KØBENHAVNS UNIVERSITET
CENTER FOR MILITÆRE STUDIER

Dansk offensiv cybermagt mellem angreb, spionage og forsvar

En komparativ analyse på tværs af Europa

Tobias Liebetrau

Maj 2020

Kolofon

Dansk offensiv cybermagt mellem angreb, spionage og forsvar

Denne rapport er en del af Center for Militære Studiers forskningsbaserede myndighedsbetjening for Forsvarsministeriet og de politiske partier bag forsvarsforliget. Formålet med rapporten er at understøtte og kvalificere debatten om anvendelse af dansk cybermagt til at imødegå skadelige cyberoperationer, der falder under tærsklen for krig. Rapporten foretager en komparativ analyse på tværs af Europa og kommer med en række anbefalinger til mulige danske initiativer på området. Anbefalingerne er rettet mod såvel folketingsmedlemmer som statslige myndigheder.

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

Denne rapport er et analysearbejde baseret på forskningsmæssig metode. Rapportens konklusioner er ikke et udtryk for holdninger hos den danske regering, det danske forsvar eller andre myndigheder.

Læs mere om centret og dets aktiviteter på: http://cms.polsci.ku.dk/.

Forfattere:
Postdoc, ph.d. Tobias Liebetrau

Masthead

Danish offensive cyber power between attack, espionage and defence

This report is a part of Centre for Military Studies' policy research services for the Ministry of Defence and the political parties to the Defence Agreement. The purpose of the report is to support and qualify the debate on Denmark's use of cyber power to counter harmful cyber operations that fall below the threshold of war. The report performs a comparative analysis across Europe and provides recommendations for future Danish initiatives in this area. The recommendations are directed at both members of parliament and state authorities.

The Centre for Military Studies is a research centre at the Department of Political Science at the University of Copenhagen. The Centre undertakes research on security and defence issues as well as military strategy. This research constitutes the foundation for the policy research services that the Centre provides for the Ministry of Defence and the political parties to the Defence Agreement.

This report contains an analysis based on academic research methodology. Its conclusions should not be understood as a reflection of the views and opinions of the Danish Government, the Danish Armed Forces or any other authority.

Read more about the Centre and its activities at http://cms.polsci.ku.dk/.

Authors:
Postdoc, Dr. Tobias Liebetrau

ISBN: 987-87-7393-852-2

Indholdsfortegnelse

Dansk resumé og anbefalinger

Danmark er i stigende grad udsat for skadelige cyberoperationer under tærsklen for krig. De enkeltstående cyberhændelser lever ikke op til de juridiske definitioner af væbnet konflikt og krig, men akkumuleret og over tid medfører de betydelige omkostninger for Danmark. En særlig udfordring, der er forbundet med at imødegå cyberoperationer under tærsklen for krig, er, at velkendte politisk-strategiske og juridiske begreber, definitioner og rammer er vanskelige at anvende. Desuden besværliggøres grænsedragning mellem digitale forsvars-, spionage- og angrebsoperationer af usikkerhed angående afsenders identitet og intention samt operationens effekt. Den situation nødvendiggør en principiel diskussion af, hvordan Danmark vil, kan og bør anvende offensive cybermidler defensivt til at imødegå skadelige cyberoperationer under tærsklen for krig.

Denne rapport bidrager til at understøtte og kvalificere diskussionen om Danmarks offensive cyberforsvarspolitik ved 1) at belyse dens nationale og internationale rammer, 2) sammenligne og analysere diskussioner og tiltag på området i Holland, Norge og Frankrig 3) samt identificere en række centrale forhold på politisk-strategisk, juridisk og organisatorisk niveau, som Danmark bør forholde sig til, således at Danmarks offensive cyberforsvar opnår de bedste mulige rammer.

Et afgørende spørgsmål er, om Danmark ønsker en mere operationel efterretningstjeneste, der aktivt anvender offensive cybermidler til at imødegå cyberoperationer under tærsklen for krig. Et spørgsmål, der 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 således ikke risikofrit at anvende offensive cyberforsvarsmidler under tærsklen for krig, men over tærsklen for diplomati.[1] Anvendelsen af cybermidler til at imødegå skadelige cyberoperationer i denne gråzone risikerer at blive mødt af beskyldninger om dobbeltmoral og uberettiget indblanding i andre staters anliggender samt gengældelsesaktioner.

Disse overvejelser understreger behovet for, at danske beslutningstagere tager aktivt stilling til de politisk-strategiske, juridiske og organisatoriske vilkår og rammer for anvendelse af offensive cybermidler i ikke-krigssituationer. Uden et klart politisk-strategisk mandat og et tidssvarende lovgrundlag, der opstiller mål, midler og måder, hvorpå Danmark kan og bør anvende offensive cybermidler til at imødegå cyberoperationer i ikke-krigssituationer, risikerer Danmarks mulighed for at forsvare sig og agere strategisk i den verserende konflikt i cybergråzonen at blive alvorligt svækket.

Hovedanbefaling

Forsvarets Efterretningstjeneste bør kunne levere begrænsede cybereffekter

I dag danner en skarp adskillelse mellem angreb, spionage og forsvar udgangspunktet for anvendelsen af Danmarks militære cyberenhed – computer network operations-kapaciteten (CNO-kapaciteten). Med afsæt i analysens afdækning af udviklingen i Holland, Norge og Frankrig og som reaktion på de ændrede geopolitiske vilkår og nye cyberkonfliktmønstre udleder rapporten én større hovedanbefaling. Den er, at Danmark bør løsne op for adskillelsen, således at Forsvarets Efterretningstjeneste (FE) bliver i stand til at levere begrænsede cybereffekter til brug for forsvar mod skadelig aktivitet, der foregår under tærsklen for krig.

Øvrige anbefalinger

Udvikling af selvstændigt retsgrundlag for CNO-kapaciteten

- Regeringen og Folketinget bør udvikle et selvstændigt lovgrundlag for CNO-kapaciteten.

Udvidelse af Tilsynet med Efterretningstjenesternes mandat

- Regeringen og Folketinget bør udvide Tilsynet med Efterretningstjenesternes mandat. Tilsynet bør sikre korrekt, ansvarlig og effektiv anvendelse af Danmarks CNO-kapacitet til imødegåelse af skadelige cyberoperationer under grænsen for krig.

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.

Udvikling af en dansk international cybersikkerhedspolitik

- De ansvarlige myndigheder bør udvikle en international cybersikkerhedspolitik, der fokuserer 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.

Abstract and recommendations

Denmark is increasingly exposed to harmful cyber incidents that fall below the threshold of war. In isolation, these cyber incidents do not live up to the legal definitions of armed conflict and war. Accumulated over time, they do, however, cause significant harm to the Danish society. One particular challenge associated with addressing cyber operations below the threshold of war is that strategic and legal concepts and definitions are difficult to apply. In addition, drawing boundaries between digital defence, espionage and attack operations are made difficult due to the challenges associated with determining attribution, intention and effect of cyber incidents. This situation demands a fundamental discussion of how Denmark can apply offensive cyber power to counter hostile cyber operations that fall below the threshold of war.

This report seeks to support and qualify the discussion on Denmark's use of offensive cyber power by 1) elucidating its national and international framework respectively, 2) comparing and analyzing discussions and initiatives on the topic in the Netherlands, Norway and France 3) and identifying key issues at political-strategic, legal and organizational level that Denmark should act upon in order to achieve the best possible configuration of Danish cyber defence.

A crucial question is whether Denmark wants a more operational intelligence service that actively uses offensive cyber power to counter hostile cyber operations that fall below the threshold of war. An issue that raises concerns about the fear of escalation, the possibility of deterrence, the effect on international norm formation, the need for political responsibility, decision-making and control, and further oversight with the intelligence service. Thus, it is not risk-free to deploy cyber power for defensive purposes below the threshold of war, but above the threshold of diplomacy. The use of cyber power to counter harmful cyber operations in this grey-zone carries the risk of being met by allegations of applying double standards, unjustified interferences in the affairs of foreign states and retaliatory action.

These considerations underline the need for Danish policy makers to take an active stance on the political-strategic, legal and organizational conditions and structures that concern the use of cyber power below the threshold of war. Without the development of a clear political-strategic mandate and a contemporary legal basis that together establish the goals, means and ways in which Denmark should deploy cyber power to counter hostile cyber operation below the threshold of war, Denmark’s capacity to defend itself and act strategically in the pending cyber grey-zone conflict risk is being severely weakened.

Key Recommendation

The Danish Defense Intelligence Service should be able to deliver limited cyber effects

Today, a sharp separation between attack, espionage and defence forms the baseline for the use of Denmark's military cyber unit - the Computer Network Operations (CNO) unit. Based on the analysis's coverage of the developments in the Netherlands, Norway, and France and in response to the changed geo-political conditions and new cyber conflict patterns, the report deduces one major recommendation: Denmark should loosen up this separation by allowing the Danish Defense Intelligence Service (FE) to deliver limited cyber effects in defense against harmful activity that fall below the threshold of war.

Additional recommendations

Development of an independent legal basis for the CNO unit

- The Danish government and the Parliament should develop an independent legal basis for the CNO unit.

Extending the mandate of the Danish Intelligence Oversight Board

- The Government and the Parliament should extend the mandate of the Danish Intelligence Oversight Board. The oversight board should ensure the correct, responsible, and effective use of Denmark's CNO unit to address harmful cyber operations below the threshold of war.

Strategic planning for the use of CNO unit

- The responsible Danish authorities should strengthen the strategic planning regarding the use of the CNO unit to strengthen the entire strategic framework for Denmark's use of cyber power below the threshold of war.

Development of a Danish international cyber security policy

- The responsible authorities should develop an international cyber security policy with a broad focus on Denmark's international cyber security work, including the legal, economic, diplomatic and military challenges arising from the growing global use and development of digital technology.

1 Offensivt cyberforsvar og efterretningstjenestens nye rolle

Danmarks militære cyberenhed – computer network operations-kapaciteten (CNO-kapaciteten) – blev ved årsskiftet 2019/2020 fuldt operationel. Enheden, der skal udføre digitale spionage-, forsvars- og angrebsoperationer, er placeret i Forsvaret Efterretningstjeneste (FE). Dermed er FE's position som centrum for forsvarets cybereksperise blevet styrket. Det illustrerer, hvordan fremvæksten af det digitale domæne har medført, at efterretningstjenester verden over har fået nye defensive og offensive arbejdsopgaver.[2] Digitaliseringen af vores samfund har således understøttet en diversificering af efterretningstjenesters rolle, der nu inkluderer ansvar for beskyttelse af offentlige og private netværk samt udførelse af offensive cyberoperationer. Det betyder, at den tidligere klare adskillelse mellem det militære og det efterretningsmæssige udviskes.

Forskellen mellem på den ene side langsigtede og strategiske efterretningsoperationer og på den anden side defensive og offensive militære indgreb bliver dermed mindre tydelig. Danmark er derfor stillet over for et afgørende politisk-strategisk spørgsmål: Hvordan bør, kan og skal CNO-kapaciteten anvendes, når landet ikke er i krig?

Tekstboks 1:
Hvad er computer network operations?

CNO består af tre dele

Den offensive militære del af CNO-kapaciteten bliver kaldt **computer network attack** (CNA). Den har til formål at påvirke en fjendtlig aktør gennem militære angreb på dennes digitale infrastruktur. Funktionen huses af FE, men er funktionelt underlagt forsvarschefen og Forsvarskommandoen.

Ved **computer network exploitation** (CNE) søger man at sikre sig adgang til at indhente informationer fra lukkede it-netværk, it-systemer eller computere. CNE kan dog også omfatte handlinger, der har til formål at imødegå andres offensive netværksbaserede handlinger. Brugen af CNE har ikke til formål at skabe ødelæggelse, da der i så fald som udgangspunkt ville være tale om et CNA. Anvendelse af CNA er afhængig af informationer og adgange til computernetværk. CNE er således forudsætningsskabende for effektivt CNA. Funktionen huses og anvendes af FE.

Computer network defence (CND) er rene forsvarshandlinger. CND dækker over varsling, analyse, intern imødegåelse af hændelser, afhjælpning af konsekvenser ved sikkerhedshændelser samt samarbejde med andre landes tilsvarende myndigheder. I Danmark er Center for Cybersikkerhed (CFCS) under FE et eksempel på en myndighed, der varetager en CND-funktion.

Ovenstående er baseret på "Redegørelse fra den tværministerielle arbejdsgruppe om Folketingets inddragelse ved anvendelse af den militære Computer Network Attack (CNA)-kapacitet".

Det er i dag alment anerkendt og accepteret, at offensive cybermidler kan anvendes i krig og væbnet konflikt. I Danmark bliver anvendelse af offensive cybermidler til at understøtte og udføre militære operationer i væbnet konflikt og krig behandlet i forsvarets militære cyberdoktrin fra 2019.[3] Når CNO-kapaciteten ikke bliver anvendt i militære operationer, så står CNO-enheden til rådighed for chefen for FE, der kan lade kapaciteten indgå i løsningen af tjenestens opgaver.[4]

En udfordring i forbindelse med anvendelsen af CNO-kapaciteten til at imødegå fjendtlige cyberoperationer i ikke-krigssituationer er, at anvendelsen ofte vil gå på tværs af de traditionelle skillelinjer mellem forsvar (CND), angreb (CNA) og efterretning (CNE). Det gør sig gældende, når offensive cybermidler bliver anvendt til dynamiske og fremadrettede forsvarsoperationer, hvor man forsvarer sig ved at krydse over i angriberens netværk for at udføre efterretningsoperationer, afbryde igangværende eller planlagte angreb samt straffe angriberen ved ødelæggende operationer. Den strategiske og operationelle adskillelse af CNA, CNE og CND er således mere broget end den funktionelle adskillelse umiddelbart tilsiger. Det er denne spænding, som rapporten forsøger at indfange og fastholde ved at beskrive anvendelsen af offensive cybermidler som forsvar. De politiske og juridiske grænser for den mangeartede aktivitet i gråzonen mellem krig og fred samt efterretning og magtanvendelse har aldrig været nøjagtigt definerede og globalt anerkendte. Der er imidlertid bred enighed om, at den stigende digitalisering samt introduktionen af cyberoperationer har sløret billedet yderligere.[5] Eksempelvis er det oftest nødvendigt at identificere modstanderens it-systemer, kortlægge netværksinfrastruktur og udnytte en eller flere sårbarheder for at kunne udføre CNE og CNA. 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.[6]

Danske politikere og myndigheder bør bruge den fulde indfasning af CNO-kapaciteten som en anledning til at tage stilling til, hvorvidt og hvordan Danmark vil og kan anvende CNO-kapaciteten til offensive cyberforsvarsoperationer under tærsklen for krig. Det rejser en række afledte spørgsmål. Såfremt Danmark skal anvende offensive cyberforsvarsmidler under tærsklen for krig, hvad er så de juridiske og operationelle rammer? Hvor går grænsen mellem gråzonekonflikter og væbnet konflikt i cyberspace? Hvordan sikrer vi politisk autoritet, ansvar og kontrol med anvendelse af offensive cyberforsvarsmidler under tærsklen for krig? Hvordan vil vores modstandere opleve og reagere på et intensiveret dansk cyberforsvar under tærsklen for krig? Vil dansk anvendelse af offensive cybermidler i ikke-krigssituationer øge risikoen for eskalation og ustabilitet, eller kan det tværtimod være en afskrækkende og stabilitetsskabende faktor? Skal Danmark udføre offensive cyberforsvarsoperationer for at beskytte danske virksomheder mod spionage og befolkningen mod misinformationskampagner, når landet ikke er i krig? Vil danske borgere og virksomheder opleve offensivt cyberforsvar som beskyttende og trygghedsskabende eller aggressivt og konfliktoptrappende?

Med disse spørgsmål som inspiration leverer rapporten en analyse og en diskussion af de betingelser, muligheder og begrænsninger, der er forbundet med udviklingen og anvendelsen af offensive cyberforsvarsmidler. Rapporten har særligt fokus på de udfordringer, der angår anvendelse af offensive cybermidler i situationer, der falder under tærsklen for krig.

Rapporten bidrager dermed til at styrke den offentlige samtale og den konkrete udvikling af politisk-strategiske, juridiske og organisatoriske anvisninger med hensyn til anvendelsen af CNO-kapaciteten i forsvars-, spionage- og angrebsøjemed. Rapporten fokuserer i mindre grad på forandringer i trusselsbilledet – som forventes fortsat at udvikle sig negativt[7] – og i højere grad på de overvejelser og tiltag, som sammenlignelige lande har gennemført, og

som danske politiske og militære beslutningstagere derfor kan spejle sig i. Rapporten foretager en sammenlignende analyse af, hvordan Frankrig, Holland og Norge har forholdt sig til udvikling og anvendelse af offensive cybermidler på henholdsvis politisk-strategisk samt juridisk og organisatorisk niveau. På den baggrund formulerer rapporten en række anbefalinger til de danske politiske og militære beslutningstagere.

1.1 Formål, metode og opbygning

Formålet med denne rapport er at understøtte prioriteringer og beslutninger på CNO-området ved at belyse betingelser, begrænsninger og muligheder for anvendelse af dansk cybermagt under tærsklen for krig. Rapporten opstiller en række anbefalinger, der understøtter en diskussion af behovet for udvikling af politisk-strategiske, juridiske og organisatoriske rammer for anvendelse af offensive cyberforsvarsmidler i ikke-krigssituationer. Dermed begrunder rapporten behovet for en bred forsvarspolitisk debat i Danmark vedrørende anvendelse af CNO-kapaciteten. Rapporten baserer sig på et deskstudy, herunder omfattende indsamling og behandling af offentligt tilgængelige oplysninger om NATO-medlemmers cybersikkerhedsstrategier og cyberforsvarspolitikker med særligt fokus på amerikanske, hollandske, norske, franske og danske forhold. Desuden er en række interviews og uformelle samtaler med nøglepersoner i Holland, Norge, Frankrig og Danmark blevet gennemført for yderligere at belyse rapportens genstandsfelt. Rapporten er endvidere kvalitetssikret gennem intern og ekstern fagfællevurdering.

Analytisk gør rapporten tre ting. I kapitel II beskriver rapporten de eksisterende rammer for det danske cyberforsvar og ridser en række udfordringer op. Herefter kortlægger rapporten i kapitel III den overordnede udvikling i international cybersikkerhedspolitik med særligt fokus på imødegåelse af skadelige cyberoperationer, der falder under grænsen for krig. Dermed skaber rapporten et samlet blik på forandringerne i de internationale rammebetingelser for dansk cyberforsvarspolitik. Kapitlet fokuserer særligt på USA's ledende rolle, herunder amerikanernes strategiske fokus på vedvarende engagement og fremadrettet forsvar. I kapitel IV analyserer og sammenligner rapporten diskussioner og tiltag for anvendelse og udvikling af offensive cybermidler i Holland, Norge og Frankrig. De tre lande repræsenterer et udsnit af NATO-lande med forskellige militære kapaciteter samt forskellige tilgange til CNO-arbejdet. Analysen består af to dele. Den første del tager udgangspunkt i Hollands, Norges og Frankrigs strategiske og doktrinære arbejde med cybersikkerhed og cyberforsvarspolitik. I analysens anden del zoomer rapporten ind på organiseringen af offensive cybermidler i de tre lande; særligt belyses ansvarsfordelingen mellem efterretningstjenester og forsvaret. Med udgangspunkt i analysen fremhæver rapporten slutteligt i kapitel V en række centrale udfordringer i forbindelse med Danmarks offensive cyberforsvarspolitik. Desuden opstiller det konkluderende kapitel en række anbefalinger på politisk-strategisk, juridisk og organisatorisk niveau, som Danmark bør forholde sig til, således at Danmarks offensive cyberforsvar opnår de bedste mulige rammer.

Rapportens indhold er påvirket af, at hemmeligholdelse har særlig relevans i forhold til sikkerheds- og forsvarspolitik. Det gælder ikke mindst for udvikling og anvendelse af offensive cybermidler. Dokumenter er hemmeligstemplede, informationer fortrolige, og døre hermetisk lukkede. Det har således været en udfordring at opnå adgang til viden om den konkrete udvikling og anvendelse af offensive cybermidler. De nævnte begrænsninger er udslagsgivende for detaljeringsniveauet i analysen. Desuden medfører de, at rapportens anbefalinger primært er af processuel karakter.

2 Den danske kontekst for anvendelse af offensive cybervåben

Cybertruslen er blevet et grundvilkår for danske myndigheder og virksomheder. Ifølge FE er det forventeligt, at cybertrusselsbilledet fortsætter med at udvikle sig i negativ retning som følge af yderligere digitalisering og geopolitisk rivalisering. Udvikling og anvendelse af offensive cyberkapaciteter spiller i dag en væsentlig rolle i det langstrakte politiske og strategiske kapløb mellem verdens stormagter.[8] Verden over anvender stater offensive cyberkapaciteter som led i skadelige operationer, der befinder sig under tærsklen for krig og over tærsklen for diplomati.[9] Denne permanente konflikttilstand under tærsklen for krig er blevet beskrevet som en gråzone mellem krig og fred. Et konfliktrum i fredstid.

CMS-rapporten "Når Hydra Angriber: Hybrid afskrækkelse i gråzonen mellem krig og fred" har for nylig kortlagt gråzonens konfliktmønstre og deres geopolitiske betydning for Danmark.[10] Rapporten beskriver, hvordan gråzonens overordnede konfliktrelation er den stigende rivalisering mellem USA, Rusland og Kina. Gråzonen er et konfliktrum, hvor verdens lande søger at undgå direkte konfrontation, men konstant udfordrer den eksisterende internationale politiske ordens normer og regler. De skadelige gråzoneaktiviteter i cyberspace består f.eks. af industrispionage, påvirkningsoperationer og aktiviteter rettet mod potentielt at kunne gøre skade på kritisk infrastruktur. Skadelige cyberoperationer under grænsen for krig udgør dermed en konstant, kompleks og alvorlig del af det samlede trusselsbillede, som Danmark skal forholde sig til.[11]

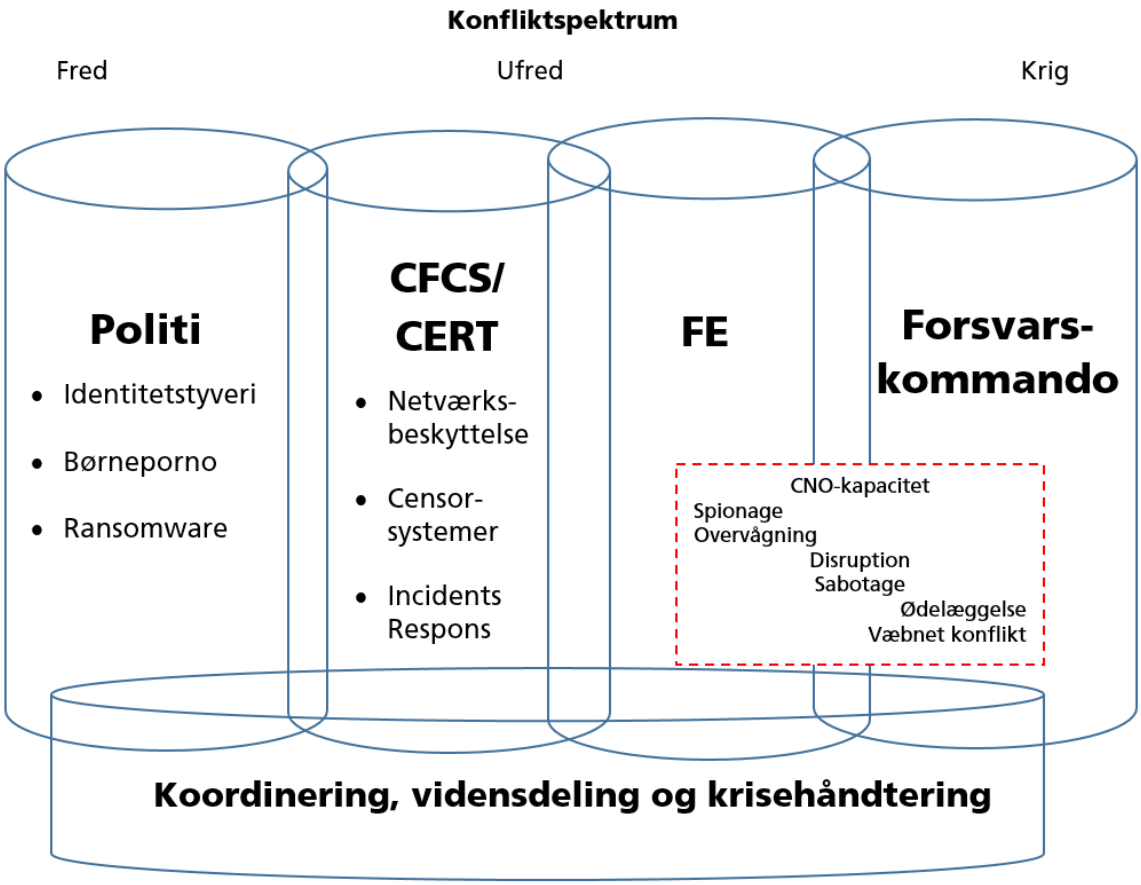
Samtidig bliver den liberale verdensorden i stigende grad udfordret. Det skyldes Kinas og Ruslands ageren på den internationale scene, tvetydigt amerikanske lederskab samt et EU, der ikke har etableret sig som en dominerende geopolitisk spiller. Den tiltagende betydning, prioritering og anvendelse af offensive cyberkapaciteter finder således sted på en baggrund af forskydninger i de geopolitiske rammevilkår for international sikkerheds- og forsvarspolitik. Trusselsbilledet samt de geopolitiske tendenser, herunder tiltagende stormagtsstrid i gråzonen mellem krig og fred samt en usikker alliancepolitisk situation, øger betydning af, at Danmark har en velovervejet og gennemarbejdet CNO-politik. En analyse og diskussion af Danmarks fremtidige cyberpolitiske ageren, herunder beslutninger om anvendelse af offensive cyberforsvarsoperationer i ikke-krigssituationer, føder dermed ind i nogle grundlæggende spørgsmål om, hvordan Danmark kan, vil og bør reagere på de ændrede forsvars- og sikkerhedspolitiske rammevilkår.

Den teknologiske udvikling og det ændrede trusselsbillede har som allerede nævnt fået danske politiske beslutningstagere til at vedtage en række initiativer på cyberområdet. I forsvarsforliget for 2010-2014 blev det gjort klart, at "cyberspace er blevet et kamprum".[12] Det blev derfor besluttet, at Forsvaret skulle oprette en CNO-kapacitet, der kan udføre cybernetværksoperationer. I de efterfølgende forsvarsforlig for henholdsvis 2013-2017[13] og 2018-2023[14] er betydningen og den politiske prioritering af at styrke Danmarks evne til at imødegå cybertruslen blevet yderligere opprioriteret. I 2018 tilkendegav Danmark, at forsvaret er klar til at bidrage med offensive cybereffekter til NATO-operationer: "Et bidrag til NATO med offensive cybereffekter

betyder, at Danmark med cyberkapaciteten (cybervåbnet) leverer en effekt mod et mål i et NATO-operationsområde. Kapaciteten indsættes fra faciliteter i Danmark, og kommandoen over kapaciteten bibeholdes nationalt, men handlingen foregår i rammen af en international NATO-operation og mod mål i udlandet."[15] CNO-kapaciteten blev fuldt funktionsdygtig ved indgangen til 2020.

Desuden oprettede regeringen i 2012 Center for Cybersikkerhed (CFCS) under FE. Centret er national it-sikkerhedsmyndighed og nationalt kompetencecenter på cybersikkerhedsområdet. Centret skal understøtte et højt informationssikkerhedsniveau i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af. Endvidere har skiftende danske regeringer lanceret to cyber- og informationssikkerhedsstrategier i henholdsvis 2014[16] og 2018[17]. Strategierne sigter mod at etablere yderligere beskyttelsesforanstaltninger for at styrke den samfundsmæssige robusthed og modstandsdygtighed. Dette indebærer oprettelse af flere og stærkere offentlig-private partnerskaber, mere og bedre uddannelse af både tekniske eksperter og civilbefolkningen samt et mere fokuseret arbejde med cyber- og informationssikkerhed i udvalgte sektorer.

Figur 1: Oversigt over organisering af cyberforsvar i Danmark



Figur 1 giver et overblik over organiseringen af Danmarks cyberforsvar. Her er det værd at bemærke, at CFCS/CSIRT (Computer Security Incident Response Team)-siloen er en del af FE, men opererer på grundlag af en særskilt lovgivning. Det fremgår af figuren, at CNO-kapaciteten er placeret mellem det efterretningsmæssige og det militære. Organisatorisk har den til huse i FE, mens den funktionelt er delt mellem FE og Forsvarskommandoen. Anvendelsen af CNA-funktionen er underlagt forsvarschefen, mens CNO-kapaciteten står til

rådighed for FE, når den ikke bliver anvendt i forbindelse med militære operationer.

Cyberforsvar et område, hvor Danmark ikke på samme måde som ellers kan sætte sin lid til USA og NATO-alliancen, da kompetencer er hemmeligholdte og sjældent deles.[18] Den fulde indfasning af den selvstændige danske CNO-kapacitet understøtter således dansk cyberforsvar på kort sigt samt dansk strategisk råderum på længere sigt. Den strategiske og operationelle grænse mellem CNA, CNE og CND 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[19] og operationelle grænsedragninger mellem især CNE og CNA, hvilket afspejles i uenigheder angående fordele og ulemper ved anvendelse af henholdsvis CNE og CNA.[20] Det gør sig som nævnt særligt gældende, når cybermidler bliver anvendt til dynamiske og fremadrettede 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.

Det er derfor nødvendigt, at de danske politiske beslutningstagere og relevante myndigheder gør sig klart, hvorvidt Danmark skal anvende CNO-kapaciteten til offensivt cyberforsvar i ikke-krigssituationer. Desuden bør de foretage en strategisk afvejning af, hvad Danmark kan opnå ved eventuel anvendelse af offensive cyberforsvarsmidler, 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. Desuden er det vigtigt at være opmærksom på, at der er risici for f.eks. eskalation, gengældelse og utilsigtede effekter forbundet med et mere aktivt dansk cyberforsvar.

3 Cyberufred: Den internationale ramme for anvendelse af offensive cybervåben

Stater anvender i stigende grad offensive cybermidler i forbindelse med målrettede operationer, der placerer sig under tærsklen for krig. Hensigten er oftest at fremme nationale politiske, økonomiske og militære formål.[21] Vi har set talrige eksempler på, at intellektuel ejendom og statshemmeligheder er blevet stjålet, og finansielle institutioner, elnet og olieraffinaderier truet, afbrudt og ødelagt.[22] Samtidig er internetbårne desinformations- og påvirkningskampagner blevet hverdag.[23] Den offentligt anerkendte og ødelæggende anvendelse af offensive cybermidler har primært rettet sig mod ikke-statslige aktører i kampen mod terrorisme.[24] Der findes også ikke-bekræftede eksempler på, at stater har anvendt offensive cybermidler som en del af militære operationer samt i forbindelse med selvstændigt ødelæggende operationer.[25]

Kapitlet præsenterer de internationale rammer for den danske offensive cyberforsvarspolitik ved at beskrive udviklingen i de vestlige landes svar på den tiltagende skadelige cyberaktivitet under tærsklen for krig. I første afsnit analyseres et paradigmeskifte i den amerikanske cyberforsvarsstrategi, hvor vedvarende engagement og fremadrettet forsvar udgør hjørnestenene. Dernæst skitserer kapitlet udviklingen i NATO's cyberforsvarspolitik samt de udfordringer, som alliancen står over for. Slutteligt viser kapitlet, hvordan vestlige demokratier i stigende grad anvender "naming, blaming og shaming" som svar på skadelige cyberoperationer, der befinder sig under tærsklen for krig.

Tekstboks 2:
Eksempler på cyberangreb

Cyberangreb mod energiforsyningen i Ukraine

I december 2015 blev flere elselskaber i det vestlige Ukraine ramt af cyberangreb. Hackerne fik adgang til elselskabernes kontrolsystemer og lukkede for strømmen i den ramte region. Halvdelen af boligerne i regionen var uden strøm i op til seks timer. Rusland er blevet tilskrevet angrebet.

WannaCry

WannaCry-ransomwaren spredte sig til computere verden over i maj 2017. Denne variant af ransomware var i stand til automatisk at kryptere filer på ofrets computer, slette originalerne og opkræve en løsesum for at dekryptere filerne igen. Samtidig installerede ransomwaren en bagdør på ofrets maskine, som gav angriberen mulighed for at installere yderligere malware. Angrebet inficerede mere end 300.000 computere. Angrebet er af flere lande, herunder USA, Storbritannien, Canada, Australien og New Zealand, blevet tilskrevet Nordkorea.

NotPetya

NotPetya-malwaren ramte verden i juni 2017. Angrebet var målrettet energiforsyningen i Ukraine, men spredte sig hurtigt til myndigheder og virksomheder verden over, herunder Mærsk, som blev ramt af alvorlige nedbrud med store økonomiske tab til følge. Mærsk har opgjort tabet til mellem 1,6 og 1,9 mia. kroner. NotPetya udgav sig indledningsvist for, ligesom WannaCry, at være ransomware. Men selv om malwaren afkrævede en løsesum, havde den reelt ikke funktionalitet til at genskabe adgangen til ofrenes filer, som det ellers teoretisk set er tilfældet ved ransomware. NotPetya blev derfor anset som et angreb med destruktive formål og ikke som en ransomwarekampagne.

Angrebet mod Sony

I 2014 blev filmselskabet Sony Pictures Entertainment hacket. Selskabets computere blev inficeret med destruktiv malware, der ødelagde data og systemer. Hackerne fik desuden adgang til intellektuel ejendom og fortrolige informationer. Efterfølgende lækkede hackerne e-mails, der belastede afsenderne, personfølsomme og medicinske oplysninger om ansatte, cheflønninger, kopier af film, der endnu ikke var udkommet, og andre informationer. Hacket resulterede i en række retssager mod Sony Pictures fra tidligere ansatte og stor kritik af selskabet for deres håndtering af sagen. USA har beskyldt Nordkorea for at stå bag hacket.

Shamoon-angrebene i Mellemøsten

I Saudi-Arabien og Qatar har virksomheder og myndigheder inden for energi, luftfart og andre sektorer gentagne gange siden 2012 været ramt af de såkaldte Shamoon-angreb, hvor malware overskriver eller sletter data på en computers harddisk. Iran menes at stå bag angrebene.

3.1 Amerikansk paradigmeskifte: Vedvarende engagement og fremadrettet forsvar

Det amerikanske forsvar præsenterede i 2018 et nyt strategisk udgangspunkt for landets cyberforsvar. Den nye strategiske linje er baseret på vedvarende engagement og fremadrettet forsvar, hvilket bliver anset som nødvendigt for at opnå dominans, sikkerhed og stabilitet i cyberspace.[26] Flere forskere har påpeget, at USA's ændrede cyberforsvarsstrategi er udtryk for et egentligt paradigmeskifte, hvad angår amerikansk cyberforsvar.[27] Årsagerne til dette skifte er flere. Et afgørende element for amerikanerne er, at fjendtlige stater i stigende grad udfører skadelige cyberoperationer under tærsklen for krig, hvilket ændrer den militærstrategiske kontekst for tilstedeværelse i cyberspace samt anvendelsen af offensive cyberkapaciteter i forsvarsøjemed.[28] Skal man forstå det amerikanske strategiske skifte, så er det altså afgørende at være

opmærksom på, at den nye strategi er forankret i en eksplicit anerkendelse af, at cyberspace som konfliktdomæne samt den geopolitiske kontekst har ændret sig grundlæggende siden 2009, hvor amerikanerne oprettede U.S. Cyber Command.

Med oprettelsen af U.S. Cyber Command i 2009 blev det amerikanske forsvarsministeries arbejde med defensive og offensive cybermidler integreret samt linket til NSA's kryptologiske og informationsikkerhedsmæssige arbejdsområde.[29] Af U.S. Cyber Commands første visionspapir fra 2015 fremgår det, at organisationens overordnede formål er at forsvare vitale amerikanske interesser i cyberspace ved yderligere at integrere og operationalisere cyberoperationer.[30] Visionspapiret er blevet beskrevet som et udvidet mission statement snarere end en egentlig strategi, da der er småt med konkrete bud på, hvordan visionens mål om f.eks. afskrækkelse og beskyttelse skal indfries.[31]
I 2018 udgav U.S. Cyber Command et nyt visionspapir, hvor det eksplicitte formål var at opnå og fastholde suverænitet i cyberspace. U.S. Cyber Command fremhæver i visionspapiret, at USA's modstandere kontinuerligt udfører skadelige cyberoperationer – såsom spionage, sabotage og desinformation – under tærsklen for krig. Derved forsøger modstanderen at udnytte de begrænsninger, som USA er underlagt, herunder den traditionelt høje tærskel for besvarelse af skadelige cyberoperationer i ikke-krigssituationer. Strategien fremhæver denne fjendtlige fremgangsmåde som "the new normal", hvorfor en ny strategisk tilgang til håndtering af den kontinuerlige cyberufred er nødvendig for at opnå større sikkerhed og øget stabilitet. U.S. Cyber Command beskriver dokumentet som en køreplan for, hvordan man opnår og vedligeholder overlegenhed i cyberspace, i takt med at man styrer, synkroniserer og koordinerer operationer i cyberspace for at forsvare og fremme nationale interesser. Vedvarende engagement og offensivt forsvar udgør kernen i den nye strategiske vision.[32] Denne tilgang blev slået fast og yderligere formaliseret i det amerikanske forsvarsministeries cyberstrategi fra 2018, hvor det blev gjort klart, at USA ønsker "at forsvare fremad for at forstyrre eller standse ondsindet cyberaktivitet ved dens udspring".[33]

Samlet set præsenterer visionspapiret og cyberstrategien en tilgang, hvis hovedfokus er kontinuerligt og vedholdende engagement mod ondsindede aktører i cyberspace. Det eksplicitte og overordnede formål med det amerikanske strategiskifte er at opnå og fastholde suverænitet i cyberspace. Den nye amerikanske strategi er et skridt væk fra det traditionelle afskrækkelsesparadigme hen imod et fokus på at opnå overlegenhed inden for cyberdomænet. Målet om vedvarende engagement og fremadrettet forsvar tilsiger, at U.S. Cyber Command skal "være til stede overalt, hele tiden og på alle måder".[34] Det amerikanske kursskifte er derfor blevet opfattet som et skifte væk fra at se cyberkonflikt og cyberoperationer gennem et prisme af isolerede cyberhændelser, der enten er væbnet konflikt eller ikke er det, mod at fokusere på langsigtede, gentagne og gradvise interaktioner inden for det digitale domæne.[35]

Siden lanceringen af de nye strategier har Trump-administrationen løsnet de operationelle regler for koordinering og anvendelse af offensive cybermidler, så det amerikanske cyberforsvar kan reagere hurtigere på fjendtlige cyberoperationer.[36] Et erklæret mål sat af den nu tidligere nationale sikkerhedsrådgiver John Bolton.[37] Desuden har Trump-administrationen sanktioneret ødelæggende cyberoperationer mod f.eks. Iran[38] og generelt skruet op for retorikken, når det kommer til offensive cybermidler. USA har dermed både i ord og i handling indtaget en mere offensiv cyberpositur de seneste år. Det er sket på baggrund af det strategiske skifte, der har rod i henholdsvis ændrede geopolitiske rammebetingelser og en ny forståelse af cyberdomænets unikke karakter. Det strategiske skifte indvarsler en fortsat amerikansk bevægelse væk fra en reaktiv og afskrækkelsesbaseret tilgang til cyberforsvar mod en

fremadrettet proaktiv tilgang baseret på vedvarende engagement og forsvar.[39] En tilgang, der uanset de specifikke rammer og grænser for det vedholdende engagement og fremadrettede forsvar antyder, at øget friktion med modstanderen under tærsklen for krig er afgørende for strategisk succes.

Tekstboks 3:
Eksempler på det amerikanske strategiske skift

To eksempler på det amerikanske strategiske skifte:

1) **Aktiv malware**: Ifølge New York Times har amerikanske embedsmænd bekræftet, at amerikanerne – som led i den nye cyberforsvarsstrategi – har svaret på russisk indblanding i midtvejsvalget i 2018 ved at placere malware i de russiske elnet med en aggressivitet, der ikke tidligere er set. Placeringen af malware skal dels ses som en advarsel og dels kunne udnyttes, hvis der skulle bryde en større konflikt ud mellem USA og Rusland[40].

2) **Cyberassistance**: I 2018 sendte U.S. Cyber Command cyberforsvarsstyrker til Ukraine, Makedonien og Montenegro for at hjælpe de tre lande med at forsvare deres netværk og indsamle efterretninger om amerikanske modstandere. Dermed forsøgte amerikanerne at sikre sig mod indblanding i midtvejsvalget i 2018. Ifølge den nuværende leder af US Cyber Command, general Nakasone, var dette "første gang, vi sendte vores cyberkrigere til udlandet for at sikre netværk uden for forsvarsministeriets egne netværk"[41]

3.2 NATO's cybersikkerhedspolitik: Koordination af nationale indsættelser

På NATO-topmødet i Prag i 2002 anerkendte alliancen for første gang behovet for at styrke cyberforsvaret. Det blev fulgt op med en egentlig cyberforsvarspolitik i 2008. Men det var først på NATO-topmødet i 2014 i Wales, at alliancens medlemmer vedtog den opdaterede cyberforsvarspolitik, der sikrer, at artikel 5 (musketereden) nu også gælder væsentlige cyberangreb.[42] På Warszawa-topmødet to år senere erklærede NATO-landene cyberspace for et operationelt domæne på linje med land, hav, luft og rum. Desuden vedtog landene den såkaldte Cyber Defence Pledge, der forpligter dem til at styrke deres nationale cyberforsvar med henblik på, at NATO-medlemslandene skal være i stand til at forsvare sig i cyberspace.[43] På NATO-topmødet i Bruxelles i 2018 føjede NATO yderligere nuancer til alliancens cybersikkerhedspolitik ved at erklære, at cybereffekter kan integreres i alliancens operationer. I lyset af tiltagende og hybride cybertrusler understregede NATO i topdeklarationen, at alliancen er "fast besluttet på at anvende det fulde udvalg af muligheder, herunder cybertiltag, til at afskrække, forsvare sig mod og imødegå det fulde spektrum af cybertrusler".[44] For at indfri det mål lancerede NATO-landene samtidig oprettelsen af et nyt Cyber Operations Center i Belgien. Centret skal tjene til at styrke NATO's kommandostruktur og understøtte, at cybereffekter effektivt bliver integreret i alliancens militære operationer. Centret forventes at blive fuldt operationelt i 2023.

De seneste års NATO-integration af medlemsstaternes offensive cybermidler til brug for afskrækkelse og forsvar er blevet beskrevet som et markant politisk og strategisk skifte.[45] I dag har størstedelen af alliancens medlemmer erklæret, at de er villige til at bidrage med offensive cyberkapaciteter til NATO-operationer. Endvidere udtalte NATO's generalsekretær, Jens Stoltenberg, i august 2019, at NATO ikke er begrænset til at svare med cybermidler, når alliancen bliver angrebet i cyberspace.[46] Det er i den sammenhæng vigtigt at understrege, at NATO er en defensiv organisation. NATO fokuserer først og fremmest på forsvar af egne netværk og systemer. Dernæst på det kollektive forsvar. Det er imidlertid uklart, hvad der vil kunne udløse et kollektivt NATO-svar på et cyberangreb. Ved ikke at sætte klare grænser for, hvornår et cyber-

angreb vil udløse artikel 5, så fastholder NATO en tvetydig afskrækkelsespolitik. En fordel ved den tvetydige tilgang er, at NATO's modstandere således ikke bevidst kan foretage cyberoperationer under den af NATO fastsatte grænse. Desuden vil modstandere konstant skulle overveje, hvorvidt de er i fare for at overskride den usynlige grænse. Omvendt kan den samme tvetydighed føre til, at modstandere udnytter gråzonen og tester alliancens beslutningsdygtighed og handleevne.

NATO som organisation har fortsat ingen officielle planer om at udvikle selvstændige offensive cybermidler.[47] Overordnet set kan NATO's potentielle anvendelse af medlemsstaternes offensive cybermidler beskrives som et reaktivt redskab, hvis anvendelse er styret af de enkelte medlemslande, der lover effekt, men ikke deler kompetencer. Det er derfor tvivlsomt, at NATO kan opnå alliancens sædvanlige grad af militær koordination, når de tophemmelige cybereffekter leveres nationalt.[48] Ovenstående medfører, at NATO har svært ved at signalere cyberslagkraft, hvilket ellers kunne bakke den tvetydige afskrækkelsespolitik op. NATO er altså udfordret af cybergråzonekonflikter, der udspiller sig mellem det defensive, efterretningsmæssige og offensive, hvorfor traditionelle afskrækkelsesstrategier og langvarigt operationelt strategiarbejde har vist sig ikke at være tilstrækkeligt.

3.3 Naming, blaming og shaming

Danmark og en række vestlige allierede har reageret på den stigende anvendelse af offensive cyberoperationer ved tiltagende at benytte offentlig "naming, blaming og shaming" som politisk svar på skadelige cyberaktiviteter. Vestlige liberale demokratier har traditionelt været tilbageholdende med offentligt at henføre og tilskrive cyberangreb til lande og regeringer. Grundet tekniske og efterretningsmæssige årsager er det da også notorisk vanskeligt med sikkerhed at udpege specifikke offensive cyberaktører.[49] Desuden spiller politiske, diplomatiske og juridiske overvejelser ind, især når et land eller en regering udpeges som aggressor. Usikkerheden til trods er vestlige liberale demokratier over de senere år blevet markant mindre tilbageholdende, når det gælder offentlige udmeldinger og tilskrivninger af konkrete offensive cyberoperationer.

Tekstboks 4:
Naming, blaming og shaming

> Naming, blaming og shaming anvendes ofte i internationale sammenhænge, når et land offentligt ønsker at udtrykke misfornøjelse med en navngiven persons, en navngiven gruppes eller et navngivent lands opførsel. Målet med naming, blaming og shaming er f.eks. at fremme overholdelsen af internationale normer og retlige forpligtelser.

USA og Storbritannien anklagede i 2017 Nordkorea og den statssponsorerede hackergruppe Lazarus for at stå bag ransomwareangrebet WannaCry.[50] I 2018 stod Storbritannien, USA, Australien og Danmark offentligt frem og udpegede Rusland og den russiske regering for at stå bag cyberangrebet NotPetya.[51] Et angreb, der ifølge den amerikanske regerings beregninger kostede ca. 60 mia. kroner globalt, herunder op mod 2 mia. kroner for Mærsk.[52] I 2018 anklagede Storbritannien og Holland Rusland for at have forsøgt at hacke sig ind i den internationale organisation, der arbejder for forbud mod kemiske våben (OPCW).[53] OPCW, der er placeret i Haag, efterforsker mulige angreb med kemiske våben, heriblandt sagen om forgiftningen af den afhoppede russiske spion Sergei Skripal samt talrige hændelser i Syrien. Endvidere har både USA, Storbritannien, Danmark og en række andre lande anklaget Kina for at stå bag omfattende industrispionage og politisk spionage samt Rusland for at stå bag desinformationskampagner og indblanding i valg. Det amerikanske justitsministerie har ydermere anklaget specifikke personer fra Iran[54], Nordkorea[55], Kina[56] og Rusland[57]for at stå bag hackerangreb mod USA.

På EU-niveau blev det i 2017 besluttet at godkende udviklingen af en fælles diplomatisk EU-responsramme (Cyber Diplomatic Toolbox, CDT[58]) med henblik på at styrke EU's muligheder for at imødegå ondsindede cyberaktiviteter rettet mod europæiske mål. Den primære hensigt bag CDT'en – der blandt andet omfatter muligheder for at tilskrive angreb og indføre sanktioner – er at udvikle og styrke unionens og medlemslandenes signalgivende og reaktive kapacitet med det formål at påvirke potentielle aggressorers opførsel. En markant udfordring har imidlertid været at omsætte CDT'en til et anvendeligt og effektivt udenrigspolitisk instrument. Det kom EU i maj 2019 et skridt nærmere, da Det Europæiske Råd etablerede et framework[59], der for første gang giver EU mulighed for at indføre målrettede, restriktive sanktioner mod individer og institutioner, som har udført eller planlagt skadelige cyberaktiviteter mod EU og dets medlemsstater. Vi har dog fortsat til gode at se, hvordan instrumentet vil blive brugt i praksis.

3.4 Konklusion: Øget friktion i gråzonen

Skiftet i den geopolitiske kontekst og trusselsbilledet, herunder særligt den kontinuerlige udførelse af skadelige cyberoperationer under tærsklen for væbnet konflikt, bliver anerkendt af både EU, NATO og USA. En reaktion herpå har bredt set været at øge den politiske "naming, blaming og shaming" i forbindelse med fjendtlige cyberoperationer. Desuden har NATO og EU de senere år taget afgørende skridt for at styrke deres arbejde med at imødegå cyberoperationer. Det er dog især USA's ændrede strategiske kurs, der har vakt opsigt. Kursændringen mod kontinuerligt og vedholdende engagement samt fremadrettet forsvar i gråzonen under tærsklen for krig samt Trump-administrationens lempelse af principperne for anvendelsen af offensive cybermidler afspejler et strategisk og operationelt skifte. Hvad dette skifte konkret kommer til at indebære politisk og militært, er fortsat til debat[60], men udviklingen tyder på en mere frembrusende og dristig amerikansk tilgang, hvilket med stor sandsynlighed vil medføre øget friktion i cybergråzonen. I lyset af rapportens formål er et væsentligt spørgsmål, hvordan USA's strategiske skifte influerer på dets allierede. De øvrige NATO-allierede står over for de samme geopolitiske forandringer og ændringer i cybertrusselsbilledet. Spørgsmålet er, om det har ført til lignende ræsonnementer angående nødvendigheden af øget cybertilstedeværelse og cyberaktivitet under tærsklen for krig. Et spørgsmål, som rapporten tager med ind i det følgende kapitel, hvor synet på offensiv cybermagt i Holland, Norge og Frankrig bliver analyseret.

4 Offensive cybermidler i Holland, Norge og Frankrig

Dette kapitel leverer en sammenlignende analyse af, hvordan man i Holland, Norge og Frankrig har diskuteret, opbygget og anvendt offensive cybermidler. De tre lande repræsenterer et udsnit af NATO-lande med forskellige militære kapaciteter samt forskellige tilgange til CNO-arbejdet. Kapitlets første afsnit analyserer de politiske og militærstrategiske overvejelser, der ligger til grund for udvikling og anvendelse af offensive cybermidler i Holland, Norge og Frankrig. Kapitlets andet afsnit zoomer ind på de konkrete typer af organisering og ansvarsfordeling, som Holland, Norge og Frankrig opererer med, når det kommer til udvikling og anvendelse af offensive cybermidler. Slutteligt bliver de tre landes tilgange opsummeret og sammenlignet. Analysen bidrager til at understøtte fremtidige beslutninger om den politisk-strategiske, juridiske og organisatoriske udvikling af – samt offentlige debat om – Danmarks offensive cyberforsvar. Kapitlet danner dermed grundlag for præsentationen af anbefalinger i rapportens konkluderende kapitel.

4.1 Det politisk-strategiske grundlag

Den følgende del af analysen zoomer ind på de hollandske, norske og franske politiske og militærstrategiske debatter om og forankringspunkter for anvendelse af offensive cybermidler. Udviklingen af offensive cybermidler er i alle tre lande blevet set som en tidssvarende udvikling af nødvendig militær kapacitet, der primært har skullet understøtte øvrige militære operationer i en krigssituation. Den dominerende politisk-strategiske ramme for udviklingen af offensive cybermidler har således været væbnet konflikt og krig. Det understreges af, at både Holland og Frankrig har udgivet selvstændige militære cyberdoktriner. Alle tre lande anerkender, at den rent militære ramme i dag udfordres af, at langt de fleste skadelige cyberoperationer sker under grænsen for krig. Holland og Frankrig har givet udtryk for, at de anvender offensive cyberforsvarsmidler til at imødegå angreb under tærsklen for krig, mens det er mere uklart, hvorvidt nordmændene gør det. Ingen af landene har fremlagt klare politiske eller strategiske mål for anvendelsen af offensive cyberforsvarsmidler som en del af gråzonekonflikter, som vi har set amerikanerne gøre det.

Holland: Afskrækkelse og normdannelse

Holland er internationalt anerkendt for tidligt at have anlagt en bredspektret strategisk tilgang til landets arbejde med cybersikkerhed. Allerede i 2011 fremlagde den hollandske regering landets første nationale cyberstrategi. Strategien tydeliggjorde rolle- og ansvarsfordelingen mellem en række hollandske myndigheder. Endvidere dannede den grundlag for etableringen af en tværgående statslig cyberarkitektur. Siden har Holland haft markant fokus på at udvikle og modne landets håndtering af cybersikkerhed. Fokus er med tiden skiftet fra at øge bevidstheden til at øge kapaciteten, skiftet fra offentlig-private partnerskaber til offentlig-privat deltagelse samt skiftet fra at skabe grundlæggende strukturer til at skabe yderligere netværk og koordination.[61]

Sideløbende med de brede nationale cybersikkerhedsstrategier har Holland fremlagt en række cyberforsvarsstrategier. Op til præsentationen af landets første cyberforsvarsstrategi udtalte den daværende forsvarsminister Hans Hillen i 2011, at de hollandske væbnede styrker over de kommende år ville udvikle offensive cybermider. Hillen fremhævede specifikt behovet for at opnå

kendskab til de digitale fjender via efterretninger samt behovet for at besidde gode digitale våbensystemer. Med Hillens egne ord: "We have to be able to slam down on our opponent. Also in the digital sense."[62] Kort efter præsenterede Holland landets første cyberforsvarsstrategi. Strategien anerkendte cyberspace som det femte domæne for krigsførelse. Samtidig slog den fast, at Holland skulle udvikle offensive cyberkapaciteter, der på sigt skulle blive en integreret del af de hollandske væbnede styrkers samlede militære kapacitet, da evnen til at udføre offensive cyberoperationer blev bedømt til at være af afgørende betydning for at sikre de væbnede styrkers fremtidige effektivitet.[63] På dette tidspunkt var det internationalt et særsyn, at lande eksplicit fremhævede, at de udviklede offensive cybermidler samt med hvilket formål.[64] Hollænderne har siden fastholdt en offensiv og afskrækkende cyberpositur.[65]

I 2014 oversendte den hollandske forsvarsminister et brev til parlamentet, hvor han påpegede, at adskillelsen mellem det militære og det efterretningsmæssige bliver udhulet i det digitale domæne. I brevet fremhævede ministeren, at det i forbindelse med udviklingen af offensive, defensive og efterretningsbaserede cyberkapaciteter er vigtigt, at der tages hensyn til sammenhængen mellem dem. Forsvarsministeren betonede særligt, at offensive og efterretningsbaserede cybermidler hviler på sammenlignelige metoder og teknikker, men anvendes med forskellige formål og under forskellige lovgivninger, hvorfor udviklingen af offensive cybermidler kræver intensivt samarbejde mellem militæret og den militære efterretnings- og sikkerhedstjeneste.[66] Den opdaterede hollandske cyberforsvarsstrategi fra 2015 fremhæver samstemmende, at Holland skal være i stand til at udføre militære operationer i det digitale domæne gennem anvendelse af både defensive, offensive og efterretningsbaserede cybermidler.[67] Desuden fremlagde den hollandske regering en redegørelse for, hvad den forventede af de forskellige cyberkapaciteter, herunder deres strategiske og militære formål.[68]

I den seneste hollandske cybersikkerhedsstrategi fra 2018 betones vigtigheden af udvikling og besiddelse af offensive cybermidler fortsat. Strategien slår fast, at Holland vil øge de væbnede styrkers offensive cybermidler med det formål at afskrække potentielle fjender.[69] I det hollandske forsvarsministeries cyberforsvarsstrategi, der ligeledes er fra 2018, bliver det understreget, at forværringen af den internationale sikkerhedssituation samt skærpelsen af geopolitiske interessekonflikter øger betydningen af digital sikkerhed. Det hollandske forsvar skal derfor "have flere muligheder for at forstyrre eller afskrække digitale angreb" samt kunne "implementere målrettede digitale midler for at opnå og bevare dominans under militære operationer".[70]

Hollænderne fremhæver ligeledes, at flere af landets allierede i stigende grad benytter sig af aktivt cyberforsvar, hvilket også det hollandske forsvarsministerie anser som en nødvendig prioritet. Det bliver dog ikke uddybet, hvornår eller hvordan de forstyrrende aktive modforanstaltninger vil og kan blive anvendt. Holland ønsker endvidere stærkere internationale aftaler på cybersikkerhedsområdet. Status quo bliver anset som uholdbar, hvorfor Holland vil anlægge en mere offensiv linje for tilskrivning af cyberangreb, der kan være med til at understøtte en international normudvikling samt gøre Holland mindre attraktivt som mål for cyberangreb.[71] Den hollandske åbenhed vedrørende landets udvikling og anvendelse af offensive cybermidler, herunder øget tilskrivning af angreb, hviler på to politiske og strategiske mål. Afskrækkelse er det ene. Det andet mål er på sigt at styrke den gensidige tillid, mindske risikoen for våbenkapløb og eskalation samt skabe yderligere international stabilitet og internationale cybernormer.[72]

Samlet set har hollænderne været konsistente, hvad angår landets politiske og militærstrategiske udmeldinger vedrørende målsætninger for udvikling og anvendelse af offensive cybermidler. Man har fra hollandsk side lagt vægt på militærets involvering i både defensive og offensive cybertiltag. Et

andet centralt træk ved den hollandske tilgang til cyberforsvar er landets opbakning til offentlig uni- og multilateral tilskrivning af skadelige cyberoperationer samt et særligt fokus på udvikling af internationale normer for cybertilskrivning[73]. Desuden påpeger den første hollandske militære cyberdoktrin fra 2019 nødvendigheden af koordination mellem efterretningstjenester og cyberkommando, da efterretningsoperationer og militære operationer ofte vil ramme samme mål. Desuden slår doktrinen fast, at forskellen på anvendelse af offensive cybermidler henholdsvis i krig og til spionage vedrører formålet og den ønskede effekt. Doktrinen fastslår, at de to former for anvendelse af cybermidler sameksisterer og overlapper, men de skal ifølge hollænderne ses som komplementære og ikke konkurrerende kapabiliteter.

Tekstboks 5:
Eksempel - Holland

Holland viser cybermuskler

I 2018 afslørede hollandske medier, at den hollandske efterretningstjeneste har givet FBI afgørende oplysninger om russisk indblanding i det amerikanske valg. Den hollandske efterretningstjeneste havde i årevis haft adgang til den berygtede russiske hackergruppe Cozy Bears netværk. Den hollandske premierminister Mark Rutte kommenterede efterfølgende på sagen. Han gik ikke nærmere i detaljer, men udtalte til medierne, at han var enormt stolt over efterretningsenhedens succes. Det harmonerer med den officielle hollandske tilgang til at modvirke konflikt i cyberspace gennem udvikling og potentiel anvendelse af offensive cybermidler. Hollænderne er åbne omkring, at de besidder både generiske og avancerede og målrettede offensive cybermidler som en forsvarsmekanisme. Hollænderne har dog ikke officielt anvendt deres offensive cybermidler i forbindelse med en større militæroperation.

Det er dog ikke beskrevet, hvordan de komplementerer hinanden i praksis. I forlængelse heraf er det uklart, hvad de politisk-strategiske mål og juridiske rammer er for det aktive og fremadrettede hollandske cyberforsvar i gråzonen. Det vil fremgå af de følgende afsnit, at denne uklarhed også er at finde i de norske og franske tilfælde.

Tabel 1: De vigtigste hollandske cyberdokumenter

År	Titel
2019	The Netherlands Armed Forces Doctrin for Military Cyberspace Operations
2018	Defense Cyber Strategy III
2018	Integrated International Security Strategy
2017	International Cyber Strategy
2015	Defense Cyber Strategy II
2014	National Cyber Security Strategy II
2012	Defense Cyber Strategy
2011	National Cyber security Strategy

Norge: Tilbageholdende og tilstedeværende

I 2019 lancerede Norge en ny strategi for digital sikkerhed. Strategien slår fast, at digitale angreb udgør en trussel mod den norske nationale sikkerhed, samt at digitale midler i stigende grad er blevet en integreret del af militære operationer. Strategien har dog udelukkende et defensivt sigte, hvilket går i spænd med de tre forudgående norske strategier for digital sikkerhed, der blev publiceret i henholdsvis 2003, 2007 og 2012. Norge var et af de første lande i verden til at præsentere en national digital sikkerhedsstrategi. Nordmændene har herefter prioriteret en helhedsorienteret tilgang til cybersikkerhed med fokus på at styrke koordinering, videndeling og uddannelse på tværs af samfundet gennem prioritering af f.eks. offentlig-private partnerskaber, civilmilitære relationer og fællesoffentlige standarder for it- og informationssikkerhed.

I den norske langtidsplan for Forsvaret fra 2012 bliver det fremhævet, at "utvikling av cyberforsvaret: Angrep i det digitale rom, også benevnt "cyberspace", er en av de raskest voksende truslene i vår tid. Forsvarssektoren skal utvikle sin evne til å møte trusler i det digitale rom. Arbeidet med forebyggende informasjonssikkerhet skal styrkes."[74] Hovedvægten i planen er lagt på at styrke modstandsdygtighed og robusthed bredt set, men det bliver understreget, at "militære operasjoner i det digitale rom har både beskyttende, etterretningsmessige og offensive siktemål. Dette har blitt en tilleggsdimensjon ved militære operasjoner og dermed et nytt krigføringsområde hvor både evnen til defensive og offensive operasjoner vil kunne være avgjørende i fremtidige konflikter."[75] Forholdet mellem det defensive, efterretningsmæssige og militære bliver dog ikke specificeret.

Nordmændene præsenterede en ny langtidsplan for forsvaret i 2016[76]. Af den fremgår det, at man skal styrke evnen til at detektere cyberangreb samt videreudvikle relevante modtiltag: "Hele forsvarssektoren må være i stand til å iverksette forebyggende sikkerhetstiltak, og evnen til å avdekke cyberangrep skal bedres. Evnen til å håndtere slike angrep, ved å iverksette relevante mottiltak, skal videreutvikles."[77] Vender man blikket mod modtiltagene, så er forsvarsplanen for 2016 bemærkelsesværdig tavs, hvad angår offensive cybermidler. Det eneste, der omtales, er, at efterretningstjenesten skal kunne indsamle efterretninger inden for cyberdomænet.[78] Derudover har forsvarsplanen fokus på videreudvikling af samarbejdet og koordineringen mellem Norges to efterretningstjenester og den nationale sikkerhedsmyndighed.

Som optakt til at den norske regering i 2020 skal fremlægge en ny langtidsplan for forsvaret, præsenterede den norske forsvarschef i oktober 2019 sine fagmilitære råd og anbefalinger til planen. Forsvarschefen fremhæver, i tråd med gråzoneudfordringen og det ændrede trusselsbillede, at det i dag kan være vanskeligt at definere konfliktsituationer, afdække, hvem som står bag aggressioner, samt træffe effektive foranstaltninger og modsvar.[79] Desuden fremhæver forsvarschefen, at evnen til at levere cyberoperationer skal styrkes. Det norske forsvar bør derfor "videreutvikle evnen til å planlegge og gjennomføre cyberoperasjoner for effekt, situasjonsforståelse og beskyttelse. Cyberoperasjoner, herunder effektoperasjoner, må integreres som en naturlig del av fellesoperasjoner på lik linje med øvrige domener."[80] Det gentages i budgettet for forsvaret for 2018-2019, hvor det fremhæves, at forsvaret skal "forbetre dei førebyggande tryggingstiltaka mot cyberåtak, vidareutvikle evna til tidleg å avdekke slike åtak og betre evna til å sette i verk relevante mottiltak".[81] I hvilket omfang disse modtiltag indebærer aktivt forsvar i gråzonen, er ikke specificeret. Det norske forsvarsministerie har dog udtalt følgende til denne rapport:

> "Forsvarsdepartementet vil vidareutvikle og styrke evna til å handtere cyberdomenet i militære operasjonar, basert på gjeldande ansvar og organisering. Handtering inneber offensive og defensive åtgjerder på fleire nivå,

og herunder også å avdekke og motverke hybride trugslar i cyberdomenet."

Norges formål med udvikling og anvendelse af offensive cybermidler "er å ha nødvendig handlefrihet i cyberdomenet for å understøtte oppgaveløsing hjemme og ute, samt detektere og motvirke ytre trusler mot Norge og norske interesser i kraft av sektorens nasjonale utenlandsetterretningsoppdrag". Begreber som afskrækkelse og tilskrivelse er en del af det norske politiske og militærstrategiske vokabular, men de bliver hverken anvendt systematisk eller udspecificeret. Den norske politiske og strategiske tilgang til udvikling og anvendelse af offensive cybermidler kan bedst beskrives som tilbageholdende, hvilket går i spænd med det overordnede norske cyberforsvarsfokus på samfundsmæssig modstandsdygtighed og resiliens. Den norske regerings seneste udmeldinger peger imidlertid i retning af et øget fokus på aktivt cyberforsvar i gråzonen, men det er ikke klart, hvorvidt nordmændene praktiserer offensivt cyberforsvar i gråzonen.

Tabel 2: De vigtigste norske cyberdokumenter

År	Titel
2019	Forsvarschefens fagmilitære råd
2019	National digitial sikkerhedsstrategi
2018	Forslag til lov om efterretningstjenesten
2016	Langtidsplan for forsvaret
2012	Langtidsplan for forsvaret
2012	National digitial sikkerhedsstrategi
2007	National digitial sikkerhedsstrategi
2003	National digitial sikkerhedsstrategi

Frankrig: Selvstændig og synlig

Frankrig har de seneste år fremlagt en stribe dokumenter, der udlægger de franske strategiske og militære interesser og prioriteter i cyberspace samt konceptualiserer den franske tilgang til cybersikkerhed og cyberforsvar. Det er en bemærkelsesværdig udvikling, der primært er blevet opfattet som et fransk politisk-strategisk ønske om at sende en klar besked til både allierede og modstandere, der fastslår, at Frankrig er en væsentlig cybermagt for hvem strategisk autonomi er afgørende. En cybermagt, som har kapaciteten til at identificere og attribuere angreb samt om nødvendigt viljen til at anvende offensive cybervåben.[82] En selvstændig og styrket fransk cyberpositur har således afteg-net sig de senere år.

I den strategiske gennemgang af forsvars- og sikkerhedspolitikken fra 2017 gjorde franskmændene det klart, at den øgede digitalisering skaber nye sårbarheder, hvorfor styrkelse af digital operationel overlegenhed samt digital suverænitet er blevet endnu vigtigere.[83] I 2018 præsenterede nu eksgeneral-

sekretær for forsvar og national sikkerhed Louis Gautier en strategisk gennemgang af det franske cyberforsvar. Et skelsættende dokument, som Gautier sammenlignede med etableringen af den franske nukleare doktrin i 1972, hvilket understreger betydningen af dokumentet, der i dag anses som en milepæl i arbejdet med fransk cyberforsvar.[84] Dokumentet, der beskriver og udvikler den franske tilgang til cyberforsvar, tager udgangspunkt i en stribe tidligere beskrevne franske positioner på cyberforsvarsområdet.[85] Overordnet set bekræfter den strategiske gennemgang af cyberforsvaret det franske princip om klar adskillelse af defensive og offensive cyberkapaciteter og -operationer.

Desuden er der et markant fokus på applikationen af folkeret i cyberspace i den franske strategiske gennemgang. Det bliver blandt andet understreget, at "Frankrig har en klar, specifik og præcis vision om anvendelsen af folkeret i cyberspace".[86] Franskmændenes prioritering af at fremlægge et så markant bud på en fortolkning af, hvordan eksisterende international lov finder anvendelse i cyberspace skyldes givetvis en kombination af følgende: 1) Den franske juridiske tradition er stærkt bundet til skreven ret frem for sædvaneret, 2) Frankrig har længe opereret med en klar opdeling mellem cyberforsvar og cyberangreb, og 3) franskmændene har ikke for vane at benytte afskrækkelsesbegrebet i forbindelse med cyberkapaciteter, men har traditionelt haft fokus på at undgå eskalation.[87] Udfordringen for franskmændene er, at disse udgangspunkter bliver udfordret af den tiltagende skadelige cyberaktivitet i gråzonen mellem krig og fred.

I januar 2019 præsenterede den franske forsvarsminister Florence Parly landets nyes militære cyberstrategi. Den består af to separate dokumenter, der fokuserer på henholdsvis cyberforsvar og cyberangreb. Dokumenterne udgør tilsammen den franske militære cyberdoktrin.[88] I forbindelse med offentliggørelsen af doktrinen udtalte Parly, at "cyberkrigen er startet, og Frankrig skal være klar til at kæmpe den".[89] Hun understregede, at Frankrig som svar på cybertrusler ikke er bange for at anvende offensive cybervåben, hvilket understreger den ændrede franske cyberpositur, hvor afskrækkelse fylder mere. Ved den officielle indvielse af den franske cyberkommandos nye domicil i Rennes i oktober 2019 fulgte forsvarsminister Parly op ved at fremhæve, at Frankrig i 2025 skal have 4.000 cyberkrigere, hvilket er 1.000 flere end i dag.[90] Parly afsluttede talen med at fremhæve, at verden i dag ved, at den kan regne med Frankrig som en cybermagt.

Den offensive cyberdoktrin er den første offentliggjorte ramme for det franske militærs anvendelse af offensive cyberoperationer i tilfælde af væbnet konflikt og krig. I doktrinen understreges vigtigheden af, at offensive og ødelæggende militære cyberoperationer udspringer af en politisk beslutning. Den strategiske ramme for anvendelsen af offensive militære cybermidler synes således operationelt afgrænset til krig og væbnet konflikt. Iagttagere har dog påpeget, at Parly i sin tale ved præsentationen af strategien indirekte sagde, at en betydelig del af de franske offensive cyberoperationer bliver foretaget af efterretningstjenesten (Direction Générale de la Sécurité Extérieure (DGSE)), der opererer uden for den militære cyberstrategi.[91] Hvor de strategiske og operationelle grænser går mellem de to typer anvendelse af offensive cybermidler, er dog ikke beskrevet. Offentliggørelsen af den offensive doktrin samt Parlys taler signalerer, at Frankrig styrker sine militære cyberkapaciteter, men siger ikke noget om, hvordan landet i øvrigt forholder sig strategisk og operationelt til anvendelse af offensive cybermidler under tærsklen for krig som en del af et offensivt forsvar.

Den defensive del af cyberdoktrinen har et stærkt fokus på at sikre Frankrigs funktionsdygtighed og selvstændighed i tilfælde af krise og konflikt. Det ligger i forlængelse af doktrinens generelle fokus på at sikre fransk strategisk autonomi og handlemulighed. Det medfører, at forsvar for franskmændene ikke alene handler om at styrke robusthed og resiliens, men også indeholder elementer af offensivt forsvar. Doktrinen siger, at det defensive arbejde så-

ledes dækker detektion og reaktion i og uden for de netværk, der skal forsvares. Samlet afslører doktrinen en fransk forståelse af cyberforsvar, der tilsiger en aktiv cyberforsvarsposition i et miljø præget af permanent konfrontation og friktion i gråzonen under tærsklen for krig. Sammenfattende fokuserer den offensive del af cyberdoktrinen på at skabe effekt hos en modstander under grænsen for krig, mens den defensive del sigter mod aktivt at bevare fransk handlefrihed i landets stræben efter strategisk autonomi, der er et overordnet princip i Frankrigs militære cyberdoktrin. Dermed minder det franske politisk-strategiske udgangspunkt om den amerikanske ide om vedvarende engagement.

Den franske cyberpositur er blevet skærpet de seneste år. Den ændrede franske cyberforsvarspositionering er sket med det formål at sætte Frankrig på det internationale cyberlandkort. Ønsket er, at Frankrig skal fremstå som en betydende og magtfuld spiller, der ikke vil undlade at fremme sine unikke visioner og interesser i det digitale rum. Et øget fokus på udvikling og anvendelse af militære offensive cybermidler træder klart frem. Det er dog endnu uklart, hvorvidt et operationelt fransk kursskifte er under opsejling. Men franskmændene holder en dør på klem for, at offensive cybermidler kan og vil blive anvendt til andet end spionage, herunder offensivt forsvar i gråzonekonflikter, men det er usikkert, hvad de konkrete strategiske, juridiske og operationelle rammer er, og hvor grænsen bliver trukket mellem de forskellige dele af det franske cyberforsvar.

Tabel 3: De vigtigste franske cyberdokumenter

År	Titel
2019	Politique ministérielle de lutte informatique défensive
2019	Éléments publics de doctrine militaire de lutte informatique offensive
2018	Revue stratégique de cyberdéfense
2017	Defence and National Security Strategic Review
2017	Stratégie de lutte contre les cybermenaces
2015	Stratégie nationale pour la sécurité du numérique'
2014	Pacte Défense Cyber
2013	Livre Blanc sur la Défense et Sécurité nationale'
2011	Défense et sécurité des systèmes d'information – stratégie de la France
2008	Livre Blanc sur la Défense et Sécurité nationale

4.2 Organisering og ansvarsfordeling

Den følgende del af analysen zoomer ind på henholdsvis den hollandske, den norske og den franske organisering og ansvarsfordeling i forbindelse med udvikling og anvendelse af offensive cybermidler. Der er forskel på, i hvilket omfang de tre lande offentligt anerkender besiddelse og anvendelse af offensive cybermidler, herunder hvilke militære- og efterretningsinstitutioner der anvender hvilke typer af cybermidler samt til hvilke formål. Analysens første del gjorde klart, at ingen af de tre lande har fremlagt entydige politisk-strategiske mål og rammer for anvendelsen af offensive cybermidler som en del af gråzonekonflikter. Analysens anden del viser, at de tre lande organiserer anvendelsen af offensive cybermidler forskelligt. Fra en hollandsk samarbejdsmodel over en norsk enhedsmodel til en skarp fransk opdelingsmodel.

Holland: Adskillelse og fleksibilitet

Mange statslige institutioner er involveret i arbejdet med at styrke den overordnede nationale hollandske cybersikkerhed. Det hollandske institutionelle cybersikkerhedslandskab er blevet karakteriseret som et deltagerstyret netværk, der forbinder partnere på et grundlag af tillid og lighed. Cyberkapaciteter og cybersikkerhedsansvar er således spredt ud på forskellige organisationer med hver med deres formål, opgaver og kultur.[92] Især inden for forsvarsministeriets arbejdsområde er der en markant administrativ og juridisk fordeling af ansvar mellem en række institutioner.

De to hollandske efterretnings- og sikkerhedstjenester – den generelle og den militære – har samlet størstedelen af deres defensive cyberkapacitet i Joint Sigint and Cyber Unit (JSCU). JSCU samler dermed kryptologer og hackere på tværs af forsvarsministeriets samt justits- og sikkerhedsministeriets områder. Enhedens primære arbejdsopgaver er signalindhentning samt tilvejebringelse af efterretninger gennem cyberoperationer. JSCU udgør således hjørnestenen i det hollandske forsvar mod avancerede statssponsorerede cyberangreb (såkaldte advanced persistent threat-angreb) rettet mod ministerier, infrastrukturudbydere og multinationale selskaber. JSCU's cyberaktiviteter må ikke forstyrre, nægte, forringe eller ødelægge. De må udelukkende indsamle oplysninger.

Når det kommer til offensive cyberoperationer, så opererer Holland desuden med en klar organisatorisk separation mellem den militære sikkerheds- og efterretningstjeneste (MIDV) og cyberforsvarskommandoen (DCC) – og således også mellem CNE og CNA. MIDV og DCC opererer under forskellige politiske og juridiske mandater. DCC, der er placeret under den øverstbefalende for de hollandske væbnede styrker, blev officielt oprettet i juni 2015. Enheden blev fuldt operationel ved årsskiftet 2016-2017. DCC's mission er at udvikle og gennemføre offensive cyberoperationer til støtte for militære operationer. Det er kun DCC, der må udøve decideret ødelæggende angreb. DCC opererer kun i tilfælde af krig og væbnet konflikt. Det er blevet fremhævet, at DCC primært vil kunne fungere som koordinator og operationelt knudepunkt, når det kommer til anvendelse af hollandske offensive cybermidler i væbnet konflikt, da DCC ikke besidder hverken den nødvendige ekspertise eller den nødvendige infrastruktur til at udføre disse cyberaktiviteter. MIVD og JSCU er derfor uundværlige samarbejdspartnere[93], når det gælder muligheden for cyberkrigsførelse.[94] Det er imidlertid uklart, hvordan de forskellige institutioner og deres ressourcer konkret vil blive bragt i spil i tilfælde af et ødelæggende cyberangreb mod Holland. Ydermere er DDC's mandat samt de beslutningsprocesser, som omgiver organisationen, afhængige af de love og procedurer, der gælder for krig og indsættelse af væbnede styrker. Ved anvendelse af offensive midler skal den hollandske cyberforsvarskommando fremlægge et såkaldt artikel 100-brev for den hollandske regering, hvor den anmoder om tilladelse.[95] Dette er grundlæggende forskelligt fra efterretningstjenesternes

juridiske mandat og tillader f.eks. ikke indgribende cyberoperationer mod potentielle modstandere i gråzonen under tærsklen for krig.

Den hollandske militære efterretningstjeneste opererer under civilt mandat. Som en del af efterretningsfællesskabet – der skal forblive objektivt og frit for politisk pres – er både MIVD og JSCU placeret under generalsekretæren for forsvarsministeriet, der er den øverste embedsmand i det hollandske forsvarsministerie (for JSCU delt med den tilsvarende embedsmand i indenrigsministeriet) og ikke den militære øverstbefalende. Det betyder, at det ikke er forsvarschefen, der er ansvarlig for og har bestemmelsesret med hensyn til, hvad efterretningstjenesten foretager sig. MIDV opererer på grundlag af lovgivningen for efterretningstjenesterne, der med stor detaljeringsgrad udspecificerer, hvilke typer af operationer som efterretningstjenesterne må foretage. Det er afgørende for det hollandske efterretningsmandat, at man forestår modoperationer inden for lovgrundlaget.[96] Der skal indhentes tilladelse hertil hos generalsekretæren for forsvarsministeriet. Afgørelsen vil blandt andet bero på en bedømmelse af kravet om nødvendighed og proportionalitet.

To hollandske tilsynsmyndigheder er involveret i disse afgørelser. Den ene (TIB-IVD) giver en juridisk vurdering af efterretningsoperationer, før de iværksættes (ex ante), mens den anden og større tilsynsmyndighed (CTIVD) fører tilsyn efter udførelse af efterretningsoperationer (ex post). De specifikke strategiske, juridiske og operationelle rammer for det hollandske offensive cyberforsvar er ikke offentligt tilgængelige, men det er overvejende sandsynligt, at hollænderne udfører aktive modoperationer i gråzonen. Hvornår, hvordan og i hvilket omfang er imidlertid uklart.

Det er kendetegnende for den hollandske organisering af cyberforsvaret, at man på den ene side ønsker en klar adskillelse – organisatorisk, operationelt og juridisk – mellem den militære cyberkommando, der kan indsættes i tilfælde af væbnet konflikt og krig, og efterretningstjenesten, der udøver cyberspionage samt aktivt forsvar. Samtidig – og delvist i modstrid med den organisatorisk klare opdeling – betoner hollænderne stærkt behovet for samarbejde mellem cyberkommandoen og efterretningstjenesterne, da førstnævnte hverken besidder den tilstrækkelige tekniske ekspertise eller har foretaget det nødvendige langsigtede planlægningsarbejde, der oftest skal til for at kunne udføre ødelæggende cyberangreb. Som svar herpå har hollænderne intensiveret samarbejdet og koordinationen mellem enhederne, men hvordan dette konkret udspiller sig samt med hvilken effekt, er uklart. Endvidere er det ikke offentligt præciseret, hvilke aktive modforanstaltninger i gråzonen, som den hollandske militære efterretningstjeneste iværksætter.

Norge: Centralisering og synergi

Norges organisering af landets anvendelse af offensive cybermidler er institutionelt den mest centraliserede og gennemsigtige. Desuden er det den, der kommer tættest på den danske organisering. Det norske forsvarsministerie er forpligtet til at sikre informationssikkerhed inden for cyberdomænet, og cyberoperationer er en integreret del af ministeriets planlægnings-, styrings- og governanceprocesser[97]. Det norske forsvar oprettede i 2012 enheden Cyberforsvaret, som er en selvstændig enhed med ansvar for etablering, drift og beskyttelse af forsvarets it-systemer og kommunikationsinfrastruktur. Desuden er cyberforsvarsenheden ansvarlig for at etablere og opretholde handlemuligheder for forsvaret inden for cyberdomænet.

Den norske militære og civile udenrigsefterretningstjeneste (Etterretningstjenesten/E-tjenesten) er ansvarlig for den offensive del af det norske cyberforsvar. E-tjenesten er således ansvarlig for de cyberoperationer, der udgøres af både CNE og CNA. Endvidere er E-tjenesten også ansvarlig for koordinering af militære defensive cyberoperationer. Den norske regering har præsenteret et "Forslag til ny lov om Etterretningstjenesten", hvori det bliver fremhævet, at:

> "[e]tterretningstjenesten har det nasjonale ansvaret for å planlegge og gjennomføre offensive cyberoperasjoner, herunder cyberangrep (Computer Network Attack), samt koordinere mellem offensive og defensive cybertiltak i Forsvaret. Etterretningstjenesten har også ansvaret for å forestå etterretningsmessig attribusjon av utenlandske trusselaktører ved alvorlige cyberoperasjoner rettet mot Norge eller norske interesser."[98]

Lovforslaget fortsætter imidlertid med følgende sætning: "Rettslig sett faller disse oppgavene utenfor rammen av en lov som dreier seg om innhenting og behandling av informasjon, og legaliteten av handlingene må derfor vurderes konkret ut fra omstendighetene." Disse omstændigheder forholder hverken lovforslaget eller andre norske offentlige dokumenter sig konkret til.

I Norge er det således ikke en særskilt cyberenhed i forsvarskommandoen, der på vegne af forsvarschefen planlægger og gennemfører CNA. Nordmændene giver klart udtryk for, at man ikke agter at ændre på dette, da det vil være omkostningsdrivende og mindske den eksisterende synergieffekt:

> "Det er etter Forsvarsdepartementet si vurdering korkje naudsynt [hverken nødvendigt] eller ønskeleg å opprette ein sjølvstendig cyberkommando utanfor Etterretningstenesta. Det ville mellom anna føresett oppretting av dupliserande kapasitetar, og resultere i eit uklart skilje mellom offensive cyberoperasjoner i og utanfor militære operasjonar. Ein cyberkommandofunksjon utanfor Etterretningstenesta vil for Noreg difor vere ei uheldig og kostbar løysing."[99]

De konkrete operationelle skelnen mellem CNA, CNE og CND er dog fortsat omgrænset af hemmeligholdelse. Som det fremgår af et høringssvar fra det norske udenrigspolitiske institut (NUPI):

> "[...] gitt den høye graden av gradering rundt disse spørsmålene, kjenner vi ikke arbeidsdelingen mellom PST [Politiets Sikkerhetstjeneste], NSM [Nasjonal Sikkerhetsmyndighet] og Etterretningstjenesten her, men det kan være krevende å opprettholde konkrete og formelle skiller mellom innhenting, effektoperasjoner og sikringstiltak i det digitale rom."[100]

Senest har det norske forsvarsministerie meldt ud, at man i 2020 vil forbedre E-tjenestens evne til at håndtere cybertrusler, før hændelser indtræffer: "I 2020 vil regjeringen blant annet videreutvikle Etterretningstjenestens evne til å håndtere trusler før hendelser inntreffer. Samarbeidet og koordineringen mellom ovennevnte aktører i militære cyberoperasjoner skal styrkes, med utgangspunkt i et militært cyberoperasjonssenter i Etterretningstjenesten. Evnen og kompetansen til offensive cyberoperasjoner skal videreutvikles." Det giver associationer til fremadrettet forsvar, men det er endnu uvist, hvordan nordmændene agter at håndtere cybertrusler i gråzonen, før skadelige hændelser indtræffer. Det står dog klart, at kompetencen alene er hos E-tjenesten.

Den norske E-tjeneste har de seneste år fået tilført flere midler, er blevet yderligere professionaliseret og globalt orienteret og er blevet mere sofistikeret, hvad angår dens arbejdsmetoder. Samtidig hævdes det, at tilsynet med E-tjenesten (EOS-udvalget[101]) lider under utilstrækkelig kapacitet og ekspertise, hvilket er et parlamentarisk problem.[102] I 2018 fremlagde den norske regering et nyt lovforslag om E-tjenesten. Særligt E-tjenestens muligheder for at tilgå grænseoverskridende elektronisk kommunikation er blevet diskuteret intenst i Norge.[103] I forbindelse med fremsættelsen af lovforslaget har EOS-udvalget rettet skarp kritik mod den forringelse af deres mulighed for at føre tilsyn, som de mener, at lovforslaget vil medføre.[104]

Det fremgår af EOS-udvalgets seneste årsrapport for 2018, at tilsynet med E-tjenesten primært er fokuseret på at føre tilsyn med følgende: "Tjenestens tekniske informasjonsinnhenting. Tjenestens behandling av opplysninger i dens datasystemer. Tjenestens informasjonsutveksling med innenlandske og utenlandske samarbeidende tjenester. Saker av særlig viktighet eller prinsipiell karakter som er forelagt Forsvarsdepartementet (foreleggelsessaker) og interne godkjenningssaker."[105] Særligt de første punkter tilsiger, at tilsyn med anvendelsen af offensive cyberforsvarsmidler kan falde ind under EOS-udvalgets tilsynsområde.

Frankrig: Adskillelse og hemmeligholdelse

Det stærke franske adskillelsesprincip mellem offensive og defensive cybermidler og cyberaktører indebærer, at den dominerende franske cybersikkerhedsinstitution (ANSSI[106]), der er en civil myndighed med ansvar for at sikre Frankrig mod fjendtlige cyberoperationer, opererer på et strengt defensivt grundlag. Det betyder, at ANSSI hverken udvikler eller anvender offensive cyberkapaciteter. Tanken bag den klare opdeling er, at den styrker tilliden til ANSSI i den private sektor og dermed gør cybersikkerhedssamarbejde og -regulering lettere. ANSSI's betydning understreges af, at myndigheden er placeret direkte under generalsekretariatet for forsvar og national sikkerhed (SGDSN). SGDSN er et interministerielt organ placeret direkte under den franske premierminister, og SGDSN's overordnede opgave er at hjælpe premierministeren med at udforme og gennemføre sikkerheds- og forsvarspolitik.

I 2013 oprettede det franske forsvar en egentlig cyberforsvarskommando (COMCYBER), der har ansvaret for at beskytte forsvarets systemer samt at koordinere de væbnede styrkers anvendelse af cyberoperationer. I 2017 blev COMCYBER placeret direkte under forsvarschefen. COMCYBER er ansvarlig for beskyttelse af det franske forsvarsministerie og militær med undtagelse af udenrigsefterretningstjenesten (DGSE) samt den militære efterretningstjeneste (DRSD). Desuden er COMCYBER ansvarlig for at udvikle offensive cybermidler til brug i væbnet konflikt.

DGSE er den mandskabsmæssigt største franske efterretningstjeneste. DGSE har generelt bevaret en relativt stor autonomi i forhold til COMCYBER, hvilket understreger den særlige og yderst hemmelige aura, der omgærder DGSE.[107] I sin tale i januar 2019 indikerede forsvarsminister Parly som nævnt, at en betydelig del af Frankrigs offensive cyberoperationer bliver udført at DGSE. Meget tyder på, at DGSE er involveret i såvel offensive som defensive cyberoperationer i gråzonen, men det er uklart i hvilket omfang. Der er blevet spekuleret i, om den tvetydighed er et bevidst strategisk træk. I alle tilfælde understreger det udfordringerne med at trække klare organisatoriske og operationelle grænser, hvad angår anvendelsen af offensive cybermidler i gråzonen.

Det samlede franske efterretningslandskab har været igennem en markant reorganisering siden 2007 med bekæmpelse af terrorisme som primært fokus.[108] Samtidig er tilsynet med de franske efterretningstjenester blevet styrket, omend det er sket ud fra et svagere udgangspunkt end i Holland og Norge, da de franske efterretningstjenester traditionelt har haft en høj grad af selvstændighed. Tilsynet er blandt andet blevet styrket gennem oprettelse af et permanent efterretningsudvalg i det franske parlament[109] (la délégation parlementaire au renseignement – et fælles udvalg mellem Sénat og Assemblée Nationale).[110] I juli 2014 blev et nyt kontrolorgan – L'Inspection des services de renseignement – ("generel inspektion af efterretningstjenesterne") oprettet. Til trods for at efterretningsområdet i Frankrig således ikke længere udgør samme undtagelse fra sædvanlige liberale regler for parlamentarisk og administrativ kontrol med efterretningstjenester, så er det franske tilsyn forholdsvis svagt, når det kommer til efterretningstjenesterne, herunder deres udvikling og anvendelse af cyberforsvarsmidler under tærsklen for krig.[111]

4.3 Konklusion

De hollandske, norske og franske beslutninger om at udvikle offensiv militær cyberkapacitet ligger ca. ti år tilbage i tiden. Udviklingen af offensive cybermidler er i alle tre lande blevet set som en tidssvarende beslutning om at investere i nødvendig militær kapacitet, der primært har skullet understøtte andre militære operationer i en krigssituation. Den dominerende politisk-strategiske ramme for udviklingen af offensive cybermidler har således været væbnet konflikt og krig. Der er imidlertid forskel på, hvordan landene offentligt kommunikerer og signalerer om besiddelse og anvendelse af offensive cybermidler, herunder hvilke militære- og efterretningsinstitutioner der anvender hvilke typer af cybermidler samt til hvilke formål.

Holland har hele vejen igennem været relativt åben omkring landets ønske om at besidde afskrækkende offensive cybermidler. Desuden tyder analysen på, at hollænderne har mulighed for at anvende offensive cyberforsvarsmidler til at imødegå skadelige cyberhændelser under tærsklen for krig. Nordmændene har været mere tilbageholdende i deres udmeldinger, men det norske forsvarsministeries ønske om aktivt at udvikle landets offensive cybervåben yderligere samt imødegå hybride trusler inden for cyberdomænet kan indvarsle et strategiskifte. Frankrig har skarpslebet landets cyberpositur de senere år. Franskmændene har investeret markant i militære offensive cybermidler til brug i krigssituationer. Desuden peger analysen på, at franskmændene kan og vil anvende offensive cyberforsvarsmidler til andet end spionage, herunder offensivt forsvar under tærsklen for krig.

En af de centrale pointer i rapporten er, at cybertrusselsbilledet har ændret sig som følge af nye geopolitiske spændinger på den ene side og intensiveret anvendelse af cybermidler under tærsklen for krig på den anden side. Holland, Norge og Frankrig har ligeledes erkendt, at skadelige cyberoperationer i dag oftest befinder sig under tærsklen for krig. Det udfordrer ideen om at se anvendelsen af offensive cybermidler som et rent krigsanliggende, hvorfor også forholdet mellem militære og efterretningsmæssige cyberenheder påvirkes. Hverken Holland, Norge eller Frankrig har dog fremlagt klare politisk-strategiske mål eller organisatoriske tiltag, der beskriver rammerne for landenes anvendelse af offensive cybermidler under tærsklen for krig. Det er med til at hindre en oplyst offentlig debat om, hvordan vestlige demokratiske lande kan, bør og skal agere i den cybergråzonekonflikt, der i dag er normaltilstanden. Endvidere risikerer hemmeligholdelse og manglende offentlig debat at minimere chancen for international norm- og regelopbygning på området. På baggrund af rapportens analyse er det muligt at udlede tre forskellige tilgange til, hvordan anvendelsen af offensive cybermidler er organiseret. Fra en skarp *fransk opdelingsmodel* over en *hollandsk samarbejdsmodel* til en *norsk enhedsmodel*. Analysens resultater er opsamlet i tabel 4.

Den massive hemmeligholdelse, der omgærder udviklingen og anvendelsen af offensive cybermidler gør, at det ikke er muligt at konkludere entydigt på, hvordan og hvornår Holland, Norge og Frankrig skelner mellem CNA, CNE og CND. Den i kapitel I omtalte spænding mellem de tre består. I lyset heraf er det nødvendigt, at de danske politiske beslutningstagere og relevante myndigheder selv gør sig klart, hvorvidt og hvordan Danmark skal anvende CNO-kapaciteten til offensivt cyberforsvar i ikke-krigssituationer. Danmark kan blive foregangsland og standardsætter ved at have en offentlig og inkluderende debat om de politisk-strategiske mål samt juridiske og organisatoriske rammer og retningslinjer for anvendelsen af offensive cyberforsvarsmidler under tærsklen for krig.

Tabel 4. Sammenligning af CNO-governance i Frankrig, Holland og Norge

	Frankrig	Holland	Norge
Politisk-strategiske målsætninger for anvendelse af offensive cybermidler i militære konflikter	Ja	Ja	Delvist
Politisk-strategiske målsætninger for anvendelse af offensive cybermidler i gråzonekonflikter	Nej	Nej	Nej
Mulighed for at anvende af offensive cyberforsvarsmidler i gråzonekonflikter	Ja	Ja	Uklart
Centraliseret eller distribueret CNO-kapacitet	Distribueret	Distribueret	Centraliseret
CNA-delen af CNO-kapaciteten integreret i efterretningsvæsnet	Nej	Nej	Ja
Tilsynsmyndigheders beføjelser	Begrænsede	Vide	Moderate

5 Danmarks offensive cybervalg: Konklusioner og anbefalinger

Denne rapport søger at bidrage til at understøtte og kvalificere debatten om Danmarks offensive cyberforsvarsprioriteringer ved at belyse de nationale og internationale rammer for en offensiv dansk cyberforsvarspolitik samt sammenligne og analysere Hollands, Norges og Frankrigs tiltag på området. Dermed identificeres en række betingelser, muligheder og begrænsninger, der fremadrettet kan støtte danske beslutningstagere i deres overvejelser om anvendelse af Danmarks offensive cyberforsvarsmidler. I forlængelse heraf opstilles i dette konkluderende kapitel en række anbefalinger til, hvordan Danmark kan sikre, at anvendelsen af CNO-kapaciteten får de bedst mulige rammer på politisk-strategisk, juridisk og organisatorisk niveau.

Danmark har – som Holland, Norge og Frankrig – haft fokus på at udvikle CNO-midler de seneste ti år. Derfor står Danmark i dag med en fuldt operationel CNO-kapacitet, der gør landet i stand til at træffe både kort- og langsigtede strategiske beslutninger om dens anvendelse. Senest har Danmark udviklet en militær cyberdoktrin, der har fokus på anvendelse af cybermidler i krigssituationer. Som det fremgår af analysen, forventes Danmarks cyberforsvar imidlertid primært at skulle rette sig mod aktiviteter, der falder under tærsklen for krig, som følge af de ændrede geopolitiske forhold samt udviklingen i cybertrusselsbilledet. Det er derfor nødvendigt, at de danske politiske beslutningstagere og relevante myndigheder træffer en række principielle beslutninger om, hvordan vi fra dansk side vil forholde os til de nye cyberkonfliktformer, herunder Danmarks anvendelse af offensiv cybermagt mellem angreb, spionage og forsvar.

I dag danner en skarp adskillelse mellem angreb, spionage og forsvar udgangspunktet for anvendelsen af Danmarks CNO-kapacitet. Med afsæt i analysens afdækning af udviklingen i Holland, Norge og Frankrig og som reaktion på de ændrede geopolitiske vilkår og nye cyberkonfliktmønstre udleder rapporten én større hovedanbefaling. Den er, at Danmark bør løsne 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.

En sådan ændring vil være med at danne grundlag for den fremtidige indretning af Danmarks cyberforsvar. Desuden vil det styrke Danmarks mulighed for at agere strategisk i forbindelse med cyberkonflikter, der falder under tærsklen for krig. Ydermere kan det være med til at understøtte den politiske forankring af og demokratiske debat om anvendelsen af Danmarks CNO-kapacitet. Skal Danmark have en mere aktiv efterretningstjeneste, er det absolut nødvendigt, at den politiske og militære beslutningskompetence og ansvarsplacering er klarlagt og transparent.

Med udgangspunkt i analysen og hovedanbefalingen giver rapporten til slut yderligere en række konkrete anbefalinger til, hvordan de danske beslutningstagere sikrer, at anvendelsen af CNO-kapaciteten får de bedst mulige rammer på politisk-strategisk, juridisk og organisatorisk niveau.

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

Analysen og 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. Rapporten anbefaler derfor, at regeringen og Folketinget gør følgende:

Udvikling af et selvstændigt retsgrundlag for CNO-kapaciteten

Styrker 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

- Udvider 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.

5.2 Styrket strategisk planlægning med hensyn til anvendelse af CNO-kapaciteten

Rapporten anbefaler, at de ansvarlige danske myndigheder styrker 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.

5.3 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.

Noter

1 Henrik Breitenbauch & Niels Byrjalsen. "Subversion, Statecraft and Liberal Democracy", *Survival* 61:4 (2019), 31-41; Dmity Adamsky. "From Moscow With Coercion: Russian deterrence theory and strategic culture", *Journal of Strategic Studies* 41:2 (2018), 33-60.

2 Sergei Boeke & Dennis Broeders. "The Demilitarisation of Cyber Conflict", *Survival* 60:6 (2018), 73-90.

3 Forsvarsakademiet. "Værnsfælles Doktrin for Militære Cyberspaceoperationer", 2019. København: Forsvarsakademiet.

4 Forsvarsministeriet. "Offensive cybereffekter", 2019 (6. april 2020): https://fmn.dk/temaer/nato/Documents/2018/Faktaark-cyber-effekter.pdf.

5 Ben Buchanan. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations.* New York: Oxford University Press, 2016; Lucas Kello. *The Virtual Weapon and International Order.* New Haven and London: Yale University Press, 2017.

6 Buchanan. *The Cybersecurity Dilemma*

7 Forsvarets Efterretningstjeneste. *Forsvarets Efterretningstjenestes Årlige Risikovurdering 2019*, 2019 (tilgået 4. april 2020): https://fe-ddis.dk/Produkter/Risikovurderinger/Documents/Efterretningsm%C3%A6ssig%20Risikovurdering%202019.pdf; Center for Cybersikkerhed. *Trusselsvurdering: Cybertruslen mod Danmark 2019*, 2019 (tilgået 4. april 2020): https://fe-ddis.dk/cfcs/publikationer/Documents/Cybertruslen-mod-Danmark-2019.pdf.

8 Forsvarets Efterretningstjeneste; Center for Cybersikkerhed, 2019.

9 Breitenbauch & Byrjalsen, "Subversion, Statecraft and Liberal Democracy", 31-4.

10 Ken André Jacobsen. *Når Hydra angriber: Hybrid afskrækkelse i gråzonekonflikter mellem krig og fred,* Center for Militære Studier (2019), København: Københavns Universitet.

11 Forsvarets Efterretningstjeneste, 2019.

12 Venstre, Socialdemokraterne, Dansk Folkeparti, Socialistisk Folkeparti, Det Konservative Folkeparti, Radikale Venstre og Liberal Alliance. "Forsvarsforlig 2010-2014", 2009. København.

13 Socialdemokraterne, Radikale Venstre, Socialistisk Folkeparti, Venstre, Dansk Folkeparti, Liberal Alliance og Det Konservative Folkeparti. "Aftale på forsvarsområdet 2013-2017", 2012. København.

14 Venstre, Liberal Alliance og Det Konservative Folkeparti, Socialdemokratiet, Dansk Folkeparti og Radikale Venstre. "Aftale på forsvarsområdet 2018-2023", 2018. København.

15 Forsvarsministeriet, 2019.

16 Regeringen. *National strategi for cyber- og informationssikkerhed: Øget professionalisering og mere viden*, 2014. København.

17 Regeringen. *National strategi for cyber- og informationssikkerhed 2018-2021,* 2018. København.

18 Cyberforsvarsområdet er altså særligt også i den henseende, at muligheden for freeriding er meget begrænset.

19 I den kommende rapport "Modforanstaltninger i Cyberdomænet" identificerer Astrid Kjeldgaard-Pedersen og Marc Schack (2020) adskillige grundlæggende uklarheder i den folkeretlige regulering af, hvornår, hvordan og mod hvem stater lovligt kan gennemføre modforanstaltninger i cyberdomænet.

20 Buchanan, 2016; Max Smeets. "A matter of time: On the transitory nature of cyberweapons", *Journal of Strategic Studies* 41:1-2 (2018), 6-32; Max Smeets. "The Strategic Promise of Offensive Cyber Operations", *Strategic Studies Quarterly* 12:3 (2019), 90-113; Herbet Lin & Amy Zegart. "Introduction" in *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, edited by Herbert Lin & Amy Zegart. Washington D.C.: Brookings Institution Press, 2018.

21 Forsvarets Efterretningstjeneste, 2019.

22 Ben Buchanan. *The Hacker and The State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, Massachusetts and London: Harvard University Press, 2020; Adam Segal. *The Hacked World Order: How Nations Fight, Trade, and Manipulate in the Digital Age*. New York: Public Affairs, 2017.

23 Jacobsen, 2019.

24 USA's angreb på ISIS i 2016 er et eksempel herpå. Se David E. Sanger. "U.S. Cyberattacks Target ISIS in a New Line of Combat", *New York Times,* 2016.

25 Buchanan, 2020; Segal, 2017; David E. Sanger. *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*. New York: Broadway Books, 2019.

26 U.S. Cyber Command. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command", 2, 2018 (tilgået 6. april 2020): https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

27 Max Smeets & Herbert Lin. "A Strategic Assessment of the U.S. Cyber Command Vision" in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. edited by Herbert Lin & Amy Zegart. Brookings Institution Press, 2018; Hoffman, Wyatt. "Is Cyber Strategy Possible?" *The Washington Quarterly*, 42:1 (2019), 131-152.

28 U.S. Cyber Command. "Achieve and Maintain Cyberspace Superiority". 3, (2018).

29 Michael Warner. "U.S. Cyber Command's Road to Full Operational Capability" in *Stand Up and Fight: The Creation of U.S. Security Organizations, 1942–2005*. Edited by Ty Seidule & Jacqueline E. Whitt. Carlisle, Pa. Strategic Studies Institute and U.S. Army War College Press, 2015.

30 U.S. Cyber Command, *Beyond the Build: Delivering Outcomes through Cyberspace. The Commander's Vision and Guidance for US Cyber Command*, 2015 (tilgået 6. april 2020): https://www.hsdl.org/?view&did=787006.

31 Smeets & Lin, 2018.

32 U.S. Cyber Command, 2018.

33 Department of Defense. "Summary of 2018 National Defense Strategy of the United States of America", 2018 (tilgået 6. april 2020): https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

34 Schneider, G., Jacquelyn. "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy", 2019 (tilgået 6. april 2020): https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.

35 Hoffman, 2019.

36 U.S. Cyber Command, 2018.

37 Rudesill, S., Dakota, "Trump's Secret Order on Pulling the Cyber Trigger", 2018 (tilgået 6. april 2020): https://www.lawfareblog.com/trumps-secret-order-pulling-cyber-trigger; Dustin Volz 2018, "White House Confirms It Has Relaxed Rules on U.S. Use of Cyberweapons", *The Wall Street Journal,* 2018 (tilgået 6. april 2020): https://www.wsj.com/articles/white-house-confirms-it-has-relaxed-rules-on-u-s-use-of-cyber-weapons-1537476729.

38 Julian E. Barnes. "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say", *New York Times*, 2019 (tilgået 6. april 2020): https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html; Robert Chesney. "A Cyber Command Operational Update: Clarifying the June 2019 Iran Operation, 2019" (tilgået 6. april 2020) https://www.lawfareblog.com/cyber-command-operational-update-clarifying-june-2019-iran-operation.

39 Jason Healey. "The implications of persistent (and permanent) engagement in cyberspace", *Journal of Cybersecurity*, 5:1 (2019), 1-15.

40 David E. Sanger & Nicole Perlroth. "U.S. Escalates Online Attacks on Russia's Power", *The New York Times,* 2019 (tilgået 4. Maj 2020): https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

41 Paul M. Nakasone, (2019). *Statement of General Paul M. Nakasone, Commander, U.S. Cyber Command, before the Senate Committee on*

Armed Services. S. 21. https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf

42 NATO. "Wales Summit Declaration 2014", 2014 (tilgået 6. april 2020): https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

43 NATO. "NATO Cyber Defence Pledge", Press Release, 124, 8. juli 2016 (tilgået 6. april 2020): https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

44 NATO. "Bruxelles Summit Declaration 2018", 2018 (tilgået 6. april 2020): https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

45 Sophie Arts. "Offense as the New Defense: New Life for NATO's Cyber Policy", *The German Marshall Fund of the United States*, Policy Brief, 39 (2018), 1-9.

46 Jens Stoltenberg, "Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference", London 2019 (tilgået 6. april 2020) https://www.nato.int/cps/en/natohq/opinions_166039.htm.

47 NATO. "NATO Cyber Defence, Factsheet", 2019 (tilgået 6. april 2020): https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf.

48 NATO's normale brug af øvelser er f.eks. en mulighed, når det kommer til anvendelse af nationale offensive cybermidler.

49 Buchanan, 2016, 2020; Kello, 2017; Sanger, 2019.

50 Buchanan, 2020; Sanger, 2019.

51 Buchanan, 2020; Sanger, 2019.

52 Andy Greenberg. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired,* 2018 (tilgået 6. april 2020): https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

53 Pippa Crerar et. al. "Russia accused of cyber-attack on chemical weapons watchdog", *The Guardian,* 2018 (tilgået 6. april 2020): https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body.

54 US district court. "Indictment of Iranian hackers by the Department of Justice of the United States of America", 2018 (tilgået 6. april 2020): https://www.justice.gov/usao-sdny/press-release/file/1045781/download; https://www.justice.gov/opa/press-release/file/1114741/download.

55 US district court. "Indictment of North Korean hackers by the Department of Justice of the United States of America", 2018 (tilgået 6. april 2020): https://www.justice.gov/opa/press-release/file/1092091/download.

56 US district court. "Indictment of Chinese hackers by the Department of Justice of the United States of America", 2018 (tilgået 6. april 2020): https://www.justice.gov/opa/press-release/file/1121706/download.

57 US district court. "Indictment of Russian hackers by the Department of Justice of the United States of America", 2018 (tilgået 6. april 2020): https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election; https://www.justice.gov/opa/page/file/1098481/download.

58 Council of The European Union. "Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomacy Toolbox", 2017 (tilgået 6. april 2020): http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.

59 Council of The European Union. "Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States", 2019 (tilgået 6. april 2020): http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf.

60 Diskussionerne vedrørende den amerikanske strategi drejer sig blandt andet om frygten for eskalation, manglende fokus på stabilitet og normbygning. Se eventuelt: P. Fischerkeller, Michael & J. Harknett, J., Richard. "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace", 2018 (tilgået 6. april 2020): https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace; Max Smeets, "There Are Too Many Red Lines in Cyberspace", 2019 (tilgået 6. april 2020) https://www.lawfareblog.com/there-are-too-many-red-lines-cyberspace; Jason Healey. "Getting the Drop in Cyberspace", 2019 (tilgået 6. april 2020) https://www.lawfareblog.com/getting-drop-cyberspace.

61 Sergei Boeke. "National cyber crisis management: Different European approaches", *Governance*, 31:3 (2018), 449-464.

62 Hillen, Hans (2011) in Dennis Broeders, 2015, *Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance*, Research study commissioned by the Netherlands Defence Academy (DoD).

63 Alexander Claver. "Governance of cyber warfare in the Netherlands: an exploratory investigation", *The International Journal of Intelligence, Security, and Public Affairs*, 20:2 (2018), 155-180.

64 Marie Baezner & Sean Cordey. "National Cybersecurity Strategies in Comparison – Challenges for Switzerland", *Center for Security Studies (CSS)*, ETH Zürich, 2019.

65 I forbindelse med at cyberkommandoen blev erklæret fuldt operationel ved årsskiftet til 2017, fremhævede det hollandske forsvarsministerie, at den tjener til afskrækkelse og skal understøtte militære operationer ved at udvikle og anvende offensive cybervåben til brug i forbindelse med væbnet konflikt.

66 Dennis Broeders. "Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance", *the Netherlands Defence Academy (DoD*), 28, 2015.

67 Ministry of Defense. "The Defence Cyber Strategy", 2015 (tilgået 6. april 2020): https://english.defensie.nl/topics/cyber-securi-ty/defence-cyber-strategy.

68 J. A. Hennis-Plasschaert. *Actualisering Defensie Cyber Strategie*. Ministerie van Defensie (2015); Alexander Claver. Governance of cyber warfare in the Netherlands: an exploratory investigation, *The International Journal of Intelligence, Security, and Public Affairs*, 20:2 (2018), 155-180.

69 Ministry of Justice and Security. "National Cyber Security Agenda: A cyber secure Netherlands", 2018 (tilgået 6. april 2020): https://www.ncsc.nl/english/current-topics/national-cyber-securi-ty-agenda.html; Foreign Ministry, "'Building Digital Bridges' International Cyber Strategy – Towards an integrated international cyber policy", 2017 (tilgået 6. april 2020): https://www.government.nl/binaries/govern-ment/documents/parliamentary-documents/2017/02/12/international-cyber-strategy/International+Cyber+Strategy.pdf.

70 Ministerie van Defensie. "Defensie Cyber Strategie 2018 Investeren in digitale slagkracht voor Nederland", 2018 (tilgået 6. april 2020): https://www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018

71 Max Smeets, "Werkt de Nederlandse wijzende vinger bij cyberaanvallen?, Clingendael Spectator", 2019 (tilgået 6. april 2020): https://spectator.clingendael.org/nl/publicatie/werkt-de-nederlandse-wijzende-vinger-bij-cyberaanvallen.

72 Foreign Ministry. "'Building Digital Bridges' International Cyber Strategy – Towards an integrated international cyber policy", 2017 (tilgået 6. april 2020): https://www.government.nl/binaries/govern-ment/documents/parliamentary-documents/2017/02/12/international-cyber-strategy/International+Cyber+Strategy.pdf.

73 Den hollandske regering præsenterede i 2019 en fyldig redegørelse for sit syn på applikationen af folkeretten i cyberspace. Se: Government of the Kingdom of the Netherlands, 'Appendix: International law in cyberspace', 2019, (tilgået 6. april 2020): https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf

74 Forsvarsdepartementet. *Et forsvar for vår tid – Langtidsplan for Forsvaret 2013-2016*, 11, 2012.

75 Forsvarsdepartementet, 12, 2012.

76 Forsvarsdepartementet. *Kampkraft og bærekraft 2017-2020,* 2016. Den norske regering fremlagde 17. april 2020 en ny langtidsplan for forsvarssektoren (2021-2024). Planen bliver ikke behandlet i rapporten. Planen giver ikke umiddelbart anledning til ændringer i rapportens analyser og konklusioner. Se https://www.regjeringen.no/no/tema/forsvar/ltp/LTP/id2611090/.

77 Forsvarsdepartementet. 19, 2016.

78 Forsvarsdepartementet. 24, 2016.

79 Forsvaret. "Et styrket forsvar – Forsvarssjefens Fagmilitære Råd", 14, 2019 (tilgået 6. april 2020): https://forsvaret.no/ForsvaretDocuments/FMR_2019_fullversjon_Godkjent.pdf.

80 Forsvaret, 30, 2019.

81 Forsvarsdepartementet. "Proposisjon til Stortinget for Budsjettåret 2019", 46, 2018.

82 Florence Parly. "Stratégie cyber des Armées", 2019a (tilgået 6. april 2020): https://www.vie-publique.fr/discours/269137-florence-parly-18012019-strategie-cyber-des-armees-cyberdefense.

83 Ministère des Armées. *Defence and National Security Strategic Review 2017*. 2017.

84 François Delerue & Aude Géry. *France's Cyberdefense Strategic Review and International Law,* 2018 (tilgået 6. april 2020): https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law.

85 Ministère des Armées. *Livre Blanc sur la Défense et Sécurité nationale 2013*. 2013; Ministère des Armées 2017.

86 Delerue, 2018.

87 Fremhævet af interviewpersoner i Paris i november 2019.

88 Ministère des Armées, "Politique ministérielle de lutte informatique défensive", 2019 (tilgået 6. april 2020): https://www.defense.gouv.fr/content/download/551498/9394005/Politique%20ministrielle%20de%20lutte%20informatique%20DEFENSIVE.pdf; Ministère des Armées, "Éléments publics de doctrine militaire de lutte informatique offensive", 2019 (tilgået 6. april 2020): https://www.defense.gouv.fr/content/download/551497/9393997/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf.

89 Parly, 2019a.

90 Florence Parly, "Le discours de Florence Parly, ministre des Armées, à l'inauguration du premier bâtiment du commandement de la cyberdéfense du ministère des Armées", 2019b (tilgået 6. april 2020): https://www.defense.gouv.fr/english/salle-de-presse/discours/discours-de-florence-parly/discours-de-florence-parly-ministre-des-armees-a-l-inauguration-du-premier-batiment-du-commandement-de-la-cyberdefense-du-ministere-des-armees.

91 Stéphane Taillat. Signaling, "Victory, and Strategy in France's Military Cyber Doctrine", 2019 (tilgået 6. april 2020): https://warontherocks.com/2019/05/signaling-victory-and-strategy-in-frances-military-cyber-doctrine/.

92 Boeke, 2018.

93 Fremhævet af interviewpersoner i Holland i oktober 2019.

94 Alexander Claver. "Governance of cyber warfare in the Netherlands: an exploratory investigation", *The International Journal of Intelligence, Security, and Public Affairs*, 20:2 (2018), 155-180.

95 Der kan i særlige tilfælde gives ex ante-tilladelse uden parlamentets formelle inddragelse (artikel 100-brev), hvis situationen kræver det, men beslutningen vil efterfølgende blive vurderet af parlamentet og/eller tilsynet. Se Paul Ducheine; Kraesten Arnold & Peter Pijpers. "Decision-Making and Parliamentary Control for International Military Cyber Operations by the Netherlands Armed Forces", *Amsterdam Law School Legal Studies*, Research Paper, 2020:07, 2015.

96 "Tot slot kan de MIVD binnen de kaders van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) op basis van inlichtingen ook zélf in actie komen om acute dreigingen in het digitale domein te verstoren". Ministerie van Defensie. "Defensie Cyber Strategie 2018 Investeren in digitale slagkracht voor Nederland", 2018 (tilgået 6. april 2020): https://www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018: 7

97 Cyberforsvaret har ikke ansvar for civil infrastruktur, men det kan yde bistand til aktører, der har dette, som f.eks. NorCERT. Enheden har i dag ca. 1.200 ansatte. Se https://forsvaret.no/cyberforsvaret.

98 Forsvarsdepartementet, "Lov om Etterretningstjenesten" (etterretningstjenesteloven), Prop. 80 L (2019–2020), 2018 (tilgået 6. april 2020): https://www.regjeringen.no/contentassets/b7bada5f31bc482092318df675a2019d/no/pdfs/prp20192020008 0000dddpdfs.pdf.

99 Skriftlig formidling fra det norske forsvarsdepartement til rapportens forfatter.

100 Karsten Friis. "Høringssvar fra NUPI", *Norsk utenrikspolitisk institutt,* 2019 (tilgået 6. april 2020): https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=d4630119-b015-4ef7-8110-60be2a90c0be.

101 Norges ikke-parlamentariske kontrolorgan (EOS-utvalget) fører tilsyn med alle norske myndigheder, der beskæftiger sig med efterretnings- og overvågningsaktiviteter og sikkerhedsvirksomhed. EOS-udvalgets formål er at tilse, at tjenesterne ikke bryder lovgivningen eller benytter uproportionale midler, og at menneskerettighederne overholdes. EOS-udvalget kontrollerer både behandlingen af personoplysninger, tvangsindgreb og tilsyn med, at borgeres retssikkerhed og individuelle rettigheder respekteres. EOS-udvalget består af syv medlemmer samt et sekretariat, hvor der i dag er 14 personer ansat. Se https://eos-utvalget.no/.

102 Tormod Heier, "Is effective oversight possible?: the rising influence of Norway's intelligence service" in *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*, edited by Ian Leigh & Njord Wegge. London and New York: Routledge, 2019.

103 Per Anders Johansen, "Dramatisk oppgjør mellom Norges hemmelige tjenester: PST og E-tjenesten er dypt uenige om ny spionlov", *Aftenposten*, 2019 (tilgåpet 6. april 2020): https://www.aftenposten.no/norge/i/3jAa7M/dramatisk-oppgjoer-mellom-norges-hemmelige-tjenester-pst-og-e-tjenesten-er-dypt-uenige-om-ny-spionlov; Sveinung Berg Bentzrød, "Utvalget som skal kontrollere Norges hemmelige tjenester, er sterkt kritisk til ny etterretningslov", *Aftenposten*, 2019 (tilgået 6. april 2020): https://www.aftenposten.no/norge/i/216zAv/utvalget-som-skal-kontrollere-norges-hemmelige-tjenester-er-sterkt-kritisk-til-ny-etterretningslov; Se også høringssvar: https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?expand=horingssvar&lastvisited=7fb7c142-e17d-4ca4-bf49-3f7afb1ee1fc.

104 I sit høringssvar skriver EOS-udvalget: "De fire ekstra årsverkene som Forsvarsdepartementet mener vil være nok for å ivareta den nye kontrolloppgaven av tilrettelagt innhenting, mener vi er for lite. Om vi ikke får nok ressurser, vil det kunne føre til en risiko for redusert kapasitet til å kontrollere de andre EOS-tjenestene og andre sider ved E-tjenestens virksomhet." Se "Høringssvar fra EOS-utvalget", 2019 (tilgået 6. april 2020): https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=7fb7c142-e17d-4ca4-bf49-3f7afb1ee1fc.

105 EOS-utvalget, "Årsmelding 2018 Dokument 7:1 (2018-2019)", s. 32, 2018 (tilgået 6. april 2020): https://www.stortinget.no/globalassets/pdf/dokumentserien/2018-2019/dok7-201819-001.pdf

106 ANSSI blev oprettet i 2009. ANSSI har i dag ca. 600 medarbejdere – et tal, der forventes at stige til ca. 1.000 over de næste fem år. Se https://www.ssi.gouv.fr/en/.

107 Oliver Chopin, "Intelligence reform and the transformation of the state: the end of a French exception", *Journal of Strategic Studies*, 40:4 (2017), 532-553.

108 Bertrand Warusfel, "The intensification of French intelligence and its oversight under the impact of counter-terrorism" in *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*, edited by Ian Leigh and Njord Wegge. London and New York: Routledge, 2019.

109 "La Délégation Parlementaire sur le Renseignement". Et udvalg bestående af medlemmer fra både senatet og nationalforsamlingen. Se http://www.senat.fr/commission/renseignement/index.html og http://www2.assemblee-nationale.fr/15/les-delegations-comite-et-office-parlementaire/delegation-parlementaire-au-renseignement.

110 Warusfel, 2019.

111 Chopin, 2017; Warusfel, 2019.

Litteraturliste

Adamsky, Dmity. "From Moscow With Coercion: Russian deterrence theory and strategic culture", *Journal of Strategic Studies*, 41:2 (2018), 33-60.

Arts, Sophie. *Offense as the New Defense: New Life for NATO's Cyber Policy*, The German Marshall Fund of the United States, Policy Brief, 39 (2018), 1-9.

Barnes, E., Julian. "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say". *New York Times*, (tilgået 6. april 2020) https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html.

Boeke, Sergei. "National cyber crisis management: Different European approaches". *Governance* 31:3 (2018), 449-464.

Boeke, Sergei & Dennis Broeders. "The Demilitarisation of Cyber Conflict", *Survival*, 60:6 (2018), 73-90.

Breitenbauch, Henrik & Niels Byrjalsen. "Subversion, Statecraft and Liberal Democracy", *Survival*, 61:4 (2019), 31-41.

Broeders, Dennis. "Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance." Research study commissioned by the Netherlands Defence Academy (DoD), 28, 2015.

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. New York: Oxford University Press, 2016.

Buchanan, Ben. *The Hacker and The State: Cyber Attacks and the New Normal of Geopolitics.* Cambridge, Massachusetts and London: Harvard University Press, 2020.

Center for Cybersikkerhed, "Trusselsvurdering: Cybertruslen mod Danmak 2019". Forsvarets Efterretningstjeneste, 2019 (tilgået 4. april 2020) https://fe-ddis.dk/cfcs/publikationer/Documents/Cybertruslen-mod-Danmark-2019.pdf.

Chesney, Robert. "A Cyber Command Operational Update: Clarifying the June 2019 Iran Operation", *Lawfare* (tilgået 6. april 2020) https://www.lawfareblog.com/cyber-command-operational-update-clarifying-june-2019-iran-operation.

Chopin, Olivier. "Intelligence reform and the transformation of the state: the end of a French exception", *Journal of Strategic Studies*, 40:4 (2017), 532-553.

Claver, Alexander. Governance of cyber warfare in the Netherlands: an exploratory investigation, *The International Journal of Intelligence, Security, and Public Affairs*, 20:2 (2018), 155-180.

Council of The European Union. "Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomacy Toolbox)", Bruxelles, 7. juni 2017: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf (tilgået 6. april 2020).

Council of The European Union. "Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its MemberStates", Bruxelles, 14. maj 2019: http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf. (tilgået 6. april 2020).

Crerar, Pippa et. al. "Russia accused of cyber-attack on chemical weapons watchdog", *The Guardian*, (tilgået 6. april 2020): https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body.

Delerue, François & Aude Géry. "France's Cyberdefense Strategic Review and International Law", *Lawfare* (tilgået 6. april 2020) https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law.

Department of Defense. *Summary of 2018 National Defense Strategy of the United States of America*. 2018.

Fischerkeller, P., Michael & Richard J. Harknett. "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace", *Lawfare* (tilgået 6. april 2020): https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

Forsvaret. "Et styrket forsvar – Forsvarssjefens Fagmilitære Råd", 2019 (tilgået 6. april 2020): https://forsvaret.no/ForsvaretDocuments/FMR_2019_fullversjon_Godkjent.pdf.

Forsvarsakademiet. "Værnsfælles Doktrin for Militære Cyberspaceoperationer", København: Forsvarsakademiet. 2019.

Forsvarsdepartementet. *Et forsvar for vår tid – Langtidsplan for Forsvaret 2013-2016*, 11, 2012.

Forsvarsdepartementet. *Kampkraft og bærekraft 2017-2020*, 19, 2016.

Forsvarsdepartementet. *Proposisjon til Stortinget for Budsjettåret* 2019, 46, 2018.

Forsvarsministeriet. *Offensive cybereffekter* (tilgået 6. april 2020): https://fmn.dk/temaer/nato/Documents/2018/Faktaark-cyber-effekter.pdf.

Forsvarets Efterretningstjeneste. "Forsvarets Efterretningstjenestes Årlige Risikovurdering 2019", 2019 (tilgået 4. april 2020): https://fe-ddis.dk/Produkter/Risikovurderinger/Documents/Efterretningsm%C3%A6ssig%20Risikovurdering%202019.pdf.

Government of the Kingdom of the Netherlands, 'Appendix: Interna-tional law in cyberspace', 2019 (tilgået 6. april 2020): https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf

Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired*, (tilgået 6. april 2020) https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Healey, Jason. "The implications of persistent (and permanent) engagement in cyberspace", *Journal of Cybersecurity*, 5:1 (2019), 1-15.

Healey, Jason. "Getting the Drop in Cyberspace", *Lawfare* (tilgået 6. april 2020): https://www.lawfareblog.com/getting-drop-cyberspace.

Heier, Tormod. "Is effective oversight possible?: the rising influence of Norway's intelligence service". In *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*, edited by Ian Leigh and Njord Wegge. London and New York: Routledge, 2019.

Hillen Hans. Research study commissioned by the Netherlands Defence Academy (DoD) (2011). In *Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance* by Dennis Broeders. 2015.

Hoffman, Wyatt. "Is Cyber Strategy Possible?", *The Washington Quarterly*, 42:1 (2019), 131-152.

Jacobsen, Ken André. "Når Hydra angriber: Hybrid afskrækkelse i gråzone-konflikter mellem krig og fred". *Center for Militære Studier*, 2019.

Kello, Lucas. *The Virtual Weapon and International Order.* New Haven and London: Yale University Press, 2017.

Lin, Herbet & Amy Zegart. "Introduction". In *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations,* edited by Herbert Lin and Amy Zegart. Washington D.C: Brookings Institution Press, 2018.

Ministère des Armées. *Livre Blanc sur la Défense et Sécurité nationale 2013.* 2013.

Ministère des Armées. *Defence and National Security Strategic Review 2017.* 2017.

Nakasone, Paul M. *Statement of General Paul M. Nakasone, Commander, U.S. Cyber Command, before the Senate Committee on Armed Services.* 2019. https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf

NATO. "Wales Summit Declaration 2014", Press Release 120, 5. september 2014 (tilgået 6. april 2020): https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

NATO. "NATO Cyber Defence Pledge", Press Release, 124, 8. juli 2016 (tilgået 6. april 2020): https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

NATO. "Bruxelles Summit Declaration", Press Release, 074, 11. juli 2018 (tilgået 6. april 2020): https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

Parly, Florence (2019a). "Stratégie cyber des Armées", *Vie Publique* (tilgået 6. april 2020): https://www.vie-publique.fr/discours/269137-florence-parly-18012019-strategie-cyber-des-armees-cyberdefense.

Parly, Florence (2019b), "Discours de Florence Parly, ministre des Armées, à l'inauguration du premier bâtiment du commandement de la cyberdéfense du ministère des Armées", *Ministère des Armées* (tilgået 6. april 2020): https://www.defense.gouv.fr/english/salle-de-presse/discours/discours-de-florence-parly/discours-de-florence-parly-ministre-des-armees-a-l-inauguration-du-premier-batiment-du-commandement-de-la-cyberdefense-du-ministere-des-armees.

Socialdemokraterne, Radikale Venstre, Socialistisk Folkeparti, Venstre, Dansk Folkeparti, Liberal Alliance og Det Konservative Folkeparti. *Aftale På Forsvarsområdet 2013-2017.* København, 2012.

Regeringen. *National strategi for cyber- og informationssikkerhed: Øget professionalisering og mere viden.* København, 2014.

Regeringen. *National strategi for cyber- og informationssikkerhed 2018-2021.* København, 2018.

Rudesill, S., Dakota. "Trump's Secret Order on Pulling the Cyber Trigger", *Lawfare* (tilgået 6. april 2020): https://www.lawfareblog.com/trumps-secret-order-pulling-cyber-trigger.

Sanger, E., David. "U.S. Cyberattacks Target ISIS in a New Line of Combat", *New York Times*. 2016.

Sanger, E., David. *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*. New York: Broadway Books, 2019.

Sanger, David E. & Perlroth, Nicole. "U.S. Escalates Online Attacks on Russia's Power", *The New York Times*, 2019 (tilgået 8. Januar 2020): https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

Schack, Marc & Kjeldgaard-Pedersen, Astrid, "Modforanstaltninger i cyberdomænet". *Det Juridiske Fakultet, Københavns Universitet*, 2020 (forthcoming).

Schneider, G. Jacquelyn. "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy", *Lawfare* (tilgået 6. april 2020): https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, and Manipulate in the Digital Age*. New York: Public Affairs, 2017.

Smeets, Max. "A matter of time: On the transitory nature of cyberweapons", *Journal of Strategic Studies,* 41: 1-2 (2018), 6-32.

Smeets, Max. "The Strategic Promise of Offensive Cyber Operations", *Strategic Studies Quarterly* 12:3 (2019), 90-113.

Smeets, Max. "There Are Too Many Red Lines in Cyberspace", *Lawfare* (tilgået 6. april 2020): https://www.lawfareblog.com/there-are-too-many-red-lines-cyberspace.

Smeets, Max & Herbert Lin. "A Strategic Assessment of the U.S. Cyber Command Vision". In *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, edited by Herbert Lin & Amy Zegart. Washington D.C: Brookings Institution Press, 2018.

Stoltenberg, Jens, "Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference", London, 23. maj 2019 (tilgået 6. april 2020): https://www.nato.int/cps/en/natohq/opinions_166039.htm.

Taillat, Stéphane. "Signaling, Victory, and Strategy in France's Military Cyber Doctrine", *War on the Rocks* (tilgået 6. april 2020): https://warontherocks.com/2019/05/signaling-victory-and-strategy-in-frances-military-cyber-doctrine/.

U.S. Cyber Command. *Beyond the Build: Delivering Outcomes through Cyberspace. The Commander's Vision and Guidance for US Cyber Command.* 2015.

U.S. Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. 2018.

US district court. *Indictment of Iranian hackers by the Department of Justice of the United States of America*, New York, 18 Cr., 2018 (tilgået 6. april 2020): https://www.justice.gov/usao-sdny/press-release/file/1045781/download; https://www.justice.gov/opa/press-release/file/1114741/download.

US district court. *Indictment of North Korean hackers by the Department of Justice of the United States of America*, California, 8. juni 2018 (tilgået 6. april 2020): https://www.justice.gov/opa/press-release/file/1092091/download.

US district court. *Indictment of Chinese hackers by the Department of Justice of the United States of America*, New York, 18 Cr., 17. december 2018 (tilgået 6. april 2020): https://www.justice.gov/opa/press-release/file/1121706/download.

US district court (2018). *Indictment of Russian hackers by the Department of Justice of the United States of America*, (tilgået 6. april 2020) https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.

Venstre, Socialdemokraterne, Dansk Folkeparti, Socialistisk Folkeparti, Det Konservative Folkeparti, Radikale Venstre og Liberal Alliance. *Forsvarsforlig 2010-2014.* København, 2009.

Venstre, Liberal Alliance og Det Konservative Folkeparti, Socialdemokratiet, Dansk Folkeparti og Radikale Venstre. *Aftale På Forsvarsområdet 2018-2023*. København, 2018.

Volz, Dustin. "White House Confirms It Has Relaxed Rules on U.S. Use of Cyberweapons", *The Wall Street Journal*, (tilgået 6. april 2020): https://www.wsj.com/articles/white-house-confirms-it-has-relaxed-rules-on-u-s-use-of-cyber-weapons-1537476729.

Warner, Michael. "U.S. Cyber Command's Road to Full Operational Capability". In *Stand Up and Fight: The Creation of U.S. Security Organizations, 1942–2005*, edited by Ty Seidule and Jacqueline E. Whitt. Pa. Carlisle: Strategic Studies Institute and U.S. Army War College Press, 2015.

Warusfel, Bertrand. "The intensification of French intelligence and its oversight under the impact of counter-terrorism". *In Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*, edited by Ian Leigh and Njord Wegge. London and New York: Routledge, 2019.