyberoperasjoner reiser på best mulig måte, ble aktører fra strategisk nivå, de operasjonelle miljøene i Forsvaret og det juridiske fagmiljøet invitert til å snakke om og diskutere aktuelle problemstillinger. Presentasjonene deres er gjengitt her slik at de kan fortsette å bidra til kompetanseheving også for personer som ikke hadde anledning til å delta på konferansen.

Innholdsfortegnelse

Del 1: Hybride trusler

Del 2: Cyberoperasjoner

Del 1: Hybride trusler

Innledende kommentarer

Jo Andreas Sannem (Forsvarets høgskole)

Hva er det vi snakker om når vi snakker om hybride trusler eller hybrid krigføring? Er det hybride noe nytt eller er det bare ny terminologi?

Det synes å innta mange former: Anslag mot kommunikasjonssystemer og infrastruktur, propaganda, desinformasjon og påvirkning av demokratiet, voldelig opptreden med et forvirrende element, cyberangrep for å slå ut samfunnsviktige funksjoner, operasjoner for å tappe håndteringssystemet for ressurser og fokus, «grønne menn», svarte svaner ...

Karakteriseres det hybride ikke av hver enkelt aktivitet, men av at det er et mylder, og kanskje et synkronisert mylder? Eller er det det uklare eller tvilen som er det hybrides kjerne? Er det rett og slett snakk om ukonvensjonelle trusler eller ukonvensjonell krigføring, som bruk av ikke-regulerte midler eller ulovlig stridende?

Snakker vi om både kinetiske og ikke-kinetiske virkemidler? Må det være snakk om en viss intensitet og størrelsesorden før vi kan karakterisere en aktivitet som en hybrid trussel? Når kan en hybrid trussel regnes som hybrid krigføring? Spiller det hybride en like stor rolle både under og over terskelen for væpnet konflikt?

Kan jeg være et element i en langsom hybrid krigføring, plantet som moderator i en debatt om hybrid krigføring? Kan det være muldvarper i salen eller som planlegger ladede spørsmål for å styre forståelsen i en viss retning, som en svart svane, en usynlig sufflør? Hvordan håndteres personer som opptrer i kommentarfelt som en omvendt spion – en som ikke innhenter informasjon, men som planter den eller styrer retningen for den? Hvordan håndteres trollfabrikker?

Hvordan håndteres slike trusler på strategisk nivå? Kan vi i det hele tatt ha planer for håndteringen av noe vi ikke helt vet hva er? Eller vet vi det? Er det ikke nettopp situasjonsforståelsen som premiss som det hybride utfordrer?

Hvordan håndteres det hybride av jussen, herunder krigens folkerett? Kan vi i det hele tatt snakke om hybrid krigføring under terskelen for væpnet konflikt? Hvordan er det med ansvarliggjøring når det hybride ofte går ut på å opptre uklart og vanskeliggjøre eller umuliggjøre attribusjon?

Vi har lært at i krig og kjærlighet er alt lov, men vi som jobber med jussen pleier jo ikke å være enige i det, men søker det hybride å likevel gå klar av rettslig regulering? Er det rett og slett en form for lawfare ved at man spiller på hull eller svakheter i motstanderens juridiske systemer eller systemer for håndtering av trusler og uønsket aktivitet? Er det en mekanisme som er designet for å unngå mottiltak som for eksempel aktivisering av NATO-pakten art. 5? Hvordan virker retten på det som synes å manøvrere utenom retten?

Hvilken rolle vil det hybride ha for et framtidig forsvar av landet? Driver Norge med hybrid krigføring? Er det et konsept eller en strategi, og er det i så fall en småstatsstrategi eller storstatsstrategi? Er det egentlig nytt, eller er det bare «same shit, new wrapping»?

Nå har jeg reist flere svar enn det kanskje er mulig å svare på, men noen av dem vil vi nok få svar på, og jeg ser frem til å lære mer om tema hybride trusler. Først vil vi få et praktisk perspektiv fra Forsvaret på hva vi egentlig snakker om når vi viser til såkalte «hybride trusler». Dette vil bli etterfulgt av en presentasjon fra Justisdepartementet på hvordan Norge som stat tilnærmer seg hybride trusler, før vi til slutt ser på noen av de rettslige utfordringene som reises ved hybridkrig.

Hva er hybride trusler?

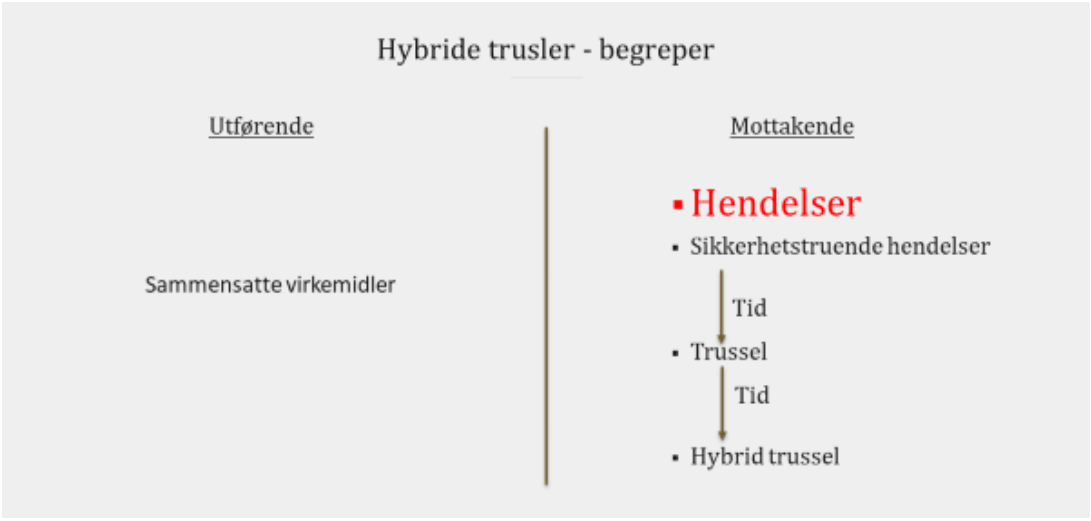
Endre Jessen (Forsvarets Sikkerhetsavdeling)

Kjernen i hybrid krigføring er at man må dra terskelen mellom det som er krig og det vi opplever som fred, men som ikke nødvendigvis er fred. Dette gjør at man utfordres på alle mulige områder. Fokus for presentasjonen vil være på å belyse tematikken fra Forsvarets perspektiv. Mye av tematikken her kommer fort over i gradert informasjon, men jeg skal prøve å holde dette ugradert og relativt enkelt.

Hybride trusler - begreper

Tematikken er veldig komplisert, og i Forsvarets Sikkerhetsavdeling bruker vi mye tid på å diskutere hva vi ser og opplever i det daglige som knytter seg til det hybride. Det er veldig mange aktører som kan knyttes inn i tematikken. Jeg skal forsøke å dra det litt ned og skape en større forståelse for hva det egentlig er vi snakker om. Ofte tenker man på hybrid krig som noe som er langt der fremme. Min påstand er at det er rundt oss hele tiden, hver dag, uten at vi nødvendigvis legger merke til det.

Seminaret her er delt inn i to bolker; hybrid og cyber. For vårt vedkommende er går dette inn i hverandre. I FSA er vi forsiktige med å bruke begrepene hybrid og trussel sammen. Det er alltid to parter man diskuterer her; den utførende og den mottakende. Den utførende parten er den som benytter seg av sammensatte virkemidler mot en eller annen aktør. Den mottakende er den som blir utsatt for disse sammensatte virkemidlene.



Jeg vil heller kalle hybride trusler for hybride hendelser, fordi det er akkurat det det er: hendelser. Det er en lang vei fra selve hendelsen til å definere det som en hybrid trussel. I Forsvaret rapporteres alle hendelser som kan oppleves sikkerhetstruende inn til Forsvarets sikkerhetsavdeling, i henhold til Sikkerhetsloven. Det kan være stort og smått, alt fra en vaktsoldat som opplever at noen på utsiden av gjerdet oppfører seg rart, til en bil som kjører forbi. Det er lav terskel for å rapportere inn det noen subjektivt opplever som sikkerhetstruende. Disse rapporteringene analyseres og enkelte ganger vurderes hendelsene til å være en trussel. Når mange hendelser er innrapportert og analysert så kan hendelsene man har definert som trusler, kontekstualiseres og kanskje settes i

sammenheng med andre hendelser. Det er først da vi begynner å snakke om det hybride. Det hybride smetter inn i alle former og fasinger der hvor det finnes sårbarheter.

Formålet med sammensatte virkemidler

Sammensatte virkemidler treffer ikke nødvendigvis Forsvaret. Det kan treffe alle steder i samfunnet, men ha en indirekte effekt for å oppnå den endelige målsetningen. Hva er så formålet med de sammensatte virkemidlene? Jeg vil først trekke frem to punkter. Det første handler om å degradere statens evner. Det ultimate målet vil være å på en eller annen måte gjøre noe med en stat. Man driver ikke cyberangrep for å mobbe, man har et spesifikt mål. Videre er det slik at verden er et anarki. Alle stater er suverene, og det at man har allianser utfordrer noen stater. Derfor kan det å bryte alliansene også være et formål. I det øyeblikket Brexit var et faktum, vil jeg tro at noen spratt en champagneflaske. Allerede der har man begynt å bryte ned alliansene. Ytterligere handler dette om å svekke attribusjonsevne. Det er i kjernen av hvorfor man bruker sammensatte virkemidler. Noe av poenget er at det skal være vanskelig å tilskrive handlingen til en gitt aktør eller en gitt stat. Det å identifisere, attribuere, hvem som er kilden bak en eller annen hendelse tar lang tid. Sammensatte virkemidler brukes også for å unngå å benytte kinetisk krigføring (militærmakt). Man kan oppnå de samme effektene vi tradisjonelt tenker på ved bruk av militærmakt ved å bruke sammensatte virkemidler.

Til sist bruker man også sammensamme virkemidler for å utnytte demokratiets sårbarheter. Vi er ikke et overvåkningssamfunn og vi er ingen politistat, det skal vi heller ikke være. Men på en annen side, hadde vi vært en politistat eller et diktatur, så hadde det vært vanskeligere å bli påvirket av de sammensatte truslene. Nettopp fordi man i slike samfunn kan ha full kontroll på staten og på menneskene. Det er klart at vi ikke vil dit, fordi vi skal være et demokrati, men vi må likevel forstå at vi vil være utsatt for sammensatte virkemidler, og at det er en de av samfunnet vi lever i, og at en potensiell motstander utnytter dette.

Eksempler på sammensatte virkemidler

Jeg skal gi noen eksempler for å belyse mulighetsrommet de hybride aktørene har. Eksemplene er tatt fra saker som finnes i media. Cyber er en tematikk senere på konferansen, men cyber og hybrid blander seg fort i hverandre. Teknologi gjør samfunnet mer lettvint, men også veldig sårbart. Bruk av apper og mobiltelefoner gjør at man kan påvirke befolkningsmasser rett inn i stuene deres, og gå rett på individer og vri meningene deres i den retningen man ønsker.

Aftenposten har skrevet en artikkel om en politiker som hadde tagget posisjonene sine på Instagram. Aftenposten hadde rett og slett gått inn og sett på den åpne Instagramkontoen og sett på mønsteret vedkommende beveger på seg. Når man kan finne ut hvordan politikeren beveger seg, hvor vedkommende går på kafé etc, da kan du også bruke denne informasjonen til å påvirke vedkommende for å oppnå en ønsket effekt.

Et eksempel jeg pleier å trekke frem, er en gang jeg opplevde å komme på kontoret og lese om et strømbrudd som hadde vært i Oslo sentrum. Det skjer jo fra tid til annen at man opplever strømstans, også kommer strømmen tilbake og man tenker ikke mer over det. Men vet vi egentlig årsaken til strømstansen? Hvis man ser på kartutsnitt for strømbrudd i Oslo sentrum kan man se at for eksempel VG-desken, som kan påvirke opinionen, var rammet. Andre som ble påvirket inkluderte blant annet Høyesterett. Kanskje vi må vurdere om noen

bevisst har gått inn for å skru av strømmen, for å se hvilke instanser man tar ut i dette området, slik at man senere kan bruke dette som et virkemiddel? Det samme gjelder for et strømbrudd som var i Trysil, som rammet 11 000 kunder. Her visste man ikke årsaken umiddelbart, men effekten får du likevel med en gang. Det tar tid før man finner årsaken. Har man her de riktige brillene på når man forsøker å finne årsaken til strømstansen?

Trollfabrikker har blitt nevnt innledningsvis. Det er noe som *de facto* skjer og har skjedd. Det ble ikke fanget opp under valget, men man fant det ut i ettertid. Effekten var der umiddelbart, årsaken fant man lang tid etterpå. Det å fange opp disse signalene er veldig vanskelig, og dette er på mange måter også formålet med bruk av sammensatte midler.

Tsjekkia anklaget i år Russland for en eksplosjon i et våpenlager i 2014. I 2014 skjedde også Krim. Det er ikke sikkert disse hendelsene er relatert til hverandre, men det kan godt være at akkurat denne eksplosjonen hadde en direkte effekt på det som skjedde på Krim, akkurat der og da. Syv år etter eksplosjonen går Tsjekkiske myndigheter ut og attribuerer handlingen til Russland. Det er lang tid etterpå, og det gjør dette veldig krevende.

Faksimiler fra Nrk.no

Det som på mange måter utfordrer oss i hverdagen, er at skillet mellom hva som er kriminalitet, hva som er krig og hva som er dette som skal påvirke en stat, utviskes. Dette har vært tema på såkalte table top-øvelser, som er en teoretisk metode for å se på hvordan dette kan virke. Mye av utfordringen er at dette ikke treffer direkte. Vi sier hybrid krig, men da begynner vi med en gang å blande inn og rette dette mot Forsvaret. Veldig mange av disse hendelsene er ikke mot Forsvaret, men det kan indirekte påvirke Forsvaret i neste omgang. Man skal også være var på å definere en eller annen hendelse til å være en krigslignende tilstand, for da ender man kanskje opp med å dra dette i en retning vi ikke ønsker, eller over en terskel vi ikke kan håndtere.

Til slutt vil jeg poengtere at det eneste vi vet med sikkerhet er alt er usikkert. Sammensatte virkemidler er fryktelig usikkert, og det er samtidig hele formålet; å gjøre det vanskelig og utnytte sårbarhetene som finnes i et demokrati. Det vi kaller sårbarheter er jo et mulighetsrom for andre aktører.

Strategisk håndtering av hybride trusler

Veronika W. Karlson (Justisdepartementet)

Det er mange gode og tidvis vanskelige spørsmål som reises med temaene som diskuteres her i dag. En ting er å forstå endringene, noe annet er å finne de rette tiltakene for å håndtere utfordringene. Bakteppet er veldig alvorlig, og i Justisdepartementet jobber vi hver dag med å finne hensiktsmessige tiltak. I dette innlegget vil jeg ha fokus på fem hovedpunkter: ansvar og roller på dette feltet, begrepsbruk og utfordringsbildet, sentrale strategiske dokumenter og noen arbeidsspor vi har hatt fokus på i det siste. Internasjonalt samarbeid er også en stor del av hvordan vi jobber med denne tematikken.

Det strategiske arbeidet med å motvirke sammensatte trusler – roller og ansvar

Justisdepartementet har et hovedansvar for å følge opp og koordinere regjeringens arbeid med sammensatte trusler. Vi har et tett samarbeid med Forsvarsdepartementet og Utenriksdepartementet, både på strategisk nivå og når konkrete saker dukker opp som skal behandles i regjeringen. I andre sammenhenger har vi også samarbeid med andre berørte departementer.

Innsatsen mot sammensatte trusler har fire hovedelement: deteksjon (avdekke hendelser), identifikasjon (forstå hva formålet med virkemiddelbruken er), attribusjon (avdekke hvem som står bak) og reaksjon (håndtere hendelsen). Både deteksjon og reaksjon og spesielt identifikasjon kan være krevende, fordi aktørene bak ofte vil søke å skjule både sin virkemiddelbruk.

Fremmede staters etterretnings- og påvirkningsforsøk mot Norge og norske interesser, eller mistenkte forsøk på slik påvirkning, håndteres i det daglige av Politiets sikkerhetstjeneste (PST), Etterretningstjenesten (E-tjenesten) og Nasjonal sikkerhetsmyndighet (NSM). Deres arbeid er regulert gjennom politiloven, etterretningstjenesteloven og sikkerhetsloven med tilhørende forskrifter. Både sikkerhetsloven og straffeloven har høringsnotat ute med forslag til nye bestemmelser for å styrke arbeidet med sammensatte trusler.

God koordinering mellom ulike sektormyndigheter er også svært viktig i det strategiske arbeidet med å motvirke sammensatte trusler. Det er nettopp det å se helheten i trusselbildet; det å bygge en god situasjonsforståelse, som er en særlig utfordring for oss. I tillegg eies og driftes en stor andel av kritisk infrastruktur i Norge av private aktører, og en rekke norske private og halvstatlige virksomheter utvikler kunnskap og teknologi som kan være av interesse for fremmede aktører. Det er derfor også viktig med god dialog mellom myndighetene og private virksomheter.

Videre er det viktig at norske virksomheter varsler om hendelser de mistenker kan være et påvirkningsforsøk. Virksomheter som er underlagt sikkerhetsloven, plikter å rapportere sikkerhetstruende virksomhet eller mistanke om dette til sikkerhetsmyndigheten (NSM).

Sentrale dokumenter

Grunnlagsdokumentene, selve premissene for vårt arbeid på departementsnivå, finner vi særlig i Samfunnssikkerhetsmeldingen (Samfunnssikkerhet i en usikker verden, Meld. St. 5 (2020–2021) og i Langtidsplan for forsvarssektoren (Prop. 14 S (2020–2021). I begge disse meldingene til Stortinget er arbeidet mot sammensatte trusler beskrevet med konkrete tiltak som myndigheter har arbeidet med gjennom flere år.

Sammensatte truslerI Justisdepartementet bruker vi begrepet «sammensatte trusler» eller «sammensatte virkemidler» om situasjoner der en aktør bruker et spekter av virkemidler for å påvirke oss. Eksempler på det vi anser som mulig virkemiddelbruk er desinformasjon, investeringer i næringsvirksomhet, korrupsjon, sjikane mot myndighetspersoner, påvirkning av valg, rekruttering eller innplassering av innsidere/utro tjener i kommersielle eller offentlige virksomheter, samt digitale angrep.

Virkemidlene kan brukes hver for seg eller settes sammen og koordineres slik at de understøtter og forsterker hverandre. De kan også brukes over en lang tidsperiode. Vi må ruste oss på en slik måte at vi er motstandsdyktige mot det som måtte komme.

Norske borgere, politikere og offentlige og private virksomheter kan være utsatt for slik virkemiddelbruk. Vår tiltakspakke er derfor rettet mot veldig ulike nivå i det norske samfunnet.

Sammensatt virkemiddelbruk kan ha som mål å destabilisere samfunnet for å gjøre det mer sårbart. I en eventuell situasjon der vi befinner oss nær opp til eller i en militær konflikt, vil militær virkemiddelbruk kunne kombineres med ikke-militære virkemidler for å oppnå størst mulig effekt. Den potensielle bredden i virkemiddelbruken gjør det krevende å etablere en best mulig situasjonsforståelse på tvers av sektorer og ulike virkemidler. Dette kan svekke den eksisterende samfunnsorden og det fundamentet som liberale demokratier er bygget på ved å svekke tilliten mellom innbyggere, næringsliv og myndigheter, og ved å undergrave tiltroen til offentlige institusjoner og offentlige myndigheter og deres evne til å utføre sine oppgaver. Politiske stridsspørsmål kan gjøres til gjenstand for ekstern påvirkning, ikke nødvendigvis ved å gi støtte til en bestemt politisk posisjon, men ved å nøre opp under polarisering i samfunnet.

Nærmere om ulike arbeidsspor

Jeg vil nevne litt om fire hovedtemaer vi har jobbet spesielt med de siste årene.

Screening av utenlandsinvesteringer

Screening av utenlandsinvesteringer er en måte å motvirke økonomisk virkemiddelbruk til sikkerhetstruende virksomhet. Her har vi jobbet med regelverksutvikling for å styrke sikkerhetsloven som et verktøy, for å bedre kunne håndtere saker som kan dukke opp. Vi har sendt på høring endringsforslag til reglene i sikkerhetsloven kapittel 10 om eierskapskontroll, som skal sette oss bedre i stand til å håndtere denne trusselen.

Vi har identifisert et behov for en helhetlig oversikt over det totale fotavtrykket som enkelte økonomiske aktører har i Norge, med den kunnskapen om at hver enkelt investering eller oppkjøp eller finansiering av for eksempel forsknings- og utviklingsprosjekter isolert sett ofte er uproblematisk, men at det samlet over tid kan utgjøre en trussel mot nasjonale sikkerhetsinteresser. Sett under ett, og i lys av at enkelte stater jobber svært langsiktig med

virkemidler som tilsynelatende fremstår som rent kommersielle interesser, kan disse investeringene være uforenelig med nasjonale sikkerhetsinteresser. Å adressere disse utfordringene innebærer derfor blant annet å se et lands økonomiske engasjement i Norge samlet og over tid.

Vi har et bredt internasjonalt samarbeid på dette området, nettopp fordi denne trusselen er felles for veldig mange europeiske og vestlige land. Den kunnskapen som enkeltland har utviklet når det gjelder håndtering av utenlandsinvesteringer, ser vi at vi kan dra nytte av. De siste årene har vi også gjort oss egne erfaringer som vi kan bringe inn i det samarbeidet.

Kunnskapen om at enkelte stater bruker investeringer og oppkjøp som strategiske virkemidler, gjør at flere europeiske land, samt USA, Canada, Australia og New Zealand, vurderer tiltak for å redusere risikoen knyttet til utenlandske investeringer. Enkelte land har utviklet og bruker screening-mekanismer for å identifisere og håndtere denne risikoen. I Norge er vi så heldige å ha en tverrsektoriell sikkerhetslov med bestemmelser om eierskapskontroll og en tverrsektoriell sikkerhetsmyndighet, NSM. NSM er nasjonalt kontaktpunkt for screening.

Vi har også hatt et fokus på forskning som basis for politikkutvikling innenfor dette området. Trussel- og risikobildet som enkelte utenlandske investeringer kan representere, er felles for mange europeiske og vestlige land.

Trussel- og risikovurderinger fra EOS-tjenestene har fremhevet at flere stater bruker økonomiske virkemidler til andre formål enn forretninger. Investeringer og oppkjøp kan brukes som virkemiddel for å få innsikt i sensitiv informasjon knyttet til for eksempel beredskapsordninger, kritisk infrastruktur og politiske beslutningsprosesser. Det kan også gi tilgang til teknologi og ressurser av strategisk betydning. Kjøp av strategisk plasserte eiendommer kan for eksempel ha som formål å skaffe en plattform til fordekt etterretningsvirksomhet mot norsk og alliert militær aktivitet.

Desinformasjon og strategisk kommunikasjon

Desinformasjon kan utgjøre en vesentlig del av sammensatt virkemiddelbruk, men det kan også være et potent virkemiddel i seg selv. Fordekt påvirkning av valg er en trussel mot liberale demokratier, og kan brukes strategisk som virkemiddel av ulike aktører. Regjeringen lanserte en tiltakspakke for å styrke motstandsdyktigheten mot uønsket påvirkning ved årets stortings- og sametingsvalg. De 13 tiltakene var rettet både mot kandidater til valget, innbyggere, medier og de som er ansvarlige for gjennomføring av valget.

Et viktig tiltak er å styrke skolens viktige rolle i evnen til utvikling av kildekritikk. Kritisk tenkning, kildekritikk og kildebruk har blitt forsterket i det nye læreplanverket, som ble tatt i bruk i skolen fra høsten 2020. Videre er medienes rolle viktig. Diskusjonene og problemstillingene knyttet til sammensatte virkemidler er tidvis vanskelige, og heldigvis reises det diskusjoner i media om rollen myndighetene skal spille i disse problemstillingene. Redaksjonell uavhengighet er en absolutt forutsetning for de redaktørstyrte journalistiske medienes funksjon for den offentlige samtalen, og myndighetene må derfor være tilbakeholdne med tiltak som kan oppfattes som forsøk på å påvirke redaksjonelle beslutninger eller praksis. Dette er helt grunnleggende.

Viktigheten av strategisk kommunikasjon må sees i lys av det økende potensialet for at vi blir utsatt for desinformasjon. Strategisk kommunikasjon er en viktig del av det forebyggende

arbeidet, ved å forsøke å redusere effekten av fremmede aktørers påvirkning. Et grunnleggende prinsipp er derfor at norske myndigheters strategiske kommunikasjon rettet mot egen befolkning alltid skal være sannferdig.

Den menneskelige dimensjon

Den menneskelige dimensjonen er viktig inn i arbeidet med sammensatte virkemidler. Fremmede etterretningstjenester bruker store ressurser på å rekruttere både norske borgere og egne borgere som bor i Norge, og som har tilgang til informasjon eller andre verdier som er av betydning for den aktuelle staten.

Definisjonen på en innsider er en nåværende eller tidligere ansatt, konsulent eller innleid som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap. Eksternt rettede, og ofte svært kostbare, sikkerhetstiltak mister sin effekt dersom det er en innsider med tilgang gjennom sitt ansettelsesforhold som bevisst eller ubevisst kan skaffe trusselaktøren informasjon eller tilgang.

Internasjonalt samarbeid

Som tidligere beskrevet er internasjonalt samarbeid innenfor dette teamet veldig viktig. Sammensatte trusler står høyt på dagsorden i NATO, EU, og i andre internasjonale fora. Utfordringene ulike land møter for eksempel med hensyn til å etablere situasjonsforståelse, motvirke desinformasjon eller forebygge valgpåvirkning, er i stor grad sammenfallende. Internasjonal utveksling av erfaringer om trusselbildet, mulige tiltak og erfaringer fra håndteringen av konkrete trusler er derfor av stor verdi.

Norge sluttet seg i 2017 til «Center of Excellence for Countering Hybrid Threats» i Helsinki i Finland. Senteret ble etablert i 2017 på oppfordring fra EU og med støtte fra NATO. Det er åpent for land som er medlem av NATO og/eller EU. Pr. 1. oktober 2020 er 27 land medlem. Det er høy aktivitet ved senteret, primært gjennom en rekke ulike fagmøter om relevante problemstillinger. Senteret har tre faste arbeidsgrupper: 1) Påvirkning, 2) Motstandsdyktighet og 3) Strategi og forsvar.

Norge, ved Forsvarsdepartementet, er ledernasjon i NATOs integritetsprogram. Dette har som formål å styrke integriteten i medlemslandene, hos partnere og i NATOs organisasjon, samt redusere risikoen for korrupsjon og annen uønsket påvirkning.

Sammensatte trusler er også tema i det nordiske samfunnssikkerhetsarbeidet, det såkalte Haga-samarbeidet. Dette samarbeidet ble politisk initiert i 2009. Det felles overordnede målet er å styrke de nordiske lands evner til å forebygge og redusere konsekvenser av større ulykker, natur- og menneskeskapte katastrofer, samt andre samfunnskriser innen beredskapsområdet.

Avslutning

Sammensatte trusler/sammensatte virkemidler er et område som vi i Justisdepartementet jobber med til daglig. Det er utstrakt samarbeid mellom Justisdepartementet, Forsvarsdepartementet og Utenriksdepartementet om temaer innenfor denne porteføljen.

Hybride trusler og folkerett

Cecilie Hellestveit (PhD) (Folkerettsinstituttet/NIM)

Jeg skal presentere hybride trusler fra et folkerettslig perspektiv. Innledningsvis sier jeg litt om hybride trusler i et historisk lys (1). Dernest går jeg inn på spørsmålet om folkerettslig terskel: hvordan folkeretten regulerer hybride virkemidler avhenger av om de benyttes i eller utenfor væpnet konflikt (2). Jeg behandler så hva som anses som militære mål i væpnet konflikt og hvordan hybride problemstillinger fungerer under humanitærretten (3). Deretter tar jeg for meg de folkerettslige reglene som gjelder for hybride virkemidler utenfor væpnet konflikt (4). Avslutningsvis kommer jeg inn på attribusjon, altså hvordan man ilegger ansvar når hybride virkemidler har blitt benyttet (5).

Presentasjonen er overordnet, og tegner opp et større lerret enn de mer detaljerte reglene knyttet til cyberoperasjoner som vil bli gjennomgått senere. Hensikten er å plassere hybride trusler i folkerettslandskapet.

Intet nytt under solen. Hybride trusler i et folkerettslig perspektiv

Hybride trusler (som noen heller betegner som sammensatte virkemidler) er et samlebegrep for økonomiske, rettslige, sosiale og informasjonsmessige pressmidler som utnyttes til samme eller lignende formål som tradisjonelle militære maktmidler. Hybride trusler har det til felles at de kan benyttes med formål eller effekter som minner militære virkemidler. De kan benyttes istedenfor mer klassiske militære virkemidler eller i samvirke med militærmakt.

Slike pressmidler er omtrent like gamle som krigføring selv. Da jeg arbeidet med min doktoravhandling, sto «asymmetrisk krigføring» sentralt i diskursen. Asymmetriske trusler ble fremstilt som noe helt nytt som folkeretten ikke hadde tatt høyde for. Etter hvert som jeg gravde meg ned i historiske kilder, viste det seg imidlertid at litteratur fra 1700- og 1800-tallet også forholdt seg til asymmetri, og at problemstillingene hadde blitt diskutert og forvaltet helt tilbake til 1600-tallet. Min påstand er at i likhet med «asymmetrisk krigføring», representerer heller ikke hybride trusler noe nytt under solden. Hybride pressmidler er et gammelt fenomen.

I de senere år har bruken av hybride pressmidler økt i grad og omfang. Teknologisk utvikling, globalisering og rettsliggjøring av samfunnet har i sum gjort at hybride virkemidler rammer samfunnet i større grad. Det kan dreie seg om digitale angrep på infrastruktur, sabotasje, elektronisk krigføring eller økonomiske virkemidler. Eller det kan innbefatte påvirkningsoperasjoner, terrorlisting eller det å slippe en mengde flyktninger over en grense. Effektene av hybride virkemidler er større enn tidligere.

Samtidig blir verden mer urolig. Det er også flere væpnede konflikter i verden enn noensinne etter andre verdenskrig. Rivalisering blant globale og regionale stormakter gir seg utslag i militær opprustning, men det er særlig på ikke-militære områder at den tiltagende motsetningen mellom store stater spiller seg ut. Her blir hybride virkemidler benyttet i tiltagende grad. Dette gjør at også omfanget av slike virkemidler øker.

I et folkerettslig perspektiv er imidlertid hybride trusler ikke noe grunnleggende nytt. Økende effekter og bruk av hybride virkemidler påvirker ikke i seg selv de folkerettslige rammene, fordi folkerettens regler for krig og fred har blitt utviklet med denne typen virkemidler i mente.

Hybride virkemidler rikker ikke ved hovedhensynene bak reglene for krig i folkeretten. Både de kodifiserte reglene i traktater og de ukodifiserte reglene som anses som sedvanerett er gjennomsyret av to hovedhensyn. For det første er det hensynet til freden. Reglene skal hindre utbrudd av krig særlig mellom stater. Reglene er derfor innrettet og tolkes slik at de skal unngå å gi incitament til eskalering av stridigheter. For det andre dreier det seg om hensynet til individet. Dette må ikke reduseres til kun hensynet til de sivile. Det er hensynet til stridende og sivile – altså hensynet til å beskytte alle individer som rammes av væpnet konflikt som de ikke selv har ansvar for eller kan kontrollere gangen i – altså i praksis alle som deltar i eller berøres direkte av partenes krigføring. Disse to hovedhensynene står seg også i en virkelighet med hybride trusler.

Folkerettens funksjon er at den rammer inn hybride trusler. Hvilket folkerettslig regime hybride trusler reguleres av beror på om virkemidlene benyttes i eller utenfor en væpnet konflikt. Det er folkeretten som knesetter terskelen for væpnet konflikt og for hva som anses å være virkemidler i den væpnede konflikten.

Terskelspørsmålet. I eller utenfor væpnet konflikt?

Hybride virkemidler kan alene eller i kombinasjon med militære virkemidler være tilstrekkelig til å nå terskel for væpnet konflikt. Da beveger man seg inn i et nytt regelregime under folkeretten. I praksis rammer derfor folkerettens regler inn «the playing field» for hybride virkemidler. Dersom terskelen nås, kan situasjonen raskt eskalere. Samtidig gjør den folkerettslige terskelen at statlige aktører kan spekulere i hvordan de benytter hybride virkemidler til å presse en motstander så lenge de holder seg under terskel.

I det følgende er det tale om terskelspørsmålet under humanitærretten, altså reglene for krigføring, *in bello*. Dette må ikke blandes sammen med det separate og tidvis forskjellige terskelspørsmålet under FN-pakten og reglene for bruk av makt på fremmed territorium, *ad bellum*.

Folkerettens regler om terskel for «væpnet konflikt» fremgår av de fire Genève-konvensjonene av 1949 fellesartikler 2 og 3 med tilleggsprotokoller. Genèvekonvensjonene er ratifisert av samtlige stater i verden. De anses i tillegg til å være sedvanerett. Genèvekonvensjonene kommer derfor til anvendelse over alt både i kraft av traktatrett og sedvane. Etter Genèvekonvensjonene finnes det tre ulike terskler. Hvilken terskel som gjelder i et gitt tilfelle, avhenger av hvilke parter som er involvert og hvor stridighetene finner sted.

Mellomstatlig konflikt etter Genèvekonvensjonenes fellesartikkel 2 foreligger ved væpnet sammenstøt mellom de væpnede styrkene til to eller flere stater. I slike tilfeller er terskelen lav før man er over i en væpnet konfliktsituasjon etter folkeretten. Det eneste som kreves er interaksjon med våpen mellom de væpnede styrker fra to stater. I 2019 fant det sted en interaksjon mellom kinesiske og indiske soldater i fjellene i et pass mellom Kina og India. De militære styrkene fra de to atomvåpenmakter kom i håndgemeng. Soldatene benyttet never, stein og stokker i kampen, og holdt seg unna det vi må kunne kalle stridsmidler. Minst 20 soldater mistet livet på indisk side og et ukjent antall på kinesisk side. Selv om tallet «mer

enn 20 dødsfall på slagmarken» kan være over det SIPRI og PRIO regner som væpnet konflikt, var dette trolig under terskel etter Genèvekonvensjonenes fellesartikkel 2. Selv om det dreide seg om to militærapparat, unnlot de å benytte seg av militære maktmidler og det var følgelig ikke en væpnet interaksjon. Episoden var derfor trolig under terskel, og det forelå ingen «væpnet konflikt» mellom Kina og India.

Samme år ble India rammet av en terroraksjon organisert av en ikke-statlig gruppe som opererte fra pakistansk territorium. India svarte med å bombe treningsleirer for gruppen på pakistansk territorium. Operasjonen var ikke klarert med pakistanske myndigheter. De svarte med å skyte ned et av de indiske jagerflyene. Piloten overlevde og ble tatt til fange. Episoden ble ansett for å utgjøre en militær interaksjon mellom de militære styrkene fra to stater som nådde terskel for væpnet konflikt. Konklusjonen var at interaksjonen hadde vært en «væpnet konflikt» etter Genèvekonvensjonenes fellesartikkel 2 som gikk ut på at indiske militære bombet pakistansk territorium og pakistanske militære skjøt ned et indisk bombefly. Imidlertid var konfliktens stridigheter over. Følgelig oppsto plikt for konfliktens parter under til å overlevere krigsfanger etter tredje Genèvekonvensjon. Piloten måtte derfor returneres til India uten opphold, politisk kjøpslåing eller andre viderverdigheter. Slik ble også situasjonen løst. For vårt formål er det sentrale at terskelen for «væpnet konflikt» er lav så lenge det er tale om væpnet interaksjon mellom militære aktører fra to stater.

Utfordringen oppstår når det er andre statlige aktører enn de militære som står for maktbruken, for eksempel fiskekontrollører eller tollvesen. Her må det normalt mer maktbruk til for at terskelen skal anses å være nådd. Et beslektet problem oppstår når maktbruken kommer fra en ikke-statlig aktør hvor tilknytningen til statsmakten eller de væpnede styrkene er uklar. Også i slike tilfeller antas terskelen for «væpnet konflikt» å være noe høyere. Hybride virkemidler fra statlige aktører vil gjerne nettopp befinne seg i disse to kategoriene. Det skal derfor gjerne betydelig mer til for at hybride virkemidler gjør at det foreligger «væpnet konflikt» mellom stater. Folkeretten gir følgelig et betydelig handlingsrom til stater for å benytte hybride trusler uten at det når terskel.

Borgerkrig reguleres etter Genèvekonvensjonenes 2. tilleggsprotokoll, og foreligger ved utstrakt væpnet sammenstøt mellom de væpnede styrkene til en stat og en ikke-statlig militær aktør på statens territorium. Dette er en terskel som er høy i den forstand at den stiller vesentlige krav til karakteren til den ikke-statlige aktøren. Gruppen må være organisert på en måte som minner om militære styrker, ha et disiplinærsystem og være i stand til å organisere militære operasjoner av en viss styrke og varighet. Gruppen må også ha territoriell kontroll. Årsaken til den høye terskelen har sammenheng med statsmaktens rett og plikt til rettshåndhevelse på suverent territorium. Dersom for eksempel en gruppe kvener skulle ønske å frigjøre den kvenske befolkningen fra Norge og organiserer en væpnet motstand mot statsmakten med dette formål, vil terskelen for borgerkrig under 2. tilleggsprotokoll være svært høy. Utgangspunktet er at norske myndigheter både har rett og plikt til å bruke rettshåndhevelsesvirkemidler på norsk territorium. Det er først når kvenenes organisering begynner å bli så sterk at gruppen kan stå imot statlige myndigheter (organisering, militær kapasitet og territoriell kontroll) at den høye terskelen og det omfattende regelregimet for den ikke-statlige aktøren under 2. tilleggsprotokoll kommer til anvendelse. Hybride virkemidler vil vanligvis ikke bidra til å kvalifisere for terskel under 2. tilleggsprotokoll. Her er det objektive kriterier til den ikke-statlige aktørens karakter og evne til militær virkemiddelbruk som er avgjørende. Cyberangrep eller påvirkningsoperasjoner vil i

liten grad reflektere hensynene bak vilkårene - at den ikke-statlige aktøren har en form og organisering som setter den i stand til å implementere protokollen.

Til slutt er det terskelen etter Genèvekonvensjonenes fellesartikkel 3. Dette er det laveste multiplum som vil komme til anvendelse dersom det forekommer to aktører som kan være parter i humanitærrettslig forstand (stater eller ikke-statlige aktører), og stridighetene mellom dem er av en slik karakter at terskel er nådd. Mange situasjoner i våre dager vil dreie seg om ikke-statlige aktører og statlige aktører som er involvert i fiendtlige handlinger over en internasjonal grense. Genèvekonvensjonenes fellesartikkel 3 gjelder uavhengig av grenser og territorier. Den stiller enkelte grunnvilkår til organiseringen av den ikke-statlige aktøren (men mindre krav enn under 2. tilleggsprotokoll). Samtidig stiller den krav til sammenstøtenes karakter. Opptøyer og interne uroligheter faller utenfor.

Likevel er det både uklarhet og uenighet om hvor terskelen ligger i enkelte tilfeller. I dette farvannet vil man imidlertid nettopp finne mange av de hybride virkemidlene. En del av de ikke-statlige aktørene som driver med hybrid virkemiddelbruk (cyber angrep, sabotasje og enkelte terrorangrep) vil ha en statlig støttespiller som trekker i trådene. Den internasjonale domstolen i Haag tok i en sak fra 2004 (Folkemordsaken) stilling til vilkåret for å attribuere slike handlinger til den statlige aktøren når det gjelder statsansvar (det er «effektiv kontroll»). Imidlertid valgte domstolen å ikke ta endelig standpunkt til attribusjon for det som er spørsmålet her: altså hvor mye statlig støtte eller kontroll skal til før en ikke-statlig aktør anses for å være «statlig» i forhold til å etablere om en væpnet konflikt foreligger etter fellesartikkel 2. Domstolen insinuerte at dette kanskje er «overordnet kontroll», altså mindre strengt enn for statsansvar, men har ikke tatt endelig stilling til spørsmålet. Også i forhold til terskel under fellesartikkel 3 er det følgelig et betydelig handlingsrom for stater til å utnytte ikke-statlige aktører.

Et eksempel til illustrasjon er konfliktsituasjonen mellom de to statene Iran og Israel. I denne relasjonen benyttes hybride virkemidler i utstrakt grad. I Syria, Irak og Jemen har det de siste årene vært militær interaksjon mellom aktører som støttes av Iran og israelske militære. De fleste tilfellene dreier dette seg om sammenstøt mellom iransk-støttede ikke-statlige aktører og israelsk militærmakt utenfor israelsk territorium. Dette reguleres av fellesartikkel 3, men det impliserer ikke Iran og Israel direkte mot hverandre. De angrepene som har blitt iverksatt direkte mot iranske militære kapasiteter i Syria forblir gjerne uavklarte, og Israel påtar normalt ikke ansvaret for slike angrep. Likevel vil foreligger det trolig en væpnet konflikt under Genèvekonvensjonene mellom iranske soldater og israelske militær. Den er imidlertid begrenset til det syriske territoriet. Operasjonene mellom de to aktørene via tredjeparter i Irak eller Jemen kumuleres ikke som del av denne konflikten, men ses på som separate situasjoner. De når følgelig ikke terskel. Cyberaksjoner og elektronisk krigføringsmidler har vært benyttet i utstrakt grad på henholdsvis iransk og israelsk territorium. Her er det imidlertid vanskelig å attribuere handlingene. I sjødomenet har man det forekommet sabotasjeaksjoner på skip, selv om det stort sett har foregått uten tap av menneskeliv.

Dersom operasjonene i de ulike land og domener hadde blitt kumulert, ville det trolig foreligget en «væpnet konflikt» mellom Israel og Iran. Folkerettens system er imidlertid satt opp for å motvirke eskalering. I dette tilfellet er det separasjon mellom ulike territorier og domener som fungerer slik. Samtidig gir det begge parter handlingsrom til å benytte hybride virkemidler uten å frykte en ukontrollerbar eskalering til full mellomstatlig konflikt mellom

Israel og Iran «i hele regionen». I denne sammenhengen fungerer dermed terskelspørsmålet tilretteleggende for bruk av hybride virkemidler.

Utfordringene med hybride virkemidler og folkerettens terskel for væpnet konflikt i relasjonen mellom stater er mange. Stater opererer gjerne innenfor mange ulike domener. Bruk av ikke-statlige aktører innenfor ett eller flere av domenene vil bidra til å redusere risikoen for kumulering til terskel. Særlig innenfor sjødomenet er det vanskelig å identifisere hvilket opphav båter som angriper skip har, for eksempel de norske petroleumsfartøyene som ble angrepet i Gulfen i 2019 og iranske fartøyer som har blitt angrepet utenfor Jemens kyst. Selv om en cyberoperasjon har stor militær effekt, som Stuxnet som i sin tid førte til at 5000 anriknings-sentrifuger i Iran ble satt ut av effekt og trengte 18 måneder å bli reparert, er det vanskelig så lenge det ikke er helt klart hvem som står bak. Enda vanskeligere blir det jo lengre bort man kommer fra det tradisjonelle militære virkeområdet. Angrepet mot det saudiarabiske nasjonale oljeselskapet Aramco i 2012 satte 33 000 datamaskiner ut av drift. En tilsvarende effekt hadde krevet et omfattende militært angrep. Ettersom det var et selskap som var angrepet, og ingen tok på seg ansvaret, kunne dette vanskelig være et virkemiddel som talte i relasjonen mellom Saudi-Arabia og en stat som kunne stå bak. En beslektet episode fant sted i 2012 da det forekom en cyberoperasjon mot amerikanske finansinstitusjoner etter at en amerikansk produsent hadde laget en film om islam. De som ble ansatt å stå bak var Qassam-brigadene. Imidlertid var det uklart hvilken forbindelse denne ikke-statlige aktøren hadde til iranske myndigheter. Slike hybride virkemidler kan være vanskelig å knytte til en statlig aktør slik at det overhode blir tale om terskelspørsmål. Ikke-statlige aktører eller «plausible deniability» på annet vis gjør at det er langt opp til terskelen slik den er definert i folkeretten. Dertil vil hybride virkemidler typisk ikke virke samtidig, men være svar og motsvar, på en måte som gjør at det ikke er naturlig å karakterisere det for stridigheter slik dette er tenkt under folkeretten. Summen av disse elementene gjør at handlingsrommet til hybride virkemidler er betydelig for statlige aktører i rommet under terskel.

I det øyeblikket man kommer over terskel åpner det seg imidlertid en helt annen verktøy-kasse. Da er risikoen for utilsiktet eskalering betydelig. Derfor er det også en tendens blant verdens stater til å være tilbakeholden med å tolke hybride virkemidler som om de var militære for å komme over terskel, selv om effektene av hybride virkemidler kan være minst like alvorlige som militære maktmidler. Denne tilbakeholdenheten er i sin tur med på å skape enda større handlingsrom for stater som i utstrakt grad benytter seg av hybride virkemidler.

I væpnet konflikt. Hva er militære mål i en hybridsituasjon?

I det øyeblikk forholdet mellom to parter når terskel for «væpnet konflikt» etter folkerett, trer et helt annet regelverk i kraft. Dette skjer automatisk, basert på faktiske forhold og hva partene gjør, ikke hva partene sier eller hvordan partene klassifiserer forholdet.

Nå må angrep begrenses til det som er «militære mål» etter folkerettens regler. Innenfor landdomenet og luftdomenet er reglene for militære mål individorientert. Militære mål er individer som har en tilknytning til de væpnede styrkene, kombattante. Det kan også være basert på funksjon, altså sivile som deltar i stridighetene. I sjødomenet er det annerledes. Her er reglene plattformorientert. Det er fartøyene og deres tilknytning som er avgjørende,

og i noen tilfeller også deres funksjon. Reglene for gjenstander er derimot funksjonsorientert uavhengig av domene. Gjenstander er militære mål dersom de på grunn av sin natur, plassering, formål eller bruk gir et faktisk bidrag til militær handling og hvis ødeleggelse gir en klar militær fordel.

I cyberdomenet er det særlig reglene for gjenstander som dominerer. Et spørsmål er om en slik forståelse også omfatter individer i cyberdomenet. Den unge hackeren som sitter med en joystick et sted langt unna et lovlig militært mål, langt unna det som kan kalles en slagmark i humanitærrettslig forstand, er også han et militært mål som følge av sin «digitale funksjon»? Et annet spørsmål er knytte til data, altså informasjon. Er dette å regne for en «gjenstand» i humanitærrettslig forstand? Og det er i så fall den funksjonen som data har i den væpnede konflikten som skal være utgangspunktet for hvorvidt det kan angripes eller ikke? Ettersom strukturene ser annerledes ut i cyber, vil tradisjonelle avgrensninger av militære mål gjerne få helt andre (og betydelig mer ødeleggende) effekter enn det som er reglenes intensjon i den kinetiske verden.

Et annet spørsmål som oppstår i tilknytning til hybride virkemidler i væpnet konflikt, er hva som må anses som «militære angrep». I en væpnet konflikt vil gjerne de hybride virkemidlene fortsette med full styrke, eller også tilta i styrke. Enkelte av virkemidlene som i størst grad presser motparten, hindrer tilgang på logistikk, våpen eller penger, ikke er omfattet av krigens folkeretts regler for krigføring. Om man angriper et våpenlager, er det et angrep som dekkes og hvor det er klare krav til vurderinger av sivil følgeskade. Om man sørger for at våpenlageret forblir tomt gjennom sanksjoner eller gjennom blokader, er dette i mindre grad omfattet av reglene for stridighetene slik krigens folkerett tradisjonelt virker.

Under krigens folkerett og i reglene for sjøkrig, er blokader regulert. Under krigen i Jemen har flere havner vært underlagt blokader gjennom mange år. Dette har vært håndheving av FN-sanksjoner, men krigførende parter som har håndhevet blokaden har gjort dette på måter som tidvis ville kommet på kant med reglene for blokader under reglene for sjøkrig. Selv om sanksjoner har FNs Sikkerhetsrådet i ryggen, vil de ikke likefult reguleres av sjøkrigens regler når de håndheves av krigførende parter med militære virkemidler, eller blir dette «hybride virkemidler» fordi en part har Sikkerhetsrådet i ryggen? Tilsvarende spørsmål oppstår rundt økonomiske virkemidler mot valutaen til en part man er i krig med. Hadi-regjeringen, Saudi-Arabia og Emiratenes beslutning om å flytte den jemenittiske sentralbanken fra Sanaa til Aden i 2016 hadde katastrofale følger for tilgangen til mat, medisiner og i noen grad våpen for motparten i Jemen-krigen. Er dette likevel virkemidler som ikke regnes som «militære» i den væpnede konflikten, og derfor går klar av reglene om sivil følgeskade? Endel typer hybride virkemidler har også en uklar posisjon dersom det oppstår væpnede konflikter hvor krigens regler regulerer forholdet mellom partene.

Utenfor væpnet konflikt. Hvilke regler gjelder?

Befinner man seg utenfor væpnet konflikt, er det reglene for rettshåndhevelse som gjelder. Her er det de internasjonale menneskerettighetene som er folkerettens ramme, og inngrep i disse rettighetene må ha lovlige formål, være nødvendige og proporsjonale. Menneskerettighetsregimet gjelder fullt ut og binder statsmakten på eget territorium. Spørsmålet er hva som gjelder dersom statlige myndigheter opererer utenfor eget territorium, altså ekstraterritorielt. Et særlig krevende spørsmål er hvordan folkeretten regulerer ikke-statlige aktører som benyttes som statlige agenter for hybride virkemidler,

men som opererer fra utlandet, inn i tredjeland. Her er folkerettens regler i større grad tilpasset en internasjonalisert økonomi drevet av ikke-statlige selskaper enn en verden der ikke-statlige aktører er brikker i et statlig spill gjennom hybride virkemidler.

Når det gjelder rammene for ekstraterritorielle menneskerettighetsforpliktelser, altså hvilke folkerettslige regler som gjelder for operasjoner som foregår utenfor eget territorium, er det stor uenighet internasjonalt. Europeiske land som er underlagt den europeiske menneskerettighetsdomstolen og latinamerikanske stater har ganske strenge regler for dette, og mener at all aktivitet, også utenfor territoriet, i noen grad er regulert av menneskerettighetsregimet. Den tyske konstitusjonsdomstolen konkluderte i 2021 med at den tyske etterretningstjenesten er underlagt grunnlovsbestemmelsene om menneske-rettigheter også for operasjoner utenfor tysk territorium. USA, Russland og Kina, samt en rekke land i Afrika og Midtøsten har et annet syn. Her er det altså betydelig uenighet mellom statene om hva som er rammene i folkeretten, noe som også forplanter seg inn i diskusjonene om folkerettens regulering av hybride virkemidler. Også fra dette perspektivet gjør uklarheter og uenigheter om folkerettens regler at det blir en (vel stor) «playing field» for hybride virkemidler.

Attribusjon. Hvordan ilegge ansvar?

Det siste jeg skal berøre er hvordan folkeretten regulerer spørsmålet er hvordan man ilegger ansvar for hybride virkemidler. Det finnes tre ulike typer attribusjon.

Teknisk attribusjon, eller identifikasjon, er en faktisk og teknisk undersøkelse som fastslår hvem som sannsynligvis står bak en handling og som tar stilling til hvor sannsynlighets-graden. Innenfor cyberdomenet vil det dreie seg om hvilken maskin som har blitt benyttet, hvilken person som står bak og hvilken ruter angrepet har gått gjennom.

Politisk attribusjon er en politisk beslutning som går ut på å beslutte å tillegge en handling til en identifisert aktør. Formålet med politisk attribusjon er politiske effekter. Det kan foregå internt eller det kan offentliggjøres. Dersom politisk attribusjon offentliggjøres, er det gjerne for å klargjøre hvem man holder ansvarlig. Slik attribusjon får gjerne politiske følger. Man kan velge å reagere med retorsjoner, å utvise diplomater eller andre former for politiske reaksjoner. Politisk attribusjon har ikke rettslige følger. Dermed er det ikke nødvendig å vente på at for eksempel en strafferettslig etterforskning i regi av PST skal ferdigstilles. Ettersom politisk attribusjon har politiske effekter, stilles det også lavere krav til bevis.

Folkerettslig attribusjon er derimot en beslutning om å attribuere en gitt handling eller oppførsel til en annen stat, med den konsekvens at det får folkerettslige konsekvenser. Her vil attribusjonstypene variere med hvem som foretar attribusjonen og formålet med attribusjonen. For det første kan statene selv foreta folkerettslig i attribusjon. Dette innebærer at en stat erklærer at man anser at det har forekommet et folkerettsbrudd og hvem man anser som ansvarlig. Deretter tyr staten til mottiltak, eller «counter measures» på engelsk. Mottiltak åpner for muligheten til å bryte enkelte folkerettsregler i retur eller å foreta andre, mer kvalifiserte reaksjoner. Dette kan gjøres av enkelt stater eller av et kollektiv av stater.

En annen type attribusjon foregår når et kompetent folkerettsorgan foretar attribusjon. Det kan være en internasjonal domstol eller FNs sikkerhetsråd på enkelte bestemte områder. I slike tilfeller er formålet å avgjøre en folkerettstvist. Og det kan være tvisteløsning,

erstatningsansvar, strafferettslig ansvar, etterfølgende vurderinger av en stats mottiltak og maktbruk. FNs sikkerhetsråd kan for eksempel slå fast hvem rådet anser for å stå bak et væpnet angrep (attribusjon) og på bakgrunn av dette autorisere maktbruk mot vedkommende stat eller ikke-statlige aktør under kapittel VII.

Den tredje typen folkerettslig attribusjon handler om automatiske effekter. Spørsmålet om en stat involveres sammen med annen væpnet aktør i slik grad at staten impliseres i en væpnet konflikt er et slikt spørsmål, enten som medstridende part (co-belligerent) eller som statlig aktør med så mye involvering at det innebærer at terskel for væpnet konflikt mellom stater er nådd, som nevnt over. Dersom Israel skulle fastslå at Iran står bak et angrep og velger å svare, vil dette være en attribusjon som medfører at en «væpnet konflikt» under fellesartikkel 2 anses å foreligge. Dette er en mekanisme som er mye mer umiddelbar enn den som handler om kompetente folkerettsorganer over. Det som er viktig for vårt formål, er at attribusjon ikke er begrenset til internasjonale domstoler, langt unna i tid og rom. Attribusjon har altså også mye mer umiddelbare følger under folkeretten.

Hovedutfordringen med hybride virkemidler ligger nettopp her. Ettersom hybride trusler i sin natur har en uklar opphavsaktør, og det vanligvis følger med en «plausible denial», fungerer ikke folkerettssystemet slik det normalt vil gjøre, fordi mye vil handle om bevisbyrde i disse sakene. Innenfor cyber er det krevende å klargjøre hvem som egentlig står bak en operasjon, særlig dersom opphavsaktør har gjort mye for å skjule dette. Dersom et cyber-angrep attribueres til en stat syv år etter at et angrep fant sted, er det begrenset hvilke reaksjoner som kan forekomme. Det er også krevende å etablere en link mellom et individ og en stat. Hvilken type tilknytning må etableres mellom en ikke-statlig russisk hacker og russiske myndigheter før man kan legge til grunn at russiske myndigheter står bak? Hvor mye og hvilken type informasjon trenges for å konstatere at denne ikke-statlige aktøren opptrer på vegne av en stat?

Et annet alvorlig problem er at når det ikke er mulig å fastslå helt sikkert hvem som står bak, vil det gjerne være en presumsjon for at det er en statlig aktør som man har et dårlig forhold til som har iverksatt en operasjon. Slik sett legger reglene i dag opp til svært uheldige åpninger for tredjeparter (stater eller ikke-statlige aktører) for å blande seg inn i forholdet mellom to stater og provosere frem eskalering.

Avslutningsvis kan vi konkludere med at når hybride virkemidler benyttes like undre terskel for væpnet konflikt, har stater og ikke-statlige aktører et betydelig spillerom. Dette er et område hvor folkerettens regler er lite håndhevbare, uklare og i noen grad omstridte blant ganske sentrale makter i verden. I det øyeblikk man krysser grensen til en væpnet konflikt, er derimot reglene klare. Endel av de hybride virkemidlene som benyttes parallelt med de militære virkemidlene vil likevel gjerne falle utenfor reglene for krigføringen. Slik fungerer folkerettens regler i dag, til tross for at det gjerne er disse virkemidlene som i aller størst grad vil forårsaker lidelser blant sivilbefolkningen.

Del 2: Cyberoperasjoner

Innledende kommentarer

Tobias Köhler (Norges Røde Kors)

Vi har hørt masse om hybride trusler og den praktiske håndteringen her i Norge. Vi har hørt om hvordan folkeretten egentlig bryr seg om tematikken, og særlig under terskelen for væpnet konflikt. Nå skal vi gå inn i krigens folkerett, og få en større forståelse for hvordan humanitærretten eller krigens folkerett regulerer cyberkrigføring.

Mens hybride trusler kommer i mange former, utgjør cybermetoder en stor andel som fortjener en grundigere betraktning. Denne økten samlet tre perspektiver: først, definisjoner og posisjoner i cyberdomenet under krig i en presentasjon fra dr. Camilla G. Cooper (Forsvarets høgskole) av det tilsvarende kapittelet i den kommende oppdateringen av norsk manual i krigens folkerett. Den norske manualen tydeliggjør Norges posisjon om at cybermetoder i væpnet konflikt er regulert av humanitærretten. I dag er det endelig enighet om dette også blant stater generelt. Allerede i 2013 ble data ansett av Norge som objekt i seg selv, og dermed beskyttet i henhold til humanitærretten hvis den er sivil. Samtidig understrekte Cooper problemet med at kommunikasjonsinfrastruktur er ofte brukt av både sivile og militære aktører.

Dette ble etterfulgt av en presentasjon fra Forsvaret om hva cyberoperasjoner innebærer praktisk sett og hvordan man går frem for å nå målet og unngå utilsiktete følgeskader. Presentasjonen ga innsikt i hva som foregår i dag i cyberområdet. Konsekvensene er målbare, ikke minst i penger som ble brukt til å komme seg ut av et angrep med løsepengevirus. Bidrag av data fra hver eneste bruker og «the internet of things» osv. forstørrer angrepsflaten og dermed muligheten til å påvirke personer, men også samfunn og stater, med cybermetoder. Det finnes bare få eksempler av fysiske skader som en direkte følge av cyberoperasjoner, men flere stater utvikler kompetanse og viser interesse for å bruke dette domenet på en offensiv måte. Samtidig gjør kompleksiteten av slike operasjoner kombinert med kompleksiteten av moderne samfunn og infrastruktur det vanskelig å beregne effektene av en offensiv operasjon helt riktig.

Med det som bakteppe presenterte dr. Tilmann Rodenhäuser (ICRC, Genève) nøkkelutfordringene i IHR under cyberoperasjoner, med søkelys på hvordan sivile og sivil infrastruktur kan bli – og i realiteten blir – påvirket. Det er i praksis en fare for at følgeskader fort blir ganske store, noe som ikke er overraskende i en verden som blir mer og mer digitalisert. I forbindelse med dette ble det presentert et ICRC-prosjekt som undersøker blant annet om det kan være hensiktsmessig å bruke et beskyttende emblem i cyberdomenet for å markere beskyttete objekter, et «digitalt beskyttelsesemblem». Det er ikke klart enda om det er praktisk mulig, og i tillegg om det til og med kunne svekket beskyttelsen. Dessverre hadde han ikke anledning til å sende et skriftlig bidrag.

Cyberoperasjoner og krigens folkerett

Camilla G. Cooper (PhD) (Forsvarets høgskole)

Presentasjonen om cyberoperasjoner og krigens folkerett tok utgangspunkt i arbeidet som er gjort med å utvikle et eget kapittel for cyberoperasjoner i kommende versjon av den norske Manual i krigens folkerett. Jeg utviklet gjeldende versjon sammen med Lars Morten Bjørkholt (HV), og har de siste årene jobbet med å oppdatere denne. Utkastet er oversendt til FD for godkjenning. Det betyr at denne presentasjonen er basert på mitt forslag, men forslaget er utarbeidet i tett dialog med FD, så det forventes primært mindre endringer.

Ettersom ikke alle som er like kjent med Manual i krigens folkerett, vil jeg innledningsvis gi en kort introduksjon til denne. Så vil fokus være på de områdene som det har vært mest viktig og vanskelig å definere for å kunne gi bedre veiledning på for hvordan krigens folkerett skal anvendes i cyberdomenet. Disse er angrep, objekt og reglen om at sivile mister beskyttelse mot angrep i den tid de deltar direkte i fiendtligheter.

Om manual i krigens folkerett

Manual i krigens folkerett ble først utgitt i 2013, og var den første versjonen av en slik publikasjon i Norge. Den gir uttrykk for hva som er norsk syn på gjeldende rett og hvilke ytterligere begrensninger det er ønskelig å oppfordre til. Med unntak av blant annet noen innledende kommentarer om når det er lov å bruke makt mot en annen stat eller annen stats territorium, er fokus på krigens folkerett. Dette er også fokus i denne presentasjonen; hvordan folkeretten regulerer cyberoperasjoner når en væpnet konflikt er i gang. Det betyr blant annet at jeg ikke vil gå inn på spørsmål knyttet til hva som utgjør et cyberangrep i fred og krise, altså under terskelen for væpnet konflikt. Her har Regjeringen i mai i år (2021) gitt ut en erklæring, med tittelen «Norwegian positions on selected questions of international law relating to cyberspace», hvor de presenterer norsk syn på blant annet hva som utgjør et væpnet angrep etter FN-pakten i cyberdomenet.

Målgruppen for manualen først og fremst er norske styrker og andre som jobber med krigens folkerett i Norge. Dette har vært med på å definere språk, omfang, hva som prioriteres og formatet – for eksempel var Telemark Bataljon (TMBN) veldig klare på at den måtte trykkes, ha spiralisert rygg så den ikke lukker seg selv, og passe i lomma på feltbuksa. Sekundært er den med på å utvikle sedvaneretten på området siden den gir uttrykk for hvordan Norge som stat mener folkeretten skal tolkes.

Manualen er underlagt en instruks fra FSJ om at den er bindende for Forsvaret, og senere er dette utvidet til å gjelde hele Forsvarssektoren. I gjeldende versjon er cyber behandlet over noen få sider på slutten av kapitlet om krigføringsmetoder. Nå skal det som nevnt bli et eget kapittel.

Hva utgjør et angrep?

Mange av reglene i krigens folkerett er knyttet til planlegging og gjennomføring av angrep. Her menes da angrep i en pågående væpnet konflikt, ikke for eksempel angrepet på Stortinget i fjor høst. Dersom en cyberoperasjon er å anse som et «angrep» etter krigens folkerett, har dette betydning for hva operasjonen kan rettes mot, hvordan den skal

gjennomføres, og plikten til å beskytte sivile mot virkningen av operasjonen. Det er for eksempel forbudt å rette angrep mot sivile personer eller objekter. Det er derfor sentralt å avgjøre hvilke cyberoperasjoner som utgjør et angrep.

Angrep er etter krigens folkerett definert til å være voldshandlinger rettet mot motstanderen, enten offensivt eller defensivt. Henvisningen til «vold» passer kanskje dårlig i cyber-operasjoner, men det skal ikke tolkes bokstavelig: det er ment å dekke alle handlinger som har konsekvenser på linje med vold. Det avgjørende er om operasjonen med rimelighet må antas å medføre skadelige eller ødeleggende konsekvenser. For eksempel vil det å slippe ut en kjemisk gass være et angrep selv om det ikke involverer en fysisk voldshandling mot ofrene. «Cyberangrep» er derfor i gjeldende manual (2013) definert til å være cyber-operasjoner som med rimelighet må forventes å forårsake død, skade på personer eller skade eller ødeleggelse på objekter.

Det har vært og er mye diskusjon blant eksperter om tap av funksjonalitet kan anses som skade eller ødeleggelse slik at det blir et angrep og dermed forbudt å rette mot sivile. Sett i lys av den økende digitaliseringen av samfunnet, vil også tap av funksjonalitet kunne ha alvorlige konsekvenser både for militære og sivile. Anbefalingen er derfor at tap av funksjon som er permanent eller krever en fysisk handling slik som reinstallasjon av programvare, også skal anses som angrep etter krigens folkerett.

Cyberoperasjoner som ikke er cyberangrep, kan for eksempel være overvåkning og informasjonsinnhenting (CNE), psykologisk krigføring eller informasjonsoperasjoner. Blant annet vil det ikke utgjøre et angrep å gjøre en nettside som formidler motpartens propaganda midlertidig utilgjengelig gjennom et tjenestenektangrep. Ulemper eller forstyrrelser, for eksempel midlertidig tap av tilgang til internett, tregere databehandling eller tap av uvesentlig data, vil heller ikke være cyberangrep. Cyberoperasjoner som ikke er angrep, er også regulert etter krigens folkerett: for eksempel skal man ta kontinuerlig omsorg for å skåne sivile og ikke ødelegge eiendom dersom det ikke er tvingende militært nødvendig. Men reglene her er mindre begrensende enn de som regulerer angrep.

Data som objekt

Som nevnt er cyberangrep operasjoner som forventes å forårsake død eller skade på personer eller skade eller ødeleggelse på objekter. Men hva er et objekt i cyberkonteksten? Dersom det er et objekt, må data som skal angripes tilfredsstille kravene til å være lovlige militære mål. Det er forbudt å rette angrep mot sivile objekter, med mindre de brukes til militære formål, og da skal de anses som å være militære objekter. Dette inkluderer «dual-use» objekter, hvor det både er sivil og militær bruk.

I den gjeldende versjonen har vi slått fast at også data kan utgjøre et objekt. Vi diskuterte mye om vi kunne slå dette fast allerede da det ble skrevet rundt 2012, men vi valgte å gjøre det for å sikre at også cyberoperasjoner skulle være tilstrekkelig regulert. I dag ser vi at det ikke er like kontroversielt lengre, selv om det fremdeles diskuteres.

Tradisjonelt har objekter vært begrenset til det som er synlig og håndterbart, og det passer dårlig med data. Løsningen vi gikk for i gjeldende versjon var derfor å se til konsekvensene av et angrep for å vurdere om det er et objekt. Dersom det har samme virkning som voldshandlinger på cyberinfrastruktur, andre objekter eller personer, vil det være et angrep

som er regulert etter krigens folkerett selv om det som angripes ikke passer inn i den tradisjonelle forståelsen av objekter.

Hensynet til sivilbefolkningen tilsier likevel at data som er essensiell for sivilbefolkningen, slik som sivile bankkontoer og helseinformasjon, bør være beskyttet mot angrep. Det er derfor foreslått at også dette skal anses som et objekt, selv om ødeleggelse ikke nødvendigvis vil ha en virkning på lik linje med voldshandlinger.

Dette er eksempler på objekter kan være lovlige mål:

- Cyberinfrastruktur og data som utgjør komponenter i våpen eller våpensystem
- Cyberinfrastruktur og data som benyttes til logistikkstøtte til militære avdelinger, eller for produksjon eller vedlikehold av våpen og ammunisjon
- En serverpark som ved sin plassering lett kan rigges til å understøtte motpartens kommando- og kontrollsenter
- Cyberinfrastruktur og data som brukes av militære styrker til alt fra planlegging av angrep, gjennom lagring av militær data og kryptering eller dekoding av meldinger, til ordinær administrasjon av militære oppgaver.
- Cyberinfrastruktur og data som er innkjøpt eller som utvikles til militære formål.
- Cyberinfrastruktur og data som benyttes til kommunikasjon, kommando og kontroll, for eksempel en nettside som formidler kodede meldinger til styrker bak fiendens linjer.

Testen for å være et lovlig mål er at objektet ut fra sin art, plassering, formål eller bruk kan forventes å utgjøre et effektivt bidrag til fiendens militære aksjoner. I tillegg må det vurderes om total eller delvis ødeleggelse eller nøytralisering av objektet, etter de rådende omstendigheter byr på en avgjort militær fordel for angriperen.

For objekter som etter sin art er militære mål, vil den militære arten på objektene normalt tilsi at det vil gi en avgjort militær fordel å skade eller ødelegge det. For objekter som ikke er militære av sin art, er dette et viktig vilkår. Det betyr blant annet at et cyberangrep som gir en usikker militær fordel, for eksempel fordi konsekvensene kan være vanskelig å kartlegge, ikke vil være lovlig fordi det ikke gir angriperen en «avgjort» militær fordel.

Hvis objektet også brukes av sivile («dual use»), må det sivile tapet tas hensyn til i proporsjonalitetsvurderingen. Det holder ikke at noe er lovlig mål dersom det å angripe det er forventet å forårsake sivile tap som er for omfattende i for hold til den forventede militære fordelen. Dette gjelder alle typer mål.

Direkte deltakelse i fiendtligheter

Det neste spørsmålet som måtte jobbes en del med i oppdateringen av manualens behandling av cyberoperasjoner, er hvem som kan drive med cyberoperasjoner. Utgangspunktet i folkeretten er at det er militære som skal drive med militære operasjoner. Militære er medlemmer av de væpnede styrker, med unntak av sanitet og religiøst personell. De må være underlagt militær kommando og disiplinærrett, og få opplæring i krigens folkerett.

Men innenfor cyberdomenet er det også mange sivile som brukes. Spørsmålet blir da hva skal til for at sivile cyberoperatører blir lovlig mål? Det er to sider ved denne saken. Det ene

er hvem man kan rette angrep mot, det andre er hva Forsvaret kan bruke sivilt ansatte til og når det er nødvendig at operatøren er militær.

Dersom sivile deltar direkte i fiendtligheter, vil de bli lovlige mål. Dette gjelder også i cyberdomenet. Ettersom de ikke er medlemmer av de væpnede styrker, har de ikke rett til å delta, og de kan derfor straffeforfølges for eventuelle straffbare handlinger som for militære styrker ville vært lovlige krigshandlinger. I tillegg har de ikke krav på krigsfangestatus om de blir tatt til fange. Dette er en risiko Forsvaret ikke kan utsette egne sivile for. Direkte deltakelse i fiendtligheter er derfor ytterste grense for hva sivile kan settes til.

Utfordringen er at direkte deltakelse i fiendtligheter er et av de vanskeligste konseptene i krigens folkerett, og et stort internasjonalt ekspert-prosjekt for å definere det nærmere havarerte fordi ekspertene og den internasjonale røde kors ikke kunne bli enig. Det ble derfor en ren ICRC-publikasjon (*Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law*, 2009) hvor deler er forholdsvis kontroversielle. Det er likevel generell enighet om grunnvilkårene, selv om det ikke er enighet om tolkningen av dem. Direkte deltakelse innebærer at handlingen må:

- kunne forårsake skade på militære operasjoner eller stridskapasitet, eller på beskyttede personer eller objekter,
- være en direkte årsak til denne skaden, og
- være gjennomført i den hensikt å skade den ene parten i konflikten til fordel for en annen.

For å konkretisere dette vanskelige konseptet i manualen, er det i gjeldende versjon gitt flere eksempler, og disse vil nå utvides til å inkludere flere cybereksempler. Personer som er involvert i disse aktivitetene, vil kunne være lovlig mål for angrep. For Forsvaret sin del betyr det at de må være militære eller gjøres militære i tilfelle væpnet konflikt. Eksemplene er:

- cyberaktiviteter som utgjør cyberangrep
- operasjoner som muliggjør cyberangrep, slik som kartlegging av motpartens sårbare systemer eller programmering av skadevare til angrepet
- planlegging av cyberangrep
- bidra til målvalgsprosedyrer, for eksempel å identifisere, lokalisere og prioritere mål
- deltakelse i andre beslutningsprosesser som muliggjør cyberangrep
- samle eller viderebringe taktisk relevant informasjon for å støtte egne styrkers stridsoperasjoner
- gjennomføre tjenestenektangrep mot fiendens militære eksterne systemer
- motangrep mot militære mål som respons mot angrep fra motparten

Formålet med oppdateringen er å kunne gi Forsvaret ny og mer modernisert veiledning om hvordan cyberoperasjoner skal kunne gjennomføres i tråd med krigens folkerett. Jeg håper kapitlet vil være nyttig, og at det snart vil bli tilgjengelig.

Cyberoperasjoner - et praktisk perspektiv

Forsvaret

Jeg skal snakke om hva cyberoperasjoner er, aktører, og ikke minst - hva du kan gjøre for å bidra. Vi kan begynne med det som omtales som cyberspace. Cyberspace er langt mer enn bare Internett og Webben. Det inkluderer enheter som kan nås via cyberspace, om det er via kablede tilkoblinger, trådløse tilkoblinger, og de som tilsynelatende ikke er tilkoblet, men som viser seg å være tilkoblet likevel. Disse enhetene kan være potensielle mål og potensielle trusler.

Vi holder på å bygge ut 5G i Norge, det vil gjøre det mulig å koble enda flere gjenstander på nett. Tingenes internett (IoT) gir langt flere sårbarheter og muligheter enn dagens nett. SpaceX og andre firmaer skyter opp satellitter for å gi en alternativ internettilgang til områder som i dag kan ha dårlig dekning. For de transatlantiske forbindelsene, som private, stater og ikke minst finansbransjen, er avhengige av, går ca 95 % av trafikken på undersjøiske kabler. Nasjoner bygger infrastruktur; både som stat og i samarbeid med det private.

Informasjonen som beveger seg i cyberspace, blir laget av deg og meg. Av og til er det en sentralt besluttet utvikling, slik som digitalisering av statlige og kommunale tjenester, og bruk av fellesløsninger for skatt eller helse. Andre ganger er det individene som selv produserer behov og innhold, som posting av informasjon og bilder på sosiale medier. Informasjonen du gir fra deg gjenspeiler hvem du er og dermed hvor du er sårbar og påvirkelig. Summen av informasjonen vi gir fra oss har høy verdi. Slike datasett er verdifulle for andre stater og spesielt for kommersielle foretak som både selger dem og bruker dem til målrettede markedsføringskampanjer og andre innbringende foretak.

Det er også en rivende utvikling innenfor maskinlæring, et underområde av kunstig intelligens, som lever av datasett og datakraft. Denne utviklingen er også sentral for utviklingen innenfor cyberfeltet.

Ikke-statlige aktører

Før vi går over til å snakke om cyberoperasjoner i militær kontekst, skal jeg si litt om ikke-statlige aktører. Det er stor forskjell på å kunne hacke noe, og å hacke et bestemt system eller en enhet for å hente ut spesifikk informasjon eller skape en bestemt effekt, slik statlige aktører gjerne gjør. De ferdighetene du trenger for å gjennomføre mer opportunistiske cyberoperasjoner, kan du lære seg som privatperson. Utstyret man trenger, er lett tilgjengelig. Motivasjonen til aktørene kan være å ha det gøy ved å ta seg inn på ulovlige steder, gjerne uten intensjon om å gjøre noe galt. Andre er ute etter penger.

Ransomware, eller utpressing i cyberspace, er nå et velkjent fenomen. I 2020 var utbyttet fra slik utpressing ca 350 millioner dollar i kryptovaluta (Javers, 2021), en oppgang på 300 % fra året før. 80 % av løsepengene utbetalt til bare 199 såkalte cryptocurrency deposit addresses. Det forteller oss at det trolig er et fåtall store aktører der ute.

Nå er ikke tanken om å innføre nye typer valuta galt i seg selv, men historien har vist oss at det kan by på utfordringer. Overgangen til papirpenger i Frankrike før den franske revolusjon, var innovativ, men førte til sviktende tillit til staten, og at flere endte på skafottet (Barbero, 2021).

I dag er Bitcoin et virkelig "kinderegg". Der kan kriminelle komme unna med alt fra løsepenger til overgrepsmateriale uten å bli identifisert, uten skattlegging, og i tillegg forbruker systemet en energimengde som tilsvarer Danmarks årlige energiforbruk. Tilgangen til ikke-sporbar valuta sørger dermed for å opprettholde trykket innenfor operasjoner på privat side.

Det finnes også aktører som opptrer i gråsonen mellom privat og statlig. Disse kan være assosiert med statlige entiteter, men kan ha tilholdssted på steder og i organisasjoner som ikke er direkte sporbar tilbake til staten. For de aktørene som ikke er direkte statlig styrt, som er private eller opererer i denne gråsonen, kan terskelen være lavere for å iverksette en operasjon.

Cyberoperasjoner i militær kontekst

I NATO ble cyberspace erklært som et operasjonsdomene 2016, på lik linje med land-, sjø-, luftdomenet. De siste ti årene har flere stater etablert militære cyberkommandoer som en del av det nasjonale forsvarsverket. NATO skiller på offensive og defensive cyberoperasjoner.

De defensive operasjonene består i å sikre NATOs egne IKT-systemer mot digitale trusler. I Norge er det Cyberforsvarets oppgave å drifte og forsvare Forsvarets IKT-systemer. Andre, som kommersielle aktører, privatpersoner som du og jeg, vi må sikre oss selv.

De offensive operasjonene favner både etterretningsoperasjoner, og operasjoner som har til hensikt å skape en effekt hos en motstander. Og det er slike operasjoner jeg forstår er mest relevant for temaet her i dag.

For å beskrive disse effektene brukes de tradisjonelle D-ordene vi kjenner fra den militære effekttankegangen: *degrade*, *deny*, *disrupt*, *destroy, decieve*. NATO har ikke egne offensive cyberkapabiliteter. Derfor etablerte NATO nylig en mekanisme der medlemsland frivillig kan støtte NATO med cyberoperasjoner, uten å legge nasjonale kapabiliteter under NATOs kommando.

Ordningen går under det velklingende navnet SCEPVA-mekanismen: Sovereign Cyber Effects Provided Voluntarily by Allies. I Norge ligger ansvaret for offensive cyberoperasjoner i Etterretningstjenesten.

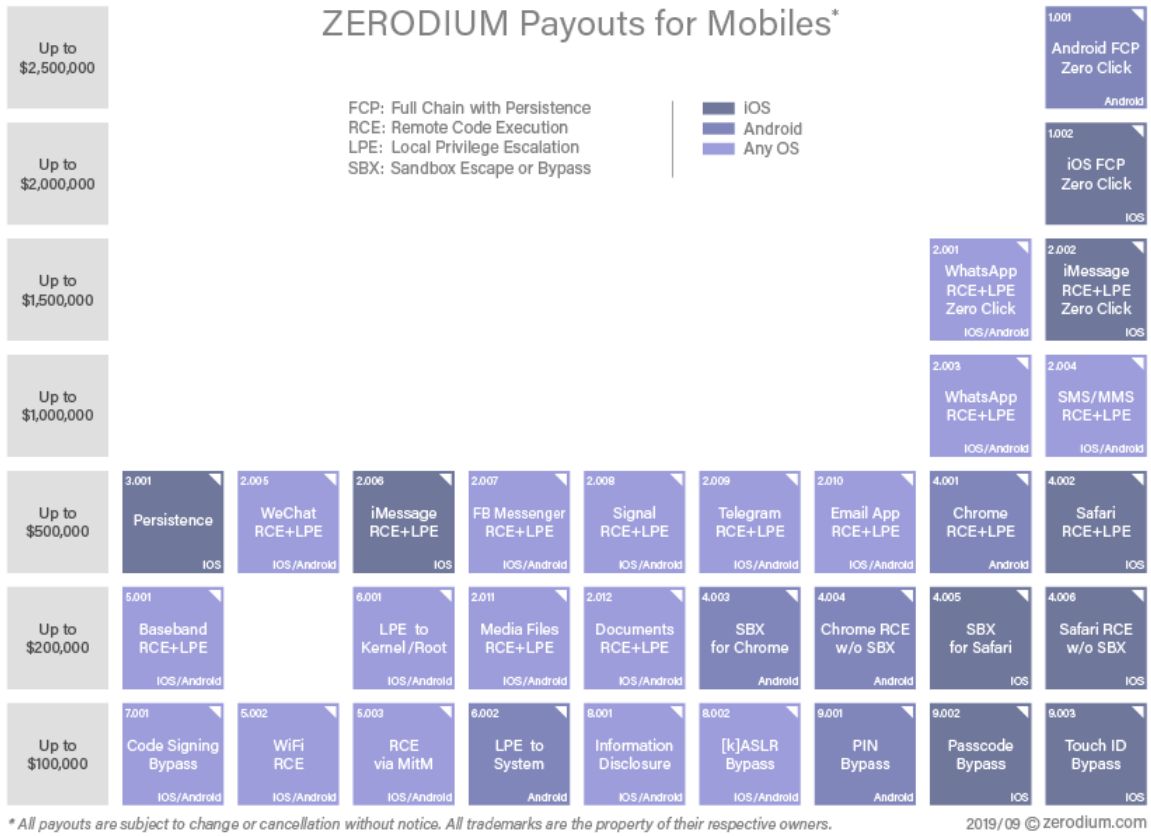
NATO beskriver cyberspace i form av tre lag: fysisk, logisk og cyberpersona. Operasjoner i cyberspace inkluderer alltid det logiske laget, men kan også inneholde aktiviteter eller

elementer fra de to andre lagene. Den effekten man ønsker å oppnå, kan eksistere på alle lagene, eller manifestere seg utenfor cyberspace.

I sin enkleste form, handler offensive cyberoperasjoner om å kjøre din kode, på noen andres datamaskin. Og aller helst ubemerket.

Og hva trengs, i praksis? Kompetanse. Mye kompetanse. Staten må finne og rekruttere hackere, og skape et miljø der disse høyt kompetente individene trives. Veldig ofte er dette høyst sivile medarbeidere, med en indre motivasjon i å løse komplekse problemer. De elsker å finne ut av hvordan de kan få ting til å virke på en måte som i utgangspunktet ikke skulle gå an. Ikke typisk det man gjerne assosierer med å jobbe i offentlig sektor.

Den statlige aktøren bruker kompetansen til å finne svakheter i systemene til aktuelle mål, og designe sin egen programvare for å ta seg inn i systemene. Gode sårbarheter omsettes som kostbar handelsvare på et lukket marked (Perlroth, 2021, *Zerodium Exploit Acquisition Program*, n.d.) - gjerne betalt med kryptovaluta. Her gjelder det å få tak i en sårbarhet før eieren av systemet blir klar over den, slik at den kan utnyttes. Øverst til venstre ser dere prisen for en sårbarhet som kan gi tilgang til en Androidtelefon – uten at du lurer brukeren til å klikke på noe for å aktivere sårbarheten.



For at målene for cyberoperasjoner skal godkjennes, vil de – i alle vestlige land – inngå i ordinære målfatningsprosesser med tilhørende godkjenningsregime. På lik linje med annen militær maktanvendelse. Et vestlig demokrati kan ikke se bort fra proporsjonalitetsprinsippet fordi man har satt merkelappen «cyber» på en effekt. Og militære cyberoperasjoner i vesten

er ikke rettet mot landets egne innbyggere. Forsvaret brukes ikke for å gjennomføre cyberoperasjoner mot norske borgere.

For å ta seg frem til et målsystem eller en bestemt enhet tilhørende motstanderen, trengs det en infrastruktur å operere på. For å skjule sine spor, hopper mange aktører gjennom det som kalles «gray space», datamaskiner og servere som geografisk befinner seg i andre land enn der målet er lokalisert, og ofte driftes av kommersielle aktører uten tilknytning til landet som gjennomfører operasjonen (Monte, 2015). Denne måten å operere på, gir en rekke juridiske og etiske utfordringer for den statlige aktøren. Når man så har fått tilgang hos en motstander, og hentet inn nok etterretning til at man kjenner systemet, kan den tilgangen brukes til å skape en effekt. Eksempelvis ved å påvirke funksjonaliteten i et system.

Det finnes teorier om at en stat kan oppnå strategisk seier ved å bruke beskjedne midler for å destabilisere infrastrukturen til en stat. Her finner vi tankene om de spektakulære, destruktive cyberoperasjonene. Det blir fremhevet som spesielt farlig, siden cyberkapabiliteter sies å være billige i utvikling.

Det eksisterer imidlertid svært få eksempler på at kode har forårsaket faktisk fysisk skade. Noen få unntak er konsekvensene av angrepene på kraftsektoren i Ukraina og ødeleggelsen av anrikningsentrifugene i Iran. Effektene av offensive cyberoperasjoner er som regel midlertidige og relativt raskt reversible, sammenlignet med andre militære maktmidler. I Ukraina gikk det timer, ikke uker, før strømmen var tilbake. Hadde noen brukt kinetiske virkemidler mot kraftnettet, hadde det blitt en kald vinter for ukrainerne. Hadde noen valgt å bombe anlegget i Nataz, kunne det ha destabilisert hele regionen.

Cyberkapabiliteter er riktig nok beskjedne i kostnad sett opp mot missiler og jagerfly. Men, de er svært kompetansekrevende og krever langsiktig investering og målrettet innsats for å skape effekter i en militær ramme.

Utført riktig, kan cyberoperasjoner midlertidig forvirre og frustrere militære systemoperatører og beslutningstakere. Militære styrker har tatt i bruk avansert teknologi soldatene ofte ikke har dybdekunnskap om, for å effektivisere operasjonene. Det man ikke forstår, er det vanskelig å ha tillit til. Når så disse systemene tukles med, påvirker det tilliten.

Å rokke ved motpartens tillit til egne evner og systemer kan være effektivt. Dersom man klarer å forvirre motstanderen tilstrekkelig til å utsette et planlagt motangrep, eller dersom forsyningslinjene forvitrer, vil det være enklere for konvensjonelle styrker å utføre sin jobb. Dette finnes det eksempler på fra kontraterroroperasjoner, der evnen til å forsinke utløsning av bomber, kan ha spart liv.

Cyberoperasjoner som en del av statsmakten

Nå skal jeg trekke frem noen ulike syn på cyberoperasjoner som en del av statsmakten.

Noen statsvitere (Valeriano et al., 2018) tar utgangspunkt i de cyberoperasjonene som er observert og beskriver hvordan stater bruker cyberoperasjoner innenfor statens allerede valgte strategi. Operasjonene komplementerer og forsterker tradisjonelle former for maktbruk, og stater bruker cyberinstrumenter for å forme langsiktig konkurranse, mer enn å søke umiddelbare innrømmelser. Empirien tilsier altså at den alt-utslettende cyberkrigen som ble varslet for ti år tilbake, har uteblitt. Foreløpig.

Det meste av den makt som utøves innenfor utenrikspolitikken er soft power, eller myk makt. Professor Joseph Nye Jr ved Harvard Kennedy School, er opphavsmannen til dette begrepet. I hard makt blir motstanderen tvunget til noe, gjennom trusler eller bruk av militærmakt. Myk makt ligger i overtalelse, overbevisning, læring og insentiver. Myk makt utøves ved å sette den internasjonale dagsordenen, beherske media, gi opplæring i hva demokrati er og lignende. Globaliseringen av media og veksten i multilateralt diplomati gjør at de fleste land er redd for sitt omdømme, da øker verdien av myk makt, hevder Nye. Hvilken investor vil sette pengene sine i en stat uten et fungerende rettssystem? Nye har også vist hvordan disse maktbegrepene kan benyttes i en cyberkontekst.

Som tabell 1 illustrerer kan man i cyberdomenet bruke informasjonsinstrumenter til å produsere myk makt i cyberspace, for eksempel gjennom å sette agenda, påvirke normer og rokke ved tilliten til IKT-systemer og informasjon. Det er også mulig å utøve hard makt (hard power) ved å organisere et distribuert denial of service-angrep ved å bruke "botnett" av kompromitterte datamaskiner som oversvømmer et selskap eller lands internettsystem og forhindre at det fungerer.

Table 1: Physical and Virtual Dimensions of Cyber Power

		Targets of Cyber Power	
		Intra cyber space	**Extra cyber space**
Information Instruments		Hard: Denial of service attacks Soft: Set norms and standards	Hard: Attack SCADA systems Soft: Public diplomacy campaign to sway opinion
Physical Instruments		Hard: Government controls over companies Soft: Infrastructure to help human rights activists	Hard: Bomb routers or cut cables Soft: Protests to name and shame cyber providers

Organisering av et botnett ved å infiltrere et virus til ikke-beskyttede datamaskiner er relativt billig, og botnett kan ulovlig leies på internett for noen hundre dollar. Noen ganger gjør kriminelle aktører dette for utpressing. I flere tilfeller har også såkalte patrioter kjørt tjenestenektangrep mot staten som hjemlandet er i konflikt med. Mest kjent er trolig den såkalte Bronsenatten i Estland i 2007 (Tapon, 2018). Det er også mulig å kombinere de ulike variantene for å lage en god plan for å få motstanderen til å gjøre som man vil.

Table 2: Three Faces of Power in the Cyber Domain

1st Face:	(A induces B do what B would initially otherwise not do)	
	Hard Power:	denial of service attacks, insertion of malware, SCADA disruptions, arrests of bloggers
	Soft Power:	information campaign to change initial preferences of hackers, recruitment of members of terrorist organizations
2nd Face:	(Agenda control: A precludes B's choice by exclusion of B's strategies)	
	Hard Power:	firewalls, filters, and pressure on companies to exclude some ideas
	Soft Power:	ISPs and search engines self monitor, ICANN rules on domain names, widely accepted software standards
3rd Face:	(A shapes B's preferences so some strategies are never even considered)	
	Hard Power:	threats to punish bloggers who disseminate censored material
	Soft Power:	information to create preferences (eg. stimulate nationalism and "patriotic hackers,"), develop norms of revulsion (eg. child pornography)

Innenfor cyberområdet er det relativt billig å etablere seg som en aktør, men de store er fortsatt størst. Det har vært en diskusjon om cybermakt skaper en asymmetrisk situasjon der småstater kan ramme stormaktene. Så langt ser ikke ut til at de har klart å utjevne skjevheter vesentlig. Fordelen med de militære aktørene er at de normalt er underlagt sterk statlig kontroll, og politisk godkjenning.

International Institute for Strategic Studies (2021) vurderer de store statlige aktørene til å være USA, Australia, Canada, Kina, Frankrike, Israel, Russland og Storbritannia. Statene som anklages for de største angrepene mot USA er Kina, Russland, Nord-Korea og Iran (Culafi, 2021).

USA har verdens mest kjente Cyber Command (*U.S. Cyber Command*, 2021). Kina gjennomfører cyberoperasjoner jevnlig (Hagestad III, 2012) og har blitt anklaget for å stå bak storskalatyveri av intellektuell eiendom (Rogin, 2012). Også Russland bruker cyberoperasjoner i kombinasjon med andre virkemidler, for å nå nasjonale målsetninger (Valeriano et. al. 2018).

Noen mener cyberoperasjoner er egnet for diplomatisk signalering og press, som andre virkemidler i DIME-spekteret. Motargumentene (Buchanan 2020) dette blir møtt med, er at cyberkapabiliteter er effektive fordi de er usynlige. I så måte er det mest relevante sammenligningsgrunnlaget «covert action» og spesialoperasjoner. Men det er utfordrende å kalibrere maktbruken. Og ikke minst, selv godt gjennomførte cyberoperasjoner er vanskelige å tolke for motparten. Statsledere og akademikere innen internasjonale relasjoner forstår ofte ikke hvilken betydning teknologien har.

Noen stater bruker også cyberoperasjoner mot egen befolkning. Den vestlige verden har en periode sett på tilgang til Internett som en mulighet til å fremme det vi mener er gode verdier. Organisasjoner har, på egenhånd eller støttet av statlige midler, fått mulighet til å sette opp informasjonsplattformer som skal hjelpe menneskerettighetsaktivister og andre til å formidle sine budskap. Autoritære regimer har gått inn for å stenge for disse budskapene gjennom å innføre murer for spredning av informasjon.

Under den arabiske våren i 2011, som ble opptakten til den syriske borgerkrigen, hadde syriske borgere muligheten til å uttrykke seg og gjøre tilgjengelig informasjon gjennom bruk av Internett. Regjeringen klarte ikke å undertrykke budskapene fra individene. Det førte til at grupperinger kunne samle tilhengere og finansiell støtte på en effektiv måte. I 2013 gikk regimetilhengere fra Syrian Electronic Army til angrep på opprørernes bruk av populære apper som Viber og Tango (Lee, 2013), senere brøt noen seg inn og stjal opprørernes planer (Kharpal, 2015).

Hvor mange internett skal vi ha?

Avslutningsvis skal jeg prøve å se litt fremover, og da går det an å spørre seg: Hvor mange internett skal vi ha?

Internett ble opprinnelig bygd som et nettverk som skulle motstå et første atomangrep, så det er en robust struktur. Det ble bygd av og for vitenskapsfolk og forskere, som forstod seg på teknologi og som var “godt oppdratt”. Selv om den teknologiske grunntanken er der, er dagens internett befolket av en helt annen gruppe - folk flest.

Noen mener internett er en fristat uten lover og regler - det er for øvrig ikke korrekt. Autoritære regimer ønsker å beholde nasjonal suverenitet og ser etter muligheter til å stenge informasjon ute og holde annen informasjon inne. Europeere vil *verne* om egen informasjon. Noen argumenterer for å redde internett ved å gå bort fra nasjonal suverenitet og mot folkestyrt suverenitet i cyberspace (Mueller, 2017). Det er viktig å være klar over at internett kan bli fragmentert, og at det kan føre med seg nye muligheter og begrensninger.

Derfor er det viktig at Norge er på banen i fora på alle nivåer der utviklingen diskuteres og bestemmes. Nå bygges det 5G, det nye Internett med fokus på virtualisering, datasentre og håndtering av milliarder av enheter. Dette er et område dere her i salen bør engasjere dere i og bidra til, for å sikre at vi har en stemme.

Det logiske laget, det som består av nuller og enere, er programmert. Der er det muligheter for å gjøre feil, og det er muligheter å patche for å rette feil. Alle oppdateringer med ny kode kan tette gamle hull, men også gi oss atter nye. De som driver med cyberoperasjoner, jakter på slike feil for å utnytte dem. Men, de som måtte snike seg inn til nattbordet og telefonen din, vil trolig ikke være en vestlig statsansatt. Det er heller noen som sniker rundt fordi det er gøy, eller for å finne noe de kan tjene penger på.

Ved å sikre at du og systemene du bruker er trygge, ved å bidra til å heve kompetanse, bruke trygge løsninger og oppfordre til lovlig og fornuftig bruk av nettet, er du en aktiv medspiller og en god forsvarer av nettet. Da reduseres behovet for at staten må bruke sine virkemidler for å beskytte deg og dine.

Kilder

Barbero, A. (2021, 5 27). *La bancarotta dello Stato: la rivoluzione francese – Intesa Sanpaolo On Air*. YouTube. Retrieved 9 26, 2021, from https://youtu.be/EqYjVG1M7ZU

Buchanan, B. (2020). The Hacker and the State. Harvard University Press.

Culafi, A. (2021, 4 20). The wide web of nation-state hackers attacking the US. TechTarget. https://searchsecurity.techtarget.com/news/252499613/The-wide-web-of-nation-state-hackers-attacking-the-US

Hagestad III, W. T. (2012). 21st Century Chinese Cyberwarfare (1st ed.). IT Governance Publishing.

Howell, C., & West, D. M. (2016, 11 7). The internet as a human right. Brookings. https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/

International Institute for Strategic Studies. (2021, 6 28). Cyber Capabilities and National Power: A Net Assessment. IISS. Retrieved 9 26, 2021, from https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

Javers, E. (2021, 4 6). The extortion economy: Inside the shadowy world of Ransomware payouts. CNBC. https://www.cnbc.com/2021/04/06/the-extortion-economy-inside-the-shadowy-world-of-ransomware-payouts.html

Kharpal, A. (2015, 2 2). Hackers pose as ‘attractive’ women in Syrian sting. CNBC. https://www.cnbc.com/2015/02/02/hackers-steal-syrian-rebel-battle-plans-by-posing-as-women-on-skype.html

Lee, L. (2013, 9 5). Syria’s war moves to electronic battlefield. Al Jazeera. https://www.aljazeera.com/features/2013/9/5/syrias-war-moves-to-electronic-battlefield-2

Monte, Matthew (2015). Network Attacks and Exploitation – A Framework. John Wiley & Sons, Indianapolis.

Mueller, M. (2017). Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace (1st ed.). Polity Press.

Nye Jr., J. (2010). Cyber Power. Harvard Belfer Center. https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

Perlroth, Nicole (2021). This is how they tell me the world ends. Bloomsbury publishing.

Rogin, J. (2012, 7 9). NSA Chief: Cybercrime constitutes the “greatest transfer of wealth in history”. Foreign Policy. https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/

Sandle, T. (2016, 7 23). UN thinks internet access is a human right. Business Insider. https://www.businessinsider.com/un-says-internet-access-is-a-human-right-2016-7?r=US&IR=T

Stadnik, I. (2019, 2 12). Sovereign RUnet: What Does it Mean? Internet Governance Project, Georgia Institute of Technology. Retrieved 9 26, 2021, from https://www.internetgovernance.org/research/sovereign-runet-what-does-it-mean/

Tapon, F. (2018, 7 7). The Bronze Soldier Explains Why Estonia Prepares For A Russian Cyberattack. Forbes. https://www.forbes.com/sites/francistapon/2018/07/07/the-bronze-soldier-statue-in-tallinn-estonia-give-baltic-headaches/

U.S. Cyber Command. (2021). https://www.cybercom.mil/

Valeriano, B., Jensen, B., & Maness, R. C. (2018). Cyber Strategy: The Evolving Character of Power and Coercion. Oxford University Press.

Zerodium Exploit Acquisition Program. (n.d.). Zerodium. Retrieved 9 26, 2021, from https://zerodium.com/program.html