KØBENHAVNS UNIVERSITET
CENTER FOR MILITÆRE STUDIER

Dansk offensiv cybermagt mellem angreb, spionage og forsvar

En komparativ analyse på tværs af Europa

Danmarks økonomi og konkurrencedygtighed bliver dagligt undermineret af cyberspionage, og den offentlige debat og demokratiet bliver destabiliseret af misinformationskampagner. I 2017 oplevede Danmark, hvordan Mærsk blev alvorligt ramt som følgevirkning af et cyberangreb mod mål uden for Danmark. Det samme kan ske for danske myndigheder og den samfundsvigtige infrastruktur, der er et yndede mål for cyberangreb.

Fælles for disser cyberangreb er, at de enkeltstående angreb ikke lever op til de gængse definitioner af krig og væbnet konflikt. De udgør snarer et konfliktrum i fredstid. Danmark og dets allierede befinder sig dermed i en langstrakt digital ufredstid, hvor Kina og Rusland angiveligt fører en subtil form for magt- og geopolitik ved konstant at udfordre og overskride eksisterende normer og regler på en tvetydig og forbeholden facon.

Danmark og dets allierede er vant til at analysere verden ud fra et skarpt skel mellem krig og fred, hvorfor det er en udfordring

CMS Memo

Maj 2020. Tobias Liebetrau

Centrale pointer

1. Danmark er i stigende grad udsat for skadelige cyberangreb. De enkeltstående cyberangreb ligger under tærsklen for de juridiske definitioner af krig, men akkumuleret og over tid medfører de betydelige omkostninger for Danmark.
2. Danmark besidder en cyberstyrke, der kan anvendes til angreb, spionage og forsvar. En skarp adskillelse mellem de tre funktioner er i dag udgangspunktet for anvendelse af cyberstyrken.
3. Danmarks mulighed for at forsvare sig og agere strategisk risikerer at blive svækket, hvis ikke adskillelsen løsnes, og den danske cyberstyrke gøres i stand til bedre at imødegå cyberoperationer i ikke-krigssituationer.

at finde passende modtræk i det nye konfliktrum. Det er problematisk, da de konstante cyberangreb ikke blot udgør en ny normatilstand af ufred, men akkumuleret og over tid medfører betydelige omkostninger for Danmark og dets allierede.

I Danmark har fokus indtil nu primært været på, at forsvare sig mod denne type cyberangreb ved at styrke samfundets generelle robusthed og modstandsdygtighed. I en tid præget af ufred, stormagtsstrid og en usikker alliancepolitisk situation, er det betimeligt at overveje, hvordan Danmarks militære cyberstyrke kan anvendes til at forsvaret landet mod cyberangreb, der falder under tærsklen for krig.

Danmarks cybermagt…

Ved årsskiftet 2019-2020 blev Danmarks militære cyberstyrke - Cyber Network Operations (CNO-kapaciteten) – erklæret fuldt aktiv. Udviklingen af Danmarks militære cyberstyrke har været en markant tværpolitisk prioritet det seneste tiår. Danmark besidder således offensive cybermidler, der gør landet i stand til at træffe både kort- og langsigtede strategiske beslutninger.

Som det fremgår af figur 1, så er cyberstyrken placeret mellem det efterretningsmæssige og det militære. Organisatorisk har den til huse i Forsvarets Efterretningstjeneste (FE), mens den funktionelt er delt mellem FE og Forsvarskommandoen. Anvendelse af de offensive cybermidler er underlagt forsvarschefen, mens cyberstyrken står til rådighed for chefen for efterretningstjenesten, når den ikke bliver anvendt i militære operationer.

…mellem angreb, spionage og forsvar

Den strategiske og operationelle grænse mellem angreb, spionage og forsvar er imidlertid ikke så let at drage som den funktionelle og organisatoriske. Orienterer man sig i de førende politiske og strategiske debatter samt forskningslitteraturen på området, står det klart, at der hersker meget stor uenighed om de strategiske, juridiske og operationelle grænsedragninger mellem især spionage og angrebsoperationer.

Eksempelvis er det oftest nødvendigt at inficere modstanderens it-systemer, kortlægge netværksinfrastruktur og udnytte en eller flere sårbarheder for at kunne udføre både spionage og angrebsoperationer. Har man først opnået adgang til modstanderens it-system, er afstanden mellem indhentning af information, disruption og ødelæggelse begrænset. Desuden er det ofte svært for modstanderen at afkode den indtrængendes intentioner med operationen samt konsekvenserne af denne.

Det gør sig særligt gældende, når cybermidler bliver anvendt til aktive forsvarsoperationer, hvor man forsvarer sig ved at krydse over i angriberens netværk for at udføre efterretningsoperationer, afbryde igangværende eller planlagte angreb samt straffe angriberen gennem ødelæggende operationer.

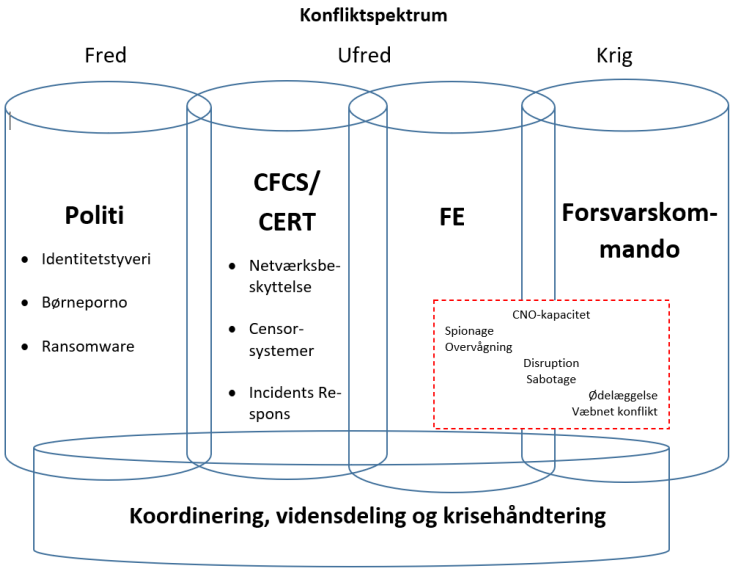
Kombinationen af konstant digital ufred samt den vanskelige skelnen mellem digitale forsvars-, spionage- og angrebsoperationer gør det nødvendigt – men også kompliceret – at svare på, hvordan Danmarks offensive cyberstyrke kan anvendes til at forsvare Danmark.

Behov for reaktion

Et afgørende spørgsmål er, om Danmark ønsker en mere operationel efterretningstjeneste, der aktivt anvender offensive cybermidler til at imødegå cyberoperationer under tærsklen for krig. Det spørgsmål medfører overvejelser angående frygt for eskalation, afskrækkelseseffekt, effekt på international normdannelse, behovet for politisk ansvar, beslutningstagning og kontrol samt yderligere tilsyn med efterretningstjenesten.

Det er altså ikke risikofrit at anvende offensive cybermidler til at forsvare sig mod angreb, der falder under tærsklen for krig. Anvendelsen af cybermidler til at imødegå skadelige cyberoperationer risikerer at blive mødt af beskyldninger om dobbeltmoral og uberettiget indblanding i andre staters anliggender samt gengældelsesaktioner. Omvendt er det ikke en holdbar løsning at lade de skadelige angreb fortsatte uden reaktion.

Det er derfor påkrævet, at danske politiske beslutningstagere og relevante myndigheder gør sig klart, hvorvidt og hvordan Danmark skal anvende sin cyberstyrke til offensivt cyberforsvar i ikke-krigssituationer. De bør foretage en strategisk afvejning af, hvad Danmark kan opnå ved at forsvare sig ved at anvende af offensive cybermidler, herunder hvilke juridiske og operationelle forhold der gør sig gældende. Det er med andre ord afgørende, at der bliver sat klare politisk-strategisk mål samt udarbejdet tidssvarende juridiske og organisatoriske rammer og retningslinjer for anvendelsen af offensive cyberforsvarsmidler under tærsklen for krig.



Figur 1: Oversigt over organisering af cyberforsvar i Danmark

Anbefalinger

I dag danner en skarp adskillelse mellem angreb, spionage og forsvar udgangspunktet for anvendelsen af Danmarks cyberstyrke. Med afsæt i en afdækning af udviklingen i Holland, Norge og Frankrig og som reaktion på de ændrede geopolitiske vilkår og nye cyberkonfliktmønstre anbefales det, at Danmark løsner op for adskillelsen, således at FE bliver i stand til at levere begrænsede cybereffekter til brug for forsvar mod skadelig aktivitet, der foregår under tærsklen for krig.

Med den overordnede anbefaling følger yderligere en række konkrete anbefalinger til, hvordan de danske beslutningstagere sikrer, at anvendelsen af cyberstyrken får de bedst mulige politisk-strategisk, juridisk og organisatoriske rammer.

Styrket politisk inddragelse og tilsyn i forbindelse med anvendelse af CNO-kapaciteten

Udviklingen i cybertrusselsbilledet understreger nødvendigheden af at indrette Danmarks cyberforsvar med øje for kontinuerlig gråzonekonflikt og -friktion. De eksisterende politisk-strategiske og juridiske rammer sikrer ikke de bedst mulige betingelser for Danmarks anvendelse af CNO-kapaciteten i en tid med nye cyberkonfliktmønstre. Regeringen og Folketinget bør gøre følgende:

Udvikling af et selvstændigt retsgrundlag for CNO-kapaciteten

- Styrke retsgrundlaget for anvendelse af CNO-kapaciteten. Det eksisterende retsgrundlag, der findes i FE-loven, er ikke tilstrækkeligt til at sikre den optimale udnyttelse af Danmarks CNO-kapacitet i en kontekst, hvor skadelige cyberaktiviteter under tærsklen for krig kontinuerligt er rettet mod Danmark. Regeringen og Folketinget bør igangsætte arbejdet med at udvikle et selvstændigt lovgrundlag for CNO-kapaciteten. I forbindelse med lovarbejdet bør regeringen og Folketinget overveje:
- Hvordan Udvalget vedrørende Efterretningstjenesterne, Forsvarsudvalget og Det Udenrigspolitiske Nævn kan spille en mere aktiv rolle i forbindelse med sanktionering, vurdering og kontrol med anvendelse af CNO-kapaciteten.
- Hvorvidt Tilsynet med Efterretningstjenesterne (TE) skal rapportere til Folketinget om anvendelse af CNO-kapaciteten. Man bør endvidere overveje, hvorvidt en sådan rapportering skal ske ad hoc (ex ante/ex post) på baggrund af indsættelse af CNO-kapaciteter i specifikke operationer eller på fastlagte tidspunkter.
- Hvorvidt TE bør være med til at formidle de operationelle beslutnings- og kontroludfordringer til Folketinget, der følger af den vanskelige skelnen mellem forsvar, spionage og angreb samt usikkerheden om målopfyldelse og levering af effekt ved anvendelsen af cyberoperationer.

Udvidelse af Tilsynet med Efterretningstjenesternes mandat

- Udvide TE's mandat – fra udelukkende at handle om korrekt behandling af personoplysninger – til også at sikre korrekt, ansvarlig og effektiv anvendelse af Danmarks CNO-kapacitet i forbindelse med imødegåelse af skadelige cyberoperationer under grænsen for krig. Som led heri bør regeringen og Folketinget overveje:
- Hvorvidt TE skal være involveret i sanktionering af brugen af offensive cyberforsvarsmidler under tærsklen for krig ved at give forudgående tilladelse eller foretage efterfølgende revision
- Muligheden for at inddrage TE for at sikre, at anvendelsen af CNO-kapacitetens offensive cyberforsvarsmidler i konfliktsituationer, der falder under tærsklen for krig, lever op til de vedtagne

politiske ønsker og juridiske beføjelser
- At søge inspiration i de hollandske og norske tilsynsmodeller.

Styrket strategisk planlægning med hensyn til anvendelse af CNO-kapaciteten

De ansvarlige danske myndigheder bør styrke det strategiske planlægningsarbejde med hensyn til anvendelse af CNO-kapaciteten med henblik på at styrke de strategiske rammer for Danmarks anvendelse af cybermagt under tærsklen for krig.

Strategisk planlægning med hensyn til anvendelse af CNO-kapaciteten

- Strategiarbejdet bør identificere og kortlægge Danmarks cybersikkerheds- og forsvarspolitiske interesser i lyset af den ændrede geopolitiske situation, cybertrusselsbilledets udvikling og vores allieredes tiltag inden for offensivt cyberforsvar.
- Strategiarbejdet bør have særligt fokus på anvendelse af CNO-kapaciteten i konfliktsituationer, der falder under tærsklen for krig, herunder de særlige juridiske og militære muligheder, begrænsninger og udfordringer, der er forbundet med anvendelsen af offensivt cyberforsvar under tærsklen for krig.
- Strategiarbejdet bør ses som en dynamisk proces, som sikrer, at Danmarks kort- og langsigtede muligheder for anvendelse af CNO-kapaciteten – herunder til cyberforsvar under tærsklen for krig – løbende bliver analyseret, evalueret og udviklet.
- Folketinget bør inddrages, når strategien skal evalueres og videreudvikles.

Dansk international cybersikkerhedspolitik

I lyset den stadig tiltagende digitalisering, de ændrede geopolitiske vilkår samt ændringerne i cybertrusselsbilledet bør de relevante danske myndigheder udvikle en international cybersikkerhedspolitik.

Udvikling af en dansk international cybersikkerhedspolitik

- Den internationale cybersikkerhedspolitik bør fokusere bredspektret på Danmarks internationale arbejde med cybersikkerhed, herunder de juridiske, økonomiske, diplomatiske og forsvarsmæssige udfordringer som følger af den tiltagende globale digitale teknologianvendelse og -udvikling.
- Politikken bør beskrive forhold angående Danmarks digitale suverænitet og strategiske autonomi.
- Politikken bør tage udgangspunkt i Danmarks engagement i eksisterende cybersikkerhedsinitiativer i Norden, EU, OSCE, NATO og FN.
- Politikken bør indeholde overvejelser om, hvordan Danmark kan styrke det internationale politiske og juridiske arbejde med at imødegå skadelige gråzoneaktiviteter i cyberspace.
- De relevante myndigheder bør hente inspiration til udarbejdelse af politikken i lande, der har udviklet lignende politikker og strategier, herunder Holland, Norge og Frankrig.

Dansk offensiv cybermagt

Dette CMS Memo bygger på CMS Rapporten **Dansk offensiv cybermagt mellem angreb, spionage og forsvar**, udgivet af Center for Militære Studier ved Københavns Universitet. Rapporten findes i sin fulde længde på Center for Militære Studiers hjemmeside.

Hvis du vil vide mere om, hvordan digitalisering påvirker forsvars- og sikkerhedspolitik, kan du også læse CMS Rapporterne:

- Informationspåvirkning som demokratisk udfordring: Desinformation, Danmark og tre præmisser for det liberale demokrati (2019)
- Når Hydra angriber: Hybrid afskrækkelse i gråzonen mellem krig og fred (2019)
- In, On, or Out of the Loop? Denmark and Autonomous Weapon Systems (2017)

Om CMS

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: Billede fra Operation Red Knight, 2018. Copyright: Forsvaret & Forsvarsgalleriet · Foto side 3: Øvelse i Forsvaret, 2019 . Copyright: Forsvaret & Forsvarsgalleriet · **ISBN**: 987-87-7393-852-2