Elektronisk krigsførelse i folkeretligt perspektiv

Forfattere: Ulrik Graff og Iben Yde

Kolofon:

Dette baggrundspapir er en del af den forskningsbaserede myndighedsbetjening, som Det Juridiske Fakultet, Københavns Universitet, i samarbejde med Forsvarsakademiet leverer til Forsvarsministeriet og de politiske partier bag forsvarsforliget. Baggrundspapiret sætter fokus på de folkeretlige rammer for anvendelsen af forskellige former for elektronisk krigsførelse. Formålet med baggrundspapiret er at kaste lys over den aktuelle retlige udvikling på området og diskutere implikationerne heraf for det danske forsvars brug af elektronisk krigsførelse i den militære opgaveløsning.

Om InterMil-projektet:

InterMil gennemfører praksisnær juridisk forskning og forskningsbaseret myndighedsbetjening inden for militære studier. InterMil-projektet er etableret ved en aftale mellem Det Juridiske Fakultet (i samarbejde med Forsvarsakademiet) og Center for Militære Studier på Københavns Universitet som led i implementeringen af forsvarsforliget 2018-2023, hvori forligskredsen har udtrykt et ønske om "øget fokus på de folkeretlige udfordringer forbundet med bl.a. deltagelse i internationale operationer, cyber, droner og højteknologiske og elektroniske kampmidler."

Dette baggrundspapir er et analysearbejde baseret på retsvidenskabelig metode. Baggrundspapirets konklusioner er ikke udtryk for holdninger hos den danske regering, det danske forsvar eller andre myndigheder.

Læs mere om InterMil-projektet på: International Law & Military Operations (InterMil) – University of Copenhagen (ku.dk)

Forfattere:
SPKONS, Ulrik Graff
Adjunkt, ph.d. Iben Yde

Indhold

Indledning

Elektronisk krigsførelse (EW) har været en integreret del af militære operationer, lige så længe som elektroniske systemer har været anvendt på kamppladsen. Siden de første velbeskrevne eksempler på aflytning af fjendtlig militær kommunikation i krigen mellem Japan og Rusland (1904 til 1905) har EW gennem tiden udviklet sig fra primært at være fokuseret på aflytning af modstanderens kommunikation, til i dag at være en samlebetegnelse for en lang række forskellige aktiviteter i det elektromagnetiske spektrum, der udgør en central militær støttefunktion for militære operationer i alle operative domæner. Men hvordan ser de folkeretlige rammer for EW-operationer ud? Giver EW anledning til bekymringer i forhold til den humanitære folkerets regulering af militære operationer i væbnet konflikt?

For at få et indtryk af de mange forskellige facetter af EW i moderne krigsførelse kan man rette blikket mod Ukraine, hvor begge parter siden konfliktens begyndelse har gjort flittigt brug af det elektromagnetiske spektrum i deres militære operationer. Jamming af droner, spoofing af præcisionsvåben, efterretningsindhentning gennem mobiltelefoner og transmission af målrettet propaganda til både soldater og civile er blot nogle af eksemplerne på, hvordan det elektromagnetiske spektrum er blevet anvendt i defensivt såvel som offensivt øjemed.[1]

I dag findes der stort set ikke materiel eller kommunikationsudstyr på kamppladsen, der ikke er afhængig eller benytter sig af det elektromagnetiske spektrum. Det gælder alt fra kommunikationssystemer og positioneringsudstyr til offensive og defensive våbensystemer.[2] EW må derfor anses som et essentielt element i enhver moderne militær organisation, også det danske Forsvar.[3]

Til trods for at EW længe har været en realitet i væbnede konflikter og formentlig kun vil få endnu større betydning i takt med den hastige digitalisering af kamppladsen, har den folkeretlige interesse for området været minimal. Der findes stort set ingen selvstændig behandling af emnet i den folkeretlige litteratur eller nationale militærmanualer, heller ikke den danske. Der kan være gode grunde til, at EW hidtil er gået under folkeretsjuristernes radar. Den primære årsag er formentlig, at en stor del af de effekter der skabes gennem det elektromagnetiske spektrum, falder uden for den humanitære folkerets regler om militære operationers anvendelsesområde, og at EW i det store hele ikke har givet anledning til problemer i praksis. Der betyder imidlertid ikke, at den manglende folkeretlige behandling er hensigtsmæssig. For det første er der allerede nu effekter og anvendelsesmåder, der giver anledning til folkeretlige overvejelser. For det andet vil sandsynligheden for at der opstår flere udfordringer givetvis stige, i takt med at anvendelsen af EW i væbnet konflikt vokser i betydning, art og omfang. Forsvaret vil derfor med stor sandsynlighed skulle tage stilling til folkeretlige spørgsmål i forbindelse med anvendelsen af EW-kapaciteter som led i vores engagement i væbnede konflikter fremadrettet.

På den baggrund undersøger dette baggrundspapir de forskellige typer af EW-effekters folkeretlige relevans og implikationer og kaster lys over nogle af de områder, hvor der er behov for yderligere afklaring. Det gælder navnlig klarhed om, hvordan den humanitære folkerets regler skal fortolkes i henhold til specifikke EW-effekter.

---

1 Se eksempelvis Thomas Withington, *Jamming JDAM: The Threat to US Munitions from Russian Electronic Warfare*, RUSI, 6. Juni 2023, tilgængelig her: https://rusi.org/explore-our-research/publications/commentary/jamming-jdam-threat-us-munitions-russian-electronic-warfare; Kieran Devine, *Ukraine War: Mobile Networks Being Weaponized to Target Troops on Both Sides of the Conflict*, Sky News, 4. Januar 2023, tilgængelig her: https://news.sky.com/story/ukraine-war-mobile-networks-being-weaponised-to-target-troops-on-both-sides-of-conflict-12577595; David Axe, *Russia's electronic Warfare Troops Knocked out 90 percent of Ukraine's Drones*, Forbes, 24. december 2022, tilgængelig her: https://www.forbes.com/sites/davidaxe/2022/12/24/russia-electronic-warfare-troops-knocked-out-90-percent-of-ukraines-drones/?sh=563da20e575c

2 rfi021008_overview.pdf (nato.int)

3 Nøjagtig hvilke EW-kapaciteter Forsvarets værn og enheder råder over, er dog uklart, da EW som så mange andre militære højteknologiske kapaciteter er et højt klassificeret område.

Det elektromagnetiske spektrum og elektronisk krigsførelse

Det elektromagnetiske spektrum[4] (EMS) er en betegnelse for de forskellige typer af elektromagnetisk stråling, herunder radio-, radar-, mikrobølger og lys, inddelt efter bølgelængde og energi. Elektromagnetisk stråling bevæger sig i forskellige bølgelængder i det frie, fysiske rum og påvirkes derfor af bl.a. vejr, jordens krumning og fysisk modstand fra forskellige objekter. Det er netop muligheden for at påvirke elektromagnetisk stråling udefra, der gør det muligt at sætte modstanderens elektriske systemer helt eller delvist ud af spil, og det er disse forskellige påvirkningsmetoder, der samlet betegnes som elektronisk krigsførelse.

I relation til elektronisk krigsførelse på det taktiske niveau, der er genstanden for dette baggrundspapir, er det særligt radio- og radarbølger, der er relevante.

Elektronisk krigsførelse er et samlebegreb for defensive og offensive militære handlinger i det elektromagnetiske spektrum. Helt overordnet fungerer EW gennem forskellige typer af påvirkning og monitorering af signaler i EMS, det vil altså sige i rummet mellem en modtager og en afsender af elektromagnetiske bølger, så som radio- eller radarsignaler. Figur 1 nedenfor viser en lang række praktiske eksempler på afsendere og modtagere og forskellige typer EW.

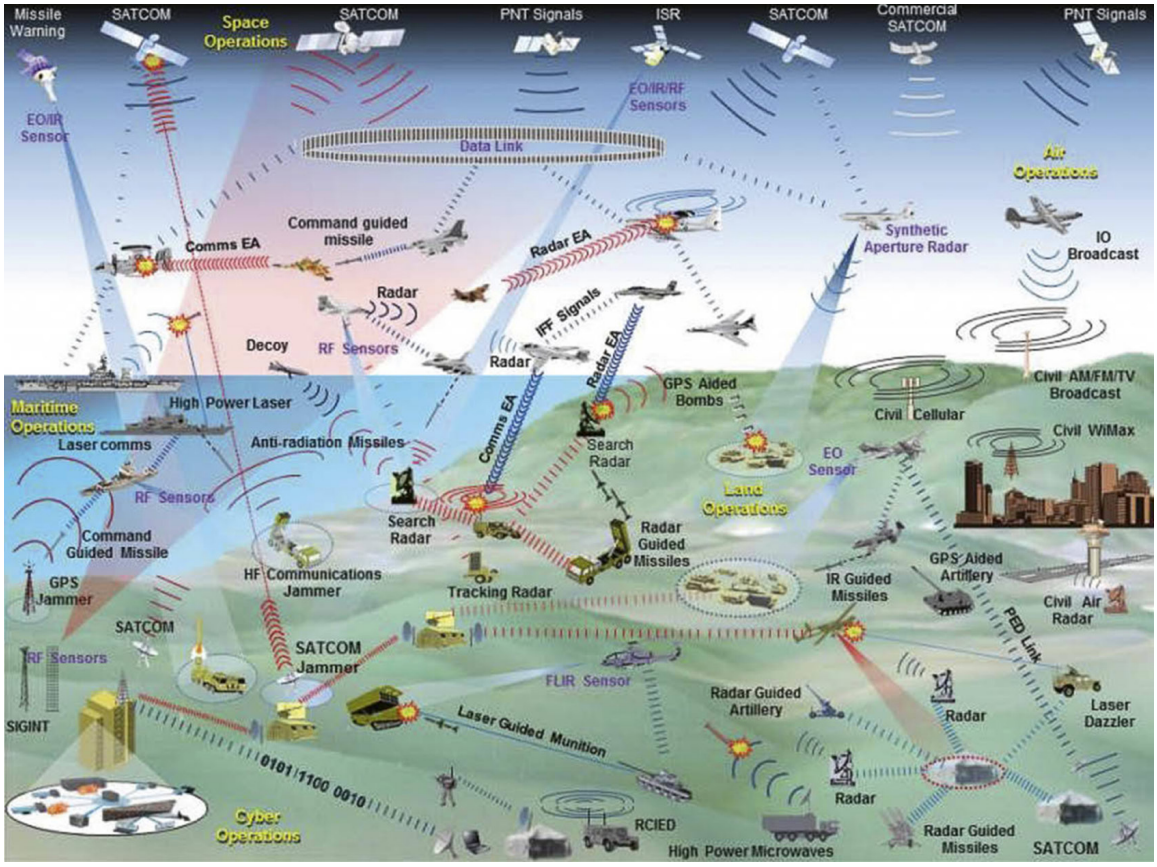


Illustration af de mange forskellige anvendelsesområder for EW

4 NATO benytter også betegnelsen the electromagnetic environment. Se https://www.nato.int/cps/en/natohq/topics_80906.htm

5 Malte von Spreckelsen, *Electronic Warfare – the Forgotten Discipline*, The Journal of the JAPPC, 27th Edition, Autumn/Winter 2018. Tilgængelig her https://www.japcc.org/journals/journal-edition-27/

EW har som militær støttefunktion til formål at skabe forudsætning for egne aktiviteter og/eller forhindre eller begrænse modstanderens mulighed for at operere et givent sted eller på en bestemt måde. De forskellige former for EW kan både anvendes til forsvar af egne systemer og styrker og angreb på modstanderens systemer. Derudover kan det elektromagnetiske spektrum også anvendes til informationsindhentning og i påvirkningsoperationer.

De centrale EW-metoder

Spoofing er en EW-teknik, der har til hensigt at bedrage modstanderen ved at skabe falske signaler, der for modstanderen fremstår ægte, hvilket gør bedraget svært at opdage.

Spoofing kan blandt andet bruges til at manipulere modstanderens systemer som f.eks. radar, kommunikation eller positionssystemer. Påvirkning af positionssystemer, såsom GPS, kan blandt andet påvirke modstanderens evne til at vide, hvor egne styrker befinder sig, mens påvirkning af offensive systemer, som eksempelvis våbensystemer og ildledningsradarer, påvirker evnen til at gennemføre præcise angreb.

Spoofing kan også bruges til produktion af såkaldte skinudsendelser, hvor der afspilles forskellige signaler for at forvirre fjendens efterretningsindhentning. En skinudsendelse kan eksempelvis foregive radarudstråling eller anden kommunikation, der får modstanderen til at tro, at et angreb foretages et andet sted, end det rent faktisk gør – eller der kan sendes vildledende signaler på modstanderens frekvenser for at foranledige dem til at tro, at der er tale om legitime ordrer eller beskeder fra egne styrker.

Endelig kan spoofing også anvendes uden for selve kamppladsen til f.eks. at forstyrre signaler til kritisk infrastruktur og derved forstyrre bl.a. offentlig transport, den finansielle sektor eller energisektoren i den ramte stat.

Jamming er kort fortalt en blokering af modstanderens signaler, der som oftest vil være tydelig for modstanderen og nem at opdage. Konkret forhindrer en jamming-operation, at en potentiel modtager af et signal rent faktisk modtager signalet, fordi det "overdøves" af et andet og stærkere signal. Jamming ændrer således ikke det oprindelige signal, og det ødelægger ikke det udstyr, som udsender dette signal, men det er ikke muligt for modtageren, der bliver jammet, at modtage signaler.

Jamming af modstanderens elektroniske systemer, som eksempelvis radar, er en integreret del af særligt luftkampagner. Der er en lang række eksempler på udbredt brug af EW til den type formål i bl.a. amerikanske luftoperationer i forbindelse med Operation Desert Storm[6] og Operation Odyssey Dawn/Operation Unified Protector.

Jamming bliver i stigende grad også anvendt til forsvar mod UAV ved at blokere signaler til disse, hvilket umuliggør fjernstyring af UAV'en. Sådan jamming vil som udgangspunkt ikke medføre forudseelige ødelæggelser, da langt de fleste UAV vil have redundans og indbyggede sikkerhedsforanstaltninger, der gør, at de ikke styrter ned, når de mister signal.

---

6 United States General Accounting Office, *Operation Desert Storm: Evaluation of the Air Campaign*, GAO/NSIAD-97-134, Appendix X:3, 1997. Tilgængelig her: https://www.gao.gov/products/nsiad-97-134; Thomas Withington, *#Desert Storm30 – Electric Avenue: Electronic Warfare and the Battle Against Iraq's Air Defence During Operation Desert Storm*, Blogpost på Balloonstodrones.com, *20. Januar 2022. Tilgængelig her: https://balloonstodrones.com/2022/01/20/desertstorm30-electric-avenue-electronic-warfare-and-the-battle-against-iraqs-air-defences-during-operation-desert-storm/*

Efterretnings- og påvirkningsoperationer i det elektromagnetiske spektrum

Det elektromagnetiske spektrum kan ikke kun anvendes til at forstyrre og blokere modstanderens systemer. Det kan som nævnt også bruges til at indsamle og sprede information.

EW-informationsindhentning omfatter både generel efterretningsindhentning om eksempelvis modstanderens placering, organisation, planer, moral m.v. og konkret indhentning med henblik på at skaffe information til brug for specifikke angreb på modstanderen. Som eksempel kan nævnes, at Rusland har EW-systemer specifikt designet til indhentning af oplysninger om mobilkommunikation. Det kan både bruges til at overvåge egentlig kommunikation og til at indhente metadata i form af telefonnumre, oplysninger om telefonernes position m.v. En række eksempler fra konflikten mellem Rusland og Ukraine tyder på, at mængden af private telefoner på kampladsen har medført, at EW kan anvendes til meget målrettede angreb på koncentrationer af personer .

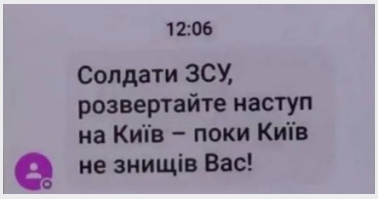
Omvendt kan man også sprede både reel information og propaganda til et bestemt område eller en bestemt befolkningsgruppe gennem det elektromagnetiske spektrum og dermed udføre **EW-påvirkningsoperationer.** Kombinationen af udviklingen i EW og det forhold, at soldater medbringer private elektroniske kommunikationsmidler på den moderne kampplads, har åbnet mulighed for meget målrettet kommunikation fra en konfliktpart til modstanderens soldater. Der er en lang række eksempler fra konflikten mellem Rusland og Ukraine på, at begge sider bruger EW til målrettede påvirkningsoperationer . EW kan også bruges til at kommunikere med civilbefolkningen i et område. Det kan eksempelvis være for at advare om angreb eller angive evakueringsruter.

Tyske flyverblade der blev kastet ud over Danmark under invasionen 9. april 1940 og SMS-advarsel sendt til omkring 5000 ukrainske soldater og politifolk i forbindelse med Ruslands invasion af Ukraine med teksten ”Soldiers of the Armed Forces of Ukraine, launch an offensive on Kyiv – before Kyiv destroys you!”


OPROP!

Til Danmarks Soldater og Danmarks Folk!

Den Tyske Kommander
Kauptsch



7 I relation til påvirknings- og efterretningsoperationer kan betegnelsen elektronisk krigsførelse virke misvisende, men det skal udelukkende forstås som en henvisning til, at der er tale om en militær aktivitet udøvet gennem det elektromagnetiske spektrum.

8 Læs mere om Leer-3-systemet og Ruslands elektroniske krigsførelse her: https://www.deagel.com/Tactical%20Vehicles/Leer-3/a003204; Samuel Cranny Evans, Fields of Silence and Broken Cycles: Russias' Electronic warfare, I Global Defence Technology Issue 133, March 2022. Tilgængelig her: https://defence.nridigital.com/global_defence_technology_mar22/russia_electronic_warfare

9 Kieran Devine, Ukraine War: Mobile Networks Being Weaponized to Target Troops on Both Sides of the Conflict, Sky News, 4. Januar 2023, tilgængelig her: https://news.sky.com/story/ukraine-war-mobile-networks-being-weaponised-to-target-troops-on-both-sides-of-conflict-12577595; Alan Yuhas, Thomas Gibbons Neff and Yousur Al Hlou, For Russian Troops, Cellphone use is a Persistent, Lethal danger, i New York Times, 4. Januar 2023, tilgængelig her: https://www.nytimes.com/2023/01/04/world/europe/ukraine-russia-cellphones.html

10 Julie Coleman, Russian Operatives Sent 5000 Text Messages in a Failed Attempt to Incite Ukrainians to Attack their Own Capitol, på Yahoo News, 1. April 2022, tilgængelig her: https://news.yahoo.com/russian-operatives-sent-5-000-203341326.html?guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAACeOe-CWThdSdlzly3wkmPq9yOGgiP9M-U7jdPbWaQLWdqhv-HWx6dgToXK9XyW3SGeOPuhasEp-dR9a7MklTsoh56utWnhKslE1FPKcRSGuppb485XR1h_Bl0Yy-29Eh4G2DXrVEQuN7m3Z7x2YJ4Cfiui4Q0L9o2LXklKqrbHo&guccounter=2 https://news.yahoo.com/russian-operatives-sent-5-000-203341326.html?guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAACeOe-CWThdSdlzly3wkmPq9yOGgiP9M-U7jdPbWaQLWdqhv-HWx6dgToXK9XyW3SGeOPuhasEp-dR9a7MklTsoh56utWnhKslE1FPKcRSGuppb485XR1h_Bl0Yy-29Eh4G2DXrVEQuN7m3Z7x2YJ4Cfiui4Q0L9o2LXklKqrbHo&guccounter=2

Den folkeretlige regulering af militære operationer

Parterne til en væbnet konflikt bestemmer i udgangspunktet selv, hvordan og med hvilke midler de vælger at bekæmpe modstanderen. Modifikationen til dette udgangspunkt er den humanitære folkerets regler om våben og angreb, der findes i Genève-konventionerne og tillægsprotokollerne til disse. Når stater anvender bestemte våben eller metoder mod modstanderen, skal det således altid ske i overensstemmelse med disse konventioners regler. Selvom ingen af reglerne retter sig specifikt mod EW, gælder det i princippet også for operationer i det elektromagnetiske spektrum, da reglerne er teknologineutrale. Det vil sige, at de gælder uanset hvilke midler og metoder, der benyttes. Det samme gælder de generelle principper om våben, der fastsætter folkeretlige begrænsninger for lovlige våben.

Det er imidlertid ikke alle militære aktiviteter og systemer, der er omfattet af den humanitære folkerets regler om militære operationer. For det første er mange af de centrale regler begrænset til operationer, der udgør angreb. Det vil her sige militære operationer, der består i voldelige handlinger rettet mod modstanderen, hvad end det er i forsvar eller angreb.[11] Med voldelige handlinger forstås handlinger, der forårsager fysisk ødelæggelse, skade eller død. Militære operationer, der ikke udgør angreb, vil, afhængig af deres art, alvor og konsekvenser, enten være underlagt væsentligt lempeligere regler eller falde helt uden for den humanitære folkerets anvendelsesområde. For det andet gælder den humanitære folkerets regler om våben kun systemer, der kan anvendes til at forårsage fysisk skade eller ødelæggelse, samt den måde disse anvendes på.[12]

Det betyder, at det kun vil være egentlige EW-våben, som vil være omfattet af de generelle våbenprincipper og ikke mindst kravet om våbenscreening.[13] De mange EW-kapaciteter, der udelukkende er designet til at forårsage forbigående effekter, der ikke udmønter sig i fysisk skade eller ødelæggelse, vil derimod ikke være våben i folkeretlig forstand og derfor ikke omfattet af disse regler.

Det er dog væsentligt at være opmærksom på, at den humanitære folkerets definitioner af angreb og våben er under pres fra stater og eksperter, der mener, at det snævre fokus på voldelige effekter i form af fysisk død og ødelæggelse er uhensigtsmæssigt i relation til cyberspaceoperationer, der ofte ikke manifesterer sig fysisk, men alligevel kan have ødelæggende effekter for den angrebne stat. Hvis udviklingen resulterer i mere rummelige angrebs- og våbenbegreber, der også omfatter midlertidige, forbigående effekter, kan det få betydning for den folkeretlige tilgang til EW, der skitseres i det følgende. Men eftersom Danmark ikke er et af de lande, der har givet udtryk for en ændret tilgang til spørgsmålene om, hvad der udgør angreb, og hvad der udgør våben i folkeretlig forstand, lægges den traditionelle, snævre tilgang afspejlet i Militærmanualen til grund i dette baggrundspapir.

---

11 Tillægsprotokol 1 af 18. juni 1977 til Genève-Konventionerne af 12. August 1949 vedrørende beskyttelse af ofre i internationale væbnede konflikter (herefter TP1), art. 49. Se Forsvarsministeriet, Militærmanual om folkeret for danske væbnede styrker i internationale militære operationer (herefter Militærmanualen), September 2016, kapitel 8, afsnit 2.1 side 280-281. Militærmanualen er tilgængelig her: https://www.forsvaret.dk/da/publikationer/militarmanual/

12 Militærmanualen definerer våben som "konventionelle våben, kemiske, biologiske, bakteriologiske våben, ammunition, våbensystemer og fremføringssystemer og instrumenter, som er designet til at kunne dræbe, ødelægge, såre eller på anden måde ukampdygtiggøre personel og materiel." Se kapitel 9 afsnit 1.4 s 324. 2

13 Våbenscreeninger har til formål at undersøge, hvorvidt et nyt våben eller våbensystems anvendelse i nogle eller alle tilfælde vil være i strid med Danmarks folkeretlige forpligtelser. Danmark er forpligtet til at foretage våbenscreeninger i forbindelse med udvikling eller anskaffelse af nye våben i medfør af Tillægsprotokol 1, art. 36. Våbenscreeningsforpligtelsen er implementeret i Dansk ret gennem CIR1H nr. 9494 af 29/05/2018.

Flyvevåbnet Fototjeneste/Forsvaret

Relevante folkeretlige regler:

Den humanitære folkerets regler om angreb, midler og metoder til krigsførelse findes først og fremmest i Tillægsprotokol 1 af 1977 til de fire Geneve-konventioner af 1949 (TP1).

Fælles regler for angreb og andre typer militære operationer, der påvirker civilbefolkningen væsentligt

- Distinktion: Art 48 fastlægger, at civilbefolkningen skal beskyttes mod de generelle farer, der udspringer af den væbnede konflikt, og bestemmer som følge deraf, at parterne i en væbnet konflikt udelukkende må rette deres militære operationer mod modstanderens militære mål, som disse er defineret i art. 52.

- Forbud mod visse specifikke kampmetoder: Art. 54 forbyder bl.a. ødelæggelse og ubrugeliggørelse af genstande, der er uundværlige for den civile befolknings overlevelse. Art. 51 (2) forbyder trusler om vold, der har til hensigt at skabe rædsel blandt civilbefolkningen.

Kun militære operationer, der udgør angreb

- Proportionalitet: Den utilsigtede ødelæggelse eller skade på civile eller civile objekter ikke må stå i åbenbart misforhold til den forventede konkrete og direkte militære fordel af angrebet (proportionalitet).

- Forsigtighedsforanstaltninger: Krav om, at der i forbindelse med "angreb" træffes forsigtighedsforanstaltninger for at verificere målet og minimere kollaterale skader.

- Særlig beskyttelse af visse objekter.

Våben

- Art. 35 forbyder anvendelsen af våben og metoder, der har til hensigt eller må forventes at forvolde udbredt, alvorlig og langvarig skade på det naturlige miljø, samt våben der forårsager overflødig skade og unødvendig lidelse. TP I Art.51 (4) (b) forbyder anvendelsen af våben, der rammer i flæng, fordi de ikke kan rettes mod et specifikt militært mål.

- TP I Art. 36 medfører et krav om, at alle nye våben på det tidligst mulige tidspunkt i anskaffelses- eller udviklingsfasen, underlægges en våbenscreening med henblik på at undersøge, om de i nogen eller alle tilfælde vil være i strid med Danmarks folkeretlige forpligtelser.

EW-aktiviteter der udgør angreb

I den humanitære folkerets forstand er det, som beskrevet ovenfor, kun voldelige offensive og defensive handlinger, der forårsager fysisk ødelæggelse, skade eller død, der betragtes som angreb.[14] Den humanitære folkerets angrebsbegreb er i den henseende effektbaseret. Det vil sige, at det er effekten af en given aktivitet, der er afgørende, ikke måden den forårsages på eller formålet med aktiviteten.

Da de fleste EW-aktiviteter "kun" sætter det angrebne system midlertidigt ud af spil eller får det til at fungere utilsigtet i en bestemt periode, vil flertallet af de aktiviteter, der finder sted i det elektromagnetiske spektrum på nuværende tidspunkt ikke anses for at udgøre angreb.

Det elektromagnetiske spektrum kan dog bruges til at gennemføre egentlige angreb i folkeretlig forstand. For det første findes der EW-våben, det vil sige EW-metoder, der specifikt er designet til at forårsage fysisk ødelæggelse gennem EMS. Det drejer sig om brugen af såkaldte directed energy weapons, eksempelvis lasere, mikrobølger eller lydbølger, der kan skabe fysisk ødelæggelse ved at rette ekstremt målrettet energi mod et objekt eller en menneskekrop[15]. På nuværende teknologiske stade er disse dog mest teoretiske og ikke til stede på kamppladsen.

For det andet kan der være situationer, hvor en EW-aktivitet som følge af den s sekundære effekt bringer den inden for definitionen af angreb. Det kan være tilfældet, hvor en EW-aktivitets effekt på det angrebne system nok er forbigående og derfor ikke umiddelbart i sig selv udgør et angreb, men hvor følgevirkningerne heraf beløber sig til fysiske ødelæggelser og dermed opfylder kriterierne for angreb.

Som eksempel kan nævnes spoofing af et skibs positioneringssystem, der får skibet til at gå på grund eller blokeringen af signalet til et ubemandet fly (UAV), der får det til at styrte ned. Som udgangspunkt vil jamming af en UAV eller spoofing af et skibs primære navigationssystem næppe i sig selv være nok til at forårsage en grundstødning eller en nedstyrtning, da de fleste fly og skibe vil have redundans til at modstå den slags aktiviteter i form af backup-systemer eller mulighed for manuel styring. Men skulle det alligevel ske, vil det i de pågældende eksempler være de respektive EW-aktiviteter, det vil sige henholdsvis spoofingen og jammingen, der er årsagen hertil. Spørgsmålet er, om sådanne fysiske følgeskader gør den pågældende EW-aktivitet til et angreb i folkeretlig forstand. Der findes ikke noget klart svar på dette i konventionerne eller den folkeretlige litteratur, men da det folkeretlige angrebsbegreb netop er effektbaseret, vil det formentlig være tilfældet, hvis den indtrufne skade er en forudsigelig effekt af den pågældende EW-aktivitet. Skaden behøver efter denne logik ikke indtræffe øjeblikkeligt eller være synlig, men den skal være en forventelig og forudsigelig følge heraf.[16]

I det omfang en EW-aktivitet som følge af dens skadevirkninger opfylder kriterierne for at udgøre et "angreb" i folkeretlig forstand, skal anvendelsen leve op til de regler, der gælder særligt for denne type militære operationer. Det gælder nærmere bestemt reglerne om distinktion, proportionalitet og forsigtighedsforanstaltninger, med henblik på at nedbringe risikoen for utilsig-

14 TP 1 art. 49. Se Militærmanualens kapitel 8, afsnit 2.1 side 280-281

15 Se https://www.nre.navy.mil/organization/departments/aviation-force-projection-and-integrated-defense/aerospace-science-research-351/directed-energy-weapons-high-power-microwaves

16 Denne tilgangsmåde til at afgøre, hvornår en handling udgør et angreb, er alment accepteret i relation til cyberspace, hvor de anvendte metoder sjældent vil forårsage fysisk ødelæggelse af de systemer, der er genstand for operationen, men hvor fysisk skade er en forudsigelig effekt heraf. Se eksempelvis Michael Schmitt (edt.)*Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge, Cambridge University Press 2013, Regel 92 om definitionen af cyberangreb.

tede skadevirkninger. I den forbindelse er det væsentligt at påpege, at EW-angreb i det omfang de retter sig mod modstanderens militære systemer i udgangspunktet vil være uproblematiske, da disse som følge af deres natur udgør lovlige militære mål.[17] Kun hvis angrebet gennemføres på en måde, der frembringer ødelæggelser på civile eller civile objekter i et omfang, der betydeligt overstiger den forventede militære fordel ved angrebet eller på anden vis tilsidesætter påkrævede forsigtighedsforanstaltninger, vil sådanne angreb være problematiske i henhold til folkeretten.

Forsvarsgalleri Søren Dreijer og Christian Thøgersen/1 Eskadre

17 TP 1, art. 52

EW-aktiviteter der ikke udgør angreb

Uanset om de doktrinært betegnes som angreb eller ej, vil langt de fleste EW-aktiviteter som nævnt ikke udgøre angreb i folkeretlig forstand, grundet deres ikke-voldelige og ofte forbigående effekt på det angrebne system. Men hvordan finder folkeretten anvendelse på denne type aktiviteter? I modsætning til det folkeretlige angrebsbegreb, der har været genstand for stor opmærksomhed og er behandlet i adskillige sammenhænge, er den folkeretlige position for aktiviteter under den humanitære folkerets tærskel for angreb mindre klar.

Krav om distinktion?

Kravet om distinktion, der af mange betragtes som den humanitære folkerets kardinalprincip, selve kernen af reguleringen af væbnede konflikter[18], spiller en afgørende rolle i bestræbelserne på at sikre civilbefolkningen mod at blive gjort til genstand for angreb. Men i modsætning til de nært beslægtede regler om proportionalitet og forsigtighedsforanstaltninger, der kun gælder angreb, fastslår den grundlæggende regel om beskyttelse af civilbefolkningen i art. 48 i ganske klart sprog, at kravet om distinktion gælder bredere end som så. Bestemmelsen anvender nemlig det generiske og væsentligt bredere begreb "militære operationer" frem for angreb og fastslår, at parterne udelukkende må rette disse mod militære mål.

I relation til EW betyder det, at mange aktiviteter vil være underlagt kravet om distinktion, selvom de ikke udgør angreb. Udforingen er imidlertid, at begrebet militære operationer ikke defineres i Tillægsprotokollen eller andre konventioner. Det rejser spørgsmålet om, hvorvidt samtlige militære aktiviteter i en væbnet konflikt er omfattet af distinktionskravet i art. 48, eller om der findes typer af operationer, der falder uden for bestemmelsens anvendelsesområde? Det er et spørgsmål, der på nuværende tidspunkt ikke er behandlet tilbundsgående i den folkeretlige litteratur, og det er derfor vanskeligt at give et entydigt svar på. Dog vil en fortolkning af bestemmelsens ordlyd og formål med stor sandsynlighed føre til en bekræftelse af eksistensen af en minimumsgrænse, der medfører, at handlinger som ikke finder sted i tilknytning til kamphandlinger, ikke vil være omfattet af distinktionskravet.[19] Den fortolkning understøttes af, at der er en række militære operationer, der direkte eller indirekte retter sig mod civilbefolkningen, og alligevel generelt synes at være accepteret af stater. Det gælder eksempelvis de fleste former for informationskampagner og efterretningsindhentning samt forskellige sikkerhedsorienterede tiltag, såsom oprettelsen af checkpoints, visitation af civile og begrænsning af civiles bevægelsesfrihed i forbindelse med militære operationer.[20] Fællesnævneren for disse ellers meget forskelligartede aktiviteter synes at være, at der til trods for deres utvivlsomt militære, operative karakter, ikke er tale om handlinger, der finder sted i snæver sammenhæng med egentlige kamphandlinger.

Spørgsmålet om, hvor snæver tilknytningen til voldsudøvelse skal være for at en handling kan anses som en militær operation omfattet af kravet om distinktion, er i høj grad relevant i forhold til EW, da det er afgørende for, i hvilket omfang EW kan rettes mod civilbefolkningen.

EW i form af jamming, spoofing og vildledelse finder ofte sted i direkte tilknytning til kamphandlinger, eksempelvis jamming af modstanderens luftforsvarssystemer forud for en luftkampagne, og er helt oplagt militære operationer omfattet af kravet om distinktion. Eftersom disse

18 Militærmanualen kapitel 4, afsnit 4 side 143.

19 Yves Sandoz et al., *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, International Committee of the Red Cross, 1986, paragraf 1875.

20 Staternes tilsyneladende accept af disse handlinger som værende lovlige, til trods for at de retter sig mod civilbefolkningen, understøttes dog ikke af klare tilkendegivelser af opinio juris på området, hvilket rejser tvivl om, hvorvidt accepten er udtryk for en sædvaneretlig regel på området.

typer EW nærmest per definition er rettet mod modstanderens militære elektriske systemer, vil distinktionskravet imidlertid næppe udgøre noget stort problem, da disse udgør lovlige militære mål som følge af deres natur eller anvendelse.[21]

Omvendt vil efterretningsindhentning og de fleste påvirkningsoperationer udført gennem EMS tilsvarende oplagt falde under tærsklen for, hvad der er omfattet af distinktionskravet, da de generelt ikke udføres i snæver tilknytning til kamphandlinger.[22] Det betyder, at de kan rettes mod såvel civile som modstanderens væbnede styrker, uden at dette strider mod den humanitære folkeret. Påvirkningsoperationer skal dog altid overholde den humanitære folkerets regler om kampmetoder, og det vil derfor eksempelvis være forbudt at bruge EW til at fremsende trusler om, at overgivelse ikke accepteres eller trusler om udslettelse. [23] [24]

Andre EW-aktiviteter er vanskeligere at bedømme. Det gælder særligt anvendelsen af EW som sikkerhedsforanstaltning i forbindelse med militære aktiviteter, der ikke er direkte knyttet til kamphandlinger. Et oplagt eksempel er midlertidig jamming af al civil kommunikation i et afgrænset område med henblik på at undgå, at civile advarer modstanderen om position og troppebevægelser i det pågældende område for at muliggøre angreb. Et andet er etableringen af såkaldte ECM-bobler, det vil sige et tredimensionelt rum omkring soldater eller militære genstande, hvori alle radiosignaler blokeres gennem jamming, med henblik på at undgå fjernudløsning af improviserede sprængladninger i forbindelse med patruljer eller troppebevægelser. Begge situationer kan finde sted i mere eller mindre snæver tilknytning til kamphandlinger, og det vil derfor være de konkrete omstændigheder, der vil være afgørende for, om de er omfattet af distinktionskravet. Det er dog værd at bemærke, at førstnævnte eksempel er umiddelbart mest problematisk, da jammingen er direkte rettet mod civilbefolkningens kommunikation, mens man oplagt kan argumentere for, at oprettelsen af ECM-boblen ikke som sådan er rettet mod civilbefolkningen, men derimod mod modstanderens fjendtlige handlinger – og dermed ikke er i strid med distinktionsprincippet.

---

21 TP I art. 52, stk. 2.

22 De almindelige regler for kommunikation til og behandling af civilbefolkningen skal overholdes ved brug af EW. Det betyder for eksempel, at man ikke må anvende EW med det primære formål at sprede rædsel blandt civilbefolkningen. TP I art. 51, stk 2, 2. pkt og GK IV art. 33. Se Militærmanualen s. 403 afsnit 2.11

23 TP I art. 40. se Militærmanualen, s. 395.

24 Mobilbesked, hvor der står "Ukrainske soldater de vil finde jeres lig når sneen smelter". Masseudsendt til ukrainske mobiltelefoner 3 km fra fronten. Er på kant med TP I, art 40. Eksemplet er taget fra Raphael Satter and Dmytro Vlasov, Ukrainian Soldiers Bombarded by 'Pinpoint Propaganda' Texts, AP, 12. Maj 2017, tilgængelig her: https://apnews.com/article/technology-europe-ukraine-only-on-ap-9a564a5f64e847d1a50938035ea64b8f

Jamming eller spoofing, der gør modstanderens våben eller angreb upræcise

Krigen i Ukraine har vist eksempler på jamming af modstanderens GPS-styrede våben, der har ført til at de bliver upræcise.[25] Det kan resultere i, at modstanderen utilsigtet benytter et vilkårligt våben, fordi jammingen af GPS-systemet gør, at det ikke kan rettes mod et specifikt militært mål.

En lignende problemstilling kan opstå, hvis modstanderens systemer spoofes på en måde, der fører til, at angrebet rammer et andet sted end angriberen har til hensigt. Det kan eksempelvis ske, hvis GPS-signal til et GPS-guidet våbensystem er blevet ændret uden angriberens viden.

I begge situationer vil den anvendte EW-metode formentlig føre til, at det påvirkede våbensystem vil være at betragte som vilkårligt, da det ikke kan styres som forudsat og dermed heller ikke kan rettes mod et specifikt militært mål, som det kræves i art. 51.[26] Spørgsmålet er, hvem der bærer ansvaret for udfaldet af anvendelsen af de påvirkede systemer? Er det den part, der gennemfører angrebet uvidende om at være udsat for spoofing eller jamming og dermed også uvidende om, at det reelt ikke kan rettes mod et specifikt militært mål? Eller er det den part, der har står bag jammingen eller spoofingen og dermed indirekte har medvirket til, at angrebet bliver vilkårligt? Dette spørgsmål er yderst komplekst, og det er ikke muligt at give et entydigt svar på i kontekst af dette baggrundspapir. Her skal det blot fremhæves, at den nævnte type EW kan skabe situationer, der resulterer i overtrædelser af den humanitære folkeret, uden at det er oplagt, hvem der bærer ansvaret herfor, hvilket ikke er hensigtsmæssigt.

På den ene side har den part, der er offer for jammingen eller spoofingen og gennemfører et angreb uden at være vidende herom, ikke umiddelbart gjort noget forkert, så længe angrebet er udført i god tro, og angriberen ikke burde have været bevidst om den provokerede fejl i systemet. På den anden side udgør modstanderens våben- og positioneringssystemer lovlige militære mål og kan derfor gøres til genstand for militære operationer, såsom jamming og spoofing. Og fordi jamming og spoofing i udgangspunktet ikke i sig selv udgør angreb i den humanitære folkerets forstand, skal den part der udfører jammingen eller spoofingen ikke tage højde for utilsigtede skadevirkninger på civile og civile objekter, lige som der heller ikke er krav om at udføre andre forsigtighedsforanstaltninger i forbindelse med operationen, da disse regler kun gælder angreb.

Med mindre spoofingen eller jammingen undtagelsesvist kan betragtes som et angreb i sig selv, fordi det rent faktisk resulterer i voldelige skadevirkninger der udgør en forventelig og forudsigelig effekt, er det vanskeligt at argumentere for, at denne form for EW-operationer er ulovlige, selvom det helt oplagt medfører risici for utilsigtede skadevirkninger for civilbefolkningen.

Det kan diskuteres om en part, der manipulerer modstanderens våbensystemer gennem jamming eller spoofing, er forpligtet til at tage højde for den risiko, det medfører for deres egen civilbefolkning efter reglerne om forsigtighedsforanstaltninger mod de skadelige virkninger af angreb i TP 1, art. 58.[27] Til trods for, at

25 Alex Marquardt, Natasha Bertrand and Zachary Cohen, *Russia's Jamming of US-provided Rocket System Complicates Ukraine's War Effort*, CNN. 6. Maj 2023, tilgængelig her: https://edition.cnn.com/2023/05/05/politics/russia-jamming-himars-rockets-ukraine/index.html

26 TP I art. 51, stk. 4 (a).

27 TPI art. 58. Militærmanualen kapitel 6, afsnit 3.4, s. 187

bestemmelsen næppe har været tiltænkt netop denne situation, tilsiger bestemmelsens ordlyd, at det beskyttelseshensyn der ligger bag forpligtelsen til at beskytte civile under egen kontrol gælder enhver form for adfærd, der medfører risici for egen befolkning. Hvis art. 58 (3) finder anvendelse i sådanne situationer, vil det dog ikke være ensbetydende med, at spoofing eller jamming af den art, der diskuteres her, altid vil være ulovlig, men det kan betyde, at parterne under visse omstændigheder vil være afskåret fra at anvende EW på sådanne særligt risikable måder. Det gælder eksempelvis jamming og spoofing rettet mod systemer, der anvendes i områder med mange civile og civile objekter, og hvor risikoen for at disse utilsigtet gøres til genstand for angreb som følge heraf er særlig stor.

GRAB optaget af Tue Skals/Forsvaret

Forbud mod vildledelse?

Folkeretten giver plads til, at parterne i en væbnet konflikt kan snyde og udmanøvrere hinanden ved hjælp af vildledelse, også kaldet krigslist, så længe det ikke indebærer misbrug af visse beskyttede emblemer eller beskyttet status. Skinudsendelse af falske signaler med henblik på at forvirre fjendens indhentning af information kan anses for krigslist og vil derfor i udgangspunktet være i overensstemmelse med folkeretten.[28]

Hvis spoofing bruges til at efterligne modstanderens eller andre enheder med beskyttet status' signaler, således at man fremstår som en af modstanderens enheder eller en enhed under særlig beskyttelse, skal reglerne om perfidi og nationale emblemer overholdes. Det vil sige, at det er forbudt at dræbe, såre eller tage en modstander til fange ved hjælp af en sådan effekt.[29] Et eksempel kunne være kampfly, der efterligner modstanderens egne fly og derfor ikke engageres af antiluftskyts og bruger muligheden for at gennemføre angreb.

For maritim krigsførelse har spillerummet for krigslist traditionelt set været udvidet. Der er derfor en diskussion om retten til f.eks. at sejle under falsk flag kan fortolkes til også at gælde udsendelse af falske radar- og akustiske signaler.[30] En nærmere fortolkning af reglerne for maritim krigsførelse ligger imidlertid uden for rammen af dette papir.

Lars, Flyvevåbnets Fototjeneste

28 TP I art. 37(2)

29 TP I art. 37, stk. 1. Se Militærmanualen s. 383 afsnit 2.1 og TP I art. 39, stk. 2.

30 MM kapitel 14 afsnit 4.6.9 side 580-581

Konklusioner

Såvel nye militære teknologier som nye måder at anvende ældre teknologi på i militære operationer giver anledning til at anskue den folkeretlige regulering i et nyt perspektiv. Selvom levering af effekter gennem det elektromagnetiske spektrum længe har spillet en vigtig rolle i militære operationer, og der fortsat udvikles nye EW-metoder, har elektronisk krigsførelse endnu ikke for alvor været genstand for sådanne overvejelser. Dette baggrundspapir peger på, at der er aspekter af elektronisk krigsførelse, der giver anledning til interessante folkeretlige spørgsmål.

Baggrundspapiret identificerer særligt tre spørgsmål, der kræver yderligere belysning, hvis den folkeretlige ramme for EW skal afklares. For det første er der generelt behov for at udbygge forståelsen for reguleringen af militære operationer, der ikke udgør angreb i den humanitære folkerets forstand. Dette er særdeles væsentligt i forhold til EW, da det vurderes at størstedelen af de EW-effekter, der ses anvendt i dag, formentlig vil falde i denne kategori, da de ikke forårsager den fysiske skade, der kræves for at bringe dem inden for anvendelsesområdet for de detaljerede regler om angreb i Tillægsprotokol 1. For det andet er der behov for yderligere afdækning af angrebsbegrebet i den humanitære folkeret, da flere EW-metoder kan have utilsigtede om end forudsigelige effekter, der rejser tvivl om, hvordan de skal kategoriseres folkeretligt og dermed også, hvilke regler der gælder for den slags aktiviteter. For det tredje giver EW-effekter rettet mod systemer, der er vitale for modstanderens evne til at udføre angreb som planlagt, herunder våben- og positioneringssystemer, anledning til vanskelige spørgsmål om ansvar for konsekvenserne heraf, nå disse beløber sig til overtrædelser af den humanitære folkeret.

Til trods for at EW ikke på nuværende tidspunkt kan siges at udgøre et stort folkeretligt problem i væbnede konflikter i praksis, viser dette baggrundspapir således, at der er områder af den humanitære folkeret, hvor der er behov for yderligere afklaring, før det er muligt at vurdere lovligheden af konkrete EW-aktiviteter med tilstrækkelig sikkerhed.

I takt med at omfanget af EW -aktiviteter i militære operationer stiger og teknologien udvikler sig, vil behovet for folkeretlig afklaring formentlig kun vokse tilsvarende. Det gælder i høj grad også for anvendelse af EW, der falder uden for dette baggrundspapirs rækkevidde, det vil sige uden for væbnet konflikt og i nationale militære operationer, hvor den retlige ramme primært udgøres af menneskeretlige regler og national lovgivning, der giver anledning til helt andre men ikke mindre interessante retlige udfordringer.

Eftersom tvivl omkring lovligheden af en given praksis eller et bestemt våben i mange situationer resulterer i afholdenhed fra at anvende det, er det også i Forsvarets interesse, at EW gøres til genstand for grundige retlige analyser. På den måde kan det sikres, at manglende forståelse for den juridiske ramme ikke står i vejen for anvendelse af de EW-kapaciteter, vi råder over.

Billede: Forsvarsgalleri, Brian Djurslev

FORSVARSAKADEMIET

Svanemøllens Kaserne
Postboks 2521

Ryvangs Allé 1
2100 København Ø
Denmark