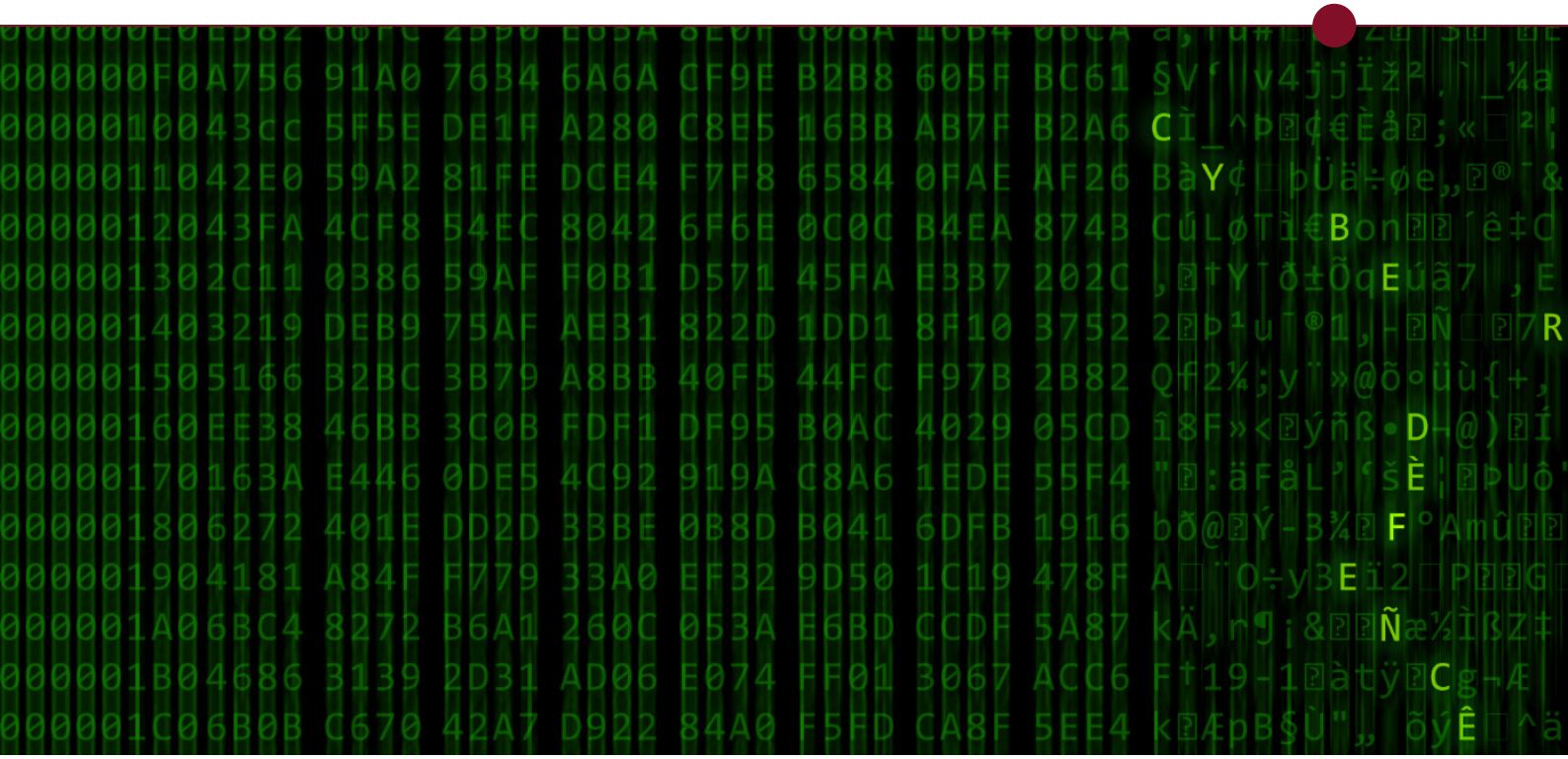
KØBENHAVNS UNIVERSITET
CENTER FOR MILITÆRE STUDIER



Lavintensive cyberoperationer og statssuveræ nitet i cyberspace

I marts 2021 blev en FN-rapport, som bekræfter, at folkeretten gælder i cyberspace, vedtaget i FN's arbejdsgruppe om sikkerhed i og ved brugen af informations- og kommunikationsteknologier (OEWG). På trods af FN-rapportens vedtagelse er der fortsat betydelig uenighed om, *hvordan* folkeretten finder anvendelse i cyberspace, eftersom staterne ikke har været i stand til at blive enige om, hvilke typer af cyberoperationer folkeretten forbyder. Hvis en cyberoperation er forbudt ifølge folkeretten, betyder det, at staterne ikke har lov til at udføre den. Gør de det alligevel, kan de holdes ansvarlige, og den forurettede stat kan lovligt iværksætte modforanstaltninger.

Staterne er især splittede i spørgsmålet om, hvorvidt cyberoperationer, som trænger ind i computersystemer lokaliseret på en anden stats territorium, men som ikke kvalificerer som magtanvendelse eller ulovlig intervention i juridisk forstand – såkaldte lavintensive cyberoperationer – er i uoverensstemmelse med folkeretten. Lavintensive cyberoperationer, som inkluderer de fleste handlinger, stater foretager i forbindelse med retshåndhævelse uden for eget territorium (herunder terrorbekæmpelse)

CMS Memo
September 2022 · Kevin Jon Heller

Centrale pointer

- Der er uenighed blandt stater om, hvorvidt lavintensive cyberoperationer, der er rettet mod computersystemer på en anden stats territorium, er ulovlige ifølge folkeretten.
- Staterne fordeler sig mellem tre positioner i forhold til spørgsmålet, hhv. 1) suverænitet som princip, 2) ren suverænitet og 3) relativ suverænitet. Mange stater, heriblandt Danmark, har ikke taget eksplicit stilling.
- En småstat som Danmark, som må forventes at være mere optaget af at forsvare sig mod cyberangreb end at anvende cybermidler offensivt, bør tilslutte sig en position, der retligt regulerer staternes brug af lavintensive cyberoperationer.

og spionage, er den mest almindelige type cyberoperation, og de vil formentlig blive endnu mere udbredte med tiden pga. deres relativt lave omkostninger og høje nytteværdi for staterne.

CMS-rapporten *Low-Intensity Cyber Operations and State Sovereignty in Cyberspace* sammenligner og vurderer tre forskellige positioner med hensyn til, hvorvidt lavintensive cyberoperationer overtræder territorialstatens suverænitet og dermed er ulovlige ifølge folkeretten.

Den første position, som indtages af Storbritannien og indtil for nylig af USA, er, at lavintensive cyberoperationer aldrig er uretmæssige, eftersom suverænitetsbegrebet blot er et princip i folkeretten og ikke en primær regel, der selvstændigt kan blive overtrådt. Denne position kaldes "suverænitet som princip"-tilgangen.

Den anden position, som især Frankrig er fortaler for, er, at lavintensive cyberoperationer altid er uretmæssige, fordi suverænitetsprincippet udgør en bindende folkeretlig regel, som overtrædes ved enhver indtrængen uden samtykke i et computersystem lokaliseret på en anden stats territorium. Denne position kaldes den *rene* suverænitetstilgang.

Den tredje position, som indtages af bl.a. USA og Norge, er, at selvom suverænitetsprincippet er en bindende folkeretlig regel, er det kun den delmængde af lavintensive cyberoperationer, som forårsager en form for fysisk skade på territorialstaten eller efterlader dens cyberinfrastruktur ude af funktion, der er uretmæssige. Denne position kaldes den *relative* suverænitetstilgang.

Staterne indtager dermed tre forskellige positioner med hensyn til, hvordan suverænitetsprincippet – og dermed folkeretten – finder anvendelse i cyberspace, når det gælder lavintensive cyberoperationer, hhv. 1) suverænitet som princip, 2) ren suverænitet og 3) relativ suverænitet. Dertil kommer en lang række stater, heriblandt Danmark, som ikke har taget eksplicit stilling til spørgsmålet.

Den manglende konsensus afspejler dels reelle uenigheder mellem staterne om folkerettens indhold og dels politiske forskelle med hensyn til staternes ønske om at kunne bruge lavintensive cyberoperationer til offensive formål, fx i forbindelse med terrorbekæmpelse, bekæmpelse af transnational kriminalitet og spionage. "Suverænitet som princip"-tilgangen, der efterlader lavintensive cyberoperationer uregulerede, er således primært en fordel for stater, som ønsker at udføre offensive lavintensive cyberoperationer, og som har den teknologiske kapacitet til at forsvare sig mod lignende operationer.

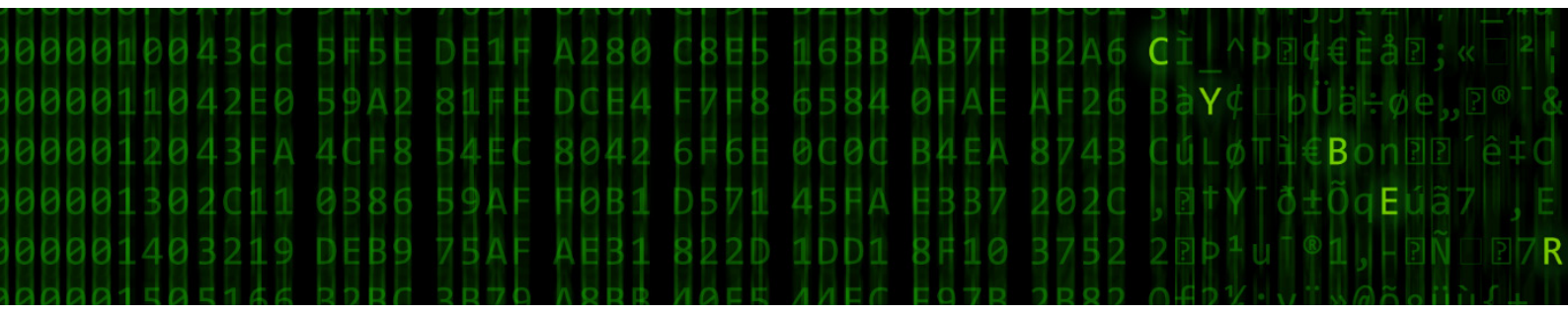
En konsekvens af den manglende konsensus er, at den bidrager til at underminere stater som Danmarks evne til at udvikle og eksekvere deres cyberstrategier. Når der er forskellige opfattelser af, om lavintensive cyberoperationer er i uoverensstemmelse med folkeretten, og dermed også om modforanstaltninger er tilladt, øger det sandsynligheden for, at en given operation vil skabe juridisk og politisk konflikt mellem stater. Staternes manglende stillingtagen til spørgsmålet reducerer desuden evnen til at afskrække lavintensive cyberoperationer.

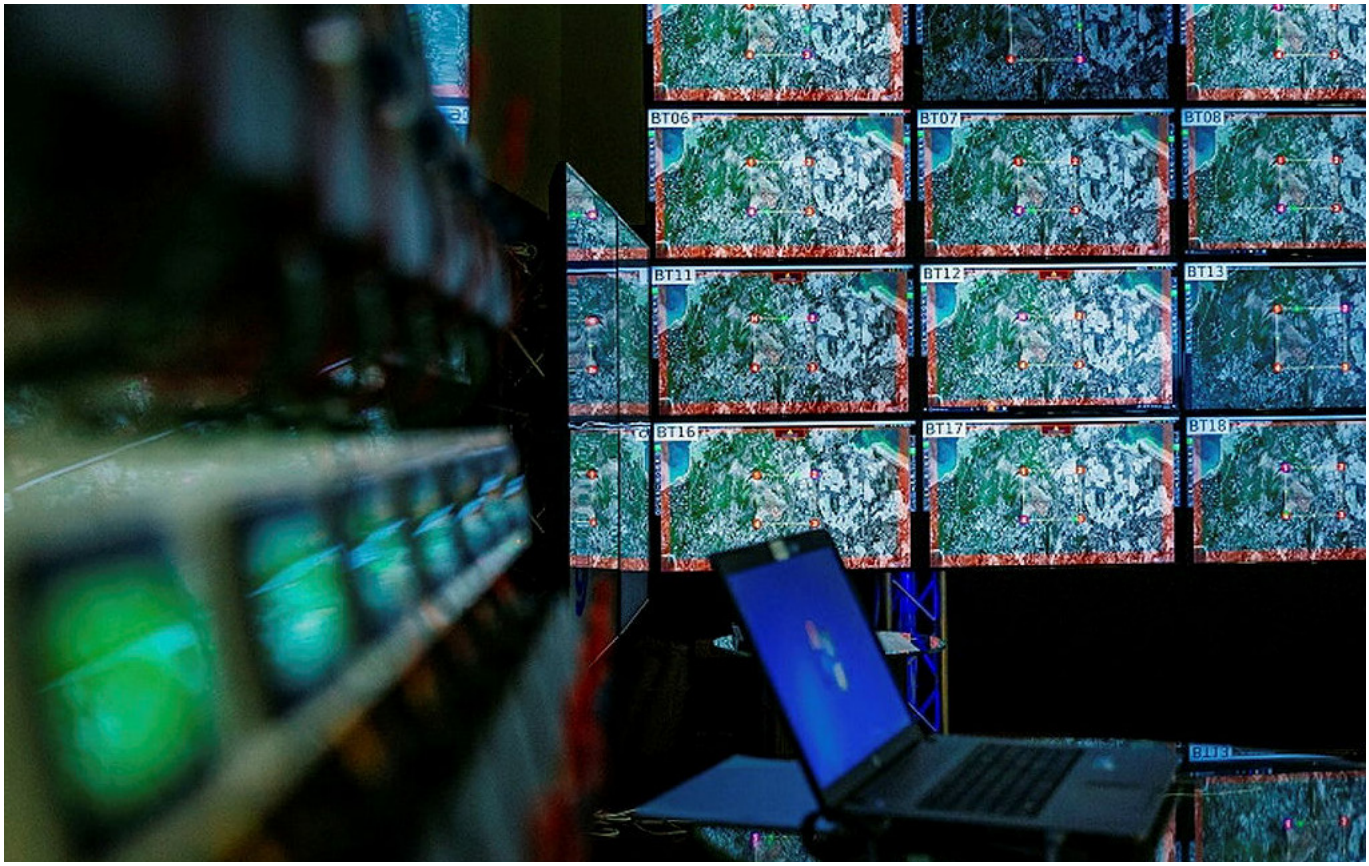
En småstat som Danmark, der må forventes at være mere optaget af at forsvare sig mod cyberangreb end at anvende cybermidler til offensive formål, har en interesse i at fremme positioner, der regulerer staternes brug af lavintensive cyberoperationer. Rapporten konkluderer derfor, at Danmark bør tilslutte sig enten den rene eller den relative suverænitetstilgang.

Hvilken position der er mest attraktiv, vil afhænge af en afvejning af retlige og politiske hensyn. På den ene side er den rene suverænitetstilgang mest i overensstemmelse med den traditionelle forståelse af, hvordan suverænitet fungerer i den fysiske verden og vil bedre kunne beskytte en stat mod ødelæggende cyberspionage end den relative tilgang.

På den anden side giver den relative suverænitetstilgang staterne mulighed for at udføre cyberspionage, som ikke resulterer i fysisk skade, hvilket især er attraktivt for teknologisk sofistikerede stater, der besidder kapaciteten til at udføre avanceret cyberspionage, såsom NSA-overvågningen afsløret af WikiLeaks: monitorering af kommunikation, eksfiltrering af information, sletning eller ændring af data. Ifølge den relative tilgang kan staterne dermed heller ikke påberåbe sig retten til at iværksætte modforanstaltninger mod en sådan ikke-skadelig cyberspionage, og eftersom selv denne form for spionage kan være en væsentlig trussel mod teknologisk avancerede stater, kan dette være et argument for at foretrække den rene suverænitetstilgang.

Andre såvel retlige som politiske hensyn – herunder hensynet til allieredes valg – kan være relevante i fastlæggelsen af Danmarks position på området.





Anbefalinger

Danmark er én blandt mange stater, som ikke har taget eksplicit stilling til, om lavintensive cyberoperationer overtræder territorialstatens suverænitet. Af rapporten *Low-Intensity Cyber Operations and State Sovereignty in Cyberspace* kan der uddrages følgende opmærksomheds- og handlingspunkter:

- Danmark bør fremme den folkeretlige regulering af lavintensive cyberoperationer og bør derfor tilslutte sig enten den rene eller den relative tilgang til suverænitet. Såvel retlige som politiske overvejelser bør indgå i beslutningen om, hvilken position Danmark skal vælge.

- Den rene suverænitetstilgang forbyder alle former for lavintensive cyberoperationer, herunder cyberspionage, og er mest i overensstemmelse med den traditionelle forståelse af, hvordan suverænitet fungerer i den fysiske verden. Tilgangen tillader en stat, der bliver udsat for en lavintensiv cyberoperation, at iværksætte modforanstaltninger.

- Den relative suverænitetstilgang tillader lavintensive cyberoperationer, som ikke forårsager umiddelbar fysisk skade, fx cyberspionage. Tilgangen giver ikke mulighed for, at en stat, der bliver udsat for cyberspionage, kan påberåbe sig retten til at iværksætte modforanstaltninger.

- Danmarks valg af suverænitetstilgang vil kunne bidrage til at afskrække lavintensive cyberoperationer, eftersom andre stater vil vide, at Danmark påberåber sig retten til at iværksætte modforanstaltninger i tilfælde af et angreb. Den relative suverænitetstilgang vil ikke kunne bidrage til at afskrække cyberspionage.

- Danmarks vigtigste allierede, herunder USA og Norge, har tilsluttet sig den relative tilgang, hvilket kan gøre denne position attraktiv ud fra et diplomatisk perspektiv.

- Uanset hvilken position der vælges, bør Danmark udsende en offentlig erklæring, der annoncerer landets position og forståelse af, hvordan folkeretten finder anvendelse i cyberspace. Vælges den rene tilgang, vil det være tilstrækkeligt blot at erklære det offentligt. Vælges den relative tilgang, kan Danmark yde et væsentligt bidrag til udviklingen af denne position i international henseende ved at specificere, præcis hvilke former for lavintensive cyberoperationer Danmark mener, er suverænitetskrænkende.

- Uanset hvilken suverænitetstilgang der vælges, vil Danmark med en offentlig erklæring lægge afstand til stater med en anden position.

- En offentliggørelse af Danmarks position vil kunne bidrage til at afskrække andre stater fra at iværksætte lavintensive cyberoperationer mod Danmark, eftersom de vil vide, at Danmark vil påberåbe sig retten til reagere med modforanstaltninger.

- En offentliggørelse af Danmarks position vil kunne bidrage til dannelsen af international sædvaneret om lovligheden af lavintensive cyberoperationer.

- Danmark bør deltage aktivt i den nyetablerede FN-arbejdsgruppe (OEWG), som afrapporterer sine konklusioner til FN's Generalforsamling i 2025. Det vil sikre, at Danmarks interesser for så vidt angår suverænitet bliver tilstrækkeligt repræsenteret, mens folkerettens anvendelse i cyberspace fortsætter sin udvikling.

Lavintensive cyberoperationer

- Lavintensive cyberoperationer refererer til indtrængning i computersystemer lokaliseret på en anden stats territorium, men som ikke kvalificerer som magtanvendelse eller ulovlig intervention i juridisk forstand.

- Lavintensive cyberoperationer optræder ofte ifm. cyberspionage og terrorbekæmpelse, hvor hensigten er at overvåge eller eksfiltrere elektronisk kommunikation, data eller anden information samt at udtrække digitale beviser eller fjerne information (fx terrorpropagandavideoer).

- Lavintensive cyberoperationer er den mest anvendte form for cyberoperation, pga. dens relativt lave omkostninger og store nytteværdi for stater.

- Ifølge Council on Foreign Relations (CFR) har 34 stater engageret sig i lavintensive cyberoperationer siden 2005, og frekvensen af sådanne cyberoperationer er steget over tid.

Lavintensive cyberoperationer og statssuverænitet i cyberspace

Dette CMS Memo bygger på CMS-rapporten *Low-Intensity Cyber Operations and State Sovereignty in Cyberspace*, udgivet af Center for Militære Studier ved Københavns Universitet i samarbejde med Djøf Forlag. Rapporten findes i sin fulde længde under 'Publikationer' på Center for Militære Studiers hjemmeside.

Hvis du vil vide mere om den folkeretlige regulering af cyberspace, kan du også læse følgende rapporter udgivet af vores samarbejdspartnere Det Juridiske Fakultet på Københavns Universitet og Forsvarsakademiet i forbindelse med forskningsprojektet "International Law & Military Operations (InterMil)" på https://jura.ku.dk/icourts/research/intermil/

- *Staters folkeretlige forpligtelse til at udvise "due diligence" i cyberspace (2022)*
- *Modforanstaltninger i cyberdomænet - Den folkeretlige ramme (2020)*

Om Center for Militære Studier

Center for Militære Studier er et forskningscenter på Institut for Statskundskab, Københavns Universitet. På centret forskes i sikkerheds- og forsvarspolitik samt militær strategi. Forskningen danner grundlag for forskningsbaseret myndighedsbetjening af Forsvarsministeriet og de politiske partier bag forsvarsforliget.

Kontakt os
E-mail: cms@ifs.ku.dk
Telefon: +45 35 32 40 88
Besøg vores hjemmeside: cms.polsci.ku.dk

Følg os
Facebook: facebook.com/centerformilitaerestudier
Twitter: @MilstudiesCPH
LinkedIn: linkedin.com/company/centre-for-military-studies

Kolofon · Forsidefoto: DOD networks are highly susceptible to attack. Military cyber professionals are trained to defend the network. (fotograf: C. Todd Lopez) Copyright: U.S. Department of Defense · Foto side 3: International Live-Fire Cyber Defence Exercise Kicked Off This Week (fotograf: Amo Mikkor) Copyright: UK Ministry of Defence · **ISBN**: 978-87-7393-956-0