UiT Norges arktiske universitet

Det juridiske fakultet

Cyberkrigføring

Enkelte utvalgte utfordringer for krigens folkerett som følge av cyberkrigføring - særlig om distinksjonsprinsippet og proporsjonalitetsprinsippet

Erlend Nygård

Masteroppgave i Rettsvitenskap JUR-3902 Desember 2020

Innholdsfortegnelse

1 Innledning

1.1 Cyberkrigføring

Datateknologi er blitt en grunnpilar i det moderne samfunn. Gjennomsnittsmenneskets hverdag er preget av internett og annen databasert teknologi. Økt globalisering som resultat av teknologiens frammarsj har utvilsomt bragt med seg mye positivt, men utviklingen har også åpnet en ny digital slagmark. Tilliten og «avhengigheten» av den nye teknologien kan utnyttes, og cybersikkerhet har derfor blitt et stort fokusområde. Utviklingen er akselererende, og har allerede bragt med seg store rettslige utfordringer i forhold til lovanvendelse ovenfor cyberkriminalitet, cyberterrorisme og cyberkrigføring.[1]

Hva er så «cyberkrigføring»? Ordet «cyber» eksisterer hverken i Genèvekonvensjonene av 1949 eller i tilleggsprotokollene av 1977.[2] I følge Store Norsk Leksikon (SNL) er «cyber-» et prefiks som brukes om noe som relaterer til kybernetikk, cyberspace, eller liknende.[3] SNL beskriver «cyberspace»-begrepet på følgende måte:

> *«Cyberdomenet, cyberspace, er et menneskeskapt globalt og stadig skiftende domene karakterisert av kombinert bruk av elektroner og det elektromagnetiske spektrum for det formål å generere, lagre, endre, utveksle, dele, hente og eliminere informasjon og ødelegge fysiske ressurser.»*[4]

«Cyberkrigføring» må følgelig være all krigføring som foretas i «cyberspace». I SNL konstateres det videre at:

> *«[c]yberdomenet består av fysisk infrastruktur som kopler sammen, trådløst eller med kabel: sambandssystemer; datasystemer med tilhørende programvare; nettverk mellom datasystemer (intranett); nettverk av nettverk mellom datasystemer (internett); knutepunkter for brukertilgang; og data som er latent til stede i systemene.»*[5]

---

[1] Sandvik, K. B. (2013). Cyberkrig og internasjonal rett. Internasjonal politikk, 71(02), 252-262. Side 252
[2] Solis, G. D. (2014). Cyber warfare. Mil. L. Rev., 219, side 3
[3] cyber- i Store norske leksikon på snl.no. Hentet 15. desember 2020 fra https://snl.no/cyber-
[4] Børresen, Jacob: cyberdomenet i Store norske leksikon på snl.no. Hentet 15. desember 2020 fra https://snl.no/cyberdomenet
[5] Ibid.

Forstyrrelser eller ødeleggelse av slik infrastruktur eller data som nevnt ovenfor, utført av en part i en væpnet konflikt, er etter en naturlig forståelse av ordlyden det som må regnes som cyberkrigføring.

Det amerikanske forsvarsdepartementet trekker frem cyberdomenet som et av fem domener hvor krigføring kan utspille seg, hvor de øvrige domene er land, vann, luft og rom.[6] Cyberkrigføring utkjempes således i et nytt og eget domene. Luftkrigføringens inntreden i krigsbildet på 1900-tallet er sammenlignbart i den forstand at den åpnet for krigshandlinger i et nytt domene. De nye luftstyrkene benyttet fremdeles kinetisk ammunisjon, på samme måte som artilleri og marinevåpen allerede hadde gjort i mange år. Krigshandlinger i det nye luftdomenet brakte derfor bare i begrenset grad med nye juridiske utfordringer – de samme grunnleggende reglene gjaldt slik som før.[7] Cyberkrigføring har på sin side bragt med seg en rekke nye og unike problemstillinger knyttet til anvendelsen av *jus in bello og jus ad bellum*.

1.2 Avgrensning, rettslig kildegrunnlag og metodiske utfordringer

Den rettslige rammen for oppgaven er krigens folkerett. Krigens folkerett trekker grensene for lovlig adferd under krig eller annen væpnet konflikt. Regelsettets primære fokus er forholdet mellom de stridende partene, men forholdet til nøytrale parter er også inkludert. Krigens folkerett betegnes også som internasjonal humanitærrett og *jus in bello,* og må adskilles fra *jus ad bellum*[8]. Krigens folkerett består av mellomstatlige avtaler (traktater og konvensjoner) og sedvanerett.[9] I denne oppgaven vil cyberkrigføring kun ses på i forhold til internasjonale væpnede konflikter. Altså forutsettes en pågående internasjonal væpnet konflikt som aktiverer krigens folkerett som et bakteppe ved vurdering av reglene. Krigens folkerett omfavner for så vidt også ikke-internasjonale væpnede konflikter, men regelsettet er mer begrenset for denne

---

[6] David Vergun (2015). Multidomain Operations Rely on Partnerships to Succeed - https://www.defense.gov/Explore/News/Article/Article/1755520/multidomain-operations-rely-on-partnerships-to-succeed/ - sist hentet 18.11.2020

[7] Brown, G. D. (2016). International Law Applies to Cyber Warfare: Now What. Sw. L. Rev., 46, side 366

[8] *Jus ad bellum* er regelsettet som oppstiller kriteriene for når en stat kan lovlig intervenere eller bruke væpnet makt mot en annen stat.

[9] Cooper, Camilla Guldahl; Larsen, Kjetil Mujezinović: krigens folkerett i Store norske leksikon på snl.no. Hentet 15. desember 2020 fra https://snl.no/krigens_folkerett

typen væpnede konflikter.[10]

Oppgaven avgrenses mot særlig *jus ad bellum* og internasjonale menneskerettigheter, men også folkeretten for øvrig. Konsekvensen av den tematiske avgrensningen mot *jus ad bellum* er for så vidt at mange spennende cyberproblemstillinger faller utenfor oppgavens omfang (f.eks. vurderingen av hva som skal til for at en cyberoperasjon etter *jus ad bellum* utgjør et væpnet angrep etter selvforsvarsretten), men rammene for en liten masteroppgave åpner ikke for en fyllestgjørende behandling av også det feltet. Det må videre trekkes et skille mellom cyberkrigføring og cyberkriminalitet. Cyberkriminalitet referer til cyberhandlinger som er ulovlige etter nasjonal rett. Typiske eksempler på cyberkriminalitet er anskaffelse ulovlig tilgang, ødeleggelse av data, misbruk av enheter, og «avlytting» av data.[11] I tillegg kan flere tradisjonelle lovbrudd gjennomføres helt eller delvis ved hjelp av internett og dermed defineres som cyberkriminalitet. Det er utarbeidet en flernasjonal cyberkriminalitet-traktat, «Budapestkonvensjonen»[12], men den er likevel ikke relevant for cyberkrigføring.

Wien-konvensjonen om traktatstolkning[13] utgjør grunnlaget for analyse av traktatstekst, og er betydningsfull ettersom krigens folkerett i nyere tid primært bygger på traktatstekst. Av særlig betydning er fortolkingsregelen i artikkel 31 som fastslår at tolking skal skje i god tro og i samsvar med ordinær ordlydsbetydning. Bestemmelser skal også tolkes i sammenheng og i lys av traktatens formål og hensikt. Det er i denne oppgaven bevist valgt å benytte norsk oversettelse av traktatsteksten, dersom slik oversettelse er tilgjengelig på Lovdata. Dette til tross for at norsk ikke er en av de formelle språkversjonene på disse avtalene. Valget er gjort både for å opptre i tråd med innarbeidet norsk terminologi på feltet, og for å øke oppgavens leservennlighet.

---

[10] ICRCblog (2017) When does IHL apply? - https://blogs.icrc.org/ilot/2017/08/13/when-does-ihl-apply/ - sist hentet 03.12.2020
[11] Solis (2014) side 2
[12] Konvensjon om datakriminalitet – ETS nr. 185; https://lovdata.no/dokument/TRAKTAT/traktat/2001-11-23-1/KAPITTEL_1#KAPITTEL_1 – sist hentet 15.12.2020
[13] Wien-konvensjonen om traktatretten: https://treaties.un.org/doc/Publication/UNTS/Volume%201155/volume-1155-i-18232-english.pdf - sist hentet 15.12.2020

Cyberkrigføring som sådan er for så vidt ikke underlagt en egen regulering. Det eksisterer dermed ingen internasjonal avtale som spesifikt omhandler krigføring i cyberdomene. Krigens folkerett er imidlertid generelt utformet, og utgangspunktet er at den skal anvendes på all krigføring, uansett type – den er teknologinøytral. Det har da også lenge vært et grunnleggende prinsipp at krigførende parter ikke har ubegrenset frihet ved valg av metoder, virkemidler eller våpentyper.[14] Dermed ikke er det ikke overraskende at det er stor enighet blant eksperter om at krigens folkerett, og følgelig også dens kjerneprinsipper, skal anvendes på cyberkrigføring.[15]

I fraværet av spesiell regulering kan Tallinmanualen trekkes frem som et særlig interessant kildematerie. Manualen er ikke et bindende lovverk, men en utredning om hvordan *jus ad bellum* og *jus in bello* bør anvendes på cyberkrigføring. På invitasjon fra NATO Cooperative Cyber Defence Centre of Excellence utarbeidet en gruppe på om lag 20 internasjonale eksperter Tallinmanualen, som ble publisert i april 2013.[16] Manualen regnes som det første omfattende forsøket på å kartlegge rettstilstanden rundt cyberkrigføring, *de lege lata*. Mange ulike problemstillinger behandles, men flere temaer behandles uten at ekspertene kommer til fullstendig enighet. I februar 2017 kom en ny utgave, Tallinmanualen 2.0, som utvidet prosjektomfanget.[17] En interessant endring er her at Tallin 2.0 endrer begrepet cyber «conflict» til cyber «operation». Den første utgaven av manualen omhandler primært de aller mest alvorlige og ødeleggende cyberoperasjoner, mens 2.0-versjonen også tar stilling til cyberoperasjoner av mindre alvorlig grad. Ved analyse av reglene utover i oppgaven er det først og fremst fokusområdet i den originale manualen, de mest alvorlige og ødeleggende cyberoperasjoner, som er relevant. Dette er begrunnelsen for at flertallet av henvisningene utover i oppgaven leder til den originale manualen, til tross for eksistensen av en nyere utgave.

---

[14] Tilleggsprotokoll til Genève-konvensjonene av 12-08-1949 hva angår beskyttelse av ofre for internasjonale væpnede konflikter (Første tilleggsprotokoll) artikkel 35
[15] ICRC expert meeting, «THE POTENTIAL HUMAN COST OF CYBER OPERATIONS» s. 37: https://www.icrc.org/en/document/potential-human-cost-cyber-operations - sist hentet 03.10.2020
[16] Schmitt, M. N. (Ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press.
[17] Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

Manualen har imidlertid bare i begrenset grad blitt akseptert internasjonalt som en nøyaktig presisering av gjeldende rett. Russland oppfatter manualen som for preget av det vestlige rettslige synet og innretter seg derfor ikke etter den.[18] Kina har også stilt seg et kritisk til manualen[19], og kinesiske kommentatorer har beskrevet manualen som en forlengelse av USAs syn på cyberkrigføring og følgelig som et forsøk på å gi amerikansk cyberkrigføring et slør av legalitet.[20] Kritikken bygget delvis på at flertallet av ekspertene som utarbeidet den første manualen var av vestlig opprinnelse.[21] I 2.0 ble ekspertutvalget gjort bredere i opprinnelse, men arbeidet ble fortsatt tilrettelagt og ledet av NATO.[22] De kritiske betenkelighetene er derfor bare delvis imøtekommet. Dersom verdenssamfunnet ikke tilslutter seg og praktiserer retten slik den kommer til utrykk i manualen, vil den rettslige verdien være minimal. Foretar f.eks. stormakter som Russland og Kina cyberkrigføring uten hensyn til Tallinmanualen, vil andre nasjoner være presset til å gjøre det samme. Det er videre bekymringsverdig at tungvektere innenfor cyberaktivitet har hatt en tendens til å forholde seg stille i forhold til hvilke rettigheter som gjelder i forhold til cyber. Da UN Security Council holdt sitt første uformelle møte om cybersikkerhet i 2016, var det uten deltagelse fra Russland, og med et USA som unngikk temaet.[23]

Internasjonale manualer som Tallinmanualen er som sådan ikke avtaletekst, og regnes ikke som primærrettskilder etter opplistingen i ICJ statuttene artikkel 38(1)(a)-(c).[24] Selv om manualen i utgangspunktet ikke er rettslig bindende, vil den over tid kunne oppnå status som

---

[18] James Conca (2018) When Would Russia's Cyber Warfare Morph Into Real Warfare? Refer To The Tallinn Manual: https://www.forbes.com/sites/jamesconca/2018/08/09/when-would-russias-cyber-warfare-morph-into-real-warfare-refer-to-the-tallinn-manual/?sh=706ff8306b27 – sist hentet 23.11.2020

[19] Ku, J. (2017). How China's Views on the Law of Jus ad Bellum Will Shape Its Legal Approach to Cyberwarfare. Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1707. Side. 17-18

[20] Hsu, K., & Murray, C. (2014). China and international law in cyberspace. US-China Economic and Security Review Commission. Side 5

[21] CyberDiplomacy (2019) Tallinn Manual — A Brief Review of the International Law Applicable to Cyber Operations: https://medium.com/@cyberdiplomacy/tallinn-manual-a-brief-review-of-the-international-law-applicable-to-cyber-operations-5643c886d9e2 – sist hentet 11.12.2020

[22] NATO Cooperative Cyber Defence Centre of Excellence on Tallinmanual 2.0: https://ccdcoe.org/research/tallinn-manual/ - sist hentet 11.12.2020

[23] Deborah Brown (2020) It's Time to Treat Cybersecurity as a Human Rights Issue: https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue - sist hentet 11.12.2020

[24] Vedtekter for Den internasjonale domstol: https://lovdata.no/pro/#document/TRAKTAT/traktat/1945-06-26-2/a38 - lest 13.12.2020

internasjonal sedvanerett.[25]

Det kan tenkes at det er mest nærliggende å kategorisere disse som noe lignende rettslig litteratur, om enn med mer offisiell statlig input enn tilfellet er med juridisk litteratur, hvor det kan finnes tolkninger eller informasjon om primærkildene. Det samme gjelder til en viss grad for nasjonale manualer. To eksempler på et slike manualer er den amerikanske «Department of Defense: Law of War Manual» fra 2015 og den norske «Manual i krigens folkerett» fra 2013.[26] Slike nasjonale manualer er imidlertid i noen grad å anse som relevant statspraksis (i forhold til internasjonal sedvanerett), selv om de riktignok ofte har passuser om at dokumentet ikke nødvendigvis gjenspeiler den aktuelle statens offisielle syn på rettstilstanden.

1.3 Videre fremstilling

Oppgaven vil i kapittel 2 ta for seg ulike typer cybervåpen og cyberoperasjoner, og hva som er forskjellen mellom ulovlig bruk av et våpen og et våpen som er ulovlig. Kapittelet inneholder i tillegg en begrenset redegjørelse for cybervåpen med kunstig intelligens, og hvilken betydning autonomi vil kunne ha i forhold til reguleringen av cyberkrigføring. De mest nærgående analysene foretas i kapittel 3 og 4. Kapittel 3 redegjør innholdet i distinksjonsprinsippet, og de aktuelle utfordringene som oppstår i forhold til cyberkrigføring. Herunder drøftes det grundig hva som utgjør et cyberangrep. Reglene om forhåndsregler ved angrep gjennomgås også i dette kapittelet. I Kapittel 4 foretas en analyse av proporsjonalitetsprinsippet, og de rettslige utfordringene tilknyttet anvendelsen av prinsippet i cyberkontekst. I kapittel 5 følger en begrenset redegjørelse for Martens klausulen, og en vurdering av hvilken betydning den muligens kan tillegges ved tolkningen av krigens folkerett ovenfor cyberkrigføring. Oppgaven rundes av i kapittel 6 med overordnet vurdering av den gjeldende rettslige reguleringen av cyberkrigføring, samt en avsluttende kommentar om mulig fremtidig regulering av cyberkrigføring.

---

[25] Sandvik (2013) Side 256

[26] Preston, S. E., & Taylor, R. S. (2015). Department of Defense Law of War Manual. General Counsel of the Department of Defense Washington United States (Updated Dec 2016): https://www.hsdl.org/?abstract&did=797480 – sist hentet 05.12.2020;
Høyskole, F., & Stabsskole, F. (2013). Manual i krigens folkerett.

2 Nærmere om cybervåpen

2.1 Ulike typer cyberoperasjoner og cybervåpen

Det eksisterer ingen allment akseptert definisjon på begrepet «cybervåpen» innenfor krigens folkerett. Tallinmanualen trekker frem «means of cyber warfare» og «methods of cyber warfare» som definisjoner av rettslig betydning. I kommentaren til regel 103 i Tallinmanual 2.0 blir cybervåpen (cyber weapons) definert som:

> *«cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack.»*[27]

Rid og McBurney publiserte i 2012 en artikkel hvor de definerte cybervåpen som programvarekode *«… used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things.»*[28] En slik definisjon er muligens bredere enn rettstilstanden synes å tillate. Begrepet *functional harm* er særlig vidt i cyber-kontekst, og vil kunne resultere i en for vid definisjon av hva som utgjør et cybervåpen. I søken etter en egnet definisjon av begrepet kan det være til hjelp å se til hva som *ikke* kan regnes som cybervåpen. Programvare som er utviklet utelukkende til spionasje vil for eksempel ikke regnes som et cybervåpen, ettersom spionasje i utgangspunktet ikke reguleres innenfor krigens folkerett.[29]

Selv i fraværet av en allmenn definisjon kan det likevel trekkes frem flere momenter som sannsynligvis hører hjemme i en rettslig definisjon. Sentralt for status som våpen er at cyberverktøyet er egnet til å ødelegge (drepe) eller i alle fall gjøre skade på mennesker eller gjenstander. Eksempler på cybervåpen som kan ha potensiale til å gjøre slik skade er virus, sovende bomber, dataprogram som setter bot-nett i gang med ovennevnte, osv. Hva som regnes som skade på gjenstander innenfor cyberkrigføring er et omstridt spørsmål, som vil tas

---

[27] Schmitt (Ed.) (2017) side 452
[28] Rid, T., & McBurney, P. (2012). Cyber-weapons. the RUSI Journal, 157(1), 6-13. Side 7: https://doi.org/10.1080/03071847.2012.664354
[29] Unntaket er dersom en stridende utgir seg for å være sivil for å utføre spionasje som del av et angrep eller forberedelse av et angrep. Den stridende vil da miste både kombattantprivileget og rett til krigsfangestatus, som følge av brudd på forpliktelsen om å skille seg ut fra sivilbefolkningen. Se artikkel 44 (2) jf. (3) i første tilleggsprotokoll

opp senere i oppgaven.

I forbindelse med problemstillingen lovlige våpen/våpenbruk, må to situasjoner skilles fra hverandre. Et våpen kan være ulovlig i kraft av seg selv. Selv om øvrige regler i krigens folkerett overholdes, vil bruk av slike våpen likevel være ulovlig. Våpenets ulovlighet er et resultat av dets særegne egenskaper. Noen av disse forbudene er sedvanerettslige, mens andre er blitt til igjennom avtaler de siste 150 år. Et eksempel på et en slik avtale er forbudet mot biologiske våpen,[30] som bruk av vil være ulovlig selv om våpenet blir brukt mot et lovlig mål.

Stater er pliktige å forhåndsvurdere lovligheten av alle nye våpen. Det fremkommer i artikkel 36 i første tilleggsprotokoll:

> *«Ved studier, utvikling, anskaffelse eller godkjenning av et nytt våpen eller nye krigføringsmetoder eller -virkemidler, skal en kontraherende part være forpliktet til å avgjøre om bruken i sin alminnelighet eller i enkelte tilfeller, ville være forbudt i henhold til denne Protokoll eller til eventuelle andre folkerettsregler som gjelder for vedkommende kontraherende part.»*

Trolig er forhåndsvurderingsplikten også å regne som sedvanerettslig bindende. ICRC har i alle fall argumentert for at plikten gjør seg gjeldende ovenfor alle stater, uavhengig av om de er en kontraherende part i første tilleggsprotokoll.[31] Argumentet bygger på at plikten til forhåndsvurdering er en naturlig forlengelse av at alle stater, på sedvanerettslig grunnlag, er forbudt å benytte seg av ulovlige våpen, midler og metoder og fra ulovlig bruk av våpen, midler og metoder for krigføring.[32] I DoD Law of War Manual fremgår det amerikanske standpunktet på forhåndsvurdering av cybervåpen:

> *«This policy would include the review of weapons that employ cyber capabilities to ensure that they are not per se prohibited by the law of war. Not all cyber capabilities, however, constitute a weapon or weapons system.»*[33]

---

[30] Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction - sist hentet 31.05.2020
[31] ICRC, A. (2006). Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977, January 2006. IRRC, 88(864), side 933
[32] Henckaerts, J. M. (2005). Customary international humanitarian law: Volume 1, Rules (Vol. 1). Cambridge University Press. Side 237
[33] Preston & Taylor (2015) Side 1025

Det kommenteres videre:

> *«For example, a destructive computer virus that was programmed to spread and destroy uncontrollably within civilian internet systems would be prohibited as an inherently indiscriminate weapon.»*[34]

Bruken av begrepet «våpen» i denne sammenhengen tyder på at DoD anser destruktive cyber-egenskaper som grunnlag for våpenstatus. Ikke-destruktive og ikke-skadelige cyberegenskaper vil følgelig ikke medføre status som våpen i kontekst av forhåndsvurdering.[35]

Hensikten bak forhåndsvurderingen er at ulovlige våpen skal avdekkes tidlig i utviklingsprosessen. Våpen som ikke har et lovlig bruksområde, skal ikke produseres. Et våpen kan være ulovlig i kraft av en traktat om ulovlighet, slik som tilfellet er for biologiske våpen. Alternativt vil et våpen være ulovlig i seg selv dersom forhåndsvurdering konkluderer med at det ikke finnes noen lovlige bruksområder for våpenet. Bestemmelsen stiller videre krav om at mulige lovlige bruksområder for det aktuelle våpenet skal kartlegges.

Her kommer vi inn på den andre formen for ulovlighet - ulovlig bruk av et våpen som i utgangspunktet er lovlig. Krigens folkerett legger føringene på hva som utgjør lovlig krigføring. Noen av de konkrete reglene ses nærmere på utover i oppgaven. Sannsynligvis kan de aller fleste våpen brukes på en måte som strider mot disse reglene. Automatgeværet kan nyttiggjøre som eksempel. Automatgeværet er i seg selv regnet som et lovlig våpen, men dersom en soldat benytter geværet til å skyte på sivile som ikke deltar direkte i striden, vil bruken av automatgeværet være ulovlig.[36]

Det er viktig å skille mellom disse to formene for ulovlighet – ulovlig våpen og ulovlig bruk av våpen. En konsekvens av mangelen på spesiell regulering av cyberkrigføring er at ingen cybervåpen vil være ulovlig på avtalefestet grunnlag. Det skal mye til for å konkludere at et cybervåpen ikke har noen lovlige bruksområder, og derfor må regnes som ulovlig i seg selv.

---

[34] Preston & Taylor (2015) Side 1025-1026
[35] Biller, J., & Schmitt, M. N. (2019). Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare. Means, or Methods of Warfare (June 19, 2019), 95. side 187
[36] "Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict, Michael N. Schmitt & Jeffrey S. Thurnher - Harvard National Security Journal / Vol. 4, side 243

Kanskje kan det fremmes et argument om ulovlighet i kraft av seg selv for enkelte tenkelige typer autonome cybervåpen. Selv dersom det skulle være tilfellet, vil ulovligheten trolig være en følge av våpenets autonomi, ikke fordi det er et *cyber*våpen.

2.2 Cybervåpen og kunstig intelligens

Store norske leksikon definerer kunstig intelligens på følgende måte: *«Kunstig intelligens er informasjonsteknologi som justerer sin egen aktivitet og derfor tilsynelatende framstår som intelligent.»*[37] Det skilles gjerne mellom to ulike former for kunstig intelligens. Den første og mest primitive formen er regelbasert kunstig intelligens, såkalte *«ekspertsystemer»*. Her operer systemet «fritt» innenfor et sett med komplekse regler for intelligent atferd som er programmert av mennesker på forhånd. Den andre formen for kunstig intelligens er datadrevne modeller. Systemet benytter det som kalles «maskinlæring». Det forholder seg ikke til et absolutt forutbestemt regelsett, men «lærer» istedenfor hvilke regler som gjelder på egen hånd. Systemet vil da få et problem å løse, men ingen informasjon om hvordan det bør løses. Systemet vil ved å prøve og feile over tid forsøke å finne frem til den «beste» måten å løse oppgaven på.[38]

Systemer som benytter seg av maskinlæring må læres opp. Det eksisterer en rekke ulike modeller for gjennomføring av opplæringen. Den vanligste opplæringsmodellen er overvåket læring. Da vil systemet læres opp av et menneske som allerede vet løsningen på problemet. Eksempelvis kan et datasystem med bildegjenkjenningsteknologi få i oppgave å sortere bilder. Det får da i oppgave å sortere bilder basert på innhold. Mennesket som overvåker vet svaret, og gir systemet tilbakemelding på hva som er riktig og galt. Slik overvåket læring er ressurskrevende, ettersom det krever konstant menneskelig tilstedeværelse og tilbakemelding. Det pågår derfor store mengder forskning på andre mulige metoder for maskinlæring hvor treningen gjøres automatisk. Uovervåket læring og forsterket læring er eksempler på slike modeller. En annen sentral metode innenfor maskinlæring er «dyp læring».[39] Dyp læring er inspirert av den menneskelige hjernen, og går ut på å lære opp flere lag med kunstige nevrale

[37] Tidemann, Axel: kunstig intelligens i Store norske leksikon på snl.no. Hentet 15. desember 2020 fra https://snl.no/kunstig_intelligens
[38] Ibid. Hele avsnittet bygger på SNLs fremstilling av «kunstig intelligens»
[39] Tidemann, Axel: dyp læring i Store norske leksikon på snl.no. Hentet 15. desember 2020 fra https://snl.no/dyp_l%C3%A6ring

nettverk.

Kunstig intelligens er stort fokusområde for utvikling av cybersystemer. Mest nærliggende er det å benytte slik teknologi i defensive cyberforsvars-systemer.[40] Det er dog ikke utenkelig at den første betydelige bruken av et offensivt autonomt våpensystem vil finne sted i cyberdomenet, i form av et cybervåpen med kunstig intelligens.[41] Et cybervåpen kan potensielt utstyres med en rekke ulike teknologier, inkludert dyp maskinlæring. Systemets algoritmer vil da tillate systemet å selvstendig «lære» av store mengder data. Basert på læringen vil systemet hele tiden endre sine identifiserbare funksjoner for å unngå oppdagelse. Et slikt autonomt cybervåpen, som ikke begrenses av menneskelige operatører, vil også kunne foreta fortløpende endringer i programkoden sin slik at den i løpet av millisekunder kan utnytte nyoppdagede sårbarheter.[42]

Dagens datamaskiner evner å utføre «handlinger» langt raskere en menneskelige operatører. Cyberkrig er derfor ikke like begrenset av tid som tradisjonell kinetisk krigføring. Den som rammes av et cyberangrep oppfatter ikke nødvendigvis at et angrep har skjedd før angrepet allerede er over, og muligheten for å reagere er passert. Hastighet er derfor helt sentralt for å kunne effektivt føre krig i cyberdomenet. Tidspress kan medføre utfordringer for overholdelse av krigens folkerett. En menneskelig operatør som må handle umiddelbart for å avverge et innkommende cyberangrep vil ha vanskeligheter med å forsvarlig vurdere en reaksjons lovligheten etter krigens folkerett. Kanskje særlig vanskelig vil det være å foreta en forsvarlig proporsjonalitetsvurdering under tidspress. Kanskje kan autonome cybersystemer, som evner å foreta kompliserte kalkulasjoner i løpet av millisekunder, være en løsning på tids-problemet.[43] Detter er trolig ikke tilfellet, i hvert fall ikke med dagens teknologi:

---

[40] Wilson da Silva (2019) War of the Bots: Artificial Intelligence in Cyber Warfare: https://medium.com/predict/spy-vs-spy-cyber-warfare-gets-automated-aba60ece738c - sist hentet 09.11.20

[41] Artificial intelligence and offensive cyber weapons (2019) Strategic Comments, 25:10, x-xii.

[42] Ibid.

[43] Margulies, P. (2020). Autonomous Cyber Capabilities Below and Above the Use of Force Threshold: Balancing Proportionality and the Need for Speed. International Law Studies, 96(1), 13. Side 440

«Along with their extraordinary speed and analytical prowess, autonomous agents have notable flaws, including brittleness, bias, and unintelligibility.»[44]

Det er omtvistet om autonome våpensystemer overhodet kan benyttes i overenstemmelse med krigens folkerett, og eventuelt i hvilken grad. Den sentrale problemstillingen er om cybervåpen med kunstig intelligens er i stand til å foreta de nødvendige vurderingene, eller om mennesker må være en del av avgjørelsesprosessen. Dersom lovlig bruk beror på betydelig menneskelig kontroll over det autonome våpensystemet, slik ICRC fremmer,[45] vil tidsargumentet muligens komme til kort. Kreves det menneskelig kontroll som medfører nevneverdige forsinkelser, vil autonomi neppe være en løsning slik foreslått ovenfor. En grundig gjennomgang av kravet om menneskelige kontroll, eller autonome våpensystemers stilling i krigens folkerett for øvrig, er utenfor oppgavens omfang.

3 Distinksjonsprinsippet

Distinksjonsprinsippet er en grunnpilar i krigens folkerett. Prinsippet krever at alle stridende parter i en konflikt skiller mellom militære mål og ikke-militære mål (sivile gjenstander og personer).[46] Hovedregelen i artikkel 48 i første tilleggsprotokoll fastslår at *angrep* må rettes mot *militære mål*. Distinksjonsprinsippet er sedvanerettslig bindene, og ICJ har kategorisert prinsippet som *«intrangressible»*.[47] Anvendelse av distinksjonsprinsippet innebærer en rekke problemstillinger når det kommer til cyberkrigføring.

Det første sentrale punktet som må avklares er hva som kan regnes som *angrep* i cyberforstand. Angrepsdefinisjonen i krigens folkerett er hjemlet i artikkel 49(1): *«Angrep» betyr voldshandlinger rettet mot motstanderen, enten offensivt eller defensivt.»*[48] Spørsmålet er så hva som er å regne som *voldshandlinger*. I ICRC-kommentaren til bestemmelsen trekkes beskrivelsen av angrep i Shorter Oxford Dictionary: *«to set upon with hostile action»*, som

[44] Margulies (2020) Side 441
[45] ICRC, Autonomy, artificial intelligence and robotics: Technical aspects of human control, August 2019, side 2
[46] Distinksjonsprinsippet er hjemlet i artikkel 48, 51(2) and 52(2) i første tilleggsprotokoll
[47] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J, side 257 (78,79)
[48] Første tilleggsprotokoll artikkel 49(1)

mest nærliggende angreps-begrepet i artikkel 49.[49] Det kommenteres videre at valget bevisst falt på en vid definisjon.[50] I Tallinmanualen fremstilles følgende definisjon på et *cyberangrep*:

> *«A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage to objects.»*[51]

Solis beskriver definisjonen i manualen som en utmerket definisjon, men tilføyer ett kriterium om at operasjonen også skal være grenseoverskridende.[52] Hvorvidt en cyberoperasjon utgjør et angrep beror dermed på en vurdering av voldeligheten av operasjonens effekter, ikke voldeligheten av operasjonens midler. Det er her snakk om operasjonens tiltenkte og sannsynlige effekter, ikke det faktiske resultatet. En cyberoperasjon kan utgjøre et angrep selv dersom den blir avverget og følgelig ikke påfører målet skade.[53] Spørsmålet videre er hvilket omfang av død, personskade, skade eller ødeleggelse som kreves for å utgjøre et *cyberangrep.* Problemstillingen synes ikke uttrykkelig avklart i krigens folkerett.

Cybertyveri, informasjonsinnhenting, og cyberinntrengsler som medfører korte eller midlertidig forstyrrelse av ikke-essensielle cybertjenester, kvalifiserer ikke som cyberangrep.[54] Slike cyberoperasjoner som faller under angrepsterskelen plasseres typisk i en egen kategori. I litteraturen benyttes ulike, men langt på vei sammenfallende begrep om slike operasjoner. To eksempler er cyber- «intrusions»[55] eller «disruptions»[56]. Videre i denne oppgaven brukes begrepet «cyberforstyrrelse», slik Brown fremstiller det, om cyberoperasjoner under angrepsterskelen:

> *«The term "cyber disruption" is used here to refer to cyber only operations that cause inconvenience, even extreme inconvenience, but no direct injury or death, and no*

---

[49] Pilloud, C., Sandoz, Y., Swinarski, C., & Zimmermann, B. (Eds.). (1987). Commentary on the additional protocols: of 8 June 1977 to the Geneva Conventions of 12 August 1949. Martinus Nijhoff Publishers. Side 603 (1879)
[50] Ibid. Side 603 (1880)
[51] Schmitt (Ed.) (2013) Side 92
[52] Solis (2014) side 12-13
[53] Schmitt (Ed.) (2013) Side 94 (15)
[54] Solis (2014) side 13
[55] Ibid.
[56] Brown (2016) side 366

destruction of property.»[57]

Beregning av skade er følgelig avgjørende for hva som regnes å utgjøre et angrep. Tradisjonelle og aksepterte metoder for vurdering av skade som benyttes i krigens folkerett er ikke spesielt godt egnet til å fange opp ikke-kinetiske følger av cyberoperasjoner. Et cyberangrep trenger ikke oppnå et kinetisk resultat for å være vellykket. Et kinetisk resultat i denne sammenheng referer til fysisk ødeleggelse eller skade på en gjenstand. Eksempelvis kan en vellykket cyberoperasjon sette et datasystem midlertidig ut av spill, uten å medføre permanent skade på systemet. Etter kort tid er systemet tilbake i normal drift og ingen permanente effekter kan påpekes – datasystemet er ikke ødelagt. Konsekvensen av at cyberforstyrrelser ikke kan betegnes som angrep, er at flere av de sentrale reglene i krigens folkerett ikke kommer til anvendelse. Dette gjelder også de grunnleggende prinsippene om distinksjon og proporsjonalitet, som aktiveres av *angrep*. Prinsippet om militær nødvendighet og hensyn til humanitet vil derimot fortsatt gjøre seg gjeldende. Det foreligger ikke allmenn enighet om hvilken definisjon på skade som skal legges til grunn for cyberkrigføring. Ekspertene i Tallinmanualen hevder at det er godt etablert i krigens folkerett at *voldshandlinger* ikke er begrenset til aktiviteter som frigjør kinetisk energi.[58] Kjemiske, biologiske og radiologiske angrep frigjør vanligvis ikke kinetisk energi, men det er ubestridt at slike angrep regnes å utgjøre angrep innenfor krigens folkerett.[59] Schmitt fremmer at formålet bak forbudene i første tilleggsprotokoll først og fremst er å begrense voldelige konsekvenser, ikke voldelige handlinger.[60] Utgangspunktet er at cyberangrep må forventes å oppnå skadelige effekter tilsvarende skadelige effekter av kinetisk art:

«Cyber operations that lack direct physical effects are not violent and so cannot be classified as attacks.»[61]

En tilknyttet problemstilling er hva som kan utgjøre en gjenstand for angrep. Artikkel 52(2) i første tilleggsprotokoll forbyr angrep mot sivile *gjenstander*. Et sentral problemstilling innen cyberkrigføring er om *data*, som ikke kan sies å være en gjenstand etter tradisjonell

---

[57] Brown (2016) side 366
[58] Schmitt (Ed.) (2013) Side 92 (3)
[59] Ibid.
[60] Schmitt, M. N. (2012). "Attack" as a term of art in international law: The cyber operations context. In 2012 4th International Conference on Cyber Conflict (CYCON 2012) (pp. 1-11). IEEE. Side 290
[61] Brown (2016) side 365

betydning, kan utgjøre en *gjenstand for angrep*. Data kan vanskelig omtales som *«visible and tangible»,* slik et objekt beskrives i ICRCs kommentar til første tilleggsprotokoll.[62] Data faller heller ikke naturlig innenfor en tradisjonell og ordinær forståelse av gjenstand-begrepet.[63] I Tallinmanualen behandles problemstillingen på følgende måte:

> *«The majority of the International Group of Experts agreed that the law of armed conflict notion of object should not be interpreted as including data. Data is intangible and therefore neither falls within the "ordinary meaning" of the term object' nor comports with the explanation of it offered in the ICRC Additional Protocols Commentary.»*[64]

Ekspertflertallet nevnte likevel at en cyberoperasjon rettet mot data i enkelte tilfeller kan oppfylle definisjonen som «angrep» dersom funksjonaliteten til et cybersystem påvirkes av operasjonen.[65] Et mindretall blant ekspertene argumenterte derimot for at data burde regnes som gjenstand ved målutvelgelse. Konsekvensen dersom data faller utenfor gjenstand-definisjonen vil være at viktige sivile datasett potensielt står uten beskyttelse fra krigens folkerett. Mindretallet var av oppfatningen at dette ville utgjøre et brudd på den rettslige forutsetningen i artikkel 48 om at sivilbefolkningen skal beskyttes generelt fra effektene av stridigheter.[66] Standpunktet bygger hovedsakelig på en formålsvurdering av artikkel 52, som vektlegger skadeomfang over type skade. Ekspertmajoriteten oppfattet ikke et slikt synspunkt som gjeldende rett, men heller som et synspunkt *de lege ferenda*.[67]

Beskyttelsen etter artikkel 51(1) vil imidlertid også kunne få betydning. Regelen fastslår at: *«Sivilbefolkningen og de enkelte sivilpersoner skal ha alminnelig beskyttelse mot farer som oppstår av militære operasjoner.»* Den alminnelige beskyttelsen knyttes til militære *operasjoner* og vil dermed gjøre seg gjeldende uavhengig av om cyberoperasjonen oppfyller kriteriene for å utgjøre et angrep. Regelen beskytter bare mot *farer*. Målet med bestemmelsen er at farene som sivilbefolkningen utsettes for skal minimeres.[68] Det aktuelle sivile datasettet må derfor trolig være av stor viktighet og sivil betydning for at ødeleggelse eller skade på det

---

[62] Pilloud, Sandoz, Swinarski, & Zimmermann (1987) Side 634 (2007 og 2008)
[63] Schmitt, M. N. (2014). The law of cyber warfare: Quo Vadis. Stan. L. & Pol'y Rev., 25, 269. Side 297
[64] Schmitt (Ed.) (2013) Side 108 (5)
[65] Ibid.
[66] Ibid.
[67] Ibid.
[68] Pilloud, Sandoz, Swinarski, & Zimmermann (1987) Side 617 (1935)

vil utgjøre en *fare* for sivilbefolkningen eller en enkelt sivilperson. Krigføring av natur vil alltid bringe med seg en negative følger for sivilbefolkningen, uten at disse følgene forbys. Det kan dermed ikke være en hvilken som helst fare det er snakk om for at bestemmelsen skal komme til anvedelse. Regelen er sannsynligvis bare anvendelig i helt spesielle tilfeller, og gir således ikke vanlige sivile datasett beskyttelse mot cyberoperasjoner under angrepsterskelen.

Mangel på statlig praksis ovenfor cyberoperasjoner rettet mot data uten fysisk skadelige konsekvenser bidrar til at rettstilstanden er uklar. Trolig vil det foregå en "objektivisering" av data som konsekvens av hyppigere og mer sofistikerte forekomster av cyberoperasjoner.[69] Prosessen vil sannsynligvis ta tid fordi stater ønsker å verne om muligheten til å lovlig gjennomføre operasjoner som involverer skade på data.[70] Et relevant eksempel er psykologiske operasjoner rettet mot sivil befolkning som involverer skade på data. Det er også tenkelig at stater vil kunne motsette seg å inkludere skade på data i proporsjonalitetsvurderingen og i vurderinger av forhåndsregler ved angrep i forhold til militær nødvendighet.[71]

Et annet omtvistet spørsmål er hvorvidt ødeleggelse av funksjonalitet generelt kan utgjøre slik skade som kreves for at en cyberoperasjon kan klassifiseres som et *angrep*. Begrepet «nøytralisering» i 52(2) i første tilleggsprotokoll åpner for at tap av funksjonalitet potensielt utgjør tilstrekkelig skade:

> *«By referring not only to destruction or capture of the object but also to its neutralization the definition implies that it is irrelevant whether an object is disabled through destruction or in any other way.»*[72]

Inkluderingen av nøytraliseringsbegrepet[73]er et utrykk for at de som utarbeidet protokollen var av den oppfatning at et *angrep* kan føre til tap av funksjon uten nødvendigvis å ødelegge

[69] McCormack, T. (2018). International Humanitarian Law and the Targeting of Data. International Law Studies, 94(1), 222-240. Side 239
[70] Schmitt, M. N. (2015). Notion of Objects during Cyber Operations: A Risposte in Defence of Interpretive and Applicative Precision. Isr. L. Rev., 48, 81. Side 108
[71] Ibid.
[72] Dörmann, K. (2004). Applicability of the Additional Protocols to computer network attacks. Int'l Committee of the Red Cross. Side 6
[73] Pilloud, Sandoz, Swinarski, & Zimmermann (1987) Side 635 (2019)

gjenstanden.[74] Muligens er definisjonen i Tallinmanualen som er sitert ovenfor derfor for smal. I følge Z. Chang er en bredere tolkning, hvor også cyberoperasjoner som ikke fører til ødeleggelse av gjenstander kan utgjøre «angrep», mer passende.[75] Enkelte hevder til og med at utvidelse av skadebegrepets omfang er en humanitær nødvendighet når det kommer til cyberkrigføring. Dette beror primært på at konsekvensen av at en slik type skade ikke er relevant for vurderinger av proporsjonalitet, vil være særlig problematisk fordi «dual use» er så vanlig i cyberverdenen.[76] «Dual use»-problematikken returneres til utover i oppgaven.

Fra distinksjonsprinsippet følger det et krav om å vurdere hva som utgjør militære mål. For at prinsippet skal overholdes kreves det at de som foretar krigshandlinger skiller mellom det som er lovlige militære mål og det som ikke er det. Artikkel 52(1) i første tilleggsprotokoll fastslår at alt som ikke er militære gjenstander skal regnes som sivile gjenstander. Ettersom sivile mål er negativt definert, er defineringen av sivilt i teorien enkelt – forutsatt kunnskap om hva som er militære mål. Vurderingen av militære mål er imidlertid mer komplisert.

Det eksisterer ingen uttømmende liste over hva som kan utgjøre et legitimt militært mål. Ved vurderingen av legitime mål er det ikke nødvendigvis av betydning hvorvidt den parten som blir angrepet har definert det aktuelle målet som en del av sin militære styrke. Det som er avgjørende er om et *angrep* mot målet vurderes å utgjøre et *effektivt bidrag* til fiendens egne militære handlinger og om *ødeleggelse, overtagelse eller nøytralisering* vil gi en *klar militær fordel*.[77] Et tradisjonelt eksempel som illustrerer dette, er ammunisjonsfabrikker. Selv om slike fabrikker er sivilt kontrollert og bemannet av ikke-stridende personer, vil et angrep rettet mot dem ikke nødvendigvis stride med distinksjonsprinsippet.[78] Selv for det tilfellet at et angrep overholder kravet om distinksjon, vil det likevel måtte foretas en følgeskadevurdering forut for angrepet. Vurdering av følgeskade behandles nærmere utover i oppgaven.

---

[74] Chang, Z. (2017). Cyberwarfare and International Humanitarian Law. Creighton Int'l & Comp. LJ, 9, 29. Side 36
[75] Ibid.
[76] Geib, R., & Lahmann, H. (2012). Cyber warfare: Applying the principle of distinction in an interconnected space. Isr. L. Rev., 45, 381. Side 399
[77] Første tilleggsprotokoll artikkel 52(2)
[78] Henckaerts (2005) Side 23

Det oppstilles også nærmere krav til hva som vil utgjøre tilstrekkelige vurderinger av hva som er militære mål. Hva som nærmere kreves av en slik vurdering kan utledes fra reglene om forhåndsregler ved angrep som er hjemlet i artikkel 57 i første tilleggsprotokoll. Artikkel 57(2)(a) er rettet mot «de som planlegger eller treffer beslutning om angrep». Forpliktelsen retter seg i hovedsak mot øvre deler av kommandokjeden. Det er der planleggingen og beslutningen i de aller fleste tilfeller foretas. Dersom det er praktisk mulig å bruke andre våpen som medfører mindre sannsynlighet for sivile tap, vil benyttelse av et cybervåpen som gir større tap være ulovlig.[79] I ICRCs kommentar til protokollen fremheves det at det som kreves av den som planlegger eller treffer beslutningen om angrepet er *«… to take the necessary identification measures in good time»* for å verne om sivilbefolkningen så langt det lar seg gjøre.[80] Bestemmelsen er videre et utrykk for at et veldig stort flertall av delegasjonene på den diplomatiske konferansen ønsket å omfavne alle situasjoner med en enkelt bestemmelse:

> *«It clearly follows that the high command of an army has the duty to instruct personnel adequately so that the latter, even if of low rank, can act correctly in the situations envisaged»*[81]

I artikkel 57(2)(b) oppstilles et krav som gjør seg gjeldende for alle ledd i kommandokjeden:

> *«et angrep skal avlyses eller stilles i bero dersom det blir åpenbart at målet ikke er et militært mål, eller at det er gjenstand for spesiell beskyttelse, eller at angrepet kan forventes å forårsake tilfeldig tap av sivilpersoners liv, skade på sivilperson, skade på sivile gjenstander eller en kombinasjon av slike følger som ville være for omfattende i relasjon til den forventede konkrete og direkte militære fordel»*

Denne avbrytnings- eller utsettelsesplikten krever at det fortløpende foretas skjønnsbaserte vurderinger. Denne plikten kan problematiseres dersom cybervåpen med kunstig intelligens benyttes.

---

[79] Første tilleggsprotokoll artikkel 57(3)
[80] Pilloud, Sandoz, Swinarski, & Zimmermann (1987) Side 682 (2198)
[81] Ibid. Side 681 (2197)

3.1 Definisjon av militære mål

Hva som utgjør militære mål fremgår i artikkel 52(2) i første tilleggsprotokoll:

> *«Angrep skal være strengt begrenset til militære mål. Når det gjelder gjenstander, er militære mål begrenset til de gjenstander som ut fra art, plassering, formål eller bruk gir et effektivt bidrag til militære aksjoner, og som total eller delvis ødeleggelse, erobring eller nøytralisering av, etter de da rådende omstendigheter byr på en avgjort militær fordel.»*

Definisjonen er ikke omstridt. Under den diplomatiske konferansen som foranlediget tilleggsprotokollene uttalte Mexico at artikkel 52: *«cannot be the subject of any reservations whatsoever since these would be inconsistent with the aim and purpose of Protocol I and undermine its basis.»*[82] Nødvendigheten av å skille mellom militære og ikke-militære mål ved utførelse av en cyberoperasjon er helt klar. Spørsmålet er hvordan denne vurderingen skal foretas i relasjon til gjenstander som er særegent knyttet til cyber og cyberkrigføring.

3.1.1 Effektivt bidrag til militære aksjoner

Et moment i vurderingen er hvorvidt det aktuelle målet egner å gi effektive bidrag til militære aksjoner. Det kreves ikke at gjenstandens effektive bidrag er avgjørende eller av sentral betydning, men kravet om at gjenstanden må utgjøre et bidrag til fiendens militære aktivitet er absolutt.[83] På den andre side er det ikke tilstrekkelig at ødeleggelse, overtakelse eller nøytralisering av gjenstanden bare potensielt eller ubestemt utgjør en fordel. Den som beordrer angrepet må besitte tilstrekkelig informasjon til å kunne overholde kravet. Dersom det foreligger tvil om hvorvidt dette kravet kan oppfylles, må protokollens formål - siviles beskyttelse - tas hensyn til.[84] Hva som utgjør et effektivt militært bidrag tolkes og praktiseres likevel ulikt. Det kan skilles mellom *krigførende* gjenstander, *krigsstøttende* gjenstander og *krigsopprettholdende* gjenstander (war-fighting objects, war-supporting objects og war-sustaining objects).[85] Krigsbekjempende gjenstander er gjenstander som brukes til krigføring.

---

[82] Henckaerts (2005) Side 25
[83] Schmitt, M. N., & Widmar, E. W. (2014). On Target: Precision and Balance in the Contemporary Law of Targeting. J. Nat'l Sec. L. & Pol'y, 7, 379. Side 392
[84] Pilloud, Sandoz, Swinarski & Zimmermann (1987) Side 636 (2024)
[85] HEADQUARTERS, U., CORPS, M., & GUARD, U. C. (2007). The Commander's Handbook on The Law of Naval Operations (EDITION AUGUST 2017). 8-2

Slike gjenstander er tydelig av militær karakter og er derfor vanligvis legitime militære mål. Vurderingen er mer krevende når det kommer til krigsstøttende gjenstander. Det er gjenstander som ikke benyttes i krigsbekjempelsen, men som direkte bidrar til krigsinnsatsen. Ammunisjonsfabrikken er et eksempel på en slik gjenstand. Det er bred enighet om at både krigsbekjempende og krigsstøttende gjenstander kan kvalifisere som lovlige militære mål.[86]

Enkelte stater - med USA i front - anser også den tredje formen, krigsopprettholdende gjenstander som lovlige militære mål. The Commander's Handbook on The Law of Naval Operations definerer krigsopprettholdende gjenstander som *«economic objects of the enemy that indirectly but effectively support and sustain the enemy's war-fighting capability …»*, og inkluderer slike gjenstander som mulige lovlige militære mål.[87]

Inkludering av krigsopprettholdende gjenstander som mulige lovlige mål innenfor overholdelse av distinksjonsprinsippet vil ha stor betydning for cyberkrigføring. Denne amerikanske posisjonen er derfor omstridt. I Tallinmanualen omtales temaet på følgende måte:

> *«The majority of the International Group of Experts rejected this position on the ground that the connection between war-sustaining activities and military action was too remote. They would limit the notion of military objective to those objects that are war-fighting (used in combat) or war-supporting (otherwise making an effective contribution to military action, as with factories producing hardware or software for use by the military) and that otherwise fulfil the criteria of a military objective as defined above.»*[88]

Flertallet av øvrige juridiske eksperter på området tilslutter seg majoritetens resonnement om at krigsopprettholdende gjenstander er for fjerne i forhold til militæraktiviteten til å kunne oppfylle kravet til effektivt bidrag.[89] USAs praksis inkluderer like fullt krigsopprettholdende gjenstander som potensielle militære mål ved tradisjonelle kinetiske operasjoner, og det er

---

[86] Schmitt & Widmar (2014) Side 394
[87] HEADQUARTERS, U., CORPS, M., & GUARD, U. C. (2007). The Commander's Handbook on The Law of Naval Operations (EDITION AUGUST 2017) 8-2 og 8-3
[88] Schmitt (Ed.) (2013) Side 111(16)
[89] Schmitt & Widmar (2014) Side 394

liten grunn til å forvente annerledes anvendelse ovenfor cyberkrigføring.[90]

Det at et mulig mål brukes av motstanderens militære er ikke nok i seg selv. En gjenstand kan benyttes av militæret for formål som helt eller delvis er urelaterte til krigsbekjempelse. Eksempler i cyberkontekst er sivile telefoni- og emailtjenester som benyttes utenfor føringen av strid. Det var dissens blant ekspertene i Tallinmanualen om slike mål kunne oppfylle kravet:

> *«The majority took the position that the cyber infrastructure upon which the services depend does not so qualify because the services do not make an effective contribution to the enemy's military action and, by extension, their denial would not yield a definite military advantage to an attacker. The minority suggested that since the use of the cyber infrastructure contributes to the morale of the enemy forces, conducting an attack against it would offer a military advantage. They cautioned that this sort of conclusion should not be crafted so broadly as to suggest that any object qualifies as a military objective if damage to it hurts enemy morale.»*[91]

Mindretallet pekte på at selv om angrep mot slike typer mål potensielt kan yte en klar militær fordel, vil eventuelle angrep begrenses av hensynet til prinsippene om proporsjonalitet og forhåndsregler i angrep. Dersom eksempelvis en e-post-tjeneste ble benyttet til kommunikasjon av militær betydning, var ekspertene i fullstendig enighet om at e-post-infrastrukturen ville være et potensielt militært mål.[92]

Dette tar oss over i en særlig relevant problematikk når det gjelder cyberkrigføring - såkalte «dual use» mål. Stater benytter seg i større grad av sivilt utstyr og sivile anlegg i cyberkrig enn i tradisjonell krigføring. Det skyldes at cyber-infrastruktur i praksis enkelt kan benyttes både til sivile og militære formål samtidig. Grensen mellom militære og sivile mål er derfor mer uklar enn ved annen krigføring. Dette byr på en utfordring for de som skal vurdere lovligheten av et angrep. Utgangspunktet er at sivile gjenstander kun er beskyttet dersom de ikke benyttes til militære formål. Det fremkommer blant annet i artikkel 27 i

---

[90] Pascucci, P. (2017). Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution. Minn. J. Int'l L., 26, 419. Side 434
[91] Schmitt (Ed.) (2013) Side 112 (24)
[92] Ibid.

Landkrigsreglementet til 4. Haag-konvensjon av 1907, som beskytter enkelte typer bygninger.[93] En gjenstand kan ikke samtidig både være et legitimt militært mål og et beskyttet sivilt mål. Det er en naturlig konsekvens av ordlyden i artikkel 52(1) i første tilleggsprotokoll: «Sivile gjenstander er enhver gjenstand som ikke er militært mål». Dersom en gjenstand etter den samlede vurderingen i 52(2) kan defineres som et militært mål, kan det ikke samtidig utgjøre en sivil gjenstand. «Dual use» av gjenstander fører heller ikke til et skjerpet krav om militært bidrag fra det potensielle målet. At en gjenstand er i «dual use» vil derimot måtte vektlegges i vurderingen av proporsjonalitet og ved overholdelse av forhåndsregler under planleggingen av angrepet.[94] En tenkelig konsekvens av at en gjenstand benyttes både militært og sivilt er at et angrep muligens må rettes mot den eller de delene av målet som benyttes til militære formål, så langt det lar seg gjøre.

3.1.2 Natur, beliggenhet, formål og bruk

En gjenstand kan utgjøre et effektivt bidrag til militære aksjoner på grunnlag av *natur, beliggenhet, formål* og/eller *bruk*. *Natur* refererer til gjenstandens iboende karakteristikker eller egenskaper som bidrar til militær handling.[95] Eksempler på gjenstander av slik natur innenfor cyberkrigføring er militære nettverk, systemer for langdistansekommunikasjon som benyttes militært, og datasystemer i våpen.[96] *Beliggenhet* omfatter enkelte lokasjoner av spesiell viktighet, uavhengig av hvordan områdene benyttes for øyeblikket.[97] Selv om «cyberdomenet» er et delvis abstrakt begrep, er infrastrukturen som utgjør nettverkene fysiske objekter som nødvendigvis må eksistere en plass. Et tradisjonelt eksempel er en bro, som enten ødelegges eller overtas på grunn av den taktiske betydningen den har i kraft av sin beliggenhet, uavhengig av om den faktisk benyttes. Tilsvarende kan cyber-infrastruktur utgjøre et militært mål på grunn av sin lokasjon. Dersom det for eksempel benyttes en spesiell programvare eller metode til å overføre data av militær betydning, kan det sannsynliggjøres at dataen vil transittere et spesifikt nettverk.[98] Det aktuelle nettverket vil da kunne utgjøre et

[93] Regulations, H. L. W. (1907). Regulations respecting the laws and customs of war on land
[94] Schmitt (Ed.) (2013) Side 113(2)
[95] Schmitt & Widmar (2014) Side 392
[96] Pascucci (2017) Side 435
[97] Schmitt & Widmar (2014) Side 392
[98] Pascucci (2017) Side 435

militært mål i kraft av sin beliggenhet.

Begrepet *bruk* omfatter nåværende benyttelse av gjenstanden. Kriteriet er aktuelt for sivile gjenstander som benyttes til militære formål. Sivile gjenstander som benyttes militært utgjør bare et militært mål i kraft av *bruk* i perioden det benyttes militært.[99] En gjenstand som benyttes militært vil utgjøre et militært mål, uavhengig av omfanget av den militære bruken. Omfanget er derimot av betydning, ettersom skade på den sivile delen av gjenstanden må vurderes i forhold til proporsjonalitet og forhåndsregler i angrep. Angrep på gjenstander som normalt betjener sivile formål, men som mistenkes å ha konvertert til militære formål, må foranlediges av en *«careful assessment of the situation»*.[100] Det kreves likevel ikke fullstendig visshet om at gjenstanden har konvertert.[101]

Formål tar for seg fremtidig bruk av gjenstanden. Kriteriet åpner for at en gjenstand kan utgjøre et militært mål, uten at gjenstanden ennå har blitt benyttet til det. Dersom et slikt formål foreligger kreves det ikke at et angrep mot et sivilt mål avventes inntil gjenstanden faktisk blir benyttet militært. Hva som er en gjenstands formål, er likevel ikke alltid tydelig. I ICRCs kommentar til artikkelen poengteres det at de fleste sivile gjenstander i fremtiden kan være av nytte for militært bruk.[102] Kommentaren gjør det klart at ved tvil om en sivil gjenstand planlegges benyttet til militære formål, må det forutsettes at gjenstanden skal betjene sivile formål, jf. artikkel 52(3).[103] Vurderingen av formål må i likhet med vurdering av bruk bero på etterretningsinformasjon. Dersom formålet ikke er tydelig avklart, kreves det at den som angriper opptrer rimelig. *Rimelighetsvurderingen* skal bygge på informasjonen som forelå for angriperen på tidspunktet for angrepet.[104] Faktum *ex ante* skal ikke legges til grunn. Andre nasjoners evne og mulighet til å innhente mer eller bedre informasjon er heller ikke av betydning. Dersom angriperen har tilstrekkelig informasjon til å tro at et nettverk vil bli benyttet militært, vil et angrep kunne rettes mot nettverket på grunn av dets formål, så fremt de øvrige vilkårene er innfridd.

---

[99] Schmitt & Widmar (2014) Side 393
[100] Schmitt (Ed.) (2013) Side 117(7)
[101] Ibid. Side 117(8)
[102] Pilloud, Sandoz, Swinarski, & Zimmermann (1987) Side 636 (2022)
[103] Ibid.
[104] Schmitt (Ed.) (2013) Side 117(9)

3.1.3 Avgjort militær fordel fra ødeleggelse, overtakelse, eller nøytralisering

Det andre kumulative kravet i bestemmelsen er at *ødeleggelse, overtakelse eller nøytralisering* av *gjenstanden* utgjør en *avgjort militær fordel*. Hva som konkret ligger i begrepet *avgjort,* er ikke definert:

> *«The term «definite» does not imply any particular quantum of advantage.»*[105]

I kommentaren til første tilleggsprotokoll kommenteres det at angrep som bare potensielt eller udefinerbart vil utgjøre en militær fordel ikke er legitime.[106] Angrep som bare forventes å resultere i en spekulativ fordel er heller ikke lovlige.[107] Det konstateres videre at den som angriper må besitte tilstrekkelig informasjon til å kunne forvente en avgjort fordel. I tillegg til at fordelen må være *avgjort,* kreves det at den er av militær natur. Fordelsvurderingen vil imidlertid omfatte angrepet i sin helhet, ikke enkelte isolerte deler av operasjonen.[108] Fordeler av utelukkende økonomisk, politisk eller psykologisk art vil likevel ikke alene kunne utgjøre en *militær* fordel.[109] Svekkelse av motstanderens sivile moral kan heller ikke utgjøre en militær fordel. Det er vil dog ikke være av betydning for vurderingen at et angrep som er rettet mot en for øvrig godkjent gjenstand, i tillegg vil medføre en svekkelse i sivil moral.[110] Innvirkningen på sivil moral har ingen påvirkning på vurderingen, hverken fra eller til.

Den militære fordelen behøver ikke nødvendigvis være et direkte resultat av skade eller ødeleggelse av det utvalgte militære målet. I Tallinmanualen brukes følgende eksempel innenfor cyberkrigføring:

> *«For instance, attacking a server through which the transmissions of an enemy command and control facility pass can result in military advantage. No damage is done to the command and control facility, but its neutralization results in definite military advantage for the attacker."*[111]

---

[105] Schmitt (Ed.) (2013) Side 111(20)
[106] Pilloud, Sandoz, Swinarski, & Zimmermann (1987) Side 636 (2024)
[107] Schmitt (Ed.) (2013) Side 112(20)
[108] Ibid. Side 111(17)
[109] Ibid. Side 111(18)
[110] Ibid. Side 112(23)
[111] Ibid. Side 111(17)

Henvisningen til «nøytralisering» i bestemmelsen åpner for at det som angripes i første rekke ikke nødvendigvis er det egentlige militære målet, men at det like fullt må utgjøre et militært mål i seg selv. Dersom formålet er nøytralisasjon, kan det i enkelte tilfeller oppnås ved å skade eller ødelegge tilknyttede gjenstander, slik som er tilfellet i eksempelet ovenfor fra manualen.

3.2 Forhåndsregler i angrep

I tillegg til distinksjonsvurderingen kreves det at det tas visse forhåndsregler i angrep. Artikkel 57 i første tilleggsprotokoll oppstiller en rekke krav. Overordnet nevnes det at *«[u]nder utføringen av militære operasjoner skal det tas kontinuerlig omsorg for å skåne sivilbefolkningen, sivilpersoner og sivile gjenstander.».*[112]

Bestemmelsen er en forlengelse av hovedregelen om distinksjon i artikkel 48. Plikten om kontinuerlig omsorg påfaller som nevnt alle typer militære operasjoner. Det kreves følgelig ikke at den aktuelle cyberoperasjoner utgjør et *angrep.* Det samme er tilfellet for artikkel 57(4):

> *«Under utøvelsen av militære operasjoner til sjøs eller i luften skal hver av partene i konflikten, i samsvar med sine rettigheter og plikter i henhold til de folkerettslige regler som gjelder under væpnet konflikt, treffe alle rimelige forholdsregler for å unngå tap av sivilpersoners liv og skade på sivile gjenstander.»*

Bestemmelsen fremmer et krav om rimelighet. Rimelighet(feasibility) er den generelle standarden også for de øvrige reglene om forhåndsregler.[113] I ICRCs kommentar til bestemmelsen poengteres det at begrepet «alle rimelige forhåndsregler» har mindre rekkevidde enn begrepet «alle praktisk mulige forholdsregler» i artikkelens andre avsnitt.[114] Likevel uttales det: «*[a]s the nuance is tenuous, the purpose of the provision appears to be to reaffirm the rules that exist to protect civilians in such situations.»*[115]

---

[112] Første tilleggsprotokoll artikkel 57(1)
[113] Schmitt (Ed.) (2013) Side 137(2)
[114] Pilloud, Sandoz, Swinarski, & Zimmermann (1987) Side 688 (2230)
[115] Ibid.

Hva innebærer det så å ta *kontinuerlig omsorg for å skåne sivilbefolkningen, sivilpersoner og sivile gjenstander* ved cyberoperasjoner? Begrepet kontinuerlig omsorg er ikke definert i krigens folkerett.[116] I Tallinmanualen var ekspertene enige om at

> *«…in cyber operations, the duty of care requires commanders and all others involved in the operations to be continuously sensitive to the effects of their activities on the civilian population and civilian objects, and to seek to avoid any unnecessary effects thereon.»*[117]

At omsorgsplikten er *kontinuerlig* betyr at de som er ansvarlige må ta de nødvendige hensynene under hele operasjonsforløpet. Det kreves altså en tilstrekkelig og fortløpende situasjonsbevissthet, ikke bare i planleggingsfasen. Cyberoperasjoner er ofte komplekse, og det kan derfor være urimelig å forvente at den ansvarlige kommandøren som planlegger et angrep på egen hånd besitter tilstrekkelig teknisk kompetanse til å ha oversikt og forståelse av cyberoperasjonens art og effekter. Derfor bør den eller de som planlegger cyberoperasjoner, dersom det er *rimelig*, assisteres av cyber-eksperter slik at nødvendige forhåndsregler tas.[118] Bruk av sivile gjenstander som «skjold» for å dekke ellers lovlige angrepsmål vil være i strid med kravet om å ta kontinuerlig omsorg.[119] Et tenkelig eksempel i cyberkontekst vil være å bevisst plassere medisinsk cyber-infrastruktur på et nettverk som allerede benyttes til militære formål, i full visshet om at nettverket for øvrig utgjør et lovlig mål.[120]

Artikkel 57(2) pålegger forhåndsregler ovenfor operasjoner som utgjør *angrep*. De som planlegger eller treffer beslutning om angrep, skal gjøre alt som er *praktisk mulig* for å forvisse seg om at angrepsmålene hverken er sivilpersoner eller sivile gjenstander, og at de ikke er gjenstand for spesiell beskyttelse.[121] Selv om ordlyden i bestemmelsen retter seg mot de som *planlegger eller treffer* beslutning om angrep, skal bestemmelsen ikke tolkes slik at den fullstendig fraskriver de øvrige leddene i kommandokjeden ansvar. I Tallinmanualen ble følgende eksempel gitt for cyberkontekst: Et cyberangrep er ferdig planlagt og forberedt. Det er foretatt etterretning og det utvalgte målet - et nettverk - er tilstrekkelig kartlagt. Det eneste som gjenstår er autorisasjon til å igangsette angrepet. En operatør foretar fortløpende

---

[116] Schmitt (Ed.) (2013) Side 138(4)
[117] Ibid.
[118] Ibid. Side 138(6)
[119] Ibid. Side 138(7)
[120] Ibid.
[121] Første tilleggsprotokoll artikkel 57(2)(a)(i)

overvåking av målet. Dersom det oppstår en materiell endring i cyberforholdene ved det utvalgte målet, kreves det at endringene rapporteres til kommandøren eller annet relevant personell som beslutter avgjørelsen om å foreta angrepet.[122] Ekspertene i manualen utleder gjennom eksempelet en form for informasjonsplikt. En slik plikt er trolig en forutsetning for at regelen skal fungere slik den er tiltenkt. Å kreve at de som planlegger eller treffer beslutning om angrep sørger for at trinnene nedover i kommandokjeden videreformidler slik relevant informasjon, er godt innenfor det som må sies å være *praktisk mulig* å foreta seg, slik det stilles krav om i bestemmelsen.

I ICRCs kommentar til første tilleggsprotokoll ble begrepet *praktisk mulig* betegnet som et spørsmål om *«common sense and good faith»*[123]. Det ble videre uttalt at:

> *«What is required of the person launching an offensive is to take the necessary identification measures in good time in order to spare the population as far as possible.»*[124]

Eksempler på slike praktisk mulige forhåndsregler i en cyberkontekst er innhenting av informasjon om det målutvalgte nettverket ved hjelp av kartlegging eller andre metoder som bidrar til å skape et bilde av det eventuelle angrepets forventede effekter. Fokuset er hovedsakelig på forventede effekter på sivile personer eller objekter.[125] Den andre siden av bestemmelsen er at det ikke stilles krav om å ta forhåndsregler som *ikke er praktisk mulige.* Det vil for eksempel være tilfellet dersom all mulighet for informasjonsinnhenting vil føre til at motstanderen oppdager den fiendtlige operasjonen og således får mulighet til å forsvare seg. Dersom det ikke er praktisk mulig å innhente tilstrekkelig informasjon om det utvalgte målet, må angrepet avvente. Alternativt må angrepets omfang begrenses slik at det bare er de deler av det aktuelle målet som det kan oppnås tilstrekkelig informasjon om til å bekrefte status som lovlige mål, som angripes.[126] Slike tilfeller er lett å se for seg innenfor cyberkrigføring. Det kan tenkes at et nettverk som benyttes til militære formål vurderes som et mulig mål. Den militære bruken kan dog bare bekreftes til en liten del av nettverket. Det er ikke praktisk mulig å innhente avklarende informasjon om bruken av resten av nettverket,

---

[122] Schmitt (Ed.) (2013) Side 139(4)
[123] Pilloud, Sandoz, Swinarski, & Zimmermann (1987) Side 682 (2198)
[124] Ibid.
[125] Schmitt (Ed.) (2013) Side 139-140(5)
[126] Ibid. Side 140(6)

som det er grunn til å tro at benyttes til sivile formål. Angriperen vil da være forpliktet å begrense angrepets omfang til de delene eller komponentene av nettverkssystemet som det foreligger tilstrekkelig informasjon om til å kunne bekrefte status som lovlig mål.[127] Dersom slik begrensing av angrepets omfang ikke er mulig, vil angrep bare kunne rettes mot hele nettverket dersom det overholder prinsippet om proporsjonalitet.

Den neste forhåndsregelen i artikkel 57 krever at «de som planlegger eller treffer beslutning om angrep, skal ta alle praktisk mulige forholdsregler ved valg av angrepsmidler og -metoder med sikte på å unngå eller i hvert fall å minske tilfeldig tap av sivilpersoners liv, skade på sivilperson og skade på sivile gjenstander».[128] Denne føringen i valg av angrepsmidler og metoder strekker ikke så vidt at den pålegger den angripende part å velge midler eller metoder som ikke er praktisk mulig eller som går på bekostning av den forventede militære fordel. Schmitt og Widmar trekker frem følgende eksempel:

> *«As an example, an attacker does not have to use a less powerful bomb against an insurgent leader in a building in order to avoid civilian casualties if doing so would significantly lower the likelihood of success (assuming all other IHL requirements are met).»* [129]

På den andre siden kommer regelen til anvendelse selv om et planlagt angrep oppfyller kravet om proporsjonalitet. Selv om forventet sivilskade ikke er å regne som overflødig i forhold til den forventede militære fordelen, må alle *praktisk mulige forhåndsregler* tas for å begrense kollateralskade. Hva som i cyberkontekst utgjør *midler* og *metoder* er avklart tidligere i oppgaven. Begrepsbruken medfører at hensyn må tas både ved valg av våpen og ved hvordan det aktuelle våpenet skal brukes. Standarden for hva som er *praktisk mulig* og hvem bestemmelsen retter seg mot er tilsvarende det som gjelder artikkel 57(2)(a)(i), som redegjøres for ovenfor.

En problemstilling som er særlig relevant i forhold til cyberkrigføring er vurdering av indirekte effekter av angrep. Det skyldes den nære tilknytningen mellom ulike datasystemer og nettverk, særlig mellom militære og sivile systemer. Ekspertene i Tallinmanualen støttet

---

[127] Schmitt (Ed.) (2013) Side 140(6)
[128] Første tilleggsprotokoll artikkel 57(2)(a)(ii)
[129] Schmitt & Widmar (2014) Side 402

det amerikanske synet om at det var hensiktsmessig å inkludere indirekte effekter ved vurdering av kollateralskade.[130] Følgelig må det også tas hensyn til indirekte effekter ved vurdering av praktisk mulige forhåndsregler. Forhåndsregelen i artikkel 57(2)(a)(iii) i første tilleggsprotokoll er en forlengelse av proporsjonalitetsprinsippet. Prinsippet om proporsjonalitet behandles i dybden i neste kapittel.

Stuxnet var et reelt cybervåpen som etter alt å dømme ble designet med hensyn til både direkte og indirekte effekter.[131] Stuxnet var en dataorm[132] som i første rekke ble brukt mot iranske kjernefysiske anlegg. I ettertid muterte ormen og spredte seg også til andre industrielle og energiproduserende anlegg. Den skadelige programvaren i det originale angrepet rett mot kjernekraftverkene var spesifikt rettet mot programmerbare logikkontrollere (PLCer)[133] som ble brukt til å automatisere maskinprosesser.[134] Stuxnet-ormen ble spredt via USB-minnepenner til datamaskiner som opererte på Microsoft Windows. Viruset søkte gjennom de infiserte datamaskinene på jakt etter Siemens Step 7-programvare. Programvaren indikerte hvilke maskiner som opptrådte som PLCer for å automatisere og overvåke elektromekanisk utstyr. Dersom en slik PLC-datamaskin ble oppdaget oppdaterte ormen sin egen kode over internett. Den nye koden begynte så å sende ondsinnede instrukser til det elektromekaniske utstyret som datamaskinen kontrollerte. Viruset justerte deretter hastigheten på sentrifugene slik at de ødela seg selv. Samtidig sendte ormen falske tilbakemeldinger til hovedkontrollen, slik at eventuell overvåking av utstyret ikke skulle kunne oppdage angrepet før skaden var skjedd.

Stuxnet er et potensielt interessant eksempel fra virkeligheten i *jus ad bellum*-kontekst fordi det er en cyberoperasjon som ble utført utenfor væpnet konflikt og som hadde en kinetisk effekt i form av ødelagte sentrifuger. Vurderinger som hvorledes Stuxnet er å regne som et

---

[130] Schmitt (Ed.) (2013) Side 140-141(5)
[131] Gervais, M. (2012). Cyber attacks and the laws of war. Journal of Law & Cyber Warfare, 1(1), 8-98. Side 570
[132] «Dataorm er en variant av et datavirus som ikke trenger noen vert for spredning. Den har de mekanismer selv som trengs for spredning, men opptrer forøvrig på samme måte som et datavirus» - Wikipedia om «Dataorm» - https://no.wikipedia.org/wiki/Dataorm – sist hentet 04.12.2020
[133] Programmerbare logikk-kontrollere er spesialisert utstyr som er designet for å motta informasjon fra et flertall sensorer samtidig. Informasjonen benyttes til å kontrollere en eller flere prosesser i sanntid.
[134] McAfee – What Is Stuxnet?: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html - sist hentet 04.12.2020

væpnet angrep etter UNC artikkel 51 er derimot utenfor denne oppgavens omfang. Grunnen til at Stuxnet trekkes frem i denne oppgaven er fordi den etter alt å dømme ble designet og utviklet med reglene i krigens folkerett i bakgrunnen. En sikkerhetsanalytiker hos N.Y Times uttalte at Stuxnet var en «marksman's job».[135] Hensynene som ligger til grunn tyder på at utviklerne og angriperne var opptatt av distinksjon og proporsjonalitet.[136] Således er den et eksempel på hvordan forhåndsregelen om valg av middel og metode kan få betydning i praksis, ved at de som benytter seg av cybermidler utvikler eller tilpasser lignende spesialiserte midler som begrenser angrepets omfang og effekter. Dersom Stuxnet-ormen hadde blitt benyttet i en internasjonal væpnet konflikt hadde den høyst trolig utgjort et cyberangrep, ettersom den medførte fysisk ødeleggelse. Ormens målrettede design ville da kunne ha oppfylt kravet om distinksjon, forutsatt at de rammede kjernekraftverkene ikke var sivile og at ormen ikke vilkårlig ødela øvrige sivile datasystemer.[137]

Forhåndsregelen i artikkel 57(2)(a)(iii) i første tilleggsprotokoll er en forlengelse av proporsjonalitetsprinsippet. Prinsippet om proporsjonalitet behandles i dybden i neste kapittel.

I artikkel 57(3) kreves det videre:

> *«Når det er mulig å velge mellom flere militære mål for å oppnå en tilsvarende militær fordel, skal det mål velges som et angrep på kan forventes å utsette sivilpersoners liv og sivile gjenstander for minst fare.»*

Også denne regelen kommer til anvendelse på operasjoner som utgjør *angrep.* Til forskjell fra artikkel 57 for øvrig, spesifiseres det ikke i lovteksten hvem regelen rettes mot. Konsekvensen av det er at regelen gjør seg gjeldende ovenfor alle som er involvert i målutvelgelse, godkjennelse og gjennomføring av angrep.[138] Ekspertene i Tallinmanualen tolket *fare*-begrepet i bestemmelsen til i første rekke å omfatte personskade, død, skade og ødeleggelse som resultat av direkte eller indirekte effekter av et cyberangrep. Flertallet av ekspertene var av den oppfatning at ødeleggelse av funksjonaliteten i et system som følge av et cyberangrep i

[135] Broad, W. J., Markoff, J., & Sanger, D. E. (2011). Israeli test on worm called crucial in Iran nuclear delay. New York Times, 15, 2011.
[136] Solis (2014) Side 46-47
[137] Gervais (2012) Side 571
[138] Schmitt (Ed.) (2013) Side 142(3)

enkelte sitasjoner også ville være inkludert.[139] Regelen forutsetter naturlig nok at det foreligger flere valgmuligheter. Mulighetene må dog være mer enn bare teoretiske alternativer. Valgmulighetene må være rimelige alternativer når det kommer til reell og militær gjennomførbarhet, samt teknologisk mulighet for suksess.[140] Det alternative målet må videre yte en tilsvarende militær fordel. Hva som utgjør en tilsvarende militær fordel, kan ikke nøyaktig måles hverken kvantitativt eller kvalitativt. Spørsmålet er om ødeleggelse, overtakelse eller nøytralisering av de ulike målene vil oppnå sammenlignbar militære effekter.[141] Den militære fordelen vurderes også i sammenheng med den militære operasjonen i sin helhet, og ikke bare det aktuelle angrepet isolert sett. Dersom et alternativt mål ikke vil gi en slik militær fordel som kreves for at angrepsoperasjonen i sin helhet er suksessfull kan det ikke kreves at det alternative målet angripes istedenfor, selv om et angrep rettet mot det alternative målet sannsynligvis ville medført mindre følgeskader.[142]

I Tallinmanualen beskrives følgende cyber-relevante eksempel[143]: En angriper ønsker å nøytralisere fiendens kommandosentral. Dette kan oppnås på to måter. Angrepet kan rettes mot det elektriske rutenettet som kommandosentralen er avhengig av. Det elektriske rutenettet benyttes i tillegg til sivil kraftforsyning og er således i «dual use». Et angrep rettet mot dette målet vil derfor, selv om det skulle være proporsjonalt, medføre betydelig følgeskade. Det andre alternative er å utføre et cyberangrep på kommandosentralen direkte. Dersom et slikt cyberangrep vil kunne medføre den ønskede militære effekten på kommandosentralen i tillegg til å resultere i mindre følgeskade, må dette alternativet velges.

I tillegg til å sette regelen i artikkel 57(3) inn i en cyberkontekst, illustrerer dette også en potensielt stor fordel ved cyberkrigføring. Cyberangrep vil i mange tilfeller kunne utgjøre en alternativ angrepsmetode som medfører færre typiske kollateralskader enn andre, tradisjonelle angrepsmetoder.[144] Som nevnt tidligere i oppgaven retter cyberangrep seg i første rekke mot gjenstander, og effektene av slike angrep er oftere av mer midlertidig eller reparerbar art enn

[139] Schmitt (Ed.) (2013)141(4)
[140] Ibid. Side 141(5)
[141] Ibid. Side 141(6)
[142] Ibid. Side 141(7)
[143] Ibid. Side 141(8)
[144] Biller & Schmitt (2019) Side 190

effektene fra tradisjonelle kinetiske angrep.[145] Denne forutsetningen om mindre kollateralskade i relasjon til forhåndsreglene ved angrep vil prinsipielt kunne medføre at cyberangrep generelt er å foretrekke fremfor tradisjonelle kinetiske angrep.[146] En plikt til å velge et mindre destruktivt cyberalternativ vil også kunne gjelde cyberoperasjoner under terskelen til å utgjøre cyberangrep. En slik forpliktelse kan utledes fra kravet om å ta «kontinuerlig omsorg» i artikkel 57(1) i første tilleggsprotokoll.[147]

Konklusjonen i forrige avsnitt ser på cyberangrep i makro-forstand. Påstanden støter på problemer dersom den granskes i et mikro-perspektiv.[148] Militære cybersystemer er ofte bedre beskyttet enn sivile systemer.[149] En uheldig konsekvens av dette kan bli at cyberoperasjoner rettes mot sivile systemer. Dersom det er lettere å angripe et sivilt system som er i «dual use» eller som oppfyller kravet om *formål* i artikkel 52(2), kan angrepet rettes mot det sivile alternativet istedenfor et militært, forutsatt at en tilsvarende militær fordel oppnås. Følgelig vil hyppigere bruk av cyberangrep ikke nødvendigvis føre til en reduksjon av sivile tap, men tenkelig kunne føre til økt negativ påvirkning på sivilbefolkningen fra krigshandlinger istedenfor.[150]

4 Proporsjonalitetsprinsippet

I likhet med distinksjonsprinsippet bygger prinsippet om proporsjonalitet på hensynet om å verne om sivile personer og gjenstander fra effektene av militære angrep. Proporsjonalitetsprinsippet stiller krav om at den militære fordel veies opp mot de sivile følgeskadene av angrepet. Prinsippet er hjemlet i første tilleggsprotokoll:

> *«et angrep som må antas å forårsake tilfeldige tap av sivilpersoners liv, skade på sivilperson, skade på sivile gjenstander, eller en kombinasjon av slike følger som ville*

[145] Preston & Taylor (2015) Side 1023
[146] Pascucci (2017) Side 441
[147] Biller & Schmitt (2019) Side 191
[148] Pascucci (2017) Side 441
[149] Gervais (2012) Side 82
[150] Pascucci (2017) Side 441

> *være for omfattende i relasjon til den forventede konkrete og direkte militære fordel.»*[151]

Et angrep som oppfyller beskrivelsen ovenfor er vilkårlig, og følgelig ulovlig.[152] Prinsippet regnes også som sedvanerettslig bindende.[153] Proporsjonalitetsprinsippet er i likhet med distinksjonsprinsippet knyttet til begrepet «angrep». Den samme utfordringen som beskrevet ovenfor i forhold til hva som utgjør som angrep innenfor cyberdomenet gjør seg dermed også gjeldende her. Cyberoperasjoner under angrepsterskelen behøver ikke overholde kravet om proporsjonalitet i artikkel 51(5)(b), 57(2)(a)(iii) eller 57(2)(b).

Artikkel 51(5)(b) definerer ikke hvem som konkret har ansvar for å foreta vurderingen om proporsjonalitet. Bestemmelsen krever bare at en tilstrekkelig vurdering av proporsjonalitet foretas forut for et angrep. Ettersom en slik vurdering er komplisert og krever god oversikt og forståelse for operasjonen som angrepet er del av, vil ansvaret trolig måtte plasseres nokså høyt i kommandokjeden. Trolig vil det kommandoledd som har best forutsetninger for å foreta de nødvendige vurderingene (forventet militære fordel vs. risiko for sivile følgeskader) måtte tillegges hovedansvaret.[154] Forhåndsregelen i artikkel 57(2)(a)(iii) i første tilleggsprotokoll krever at de som *planlegger eller treffer beslutning om angrep* skal:

> *«avstå fra å beslutte iverksatt noe angrep som kan forventes å forårsake tilfeldig tap av sivilpersoners liv, skade på sivilperson, skade på sivile gjenstander eller en kombinasjon av slike følger som ville være for omfattende i relasjon til den forventede konkrete og direkte militære fordel»*

Trolig vil den som *planlegger eller treffer beslutning om angrep* også befinne seg oppover i kommandokjeden. Bestemmelsens viktigste aspekt er at den fastslår at de som planlegger eller beslutter et angrep har et fortløpende og personlig ansvar for å vurdere proporsjonalitet.[155]

---

[151] Første tilleggsprotokoll artikkel 51(5)(b). Prinsippet kommer også til utrykk i artikkel 57(2)(a)(iii) og 57(2)(b). Den er videre også etablert i protokoll II til Våpenkonvensjonen (The Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices (Protocol II)) artikkel 3(3)(c).
[152] Første tilleggsprotokoll artikkel 51(5) jf. 51(4)
[153] Henckaerts (2005) Side 51
[154] Manual i krigens folkerett (2013) Side 35 (2.23)
[155] Schmitt (Ed.) (2013) Side 141(2)

Personell på lavere nivå i kommandokjeden, som ikke kan forventes å ha særlig god oversikt eller forståelse av angrepet og operasjonen i helhet, vil bare ha et ansvar for å avvente eller stoppe et angrep dersom den faktiske situasjonen forandrer seg eller ikke samsvarer med det som er planlagt.[156] Det følger av at artikkel 57(2)(b) gjør seg gjeldende også nedover i kommandokjeden. Bestemmelsen krever at et:

> «*et angrep skal avlyses eller stilles i bero dersom det blir åpenbart at angrepet kan forventes å forårsake tilfeldig tap av sivilpersoners liv, skade på sivilperson, skade på sivile gjenstander eller en kombinasjon av slike følger som ville være for omfattende i relasjon til den forventede konkrete og direkte militære fordel*»

Begrepet *åpenbart* medfører at avlysningsplikten bare gjelder dersom den aktuelle personen innser at det planlagte angrepet er klart ulovlig.[157]

Hvorvidt et angrep er proporsjonalt, beror på en konkret avveiing i hvert enkelt tilfelle. Proporsjonalitetsvurderingen er ikke tiltenkt å være en sammenligningsøvelse med tall.[158] Ulike mennesker og gjenstander kan ikke tilskrives en objektiv eller konstant verdi i forhold til hverandre. Det finnes eksempelvis ingen fasit på hvor stort sivil tap som kan aksepteres for å eliminere en fiendtlig stridende. Likevel er det ikke slik at all sivil lidelse skal tas hensyn til i proporsjonalitetsvurderingen. I følge Dinstein er det *«[o]nly loss of life, injury to human beings and (more than nominal) damage to property count.»* som skal inngå i vurderingen.[159]

Begrepsbruken *antas å forårsake* legger opp til at det bare trengs å foreta en proporsjonalitetsanalyse dersom man ved vurderingen av det aktuelle målet observerer at det er sivile personer eller sivile gjenstander i området, og at det derfor er risiko for kollateral skade. Det kan argumenteres for at den særegne og nære sammenhengen mellom datamaskiner og andre cybersystemer og den hyppige forekomsten av «dual use»-cybersystemer, vil nødvendiggjøre en proporsjonalitetsvurdering ved nesten alle

---

[156] Manual i krigens folkerett (2013) Side 35 (2.24)
[157] Manual i krigens folkerett (2013) Side 35 (2.24)
[158] Berntsen, T., Johansen, S., & Dyndal, G. (2016). Når dronene våkner: Autonome våpensystemer og robotisering av krig. Oslo: Cappelen Damm akademisk. side 142
[159] Dinstein, Y. (2012). The principle of distinction and cyber war in International Armed Conflicts. Journal of Conflict and Security Law, 17(2), side 270

cyberangrep.[160]

Om standarden som kreves ved vurdering av proporsjonalitet har ICTY (International Criminal Tribunal for the former Yugoslavia) uttalt:

> *«In determining whether an attack was proportionate it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack.»*[161]

Hva den konkrete kommandøren faktisk visste er altså ikke avgjørende. Spørsmålet er hva som ville vært rimelig å forvente av kommandøren. En vurderingen av om proporsjonalitetsprinsippet er overholdt i ettertid vil således bero på en *ex ante*-analyse, og de faktiske konsekvensene av et cyberangrep vil ikke være avgjørende. Proporsjonalitetsregelen skal ikke vurderes med etterpåklokskap.[162] Et cyberrelevant eksempel er dersom et cyberangrep som med rimelighet forventes å ville forårsake en midlertidig forstyrrelser av et sivilt nettsted, istedenfor resulterer i uventet ødeleggelse av en server som oppbevarer medisinske journaler, og dermed medfører indirekte pasientdødsfall. Proporsjonalitetsprinsippet vil likevel være overholdt så lenge den forventede midlertidige forstyrrelsen av nettsiden ikke kan regnes som overdreven i lys av den konkrete direkte militære fordelen som var forventet fra angrepet.[163] Å sikre overholdelse av en så komplisert vurdering er problematisk. I kommentarene til første tilleggsprotokoll ble det poengtert at ønskelig overholdelse av prinsippet avhenger av at stridende parter opptrer i fullstendig god tro og med intensjon om å overholde de generelle prinsippene om respekt for sivilbefolkningen.[164]

Med unntak av 57(2)(iii), må proporsjonalitetsregelen adskilles tydelig fra de øvrige reglene om forhåndsregler ved angrep i artikkel 57 og 58 i første tilleggsprotokoll. I motsetning til reglene om proporsjonalitet, krever de øvrige forhåndsregler at sivil skade minimeres

---

[160] Pascucci (2017) Side 446
[161] *Prosecutor v. Stanilav Galic (Trial Judgement and Opinion)*, IT-98-29-T, International Criminal Tribunal for the former Yugoslavia (ICTY), 5 December 2003. Avsnitt 58
[162] Schmitt (Ed.) (2013) Side 135(10)
[163] Pascucci (2017) Side 446
[164] Pilloud, Sandoz, Swinarski, & Zimmermann (1987) Side 625 (1978)

uavhengig av hvorvidt den forventede kollateralskaden er overflødig i forhold til den forventede militære fordelen.[165]

4.1 Vurdering av kollateralskade

Proporsjonalitetsprinsippet er «… couched in language of expectation and anticipation.»[166] Evne og mulighet til å vurdere mulig følgeskade forut for angrepet er derfor særdeles viktig.[167] For tradisjonelle kinetiske angrep eksisterer det allerede en metodologi for å vurdere sannsynlig kollateralskade: «the Collateral Damage Estimate Methodology» (CDEM).[168] CDEM-metoden er ikke egnet til å bruke ved cyberangrep, og et tilsvarende etablert system for cyberkrigføring eksisterer ikke.[169]

Proporsjonalitetsprinsippets betydning for cyberkrigføring beror i stor grad på hva som inngår i skadebegrepet i proporsjonalitetsvurderingen. Slik kunnskap er en nødvendig forutsetning for å vurdere om skaden er *for omfattende* i forhold til den forventede militære fordelen. Ekspertene i Tallinmanualen fremmet at skade på sivile objekter i enkelte situasjoner kunne inkludere tap av funksjonalitet, og at funksjonalitetstap i slike tilfeller skal inngå i proporsjonalitetsvurderingen.[170] Flertallet i manualen fremmet at svekkelse av funksjonaliteten som nødvendiggjør utskifting av fysiske komponenter utgjør et angrep.[171] I proporsjonalitetsvurderingen vil denne tolkningen medføre at slik type skade utgjør kollateralskade dersom det rammer en sivil gjenstand. De samme ekspertene var delte i synet på om skade som nødvendiggjør reinstallasjon av et operativsystem utgjør tilstrekkelig svekkelse av funksjonaliteten til at en cyberoperasjon utgjør et angrep.[172] Det er følgelig uklart om slik type skade kan medregnes ved vurdering av kollateralskade.[173] Mangelen på klarhet i Tallinmanualen er en konsekvens av at det ikke foreligger noen presis oversikt i krigens folkerett over når og i hvilken grad tap av funksjonalitet gjør seg gjeldende i

---

[165] Schmitt (Ed.) (2013) Side 136(15)
[166] Dinstein (2012) Side 270
[167] Pascucci (2017) Side 447
[168] Schmitt, M. (2013). Autonomous weapon systems and international humanitarian law: a reply to the critics. Harvard National Security Journal, 4. Side 19.
[169] Pascucci (2017) Side 448
[170] Schmitt (Ed.) (2013) Side 133(5)
[171] Ibid. Side 93(10)
[172] Ibid.
[173] Pascucci (2017) Side 448

proporsjonalitetsvurderingen.[174]

Som nevnt tidligere i oppgaven, er spørsmålet om data skal regnes som objekt omtvistet. Motviljen til å inkludere data som *gjenstand* er problematisk dersom proporsjonalitetsprinsippet skal fungere som tiltenkt. Viktigheten av data overgår i dag typisk viktigheten av den fysiske infrastrukturen som utgjør dataen. Det kan til og med argumenteres for at eksistensen av data resulterer i redusert verdi for de tilknyttede fysiske gjenstandene.[175] En forsvarlig tolkning av krigens folkerett vil kunne resultere i at en kommandør velger et cyberangrep som påregnelig kan føre til tap av utallige terabyte med data, inkludert medisinske journaler og andre viktige deler av sivile data, istedenfor et kinetisk angrep som forventes å føre til tap av eksempelvis tre sivile menneskeliv.[176] Eksempelet forutsetter at de to alternativene oppnår en tilstrekkelig sammenlignbar militær fordel. Det problematiske i eksempelet ovenfor er at cyberangrepet kan få et betydelig større endelig skadeomfang enn det kinetiske angrepet. Trolig vil mange flere sivile liv kunne gå tapt som konsekvens av datatapet.

4.2 Indirekte effekter

Proporsjonalitetsvurderingen omfavner som nevnt både direkte og indirekte effekter.[177] Eksempelvis vil de indirekte effektene på den sivile befolkningen som følge av et cyberangrep på kontrollsystemet til en elektrisk generator, innlemmes i vurderingen av proporsjonalitet. Det at datamaskiner og cybersystemer er så sammenkoblet av natur byr på utfordringer med tanke på uforutsette indirekte effekter. «Knock-on»-effekter er et begrep som har blitt benyttet i litteraturen. Begrepet tar for seg effekter som ikke er direkte eller umiddelbare resultater av et angrep, men som likevel må regnes som en konsekvens av angrepet.[178] I Tallinmanualen fremheves det at «*… indirect effects of a cyber attack comprise «the delayed and/or displaced second-, third-, and higher-order consequences of action, created through intermediate events*

[174] Pascucci (2017) Side 448
[175] Schmitt (2014) Side 297
[176] Pascucci (2017) Side 448
[177] Schmitt (Ed.) (2013) Side 140-141(5)
[178] Schmitt, M. N. (2002). Wired warfare: Computer network attack and jus in bello. Int'l Rev. Red Cross, 84, 365. Side 393

or mechanisms.»[179] Her er det snakk om at en handling gir en konsekvens som gir ringvirkninger. Disse ringvirkningene får igjen egne ringvirkninger. Slik oppstår det flere nivåer med konsekvenser. Det er uklart hvor avledet konsekvenser som inngår i proporsjonalitetsvurderingen kan være.[180] I Tallinmanualen argumenteres det for at alle indirekte effekter som med rimelighet er forutsigbare inngår i vurderingen, uavhengig av hviket nivå (*order*) effekten inntrer i.[181] En slik tolkning er i samsvar med ordbruken «antas å forårsake» i artikkel 51(5)(b).[182] Inndeling i ordener er således til begrenset hjelp ved vurderingen av hvilke effekter som skal inkluderes i proporsjonalitetsanalysen. Eksempelvis vil det likevel være mer rimelig å forvente at effekter av første orden identifiseres og inkluderes i analysen, enn effekter av fjerde orden.

Det kan problematiseres hvilken betydning kollateralskade skal tillegges i proporsjonalitetsvurderingen når det inntrer på den sivile delen av et cybersystem som er i «dual use» fordi en stat med overlegg benytter systemet til sivile og militære formål samtidig.[183] Det er ikke tvilsomt at cybersystemer som benyttes slik vil utgjøre lovlige mål for angrep. Spørsmålet er om slik kollateralskade kan ekskluderes fra proporsjonalitetsvurderingen. Dinniss konkluderer med at selv hvor systemet er konstruert slik at den militære delen ikke kan angripes uten også å skade den sivile delen, må den sivile kollateralskaden inngå i proporsjonalitetsvurderingen.[184] Resonnementet bygger på en parallell til skade på frivillige menneskelige skjold, hvor det er fremmet argumenter for at kollateralskade på frivillige menneskelige skjold skal ekskluderes fra proporsjonalitetsvurderingen. Hvorvidt slik skade skal inkluderes eller ekskluderes fra vurderingen er omstridt i litteraturen.[185] Parallellen kommer uansett til kort ettersom et frivillig menneskelig skjold har foretatt en bevist handling som resulterer i tap av beskyttelsen. Ettersom sivilbefolkning trolig vil være uvitende om den overlagte «dual use»-

---

[179] Schmitt (Ed.) (2013) Side 133(6)
[180] Dinniss, H. H. (2012). Cyber warfare and the laws of war (Vol. 92). Cambridge University Press. Side 208
[181] Schmitt (Ed.) (2013) Side 133(6)
[182] Dinniss (2012) Side 208
[183] Ibid.
[184] Ibid.
[185] Dinstein, Y. (2016). The conduct of hostilities under the law of international armed conflict. Cambridge University Press. Side 183-184;
Bosch, S. (2013). Targeting decisions involving voluntary human shields in international armed conflicts in light of the notion of direct participation in hostilities. Comparative and International Law Journal of Southern Africa, 46(3), 447-473. Side 457

bruken, vil det være mer nærliggende å sammenligne med ufrivillige menneskelige skjold.[186] Selv om enkelte argumenterer for en nedsatt betydning, er det utvilsomt at skade på ufrivillige menneskelige skjold inngår i proporsjonalitetsvurderingen.[187]

4.3 Konkret og direkte militær fordel

Den konkrete og direkte militære fordel skal på sedvanerettslig grunnlag vurderes ut fra den forventede fordelen av det aktuelle angrepet i sin helhet.[188] I likhet med fordelsvurderingen som kreves etter artikkel 52(2) i første tilleggsprotokoll,[189] må blikket heves fra enkeltstående eller isolerte deler av angrepet. Selv om det er snakk om en *forventet* fordel, legger begrepene *konkret og direkte* en klar begrensning på at fordelen ikke kan være fjerntliggende eller usannsynlig.[190] Denne begrepstolkningen støttes i ICRCs kommentar til første tilleggsprotokoll, hvor det om begrepsbruken uttales:

> *«The expression "concrete and direct" was intended to show that the advantage concerned should be substantial and relatively close, and that advantages which are hardly perceptible and those which would only appear in the long term should be disregarded.»*[191]

Dinstein oppfatter et krav om at fordelen må være «*substantial*», slik ICRC fremmer, som feilaktig. En *konkret* militær fordel må ifølge Dinstein være *«… particular, perceptible and real as opposed to general, vague and speculative»*[192]

4.4 Overflødig skade

Spørsmålet er så hva som skal til for at følgene av et angrep er *for omfattende i relasjon til den forventede konkrete og direkte militære fordel*. Hva som konkret er «for omfattende» er

---

[186] Dinniss (2012) Side 208
[187] Schmitt, M. N. (2011). Essays on law and war at the fault lines. Springer Science & Business Media. Side 196-197
[188] Schmitt (Ed.) (2013) Side 134(9)
[189] Se oppgavens kapittel 3.1.3
[190] Schmitt (Ed.) (2013) Side 134(8)
[191] Pilloud, Sandoz, Swinarski, & Zimmermann (1987) Side 684 avsnitt 2209
[192] Dinstein (2016) Side 160-161

ikke nærmere definert i krigens folkerett.[193] I ICRCs kommentar til første tilleggsprotokoll ble det poengtert at *«[t]he Protocol does not provide any justification for attacks which cause extensive civilian losses and damages. Incidental losses and damages should never be extensive.»*[194] Til tross for dette inntok flertallet i Tallinmanualen standpunktet om at slik omfattende kollateralskade er lovlig, dersom den forventede konkrete og direkte militære fordelen er tilstrekkelig betydelig. Motsatt vil liten skade kunne være ulovlig hvis den forventede militære fordelen er ubetydelig.[195] Manualen gir ingen videre veiledning om hvilke konkrete standarder som gjør seg gjeldende. Villigheten til å innta en annen posisjon enn den som kommer til utrykk i kommentaren (*extensive civilian losses and damages*) er om ikke annet et utrykk for proporsjonalitetsprinsippets grad av subjektivitet.[196] Det er ikke til å legge skjul på at anvendelse av proporsjonalitetsprinsippet ved cyberangrep er en særlig utfordrende øvelse.[197] Det er langt enklere å forsikre seg om at kinetiske angrep bare rettes mot militære mål, enn det er å vurdere om sivile cyberinteresser er viklet inn i militære cyberinteresser. Likevel kreves det at stater forut for et cyberangrep evner å vurdere og kartlegge disse kompliserte sammenhengene, og avstå fra angrep dersom de sivile og militære interessene er for sammenkoblede.[198]

5 Martens klausulen

Martens klausulen er avtalefestet i artikkel 1(2) i første tilleggsprotokoll til Genèvekonvensjonene:

> *«I de tilfelle som ikke er dekket av denne Protokoll eller av andre internasjonale avtaler, skal sivile og stridende beskyttes av og stilles under folkerettens prinsipper slik som de utspringer av fastsatte sedvaner, av humanitære prinsipper og av den offentlige samvittighets krav.»*[199]

---

[193] Schmitt (Ed.) (2013) Side 133 (7)
[194] Pilloud, Sandoz, Swinarski, & Zimmermann (1987) Side 625 (1980)
[195] Schmitt (Ed.) (2013) Side 134 (7)
[196] Pascucci (2017) Side 449
[197] Ibid.
[198] Petkis, S. (2015). Rethinking proportionality in the cyber context. Geo. J. Int'l L., 47, 1431. Side 1457
[199] Bestemmelsen eksisterer også i nesten likelydende varianter i fortalen til 2. Haagkonvensjon av 1899, fortalen til 4. Haagkonvensjon av 1907, artikkel 63/64/142/158 i de fire Genèvekonvensjonene av 1949.

ICRC anser at klausulen har oppnådd internasjonal sedvanerettslig status, og at den følgelig er generelt anvendelig.[200] I tillegg er klausulen inkorporert i en rekke avtaler.[201] Klausulen er tenkt å fungere som et sikkerhetsnett. Den skal fange opp tilfeller som ikke er direkte regulert av krigens folkerett, men som likevel bør anses ulovlig på grunnlag av hensyn til menneskelighet og offentlig samvittighet. Klausulen er først og fremst aktuell på områder hvor det kan stilles spørsmål ved om krigens folkerett har hengt med i den raske utviklingen av nye militærteknologi. Den underbygger for eksempel synet om at noe som ikke er eksplisitt forbudt av en traktat, for eksempel et nytt våpen, ikke automatisk er lovlig å benytte seg av etter krigens folkerett.[202] Martens klausulen var kjernen i argumentasjonen til Human Rights Watch (HRW) da de i en rapport anmodet alle medlemsparter til «Convention on Certain Conventional Weapons» (CCW) [203] om å inngå et samarbeid for å avtalefeste et forbud mot bruk av autonome våpensystem.[204]

Spørsmålet er så om Martens klausulen kan tillegges nevneverdig betydning ovenfor cyberkrigføring. Som et minimum støtter klausulen argumentet at det som ikke er forbudt etter avtale, ikke nødvendigvis er lovlig.[205] Klausulen kan neppe utgjøre et selvstendig grunnlag for forbud mot typer våpen eller metoder- og virkemidler for krigføring, men taler for at humanitære prinsipper og den offentlige samvittighets krav skal vektlegges ved tvilstilfeller innenfor krigens folkerett.[206]

---

[200] ICRC casebook - Martens Clause: https://casebook.icrc.org/glossary/martens-clause - sist hentet 31.05.2020
[201] Klausulen refereres til i: 1925 Geneva Gas Protocol, 1972 Biological Weapons Convention, 1980 Convention on Conventional Weapons, 1997 Mine Ban Treaty, 2008 Convention of Cluster Munitions, og 2017 Treaty on the Prohibition of Nuclear Weapons.
[202] Wallace, D. (2018). Cyber weapon reviews under international humanitarian law: A critical analysis. Tallinn Paper, (11), 22. Side 9
[203] Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects: http://disarmament.un.org/treaties/t/ccwc - sist hentet 31.05.2020
[204] Docherty, B. L. (2018). Heed the Call: A Moral and Legal Imperative to Ban Killer Robots. Human Rights Watch.
[205] Meron, T. (2000). The Martens Clause, principles of humanity, and dictates of public conscience. The American Journal of International Law, 94(1), 78-89. Side 87
[206] Ibid. Side 87-88

Den internasjonale domstolen (ICJ) har ikke bidratt til en avklaring av klausulens betydning. I en artikkel som søkte å klarlegge klausulens betydning for krigens folkerett konkluderte Ticehurst blant annet følgende:

> *«The ICJ in its Advisory Opinion did not clarify the extent to which the Martens Clause permits notions of natural law to influence the development of the laws of armed conflict. Consequently, its correct interpretation remains unclear.»*[207]

Etter å ha foretatt en gjennomgang av slike internasjonale og nasjonale saker som nevner klausulen, poengterte Cassese at klausulen ble nevnt *«… primarily to pay lip service to humanitarian demands …».*[208] Det foreligger med andre ord ikke rettspraksis som støtter bruk av Martens klausulen som en selvstendig rettskilde. I samme artikkel beskrev Cassese klausulen som et resultat av diplomatisk manøvrering heller enn en regel motivert av humanitære hensyn.[209]

Hva som spesifikt ligger i humanitære prinsipper og offentlig samvittighet er ikke tydelig presisert. Muligens kan klausulen fremmes som et argument til støtte for at øvrige regler i første tilleggsprotokoll tolkes til fordel for beskyttelse av sivile personer og gjenstander. Analysene av proporsjonalitets- og distinksjonsprisnippenes anvendelse i cyberkontekst tidligere i oppgaven har blottlagt enkelte mulige svakheter. Kanskje kan Martens klausulen tale for en tolkning som i større grad prioriterer sivil beskyttelse, der hvor enkelte aspekter av cyberkrigføring ikke omfattes av en tradisjonell tolkning av krigens folkerett slik den kommer til utrykk i første tilleggsprotokoll.

---

[207] Ticehurst, R. (1997). The Martens Clause and the laws of armed conflict. International Review of the Red Cross Archive, 37(317) - Sitatet omtaler ICJ-saken: «Legality of the Use by a State of Nuclear Weapons in Armed Conflict - Advisory Opinion of 8 July 1996 - Advisory Opinions»
[208] Cassese, A. (2000). The Martens Clause: half a loaf or simply pie in the sky? European Journal of International Law, 11(1), side 208
[209] Ibid. Side 216

6 Avslutning

Cyberdomenet er allerede et viktig fokusområde for militæret, og det er liten tvil om at viktigheten bare vil fortsette å vokse i tiden fremover.[210] Cyberangrep utgjør et billig, øyeblikkelig og effektivt alternativ til tradisjonell krigføring, ofte uten å utløse tilsvarende grad av ansvarlighet.[211] Viktigheten av egnet regulering er derfor av stor betydning. Det er som nevnt ubestridt at cyberkrigføring omfattes av den generelle reguleringen i krigens folkerett. Anvendelsen av de grunnleggende prinsippene viser seg imidlertid både utfordrende og problematisk. Prinsippene «lider» under en historisk forståelse av effekter slik de har vært definert i tradisjonell kinetisk krigføring.[212] Den historiske forståelsen kommer muligens til kort dersom betydelige tap av funksjon ikke kan regnes som skade. Videre er mangelen på en klargjøring av hvilke typer tap av funksjonalitet som skal inngå i proporsjonalitetsvurderingen en svakhet. Problematikken rundt inkludering av data som en gjenstand medfører muligens begrenset beskyttelse av sivile datasett. Dersom dette fører til at cyberoperasjoner faller under angrepsterskelen, kan konsekvensen bli mangelfull sivil beskyttelse. Mye av problematikken for øvrig er knyttet til vanskelighetene som følger av den systemiske sammenkoblingen mellom militær og sivil infrastruktur[213] og den betydelige forekomsten av «dual use» cyberinfrastruktur.[214]

Cyberkrigføring er en nyere form for krigføring, og den rettslige utviklingen på området kan derfor forventes å foregå hurtig. Hurtig rettslig utvikling er nærmest en forutsetning dersom retten skal holde følge med den akselererte teknologiske utviklingen. Det er ikke helt utenkelig at det i fremtiden kan produseres en mellomstatlig avtale som skal regulere cyberkrigføring. Slikt arbeid pågår dog ikke i skrivende stund. En fjerde tilleggsprotokoll til Genèvekonvensjonene som omhandler cyberkrigføring hadde trolig vært fordelaktig, men et slikt rettslig samarbeid er vanskelig å se for seg i dagens politiske klima. Det samme gjelder mulighetene for en eventuell tilleggsprotokoll til CCCW. Stater er motvillige mot å la andre legge føringer på hva de kan foreta seg i cyberdomenet. Tallinmanual 1.0 og 2.0 utgjør som nevnt det mest omfattende arbeidet som er produsert innenfor området. Manualen er ikke en

[210] Geib & Lahmann (2012) Side 381
[211] Gervais (2012) Side 54
[212] Pascucci (2017) Side 453
[213] Geib & Lahmann (2012) Side 381
[214] Schmitt (2014) Side 297

primærkilde, og dens rettslige betydning er sannsynligvis noe svekket som følge av internasjonal kritikk. Kanskje er det mer sannsynlig at land som Kina og Russland kan medvirke til utarbeidelse av en tredje Tallinmanual, og således bidra til en oppdatert manual med sterkere rettslig vekt.

Det eksisterer allerede utallige ulike former for cyberoperasjoner og angrepsmetoder, og utviklingen vil med sikkerhet bringe med seg enda flere. Eventuelle nye avtaler som ferdigstilles vil vanskelig kunne forutse og ta høyde for alle fremtidige former for cyberkrigføring. Tolkningen av de primære rettskildene forandres over tid. Rettslig utvikling er således ikke nødvendigvis avhengig av nye avtaler. Det er grunn til å tro at gradvis mer «moderne» og tilpassede tolkninger av krigens folkerett vil kunne avhjelpe flere av svakhetene som denne oppgaven har pekt på i forhold til cyberkrigføring. Eksempelvis spås det i litteraturen at utviklingen beveger seg mot inkludering av data i gjenstandsbegrepet.[215]

[215] Schmitt (2015) Side 108

Referanseliste

Konvensjoner og traktater

Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects - http://disarmament.un.org/treaties/t/ccwc - sist hentet 31.05.2020

Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction; http://disarmament.un.org/treaties/t/bwc/text - sist hentet 31.05.2020

Genèvekonvensjonene av 1949

Konvensjon om datakriminalitet – ETS nr. 185: https://lovdata.no/dokument/TRAKTAT/traktat/2001-11-23-1/KAPITTEL_1#KAPITTEL_1 – sist hentet 15.12.2020

Protokoll II til Våpenkonvensjonen (The Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices (Protocol II))

Regulations, H. L. W. (1907). Regulations respecting the laws and customs of war on land

Tilleggsprotokoll til Genève-konvensjonene av 12-08-1949 hva angår beskyttelse av ofre for internasjonale væpnede konflikter (Første tilleggsprotokoll)

Vedtekter for Den internasjonale domstol: https://lovdata.no/pro/#document/TRAKTAT/traktat/1945-06-26-2/a38 - sist hentet 13.12.2020

Wien-konvensjonen om traktatretten: https://treaties.un.org/doc/Publication/UNTS/Volume%201155/volume-1155-i-18232-english.pdf - sist hentet 15.12.2020

1925 Geneva Gas Protocol

1972 Biological Weapons Convention

1980 Convention on Conventional Weapons

1997 Mine Ban Treaty

2008 Convention of Cluster Munitions

2017 Treaty on the Prohibition of Nuclear Weapons.

2. Haagkonvensjon av 1899

4. Haagkonvensjon av 1907

Domsavgjørelser

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J.

Prosecutor v. Stanilav Galic (Trial Judgement and Opinion), IT-98-29-T, International

Criminal Tribunal for the former Yugoslavia (ICTY), 5 December 2003.

Manualer

HEADQUARTERS, U., CORPS, M., & GUARD, U. C. (2007). The Commander's Handbook on The Law of Naval Operations (EDITION AUGUST 2017).

Høyskole, F., & Stabsskole, F. (2013). Manual i krigens folkerett.

Preston, S. E., & Taylor, R. S. (2015). Department of Defense Law of War Manual. General Counsel of the Department of Defense Washington United States (Updated Dec 2016). https://www.hsdl.org/?abstract&did=797480 – sist hentet 05.12.2020

Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

Schmitt, M. N. (Ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press.

Bøker

Berntsen, T., Johansen, S., & Dyndal, G. (2016). Når dronene våkner: Autonome våpensystemer og robotisering av krig. Oslo: Cappelen Damm akademisk.

Dinniss, H. H. (2012). Cyber warfare and the laws of war (Vol. 92). Cambridge University Press.

Dinstein, Y. (2016). The conduct of hostilities under the law of international armed conflict. Cambridge University Press.

Henckaerts, J. M. (2005). Customary international humanitarian law: Volume 1, Rules (Vol. 1). Cambridge University Press.

Pilloud, C., Sandoz, Y., Swinarski, C., & Zimmermann, B. (Eds.). (1987). Commentary on the additional protocols: of 8 June 1977 to the Geneva Conventions of 12 August 1949. Martinus Nijhoff Publishers.

Artikler

Biller, J., & Schmitt, M. N. (2019). Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare. Means, or Methods of Warfare (June 19, 2019), 95.

Bosch, S. (2013). Targeting decisions involving voluntary human shields in international armed conflicts in light of the notion of direct participation in hostilities. Comparative and International Law Journal of Southern Africa, 46(3), 447-473.

Brown, G. D. (2016). International Law Applies to Cyber Warfare: Now What. Sw. L. Rev., 46.

Cassese, A. (2000). The Martens Clause: half a loaf or simply pie in the sky? European Journal of International Law, 11(1).

Chang, Z. (2017). Cyberwarfare and International Humanitarian Law. Creighton Int'l & Comp. LJ, 9, 29.

Dinstein, Y. (2012). The principle of distinction and cyber war in International Armed Conflicts. Journal of Conflict and Security Law, 17(2).

Dörmann, K. (2004). Applicability of the Additional Protocols to computer network attacks. Int'l Committee of the Red Cross.

Geib, R., & Lahmann, H. (2012). Cyber warfare: Applying the principle of distinction in an interconnected space. Isr. L. Rev., 45, 381.

Gervais, M. (2012). Cyber attacks and the laws of war. Journal of Law & Cyber Warfare, 1(1), 8-98.

Hsu, K., & Murray, C. (2014). China and international law in cyberspace. US-China Economic and Security Review Commission.

ICRC, A. (2006). Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977, January 2006. IRRC, 88(864).

ICRC, Autonomy, artificial intelligence and robotics: Technical aspects of human control, August 2019.

Ku, J. (2017). How China's Views on the Law of Jus ad Bellum Will Shape Its Legal Approach to Cyberwarfare. Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1707.

Margulies, P. (2020). Autonomous Cyber Capabilities Below and Above the Use of Force Threshold: Balancing Proportionality and the Need for Speed. International Law Studies, 96(1), 13.

McCormack, T. (2018). International Humanitarian Law and the Targeting of Data. International Law Studies, 94(1), 222-240.

Meron, T. (2000). The Martens Clause, principles of humanity, and dictates of public conscience. The American Journal of International Law, 94(1), 78-89.

Pascucci, P. (2017). Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution. Minn. J. Int'l L., 26, 419.

Petkis, S. (2015). Rethinking proportionality in the cyber context. Geo. J. Int'l L., 47, 1431.

Rid, T., & McBurney, P. (2012). Cyber-weapons. the RUSI Journal, 157(1), 6-13.

Sandvik, K. B. (2013). Cyberkrig og internasjonal rett. Internasjonal politikk, 71(02), 252-262.

Schmitt, M. N. (2015). Notion of Objects during Cyber Operations: A Risposte in Defence of Interpretive and Applicative Precision. Isr. L. Rev., 48, 81.

Schmitt, M. N. (2014). The law of cyber warfare: Quo Vadis. Stan. L. & Pol'y Rev., 25, 269.

Schmitt, M. N., & Widmar, E. W. (2014). On Target: Precision and Balance in the Contemporary Law of Targeting. J. Nat'l Sec. L. & Pol'y, 7, 379.

Schmitt, M. N., & Thurnher, J. S. (2012). Out of the loop: autonomous weapon systems and the law of armed conflict. Harv. Nat'l Sec. J., 4, 231. (2019) Artificial intelligence and offensive cyber weapons, Strategic Comments, 25:10, x-xii.

Schmitt, M. N. (2012, June). "Attack" as a term of art in international law: The cyber operations context. In 2012 4th International Conference on Cyber Conflict (CYCON 2012) (pp. 1-11). IEEE.

Schmitt, M. N. (2011). Essays on law and war at the fault lines. Springer Science & Business Media.

Schmitt, M. N. (2002). Wired warfare: Computer network attack and jus in bello. Int'l Rev. Red Cross, 84, 365.

Solis, G. D. (2014). Cyber warfare. Mil. L. Rev., 219.

Ticehurst, R. (1997). The Martens Clause and the laws of armed conflict. International Review of the Red Cross Archive, 37(317)

Wallace, D. (2018). Cyber weapon reviews under international humanitarian law: A critical analysis. Tallinn Paper, (11), 22.

Nettsted, presseklipp og teknisk informasjon fra nettet

Broad, W. J., Markoff, J., & Sanger, D. E. (2011). Israeli test on worm called crucial in Iran nuclear delay. New York Times, 15, 2011.

Børresen, Jacob: cyberdomenet i Store norske leksikon på snl.no. Hentet 15. desember 2020 fra https://snl.no/cyberdomenet

Cooper, Camilla Guldahl; Larsen, Kjetil Mujezinović: krigens folkerett i Store norske leksikon på snl.no. Hentet 15. desember 2020 fra https://snl.no/krigens_folkerett

cyber- i Store norske leksikon på snl.no. Hentet 15. desember 2020 fra https://snl.no/cyber-

CyberDiplomacy (2019) Tallinn Manual — A Brief Review of the International Law Applicable to Cyber Operations: https://medium.com/@cyberdiplomacy/tallinn-manual-a-brief-review-of-the-international-law-applicable-to-cyber-operations-5643c886d9e2 – sist hentet 11.12.2020

David Vergun (2015). Multidomain Operations Rely on Partnerships to Succeed: https://www.defense.gov/Explore/News/Article/Article/1755520/multidomain-operations-rely-on-partnerships-to-succeed/ - sist hentet 18.11.2020

Deborah Brown (2020) It's Time to Treat Cybersecurity as a Human Rights Issue: https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue - sist hentet 11.12.2020

«Heed The Call»: https://www.hrw.org/sites/default/files/report_pdf/arms0818_web.pdf - sist hentet 09.12.2020

ICRCblog (2017) When does IHL apply?: https://blogs.icrc.org/ilot/2017/08/13/when-does-ihl-apply/ - sist hentet 03.12.2020

ICRC expert meeting, «THE POTENTIAL HUMAN COST OF CYBER OPERATIONS»: https://www.icrc.org/en/document/potential-human-cost-cyber-operations - sist hentet 03.10.2020

ICRC casebook - Martens Clause: https://casebook.icrc.org/glossary/martens-clause - sist hentet 31.05.2020

James Conca (2018) When Would Russia's Cyber Warfare Morph Into Real Warfare? Refer To The Tallinn Manual: https://www.forbes.com/sites/jamesconca/2018/08/09/when-would-russias-cyber-warfare-morph-into-real-warfare-refer-to-the-tallinn-manual/?sh=706ff8306b27 – sist hentet 23.11.2020

McAfee – What Is Stuxnet?: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html - sist hentet 04.12.2020

NATO Cooperative Cyber Defence Centre of Excellence on Tallinmanual 2.0: https://ccdcoe.org/research/tallinn-manual/ - sist hentet 11.12.2020

Tidemann, Axel: dyp læring i Store norske leksikon på snl.no. Hentet 15. desember 2020 fra https://snl.no/dyp_l%C3%A6ring

Tidemann, Axel: kunstig intelligens i Store norske leksikon på snl.no. Hentet 15. desember 2020 fra https://snl.no/kunstig_intelligens

Wilson da Silva (2019) War of the Bots: Artificial Intelligence in Cyber Warfare: https://medium.com/predict/spy-vs-spy-cyber-warfare-gets-automated-aba60ece738c - sist hentet 09.11.20

Wikipedia om «Dataorm»: https://no.wikipedia.org/wiki/Dataorm – sist hentet 04.12.2020