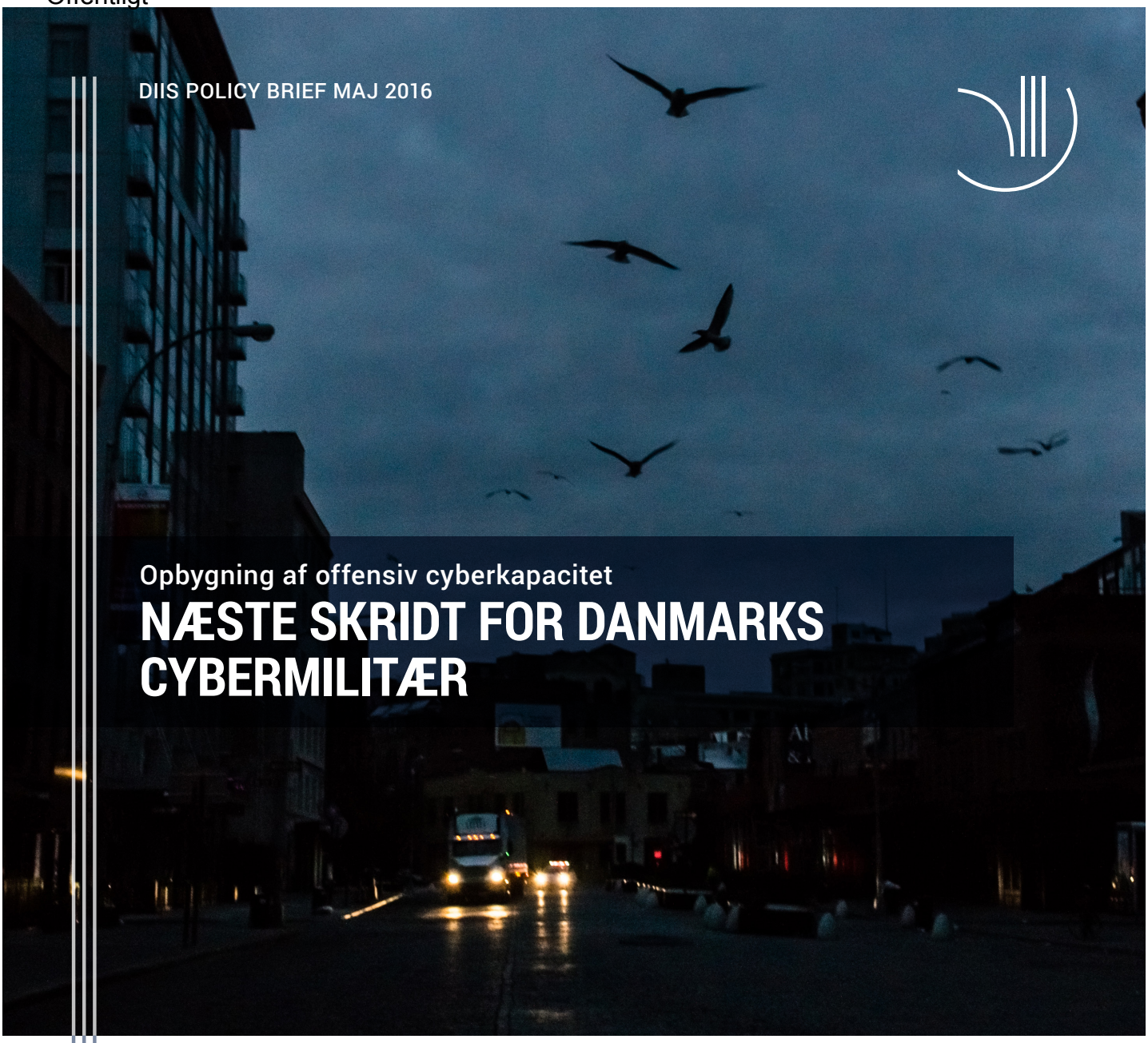

DIIS POLICY BRIEF MAJ 2016

Opbygning af offensiv cyberkapacitet

NÆSTE SKRIDT FOR DANMARKS CYBERMILITÆR

Skal cyberangreb være en effektiv del af Danmarks militære værkstøjskasse, er der brug for klare retningslinjer for udviklingen og brugen af cybervåben.

Militæreksperter har store forhåbninger til cyberangrebets operative potentiale. Mere end hundrede lande har allerede opbygget en eller anden form for militær cyberkapacitet, og det gælder også Danmark. I forlængelse af Forsvarsforliget for 2013-2017 blev det besluttet at etablere en kapacitet til militære operationer i cyberspace under Forsvarets Efterretningstjeneste (FE). Den offensive del af cyberkapaciteten kaldes Computer Network Attack (CNA) og har til formål at påvirke en modstander gennem angreb på dennes

ANBEFALINGER

- Skab klar arbejdsdeling mellem den almindelige indhentningsvirksomhed og den enhed, der skal udvikle og anvende cybervåben.
- Udvikl klare retningslinjer for, hvornår it-sårbarheder skal hemmeligholdes og udnyttes, og hvornår de skal offentliggøres.
- Øg det forsvars- og udenrigsministerielle engagement i de internationale drøftelser om cybernormer.

Et veltilrettelagt cyberangreb kan ramme på et splitsekund og i teorien alle steder i verden, hvor der er computere

"Skal cybervåben udvikles, må de militært ansatte hackere nødvendigvis undersøge fjendtlige netværk i fredstid, ellers kan det være vanskeligt at have et cybervåben parat, når politikerne beslutter sig for at engagere Danmark militært."

digitale infrastruktur. CNA har en række fordele, men rejser også flere uafklarede spørgsmål, som bør besvares, før den militære kapacitet for alvor tages i brug.

CYBERVÅBEN KORT FORTALT

Cybervåben forbindes oftest kun med avancerede angrebsformer, der både kan lamme og ødelægge it-systemer. Et cybervåben er kort fortalt et stykke software, der

1) har identificeret en fejl eller sårbarhed i et stykke software brugt af modstanderen,
2) evner at udnytte fejl til at få adgang til modstanderens it-system, og
3) indeholder en "digital sprængladning" – et stykke computerkode, der forstyrrer eller ødelægger modstanderens it-system.

Cybervåbnets to første elementer (identifikation og udnyttelse af modstanderens it-sårbarheder) er afhængige af informationsindhentning og kræver ofte en kortlægning af modstanderens netværksinfrastruktur. Ønsker man at ramme en militærinstallation, der ikke er på internettet – eksempelvis et radarsystem – kan det være svært at opnå den nødvendige adgang til systemet, og det gør udviklingen af et cybervåben særdeles tidskrævende. Skal angrebet udføres i hemmelighed, er udvikleren ofte afhængig af at kunne teste våbnet inden brug, og det medfører flere økonomiske og tidsmæssige omkostninger.

Et cybervåben er alt i alt et meget målrettet våben: Et våben, der, så snart det er brugt, giver den angrebne part mulighed for at identificere og udrede de sårbarheder, der muliggjorde angrebet. Cybervåben er således ofte et engangsvåben, der holdes hemmeligt, indtil det "affyres".

FORDELENE VED CYBERVÅBEN

Selvom cybervåben tager tid at udvikle, koster penge og sjældent kan bruges flere gange, er det stadig billigt i sammenligning med andet militært udstyr, der bruges til at påvirke fjendtlige systemer. Et veltilrettelagt cyberangreb kan ramme på et splitsekund og i teorien alle steder i verden, hvor der er computere. Det gælder også steder, hvor bomber normalt har svært ved at ramme, eksempelvis under jorden eller i bjerge.

Når en militær hacker først har fået adgang til et it-system, er afstanden mellem indhentning af information og angreb lille. Og da Danmark allerede har opbygget en velfungerende indhentningsenhed i FE, er det både billigt samt teknisk og organisatorisk belejligt også at tilføje en angrebsenhed til FE. Opbygningen af en offensiv cyberkapacitet er derudover et godt (og billigt) signal til allierede partnere i NATO om, at man tager alliancen seriøst.

TRE VIGTIGE SPØRGSMÅL OM DANMARKS CYBERMILITÆR

I Danmark er det seneste år hovedsageligt blevet brugt på at afdække nationale juridiske forhold om den militære brug af cyberangreb. I udgangspunktet kan CNA sidestilles med Forsvarets mere traditionelle militære redskaber og er derfor underlagt samme juridiske rammer ved brug. De potentielle udfordringer ved udvikling og brug af cybervåben er dog langt mere vidtrækkende end en juridisk diskussion. Her er tre spørgsmål, der bør adresseres som en del af det videre arbejde med opbygning af en offensiv cybermilitær kapacitet.

1) Hvad er CNA's eskalationspotentiale?
At cybervåben tager tid at planlægge, at de er afhængige af og overlapper med informationsindhentning i cyberspace, og at de kræver hemmeligholdelse inden brug betyder, at CNA indeholder et muligt eskalationspotentiale. Skal cybervåben udvikles, må de militært ansatte hackere nødvendigvis undersøge fjendtlige netværk i fredstid, ellers kan det være vanskeligt at have et cybervåben parat, når politikerne beslutter sig for at engagere Danmark militært.

Udvikling af cybervåben i fredstid medfører to udfordringer:

1) det er politisk kontroversielt at udpege fremtidige fjender, og
2) når andre stater ved, at Danmark er i besiddelse af en offensiv cybermilitærenhed, kan almindelig indhentningsaktivitet forveksles med forberedelse af alvorlige cyberangreb og dermed eskalere en konflikt – vel at mærke, hvis indhentningsaktiviteten opdages.

Et nødvendigt næste skridt i udviklingen af CNA må derfor være at udarbejde klare retningslinjer for den enhed, der skal udvikle cybervåben: Hvad skal/må man lave i fredstid? Hvordan udvælges potentielle mål? Disse retningslinjer samt en klar arbejdsdeling mellem en indhentnings- og angrebsenhed i FE vil kunne minimere risikoen for, at en fremmed aktør misforstår Danmarks intentioner.

2) Hvilke sikkerhedsdilemmaer medfører oprustning i cyberspace?
Fordi cybervåben indebærer udnyttelse af it-sårbarheder, kan våbnet potentielt også udnyttes af aktører, der ønsker at ramme Danmark. Et avanceret cybervåben målrettet eksempelvis en militærinstallation vil i teorien kunne nøjes med at udnytte sårbarheder, der er unikke for det specifikke mål, men i langt de fleste tilfælde vil et cybervåben kræve, at fejl i kommercielt software fra eksempelvis Microsoft udnyttes. Fejl i software, som bruges af borgere og virksomheder i Danmark, vil også kunne udnyttes af kriminelle og fjendtlige spioner. Oprustning i cyber-

@ fstop, fotograf: Caspar Benson

Fordi cybervåben indebærer udnyttelse af it-sårbarheder, kan våbnet potentielt også udnyttes af aktører, der ønsker at ramme Danmark

"Godt nok er der enighed om, at international lov gælder i cyberspace, men præcis *hvordan*, er stadig uklart. Der mangler simpelthen internationale normer for anvendelse af cybervåben som en legitim del af en militær mission."

space medfører således et sikkerhedsdilemma: Enten offentliggør man fejl, så de kan blive rettet, eller også fortier man, at man har fundet dem, så fejlene kan udnyttes af politiet eller FE – men også af kriminelle og fjendtlige aktører, hvis de får kendskab til dem.

Indtil nu er dilemmaet blevet imødegået ved, at FE råder over både indhentningsdelen og forsvarsdelen (Center for Cybersikkerhed), så informationer om sårbarheder kan deles på tværs af institutionerne. Men Centeret dækker ikke alle myndigheder og virksomheder i Danmark. Udviklingen af en offensiv cyberenhed understreger behovet for klare retningslinjer for, hvornår sårbarheder bør udnyttes offensivt, og hvornår de bør offentliggøres. En case-by-case-tilgang, som USA praktiserer, har vist sig blot at øge mistilliden til efterretningstjenesten.

3) Hvordan kan CNA bruges?

CNA indgår i den militære værktøjskasse på lige fod med andre våben, men det er stadig uklart, i hvilke sammenhænge cybervåben er at foretrække fremfor konventionelle våben. Cybervåben har ikke samme afskrækkende effekt som konventionelle våben. Dels fordi verden endnu ikke har oplevet et ødelæggende cyberangreb, og dels fordi hemmeligholdelse er en vigtig del af opbygningen af cybervåben.

Cybervåben er heller ikke at foretrække, hvis man ønsker fysisk ødelæggelse, som eksempelvis i kampen mod ISIL. Her er bombefly eller soldater stadig mere effektive. Cybervåben bør i højere grad ses som enten støttefunktion ved en militær intervention eller et irritationsværktøj – som eksempelvis USA bruger det mod ISIL – eller anvendes i sabotageaktioner, man ønsker holdt hemmelige.

Hvor sidstnævnte er politisk kontroversielt, er førstnævnte stadig omgærdet af international juridisk uklarhed. Godt nok er der enighed om, at international lov gælder i cyberspace, men præcis *hvordan*, er stadig uklart. Der mangler simpelthen internationale normer for anvendelse af cybervåben som en legitim del af en militær mission.

Netop de internationale normer for anvendelse af CNA er genstand for megen politisk bevågenhed internationalt, for eksempel i OSCE og FN. Den kommende tid vil blive afgørende for, hvordan normerne konsolideres. Forsvarsministeriet og Udenrigsministeriet bør involvere sig i dette arbejde, så Danmarks interesser på området sikres.

Jeppe Teglskov Jacobsen, ph.-d.-studerende, DIIS, jetj@diis.dk

DIIS · DANSK INSTITUT FOR INTERNATIONALE STUDIER
www.diis.dk