

Den analoge folkeret udfordres af digital cyberkrig

Af **Marc Schack** og **Iben Yde**

Den folkeretlige regulering af magt-anvendelse og krigsførelse er udviklet i og til en analog tidsalder. Men hvordan er reglerne i cyberspace og når det gælder digital krigsførelse med kunstig intelligens?

Moderne krige udkæmpes med moderne teknologier. Sådan har det altid været – og sådan bliver det formentlig ved med at være. Men hver gang en ny teknologi introduceres på slagmarken, skaber det både juridiske og etiske spørgsmål om, hvordan den skal håndteres. Er den lovlig under eksisterende lovgivning? Skal den underlægges særlig regulering? Eller skal den helt forbydes? Igennem tiden har så forskellige teknologier som armbrystet, krudt, flyvemaskiner, ubåde, kemiske/biologiske våben og atomvå-

ben været genstand for sådanne debatter. Hvor nogle af disse teknologier i dag er fuldt accepterede dele af moderne krigsførelse, er andre underlagt specifik regulering eller forbud.

I dag domineres den folkeretlige debat om nye militære teknologier af særligt tre emner: Droner, cybervåben samt autonome våbensystemer og kunstig intelligens (AI). Det kan dog til tider være svært at få klarhed over, hvad der gør disse teknologier folkeretligt problematiske, og hvor frontlinjerne går i den juridiske debat. Det forsøger vi her at skabe klarhed over.

Dronerne spøger igen

Bevæbnede droner er ikke længere et nyt fænomen. De er det ikoniske våben, der i snart to årtier har defineret den amerikanske 'krig mod terror', og

Marc Schack er adjunkt i folkeret ved Institut for Militære Operationer, Forsvarsakademiet. Han er kandidat og ph.d. i jura fra Københavns Universitet og forsker i folkeret (særligt regler for krigsførelse og brug af væbnet magt), international strafferet, humanitær intervention og afskrækkelsesteori.

som nu er blevet så demokratiseret, at snart sagt enhver aktør med et militært budget har adgang til teknologien.

Den juridiske debat om dronerne har kørt på fulde blus lige siden de første amerikanske Predator-droner bevæbnet med Hellfire-missiler tog del i kamphandlingerne i Afghanistan i 2001, og efterfølgende også blev anvendt uden for egentlige krigszoner i lande som Pakistan, Yemen og Somalia. Mange har i den proces sat spørgsmålstegn ved, om dronekrig overhovedet er lovligt, og om bevæbnede droner helt bør forbydes.

Dér er vi ikke i dag. Dronerne er kommet for at blive, og det afspejles i debatten. Der er således nu bred enighed om, at droner blot er et våbensystem, der som alle andre våbensystemer skal håndteres efter folkerettens regler for magtanvendelse og krigsførelse, omend der fortsat er uenighed om, hvad det præcist indebærer.

Den juridiske debat er dermed modnet så meget, at den nærmest er normaliseret. Det har ført til, at oprindelige stridspunkter om blandt andet de såkaldte *'targeted killings'* (målrettede drab udenfor slagmarken eller i retssystem, red.) og *'signature strikes'* (målrettede drab udenfor slagmarken eller i retssystem, red.), og problemerne omkring civile tab ved droneangreb, nu

diskuteres på et niveau, der har givet plads til at tage nye, uopdyrkede problemstillinger op. For eksempel giver det anledning til overvejelser om, hvilke specifikke retlige forpligtelser et land som Danmark skal leve op til, hvis vi anskaffer droner, som giver helt nye muligheder på slagmarken. Når krigsretten eksempelvis kræver verifikation af mål og udvælgelse af kampmidler, der i videst muligt omfang skåner civile på jorden, skal det afklares, hvordan sådanne krav implementeres i praksis af en mindre nation med begrænsede ressourcer, men som i princippet kan gennemføre sofistikerede og længerevarende rekognosceringsmissioner understøttet af moderne droneteknologi.

Herudover giver udbredelsen af droneteknologi udfordringer. Hvis en strategisk modstander for eksempel flyver droner ind i dansk luftrum, er det i dag uklart, hvordan Danmark retligt kan reagere. Hvor vi er vant til at arbejde med afvisningsberedskab over for almindelige fly, er det straks sværere at forholde sig til droner, som flyver ind i dansk luftrum. For hvor stor skal en krænkelse være, før vi reagerer på en drone sammenlignet med et bemannet fly? Hvornår kan en drone nedskydes? Og hvor meget skal vi gøre for at varsle, inden vi eventuelt skyder? Det giver folkeretten ikke klare svar

Iben Yde (f. 1981) er adjunkt ved Forsvarsakademiet og tidligere militær juridisk rådgiver ved Forsvarskommandoen. Hun er uddannet jurist med en ph.d. i folkeret ved Aarhus Universitet. I sit arbejde forsker og underviser Iben Yde i folkeretlige aspekter af militær teknologi og militære operationer, herunder med særligt fokus på angrebsfunktioner, targeting law og maritime operationer.

på i dag, og det er et emne som blandt andet kom i søgelyset da Iran 20. juni 2019 nedskød en amerikansk overvågningsdrone til en værdi af 180 millioner dollars.

En digital Genève-konvention

Den folkeretlige regulering af magt-anvendelse og krigsførelse er skrevet i og til en analog tidsalder. Derfor tager reglerne stilling til krudt og kugler, men ikke software og digitale netværk. Det har aktualiseret en række væsentlige spørgsmål om, hvordan så-

Hvis en strategisk modstander for eksempel flyver droner ind i dansk luftrum, er det i dag uklart, hvordan Danmark retligt kan reagere af USA.

danne analoge regler skal forstås i en digital tidsalder. Når krigsretten for eksempel taler om, at civile objekter skal beskyttes under krig, gælder det så udelukkende fysiske objekter, som bygninger og køretøjer? Eller omfatter reglerne også digitale 'objekter', som filerne på en personlig harddisk, banksektorens digitalt lagrede oplysninger eller hospitalers digitale journaler? Kan man med andre ord forårsage en 'skade' i krigsretlig forstand, som kun har en direkte effekt i den digitale verden? Eller skal skaden materialisere sig i den fysiske verden, før krigsretten brydes? Det er blandt de centrale spørgsmål, som folkeretsjurister diskuterer i disse år.

Selvom der er store uenigheder på området, er der også flere forhold, det er lykkedes at skabe en vis enig-

hed om. Vigtigst af alt: Cyberspace udgør ikke et lovløst område. Folkeretten finder utvivlsomt anvendelse i cyberspace. Herudover er der enighed om, at jurister er nødt til at analysere cyberoperationer i forhold til deres effekter, før vi kan vurdere de retlige forhold. Afgørende er således, om en cyberoperation skaber effekter, der er sammenlignelige med klassiske militære operationer. Gør de det, reguleres de på nogenlunde samme måde. Den praktiske udførelse af denne analyse kan dog give problemer, hvil-

ket den nævnte debat om definitionen af 'objekter' og 'skader' afspejler. Det er også derfor, at vi fortsat oplever stor uenighed om grundlæggende spørgsmål, som hvorvidt en stat kan bryde

FN-pagtens magtanvendelsesforbud, hvis staten anvender et cybervåben til at stække en anden stats militære kapabiliteter, uden at det sker gennem fysisk ødelæggelse. Vi er således fortsat langt fra at etablere generelt accepterede præmisser for den juridiske fortolkning.

Det er blandt andet på den baggrund, at mange har forhåbninger om, at uklarhederne kan løses gennem forhandling og vedtagelse af nye regler. Det omfatter blandt andet Microsofts forslag om en 'Digital Genève-konvention'. Sådanne regler får vi dog næppe vedtaget foreløbigt. Det politiske klima er simpelthen ikke til det. At den FN-forankrede proces for cyberdebatten har været så uforsonlig, at den i 2018 blev splittet i to, hvor den ene del støttes af amerikanerne, mens den anden del støttes af russerne, er et ty-

deligt symptom herpå og splittelsen tegner ikke godt for ønsket om at opnå enighed på cyberområdet.

Kunstig intelligens og menneskelig kontrol

De droner, som anvendes i dag, er kendetegnet ved at være fjernstyrede og derved underlagt direkte menneskelig kontrol, mens autonome våbensystemer – baseret på maskinlæring og andre former for AI – er i stand til at udvælge og angribe mål uden menneskelig involvering. Udviklingen af sådan teknologi, og udsigten til, at vi kan opleve fremtidige kamppladser, hvor eksempelvis ubemandede fly eller kampvogne selv søger, udvælger og angriber mål ved hjælp af sofistikerede sensorer og avancerede algoritmer, har givet anledning til stor bekymring og skarp debat. Det store spørgsmål er, hvordan krigsretten håndterer sådanne autonome våbensystemer, og den centrale udfordring baserer sig på det forhold, at reglerne oprindeligt er udarbejdet ud fra en formodning om, at ethvert våbensystem er styret af et menneske. Netop det forhold har fået mange kritikere til argumentere for, at autonome våbensystemer simpelthen er uforenelige med krigsrettens grundlæggende principper, blandt andet fordi disse våbensystemer menes per definition at udelukke menneskelige vurderinger, og fordi de vanskeliggør placeringen af ansvar, hvis der sker fejl.

Selvom der således ikke er enighed om de autonome våbensystemers folkeretlige stilling, synes der at være generel enighed om én ting: at enhver

brug af autonome våbensystemer skal tilrettelægges på en måde, der sikrer den nødvendige grad af 'menneskelig kontrol' med systemet. Den erkendelse har i en vis grad flyttet debattens tyngdepunkt væk fra de mere frugtløse binære diskussioner om, hvorvidt våbensystemerne er lovlige eller ulovlige, og hen imod en mere konstruktiv debat om, hvad der udgør 'effektiv' og 'meningsfuld' menneskelig kontrol.

Cyberspace udgør ikke et lovløst område. Folkeretten finder utvivlsomt anvendelse i cyberspace.

Men der er ingen enighed og ingen nemme løsninger. Teknologiens stigende kompleksitet og den generelle manglende forståelse for den operative kontekst, som våbensystemerne anvendes i, er fortsat en stor udfordring. Det er den nok primære årsag til, at der endnu ikke er enighed om hverken en egentlig definition af 'autonome våbensystemer' eller det nærmere indhold af begrebet 'meningsfuld menneskelig kontrol'.

Desværre bliver disse problemer ikke umiddelbart mindre med tiden. I modsætning til de mere automatiserede våbensystemer, som anvendes i dag, og som er nogenlunde forudsigelige i deres programmering og handlemønstre, er den næste generation af autonome våbensystemer langt mere komplicerede. Det vil i realiteten gøre det nærmest umuligt at få indblik i, hvordan systemerne rent faktisk fungerer, og hvordan de når frem til konkrete løsninger. I sidste ende kan det hand-

le om spørgsmål som hvorvidt en person på slagmarken vurderes at være en kombattant, som kan beskydes, el-

] Teknologiens stigende kompleksitet og den generelle manglende forståelse for den operative kon-tekst, som våbensystemerne anvendes i, er fortsat en stor udfordring.

ler en civil, som skal beskyttes. Denne manglende gennemsigtighed og forudsigelighed gør det desuden utrolig vanskeligt for en menneskelige operatør at overvåge sådanne systemer – og eventuelt gribe ind, hvis der opstår risiko for fejl.

En krævende opgave

Tiden vil vise, om de eksisterende folkeretlige regler vil være tilstrækkelige til at værne om krigsramte civilbefolkninger i disse sammenhænge, eller der opstår behov for og enighed om

yderligere regulering. Men ligesom for de øvrige teknologier er en sådan regulering ikke lige om hjørnet.

Som denne korte gennemgang af den folkeretlige debat om nye militære teknologier viser, kan det tage mange år at opnå blot nogenlunde enighed om helt basale præmisser for debatterne. Det synes desuden klart, at der er en begrænset villighed blandt stater til at indgå kompromisser og gøre alvorlige forsøg på at regulere de nye teknologier. Det betyder, at jurister også de kommende år må indstille sig på at skulle gøre et stort stykke arbejde for at opnå den nødvendige tekniske forståelse for nye militære teknologier og få analog jura af ældre dato til at passe til en moderne, digital virkelighed.

○ ○ ○