Redegørelse fra den tværministerielle arbejdsgruppe om Folketingets inddragelse ved anvendelse af den militære Computer Network Attack (CNA)-kapacitet

Resumé

Partierne bag den nuværende forsvarsaftale for 2013 - 2017 har besluttet, at der skal etableres en kapacitet til at udføre militære operationer i cyberspace, en Computer Network Operations (CNO)-kapacitet. CNO- kapaciteten skal udover at kunne forsvare og beskytte egen digital infrastruktur også have evnen til at påvirke en fjendtlig aktør gennem militære angreb på dennes digitale infrastruktur, sidstnævnte benævnes Computer Network Attack (CNA).

I forbindelse med drøftelser om den militære CNA-kapacitet blandt forligskredsens medlemmer i december 2014 efterspurgtes en nærmere afklaring af, i hvilket omfang Folketinget inddrages ved anvendelse af den militære CNA-kapacitet i fremtidige militære operationer.

Forsvarsministeriet nedsatte derfor en tværministeriel arbejdsgruppe bestående af repræsentanter fra Udenrigs-, Justits- og Forsvarsministeriet samt fra Forsvarets Efterretningstjeneste og Værnsfælles Forsvarskommando, som med denne redegørelse belyser dette spørgsmål.

Følgende er arbejdsgruppens vurdering:

- Anvendelsen af den militære CNA-kapacitet adskiller sig ikke fra Forsvarets traditionelle militære kapaciteter i forhold til, hvorvidt der skal indhentes samtykke fra Folketinget.

- Det er opgaven og den ønskede effekt af en netværkshandling, der er afgørende for, om anvendelse af CNA vurderes at være et militært magtmiddel og derfor kræver samtykke fra Folketinget. Der er ikke forskel på, om det militære magtmiddel er et militært CNA eller et mere konventionelt angreb. Uanset om CNA anvendes i sammenhæng med traditionelle militære operationer eller selvstændigt, vil det være den samlede effekt af en militær operation, der vil være afgørende for, hvorvidt Folketinget skal inddrages.

- De eksisterende nationale rammer og procedurer i Grundlovens § 19 om Folketingets samtykke til anvendelse af militære magtmidler skal følges ved anvendelse af en ny militær teknologi i form af CNA-kapaciteten.

- Folkerettens regler finder anvendelse i forbindelse med en konkret indsættelse af den militære CNA- kapacitet. De mere overordnede folkeretlige spørgsmål i forhold til suverænitet og det juridiske grundlag for deltagelse i en konkret operation skal besvares forud for indsættelsen og er ikke påvirket af, om den danske deltagelse sker ved militært CNA eller konventionelle militære bidrag.

Indledning og baggrund

Partierne bag den nuværende forsvarsaftale for 2013 – 2017 har besluttet, at der skal etableres en kapacitet til militære operationer i cyberspace, herunder såvel en evne til at beskytte egen digital infrastruktur som en evne til at påvirke en modstanders anvendelse af cyberspace. Kapaciteten skal kunne anvendes såvel defensivt som offensivt med henblik på at forsvare egen digital infrastruktur, forhindre fjendtlige aktørers udnyttelse af eller angreb på egen digital infrastruktur samt påvirke en fjendtlig aktør gennem militært angreb på dennes digitale infrastruktur. I cyberspace benævnes defensive handlinger "Computer Network Defence" (CND), og offensive handlinger "Cyber Network Exploitation" (CNE) samt "Computer Network Attack" (CNA). Alle tre handlinger betegnes samlet som "Computer Network Operations" (CNO).

Anvendelse af cyberspace bliver i stigende grad integreret i planlægningen og udførelsen af militære operationer, og den teknologiske udvikling medfører, at det danske forsvar har behov for at opbygge en offensiv militær CNO-kapacitet. Der vurderes i dag at være et stort potentiale i cyberoperationer , ligesom der er betydelige operative gevinster ved selv at udføre cyberoperationer. Derfor udvikles der verden over kapaciteter inden for CNO, og i mange lande etableres militære enheder og hovedkvarterer til at udføre sådanne cyberoperationer. Dette er blandt andet baggrunden for, at der også i Danmark oprettes en militær CNO-kapacitet, der kan udføre både defensive og offensive militære operationer i cyberspace.

For så vidt angår militære angreb på fjendtlige aktørers digitale infrastruktur - CNA – blev der i forlængelse af drøftelser med forligskredsens medlemmer i december 2014 efterspurgt en nærmere afklaring af Folketingets inddragelse ved indsættelsen af den militære CNA-kapacitet.

Når den militære CNA-kapacitet indsættes i internationale operationer, bliver den stillet til rådighed for Forsvaret, som skal planlægge og opgaveanvise indsættelsen af kapaciteten i forbindelse med den militære operation. I forbindelse med sådanne militære indsættelser af CNA-kapaciteten rejser spørgsmålet sig - som det i øvrigt er tilfældet med udsendelse af andre militære styrkebidrag - i hvilket omfang Folketinget skal inddrages i henhold til Grundlovens § 19, stk. 2.

Forsvarsministeriet har derfor nedsat en tværministeriel arbejdsgruppe, benævnt CNA/AG/JUR, som med denne redegørelse belyser spørgsmålet om inddragelse af Folketinget ved anvendelse af den militære CNA- kapacitet.

Arbejdsgruppen har haft følgende sammensætning:

Chefen for Internationalt Juridisk kontor, Forsvarsministeriet (formand)
Repræsentant fra Udenrigsministeriet
Repræsentant fra Justitsministeriet

Repræsentanter fra Forsvarsministeriet
Repræsentant fra Værnsfælles Forsvarskommando
Repræsentanter fra Forsvarets Efterretningstjeneste

Arbejdsgruppens fremstilling af Folketingets inddragelse i forbindelse med indsættelsen af den militære CNA- kapacitet fremgår af denne redegørelse og er i sin helhed uklassificeret.

Afgrænsning og definition

Der findes ikke universelt anerkendte eller autoritative definitioner på en række af de begreber, der er centrale for redegørelsen. Begreberne bliver anvendt forskelligt i den offentlige debat og af forskellige myndigheder. Dette kan bidrage til uklarhed på et i forvejen teknologisk komplekst område. Eksempelvis bliver ordet cyberangreb brugt til at beskrive en lang række forskellige netværksbaserede hændelser. Det bruges ofte synonymt med hackerangreb og dækker over en bred vifte af mere eller mindre skadelige hændelser fra it-tyveri til angreb, der medfører ødelæggelse af fysiske ting. Intentionerne bag disse handlinger kan være mangeartede, men samlet set har de oftest et formål, der er omfattet af national strafferet.

Denne redegørelse behandler ikke cyberkriminalitet omfattet af strafferetten, da det falder uden for formålet med den militære CNA-kapacitet. Endvidere behandles ikke reglerne for de øvrige dele af CNO-kapaciteten, dvs. CND og CNE, som vil blive udført i henhold til dansk ret, herunder Lov om Forsvarets Efterretningstjeneste og Lov om Center for Cybersikkerhed, samt Danmarks internationale forpligtelser.

Som beskrevet ovenfor tillægges cyberangreb mange forskellige betydninger, men i rammen af "militære magtmidler" som anført i Grundlovens § 19, stk.2, får ordet CNA en snævrere og mere kvalificeret betydning. Da denne redegørelse behandler aspekter af inddragelse af Folketinget ved brugen af militære magtmidler, er det denne mere snævre betydning, der er udgangspunktet for redegørelsens definition og behandling af cyberangreb.

Militære CNA er netværksbaserede handlinger rettet mod lukkede og åbne it-netværk, it-systemer eller computere, der forventes at skabe en effekt, der kan føre til tab af menneskeliv, personskade og/eller betydelig skade på eller ødelæggelse af fysiske objekter. Det kan være umiddelbar betydelig ødelæggelse eller betydelig ødelæggelse som sekundær effekt, f.eks. ved at et militært flys trafikkontrolsystem sættes ud af drift med forventet tab af menneskeliv og/eller betydelig skade på eller ødelæggelse af fysiske objekter til følge.

Det er således spørgsmålet om Folketingets inddragelse ved indsættelse af den militære CNA-kapacitet, der behandles i denne redegørelse.

Computer Network Attack (CNA) som ny militær angrebsform

Formålet med at opbygge en militær CNA-kapacitet er at etablere evnen til at kunne angribe en modstander igennem dennes digitale infrastruktur. Effekten af et militært CNA kan være mangeartet, men effekten opnås altid gennem modstanderens digitale infrastruktur, og formålet vil som oftest være at skade udvalgte dele af en modstanders militære kapaciteter.

Det er hensigten med CNA-kapaciteten, at den på sigt skal supplere Forsvarets øvrige militære magtmidler. Som med alt ny teknologi kan det være vanskeligt at vurdere præcist, hvilken betydning CNA vil få for fremtidige militære operationer. Mest sandsynligt er det, at CNA vil blive brugt sideløbende med mere traditionelle virkemidler/våben. På nuværende tidspunkt vurderes det mindre sandsynligt, at militære operationer vil foregå alene ved CNA.

Når CNA bruges i sammenhæng med traditionelle militære operationer, kan det være for at forberede kampplads en. Eksempelvis kan militære cyberoperationer, gennem CNA på overvågningssystemer og kommando- og kontrolsystemer i en konflikts indledende faser, skabe konkrete forudsætninger for gennemførelsen af land-, sø- eller luftoperationer. CNA kan også understøtte effekten af konventionel magtanvendelse (bomber og granater mv.) Det kan eksempelvis ske ved, at der sideløbende med konventionelle angreb på modstanderes militære installationer gennemføres et CNA, der besværliggør modstanderens militære kommunikation og adgang til anden digital infrastruktur, og dermed gør det sværere for modstanderen at reagere koordineret på angrebet.

Ved anvendelse af CNA adskiller våbnet sig fra Forsvarets traditionelle våbentyper ved ikke at være et fysisk objekt på samme måde som f.eks. en bombe. I stedet benyttes typisk skadelige computerprogramkoder i form af såkaldt malware. Programkoden anvendes til målrettet at ændre eller ødelægge en enhed som f.eks. en computers programkode, logik eller data, hvilket vil ændre funktionen af den pågældende enhed eller computer. Den skadelige programkode skal oftest specialdesignes til den enhed, computer eller netværk, der planlægges CNA imod. Derfor vil der i forbindelse med forberedelsesfasen af et CNA som udgangspunkt skulle udvikles nye programkoder.

CNA er først en mulighed, når operationsområdet er identificeret som modtageligt for angreb via den digitale infrastruktur. Det betyder for det første, at der skal være en tilstrækkelig infrastruktur, og at modstanderen anvender it-systemer, der gør det muligt at angribe disse systemer. For det andet skal sårbarheder i relevante systemer være identificeret. For det tredje skal det være teknisk muligt at få adgang og kunne udnytte de pågældende sårbarheder til at udføre et CNA. Alt dette betyder, at et CNA er et meget målrettet angreb, og at den anvendte kode vil være specialdesignet til at opnå en specifik ødelæggende effekt i et konkret udpeget militært mål.

- Den humanitære folkeret

Når CNA anvendes under væbnet konflikt, gælder den humanitære folkerets regler vedrørende angreb. Dette betyder bl.a., at udvikling af programkode til brug for CNA anses for våbenudvikling og skal vurderes på samme måde som andre nye våben. Det skal derfor sikres, at den ikke angriber vilkårligt, eller som følge af sin natur påfører overflødig skade eller unødvendig lidelse.

Der vil ligeledes skulle fortages en vurdering i forhold til Danmarks øvrige internationale forpligtelser, inden et CNA iværksættes i en væbnet konflikt. Når et CNA vurderes at have en sådan effekt, at det kan sidestilles med et konventionelt angreb i den humanitære folkerets forstand, skal angriberen

således forinden sikre sig overholdelse af den humanitære folkeret i forhold til bl.a. forsigtighedsforanstaltninger, proportionalitet samt skelnen mellem civile objekter og militære mål, også kaldet distinktion.

Der skal foretages en konkret og individuel vurdering af, hvorvidt et specifikt angreb overholder den humanitære folkeret. Et angreb må ikke gennemføres uden, at der har været foretaget en sådan vurdering. Det er dermed de samme elementer, der skal vurderes i forbindelse med et CNA som ved et konventionelt angreb. Fokus vil således være på, hvorvidt et objekt er et militært mål, hvorvidt der er taget de nødvendige forsigtighedsforanstaltninger for at minimere risikoen for civile tab, og hvorvidt angrebet er proportionelt mv.

Disse spørgsmål bliver en integreret del af at opbygge en professionel operativ CNA-kapacitet. I den opbyggende fase skal erfaring med at håndtere sådanne vurderinger etableres og udvikles. Den humanitære folkerets krav til lovligheden af militære angreb sikrer, at der ikke vil kunne gennemføres konkrete CNA, inden der er sket den fornødne afklaring og vurdering.

Det skal bemærkes, at spørgsmål om CNO i relation til den humanitære folkeret også behandles i den kommende Militærmanual om folkeret i internationale militære operationer.

- Organisation og militær indsættelse

Forsvarets Efterretningstjeneste har allerede en Cyber Network Exploitation (CNE)-kapacitet, der anvendes til at løse Forsvarets Efterretningstjenestes opgaver som Danmarks udenrigs- og militære efterretningstjeneste. De nye militære CNE- og CNA-kapaciteter vil organisatorisk blive opbygget i tilknytning til Forsvarets Efterretningstjenestes nuværende CNE-kapacitet for at skabe synergi. Denne synergi opnås bl.a., fordi det i nogen grad er samme teknologier og værktøjer, der anvendes til både CNE og CNA. Med samme rationale opbygges den militære CND-kapacitet i tilknytning til Forsvarets Efterretningstjenestes Center for Cybersikkerhed.

Forsvarets Efterretningstjenestes anvendelse af CND- og CNE-kapaciteterne vil blive udført i henhold til dansk ret, herunder Lov om Forsvarets Efterretningstjeneste og Lov om Center for Cybersikkerhed. Udover dansk ret er anvendelsen af kapaciteten som nævnt også underlagt Danmarks internationale forpligtelser.

Den militære CNA-kapacitet bliver ved indsættelse i væbnet konflikt stillet til rådighed for Forsvaret, som skal planlægge og opgaveanvise indsættelsen af kapaciteten i forbindelse med militære operationer. I forbindelse med indsættelsen af den militære CNA-kapacitet i en international operation vil vurderingen af behovet for Folketingets inddragelse i henhold til Grundlovens § 19, stk. 2, ske på samme grundlag, som det er tilfældet med udsendelse af andre militære styrkebidrag.

Den danske militære CNA-kapacitet vil kunne indsættes både i en national og international ramme. Militære cyberoperationer vil således kunne gennemføres som en integreret del af et samlet dansk styrkebidrag, dvs. til støtte for eller i samarbejde med andre danske styrkebidrag til den pågældende operation eller som et selvstændigt styrkebidrag til en militær operation i regi af NATO, FN eller en koalition.

Grundlovens § 19, stk. 2

Regeringens udenrigspolitiske kompetence fremgår af Grundlovens § 19, stk. 1, 1. pkt., der bestemmer, at regeringen "handler på rigets vegne i mellemfolkelige anliggender". Regeringens almindelige adgang til på egen hånd efter den nævnte bestemmelse at handle på rigets vegne i mellemfolkelige anliggender modificeres dog bl.a. af § 19, stk. 2., 1. pkt., som fastslår, at:

"Bortset fra forsvar mod væbnet angreb på riget eller danske styrker kan kongen ikke uden folketingets samtykke anvende militære magtmidler mod nogen fremmed stat."

Bestemmelsen er en procedureregel, der regulerer forholdet mellem regeringen og Folketinget. Bestemmelsen har ifølge Forfatningskommissionens betænkning af 1953, som ligger til grund for bestemmelsen, til formål at sikre en effektiv parlamentarisk kontrol på området.

Grundlovens § 19, stk. 2, indebærer, at Folketingets samtykke som hovedregel skal indhentes forud for anvendelse af militære magtmidler. I praksis er kravet om Folketingets samtykke blevet fortolket således, at der skal indhentes samtykke, hvis regeringen vil benytte militære magtmidler, eller hvor det efter en samlet vurdering ikke kan udelukkes, at der bliver tale om anvendelse af militære magtmidler. Samtykket meddeles i praksis ved en folketingsbeslutning, der vedtages efter to behandlinger i Folketinget, jf. nedenfor.

Grundlovens § 19, stk. 2, omfatter såvel danske styrkers deltagelse i internationale militære aktioner som rent danske militære aktioner, herunder i multinationale koalitioner i regi af FN, NATO eller andre koalitionsdannelser. Den omfatter alle former for *militære magtmidler* og har således været anvendt ved udsendelse af styrker fra såvel flyvevåbnet, søværnet som hæren.

Hverken forarbejderne til Grundlovens § 19, stk. 2, eller den statsretlige litteratur indeholder en nærmere beskrivelse af, hvad der skal forstås ved "militære magtmidler". Udtrykket blev dog indsat i Grundloven i 1953 til erstatning for udtrykket "krig" med henvisning til, at Danmark forinden havde påtaget sig internationale forpligtelser om adgangen til militær magtanvendelse, bl.a. FN-pagten. I lyset heraf og af formålet med bestemmelsen må det antages, at udtrykket "militære magtmidler" i Grundlovens § 19, stk. 2, omhandler alle former for militær magtanvendelse, uanset hvilket konkret (magt)middel der benyttes.

Anvendelsen af den militære CNA-kapacitet adskiller sig på denne baggrund ikke fra anvendelse af Forsvarets mere traditionelle militære kapaciteter i forhold til, om der skal indhentes samtykke fra Folketinget. Forsvarets netværksbaserede handlinger rettet mod it-netværk, it-systemer eller computere i andre lande må således antages også at være omfattet af Grundlovens § 19, stk. 2, i det omfang sådanne handlinger udgør magtanvendelse. Retningsgivende for, hvornår der foreligger magtanvendelse vil – i lyset af baggrunden for formuleringen af Grundlovens § 19, stk. 2 – generelt kunne være, om handlingerne falder inden for definitionen af magtanvendelse i folkeretten, jf. FN Pagtens artikel 2, stk. 4. Afgørende vil herefter generelt være omfanget og effekten af de pågældende handlinger, herunder om de er egnede til og kan forventes at føre til tab af menneskeliv, personskade og/eller betydelig skade på eller ødelæggelse af fysiske objekter.

Grundlovens § 19, stk. 2, angår efter sin formulering anvendelse af militære magtmidler "mod nogen fremmed stat". Det antages imidlertid i praksis, at denne formulering ikke skal fortolkes således, at danske styrkers anvendelse af militære magtmidler mod ikke-statslige aktører kan ske uden samtykke fra Folketinget. I praksis indhentes der således også samtykke fra Folketinget i tilfælde, hvor der er tale om anvendelse af militære magtmidler mod andre fremmede enheder end stater.

Militær magtanvendelse kan ifølge bestemmelsen i § 19, stk. 2, 1. pkt., ske uden forudgående folketingssamtykke, når der er tale om "forsvar mod væbnet angreb på riget eller danske styrker". Ved "riget" forstås ifølge bemærkningerne til § 19 i Forfatningskommissionens betænkning alene det danske territorium, og det er således forudsat, at anvendelse af militær magt som svar på angreb på fremmed territorium ikke kan ske uden Folketingets samtykke hertil. Det gælder også, selv om angrebet folkeretligt måtte kunne imødegås efter f.eks. FN-pagtens bestemmelser om kollektivt selvforsvar. Udtrykket "danske styrker" omfatter ifølge bemærkningerne selvstændige danske militærenheder, hvad enten disse måtte være under dansk eller international kommando.

Den militære magtanvendelse skal have karakter af et "forsvar". Det anføres i bemærkningerne til § 19 i Forfatningskommissionens betænkning, at:
"Da forsvar mod angreb efter sagens natur ikke kan afvente rigsdagens samtykke, er det bestemt, at [regeringen] i så fald på egen hånd kan træffe bestemmelse om anvendelse af militære magtmidler, men kun til imødegåelse af det konkrete angreb. Det må tilkomme rigsdagen at tage stilling til en eventuel udvidelse af krigshandlingerne."

Adgangen til i de nævnte tilfælde at anvende militær magt i selvforsvar uden forudgående samtykke fra Folketinget er således begrundet i uopsættelighedshensyn og bør ikke opretholdes længere end nødvendigt. Der er tale om en snæver undtagelse, som ikke finder anvendelse i situationer, hvor man uden større vanskeligheder kunne have indhentet Folketingets forudgående samtykke til magtanvendelsen.

Anvendes militære magtmidler som forsvar mod angreb på riget eller danske styrker uden Folketingets samtykke, skal de trufne foranstaltninger straks forelægges for Folketinget, jf. Grundlovens § 19, stk. 2, 2. pkt.

Folketingets samtykke

Afgivelse af Folketingets samtykke efter Grundlovens § 19, stk. 2, er ikke bundet til nogen bestemt form. Samtykket kan således meddeles i form af folketingsbeslutning, direkte i en lov, i bemærkningerne til lovforslag eller på anden vis.

Samtykke til anvendelse af militære magtmidler i henhold til Grundlovens § 19, stk. 2, meddeles normalt i form af folketingsbeslutning. Praksis er således, at regeringen fremsætter et beslutningsforslag om samtykke i Folketinget. I bemærkningerne til beslutningsforslaget redegøres der nærmere for den militære operation; hvorfor regeringen finder, at danske militære styrker bør indsættes; hvilke militære kapaciteter der er tale om og andre relevante forhold.

Beslutningsforslag om samtykke til anvendelse af militære magtmidler efter Grundlovens § 19, stk. 2, fremsættes og behandles i Folketinget efter de regler, der er fastsat om behandlingen af beslutningsforslag i Folketingets Forretningsorden, særligt kapitel VI. Heraf følger bl.a., at beslutningsforslag behandles på samme måde som lovforslag, dog således at beslutningsforslag som udgangspunkt alene undergives 2 behandlinger i folketingssalen (1. og 2. behandlingen).

Mellem 1. og 2. behandlingen behandles beslutningsforslag i et folketingsudvalg. Udvalget har i den forbindelse mulighed for at stille spørgsmål til de relevante ministre om forslaget. Udvalget afslutter sin behandling af forslaget ved at afgive en betænkning, hvorefter forslaget overgår til 2. behandling og afstemning. Beslutningsforslag om § 19-samtykke til anvendelse af militære magtmidler behandles i praksis i Forsvarsudvalget mellem 1. og 2. behandlingen.

Efter § 42 i Folketingets Forretningsordenen kan der i særdeles påtrængende tilfælde – på forslag af formanden eller efter et skriftligt indgivet forslag af 17 medlemmer – afviges fra forretningsordenens regler, for så vidt de ikke beror på grundlovsbestemmelser eller andre lovbestemmelser, når ¾ af de stemmende tilslutter sig forslaget. Det vil således være muligt inden for de rammer, som § 42 sætter, at fravige forretningsordenens regler i forhold til Folketingets behandling af beslutningsforslag om § 19-samtykke til anvendelse af militære magtmidler.

Dette gør det muligt at gennemføre folketingsbehandlingerne på kort tid, hvilket eksempelvis var tilfældet, efter FN's Sikkerhedsråd den 17. marts 2011 vedtog resolution 1973, som autoriserede FN's medlemsstater til at gennemføre en intervention i Libyen med henblik på at beskytte den libyske civilbefolkning mod overgreb. Udenrigsministeren fremsatte den 18. marts 2011 beslutningsforslag B 89 om et dansk militært bidrag med kampfly til den internationale indsats i Libyen, hvilket Folketinget vedtog natten mellem den 18. og 19. marts 2011.

Foreligger der fortrolige oplysninger om den påtænkte militære operation, de militære kapaciteter mv., vil det i almindelighed være berettiget, at regeringen undlader at redegøre for sådanne oplysninger i bemærkningerne til beslutningsforslaget. I stedet vil der kunne redegøres for oplysningerne over for f.eks. Det Udenrigspolitiske Nævn, hvor medlemmerne har en særlig tavshedspligt.

De nærmere regler om Nævnets virke er fastsat i nævnsloven[1], hvis § 2 bestemmer, at Nævnet i øvrigt har til opgave med regeringen at drøfte sager af betydning for landets udenrigspolitik og at modtage oplysninger fra regeringen om udenrigspolitiske forhold. Forhandlingerne i Det Udenrigspolitiske Nævn kan efter nævnslovens § 4 tavshedsbelægges. Praksis herom må antages at have medført, at drøftelserne i Nævnet normalt vil være undergivet fortrolighed, medmindre andet aftales. Der kan endvidere i særlige tilfælde indskærpes medlemmerne en skærpet fortrolighed, såfremt emnet for rådføringen vurderes at nødvendiggøre dette. Behandling af spørgsmål vedrørende en militær CNA-kapacitet forventes i øvrigt ikke at adskille sig fra den almindelige praksis for inddragelse af det Det Udenrigspolitiske Nævn.

Sammenfatning

Anvendelsen af den militære CNA-kapacitet adskiller sig ikke fra Forsvarets traditionelle militære kapaciteter i forhold til, hvorvidt der skal indhentes samtykke fra Folketinget.

Det er opgaven og den ønskede effekt af en netværkshandling, der er afgørende for, om anvendelse af CNA vurderes at være et militært magtmiddel og derfor kræver samtykke fra Folketinget. Der er ikke forskel på, om det militære magtmiddel er et militært CNA eller et mere konventionelt angreb. Uanset om CNA anvendes i sammenhæng med traditionelle militære operationer eller selvstændigt, vil det være den samlede effekt af en militær operation, der vil være afgørende for, hvorvidt Folketinget skal inddrages.

Det er arbejdsgruppens vurdering, at de eksisterende nationale rammer og procedurer i Grundlovens § 19 om Folketingets samtykke til anvendelse af militære magtmidler ligeledes skal følges ved anvendelse af en ny militær teknologi i form af CNA.

Det er endvidere arbejdsgruppens vurdering, at folkerettens regler finder anvendelse i forbindelse med en konkret indsættelse. De mere overordnede folkeretlige spørgsmål i forhold til suverænitet og det juridiske grundlag for deltagelse i en konkret operation skal besvares forud for indsættelsen og er ikke påvirket af, om den danske deltagelse sker ved militært CNA eller konventionelle militære bidrag.

[1] Lov nr. 54 af 3. maj 1954 om Det Udenrigspolitiske Nævn

Der vil fortsat være en tæt dialog mellem de involverede myndigheder, således at der fastholdes et højt vidensniveau i forhold til de spørgsmål, der fremover måtte opstå med denne nye militære kapacitet.

BILAG 1

DEFINITIONER

Digital infrastruktur

Digital infrastruktur bliver brugt som betegnelse for den informations- og kommunikationsteknologiske infrastruktur. Det dækker både over netværk, computere og andre systemer. Det bruges som synonym med det, der andre steder kaldes IKT-infrastruktur og IT-infrastruktur.

Computer Network Operations (CNO)

Computer Network Operations (CNO) er en fælles betegnelse for de operationer, der gennemføres i cyberspace. Der er grundlæggende tale om tre forskellige hovedspor indenfor CNO: Computer Network Defence (CND), Computer Network Exploitation (CNE) og Computer Network Attack (CNA). Alle tre operationstyper er netværksbaserede operationer og benytter samme type teknologi og værktøjer, men har forskellige formål. CND er af natur defensivt, mens CNE og CNA er offensivt.

CNO kan gennemføres som selvstændige operationer eller i samarbejde med traditionelle militære kapaciteter.

Computer Network Defence (CND)

Ved CND forstås der i denne sammenhæng de 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) et eksempel på en myndighed, der varetager en CND funktion.

Center for Cybersikkerhed indsamler løbende viden om cyberangreb og finder de digitale spor og mønstre, der identificerer et angreb. Disse digitale fingeraftryk lægges ud i specialkonstruerede alarmenheder, der placeres på internetforbindelser hos Centrets kunder. Her sammenholder alarmenheden datatrafikken, der løber gennem forbindelserne, med de digitale fingeraftryk.

Computer Network Exploitation (CNE)

CNE er aktiv netværksindhentning. CNE søger at sikre sig adgang til og 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. Det kan f.eks. gøres ved midlertidigt at blokere andres adgang til egne informationer. Der er flere eksempler på, at denne effekt er opnået gennem overbelastning af systemer, der indeholder de pågældende informationer. Når CNE udøves med henblik på at imødegå andres offensive handlinger, er det afgørende, at CNE handlingen har karakter af et afgrænset indgreb mod et specifikt mål, med begrænset virkning og i et

begrænset tidsrum. Brugen af CNE har ikke til formål at skabe ødelæggelse, da der i givet fald som udgangspunkt ville være tale om et CNA.

Både et effektivt forsvar og effektive angreb er afhængige af informationer. CNE er således forudsætningsskabende for både effektivt CND og CNA, da der i CNE regi kan tilvejebringes vigtige informationer og adgange til computernetværk.

Computer Network Attack (CNA)

Cyberangreb eller CNA tillægges mange betydninger, men i rammen af "militære magtmidler" får ordet angreb en snævrere og mere kvalificeret betydning. Da denne redegørelse behandler aspekter af inddragelse af Folketinget inden brugen af militære magtmidler, er det denne mere snævre betydning, der er udgangspunktet for redegørelsens definition af cyberangreb.

Militære CNA er netværksbaserede handlinger rettet mod it-netværk, it-systemer eller computere, der forventes at skabe en effekt, der kan føre til tab af menneskeliv, personskade og/eller betydelig skade på eller ødelæggelse af fysiske objekter. Det kan både være umiddelbar betydelig ødelæggelse, eller betydelig ødelæggelse som sekundær effekt f.eks. ved, at et militært flytrafikkontrolsystem sættes ud af drift med forudsigelige tab af menneskeliv og/eller betydelig skade på eller ødelæggelse af fysiske objekter til følge.

Militære CNA i rammen af en væbnet konflikt er underlagt den humanitære folkeret, herunder Genevekonventionerne inklusiv tillægsprotokollerne.