KØBENHAVNS UNIVERSITET
CENTER FOR MILITÆRE STUDIER

Afskrækkelse i cyberspace

muligheder og udfordringer

CMS Baggrundspapir - Juli 2020

Af Henrik Breitenbauch, Kristian Søby Kristensen, Jonas Groesmeyer

Dette baggrundspapir er en del af Center for Militære Studiers forskningsbaserede myndighedsbetjening for Forsvarsministeriet og de politiske partier bag forsvarsforliget. Baggrundspapiret beskriver udfordringer og muligheder forbundet med at afskrække modstandere i cyberspace.

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 for Forsvarsministeriet og de politiske partier bag forsvarsforliget.

Dette baggrundspapir er resultat af et analysearbejde baseret på forskningsmæssig metode. Baggrundspapirets 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/.

Forfatter: Henrik Breitenbauch, Kristian Søby Kristensen, Jonas Groesmeyer

Grafisk Design: Signs & Wonders

ISBN: 9788773938577

Indhold

Indledning 2

Baggrund: stigende evner, stigende risici i cyberspace 3

Teorien om afskrækkelse 4

Hvad er cyberspace? 6

Afskrækkelse i cyberspace 8

Hvordan? Tre udfordringer for afskrækkelse i cyberspace 11

To logikker for afskrækkelse ved straf i cyberspace 15

Danmarks sikkerhedsudfordringer 16


Data fra 29 millioner Facebook-brugere endte hos hackere
HACKER-ANGREB:
Hackere fik adgang til data hos 29 millioner brugere ved et angreb sidst i september, oplyser Facebook.
LOS ANGELES: Facebook siger ifølge Reuters, at hackerne fik adgang til data hos 29 millioner brugere ved et angreb sidst i september. Ifølge Facebook var sikkerhedsbruddet det værste nogensinde mod Facebook.
- Ukendte hackere har udnyttet en sikkerhedsbrist på Facebook til at få adgang til 50 millioner brugere, sagde Facebook sidst i september.
Facebook oplyste, at personerne bag hackerangrebet havde brugt funktionen hvervet ase, som tillader Facebookbrugere at se, hvordan deres egen profil tager sig ud for andre, til at overtage kontiene.
Selskabet siger nu, at hos 15 millioner brugere fik hackerne adgang til to forskellige sæt informationer: navne og kontakter - det vil sige blandt andet telefonnumre og/eller e-mail-adresser.
Hos andre 14 millioner fik hackerne også adgang til andre detaljer såsom brugernavne, køn, sprog, status i forbindelse med fast forhold, religion, hjemby, nuværende adresse, fødselsdage, uddannelse, arbejde og de seneste 10 hjemmesider, som de havde besøgt.
- Vi samarbejder med FBI, som efterforsker sagen. Vi har fået besked på ikke at fremsætte spekulationer om, hvem der kan stå bag angrebet, hedder i det i en Facebook-erklæring på en blog.
Der ingen oplysninger om hackernes lokation. Det vides heller ikke, om det er specifikke brugere, som personerne er gået efter. Facebooks direktør Mark Zuck-
Facebook siger, at hackere fik adgang til data hos 29 millioner
Facebook siger, at sikkerhedsbruddet var det værste nogensins
8 NYHEDER
Superviru
Total panik: En ufattelig tilfældighed redd
4 | NYHEDER | IT-SIKKERHED
Hård kritik af ny lov om cybersikkerhed:
»Helt og aldeles uacceptabelt i et demokratisk samfund«
9. OKTOBER 2015
10 | Ekstra Bladet FREDAG
KIDNAPPER DANSKERNES DATA
Det er mails som denne, hackerne bruger til kidnappe danskernes data.
POST
Du har uforløste pakken
Vi har modtaget din pakke CT54916500DK på 2015/09/15. Courier var ude af stand til at levere denne pakke til dig.
Få en adresseafgift
WARNING
we have encrypted your files with CryptOLOcker virus
Click here to pay for files recovery
Frequently Asked Questions
Sådan ser det ud, når hackerne har stået til. Kun ved at betale løsepenge, kan du få adgang til dine data.

Indledning

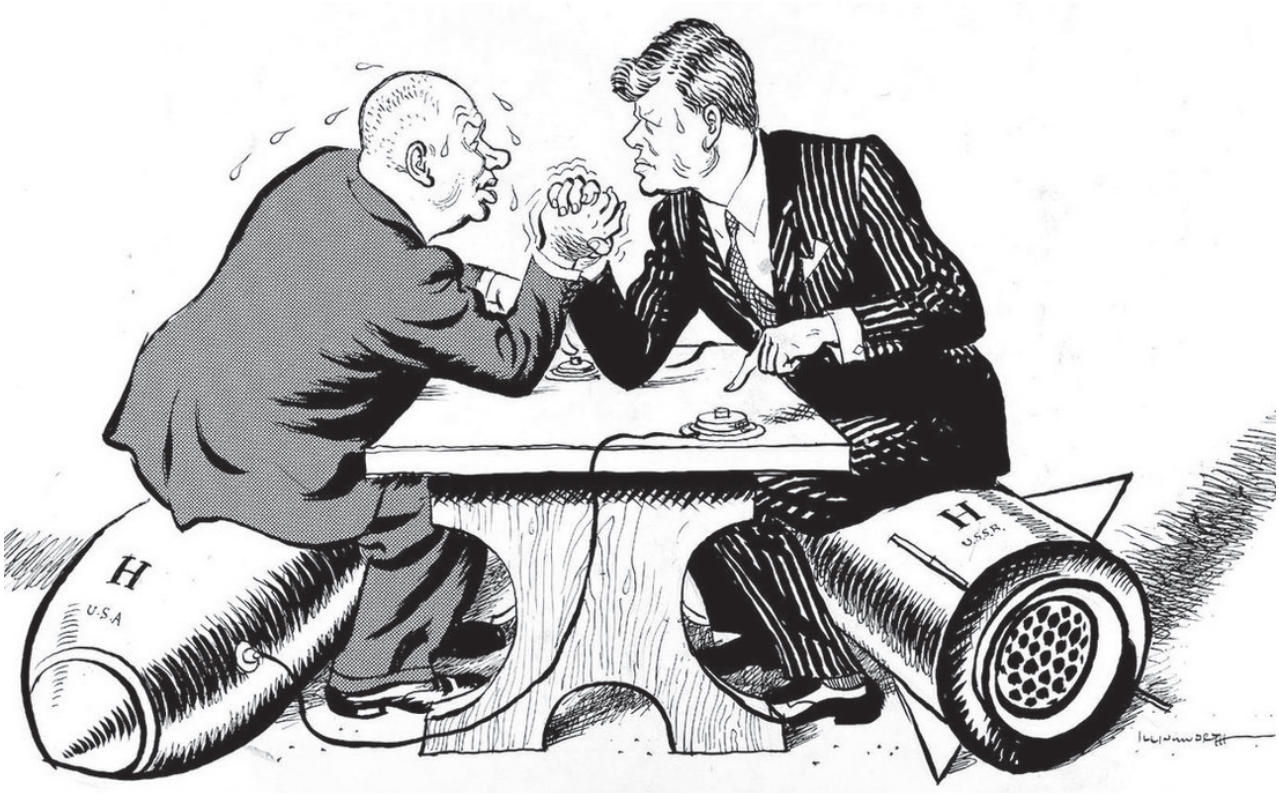
Cyberspaces øgede betydning rejser nye strategiske og politiske problemstillinger, ikke mindst vedrørende afskrækkelse.[1]

Hvordan kan stater beskytte centrale IT-systemer i og uden for cyberspace? Eller udnytte og angribe andres systemer? Hvornår er det statens ansvar at forsvare privatejede systemer? Er afskrækkelse muligt i cyberspace? Disse politiske og strategiske spørgsmål bliver debatteret i og uden for Danmark.

Tvivlen om afskrækkelse skyldes i høj grad usikkerhed om cyberspaces særlige egenskaber. Forskellige ødelæggende handlinger, såkaldte computernetværksoperationer (CNO), udfolder sig i et usynligt rum, de er hemmelige, så kun få mennesker kender til dem, og de kan på tværs af store afstande hurtigt forvolde stor skade.

Der er altså tvivl om, hvorvidt og hvordan afskrækkelse fungerer i cyberspace. Det skaber usikkerhed om spilleregler og reaktioner i dette nye rum for konkurrence og konflikt – for hvordan handler man i cyberspace, når man ikke ved, hvornår man er sikker?

Dette baggrundspapir diskuterer mulighederne for afskrækkelse i cyberspace. Det gør det ved at afdække 1) det traditionelle begreb om afskrækkelse, 2) cyberspaces natur og funktioner og 3) hvordan afskrækkelse kan eller ikke kan overføres hertil. Baggrundspapiret stiller skarpt på tre udfordringer, der opstår, når cyberspace bliver mediet for afskrækkelse. Til sidst diskuterer baggrundspapiret, hvordan Danmarks muligheder for at forsvare sig selv i cyberspace udfordres.



Kennedy og Khrushchev lægger arm i Leslie Gilbert Illingworths tegning fra avisen Daily Mail, 1962

Baggrund

STIGENDE EVNER, STIGENDE RISICI I CYBERSPACE

Forsvarets Efterretningstjenestes (FE's) risikovurdering fra 2019 viser behovet for at udvikle sikkerhed i cyberspace.

"Cyberangreb kan få alvorlige konsekvenser for Danmark. Cyberspionage kan både påvirke dansk sikkerhed og dansk konkurrencedygtighed. Cyberkriminalitet kan i værste fald betyde, at virksomheder og myndigheder ikke kan levere samfundsvigtige ydelser."[2]

FE's risikovurdering understreger cybertruslens omfang. Alle dele af det danske samfund er under angreb. Handlinger i og gennem cyberspace kan ramme både private og offentlige aktører, kan lamme målrettet kritisk infrastruktur som telenetværk og strømforsyning og kan eksponere individuelle borgeres fortrolige informationer. På politisk-strategisk niveau kan fremmede magter stjæle viden og hemmeligheder, som Danmarks velstand og handel bygger på, gennem skjult dataudvinding fra IT-systemer i eksempelvis energisektoren, forskningsinstitutioner og centraladministrationen.

Økonomisk, socialt, finansielt, politisk og sikkerhedsmæssigt er digitaliserede samfund som Danmark afhængige af cyberspace. Derfor har det alvorlige konsekvenser, når cyberangreb skader IT-systemer, der opbevarer, transmitterer og behandler samfundets data.

Selvom kritisk infrastruktur i overvejende grad bliver styret, ejet og drevet af private aktører og de civile dele af den offentlige sektor, er militærets rolle i cyberspace stigende.

I Danmark startede udviklingen i 2012, hvor Center for Cybersikkerhed blev oprettet under FE og nu har udviklet evnen til at gennemføre offensive cyberoperationer – en computernetværksoperationskapacitet.[3]

Udviklingen af en "Værnsfælles doktrin for militære cyberspaceoperationer" i 2019 viser også en omstilling i Forsvaret til at planlægge og operere i cyberspace.[4]

Traditionelt er militære styrkers rolle at afskrække andre fra at bruge militær magt, og, hvis det mislykkes, at udkæmpe en krig. Men hvordan forsvarer man sig militært i cyberspace – og hvordan virker afskrækkelse?

TEORIEN OM AFSKRÆKKELSE

"Når der er gensidig frygt, tænker mænd to gange, før de angriber hinanden." Som citatet ovenfor fra den oldgræske historiker Thukydid viser, er brugen af trusler for at beskytte egne interesser en gammel strategi. Men som teoretisk begreb blev afskrækkelse især udviklet under Den Kolde Krig.[5]

TEORIENS OPHAV

USA's bombning af Hiroshima og Nagasaki i 1945 viste, at atomvåbens altødelæggende potentiale gør ideen om at udkæmpe en atomkrig uholdbar. Stater har ikke interesse i at udkæmpe en krig med atomvåben, fordi fjendens nukleare modangreb risikerer at lede til uacceptabelt høje tab.

Den Kolde Krigs afskrækkelsesteori udspringer af det paradoks. Hvordan beskytter man status quo gennem atomvåben, hvis høje omkostninger ved anvendelse taler imod, at de faktisk bliver brugt? Fra dette paradoks udspringer ideen om, at atomvåben faktisk kan anvendes til at fastholde freden, da truslen om atomkrig og gensidig ødelæggelse vækker tilbageholdenhed.

AFSKRÆKKELSE HVORDAN

Afskrækkelse betyder, at man gennem en trussel får en aktør til at fravælge en handling. Afskrækkelse er derfor mere end truslens indhold. Den afskrækkende aktørs *troværdighed* samt modstanderens *opfattelse* heraf, er afgørende, da det er modstanderen, der i sidste ende skal vælge ikke at handle.

Derfor kræver troværdig afskrækkelse i udgangspunktet *tydelig politisk vilje og klarhed* omkring de mekanismer, den baserer sig på (se tekstboksen).

Troværdighed afhænger blandt andet af, om den afskrækkende aktør tidligere har gjort alvor af trusler, og om truslen er proportional med den handling, den skal afværge.

Afskrækkelse er derfor en politisk mere end en teknisk udfordring. Absolut afskrækkelse findes derfor ikke. Den konkrete afskrækkelse opstår i samspillet med den aktør, der skal afskrækkes. Afskrækkelse handler om troværdighed, forventninger og opfattelser, hvilket altid gør afskrækkelse usikkert.

Det viser sig eksempelvis ved, at usikkerhed også kan afskrække. *Tvetydigheder* omkring brugen af militære midler kan også være en del af en afskrækkelsesstrategi. Tydelig politisk vilje og klarhed med hensyn til truslens anvendelse kan altså udfordres af tvetydighed og uklarhed.

AFSKRÆKKELSE AF HVEM OG MED HVILKET FORMÅL?

Afskrækkelsesbegrebets historie betyder, at spørgsmål om mål, midler og aktører længe har været taget for givet. Fokus har primært været på at forstå, hvordan afskrækkelse kan medvirke til at undgå nukleare angreb mellem stormagter.

Logikken er derfor baseret på målsætningen om at undgå en omfattende atomkrig mellem Den Kolde Krigs to supermagter. Med andre ord fokuserer traditionel teoretisk viden om afskrækkelse på sammenlignelige aktører og et formål.

I dag er situationen forandret. Nye mål, midler og aktører gør afskrækkelse mere udfordrende. Ny teknologi skaber anderledes handlemuligheder i et sikkerhedspolitisk landskab, hvor aktører kan forstyrre status quo uden at gå i krig, og ikke-militære midler kan bruges til at opnå samme politiske mål som konventionelle våben. Det sætter spørgsmålstegn ved afskrækkelse. Hvad kan afskrækkes af hvem og med hvilke midler i en digitaliseret tidsalder? Den stigende afhængighed af cyberspace samt cyberspaces særegne natur er afgørende årsager bag den stigende betydning af disse spørgsmål. Derfor er det nødvendigt at belyse, hvad der gør cyberspace specielt.

AFSKRÆKKELSENS TEORI BASERER SIG PÅ EN FORVENTNING OM, AT AKTØRER HANDLER PÅ BAGGRUND AF RATIONELLE KALKULER

Hvis staten A frygter, at staten B vil foretage en handling, der er i strid med A's interesser, kan A iværksætte en trussel, som har til formål at få B til at opgive den givne handling og dermed afskrækker B.

I opstillingen af truslen kan A enten true med at reducere B's gevinster ved at foretage handlingen (nægtelse) eller ved at forøge de omkostninger, B har ved at foretage handlingen (straf).

- Perspektiv af en nyttekalkule. I denne nyttekalkule sammenligner B sin forventede nytte ved henholdsvis at foretage handlingen og fravælge handlingen.

- Hvis B samlet set vurderer, at den største nytte opnås ved at fravælge handlingen, lader B sig afskrække.

Tekstboks 1: Afskrækkelse gennem nægtelse eller straf [6]

Hvad er cyberspace?

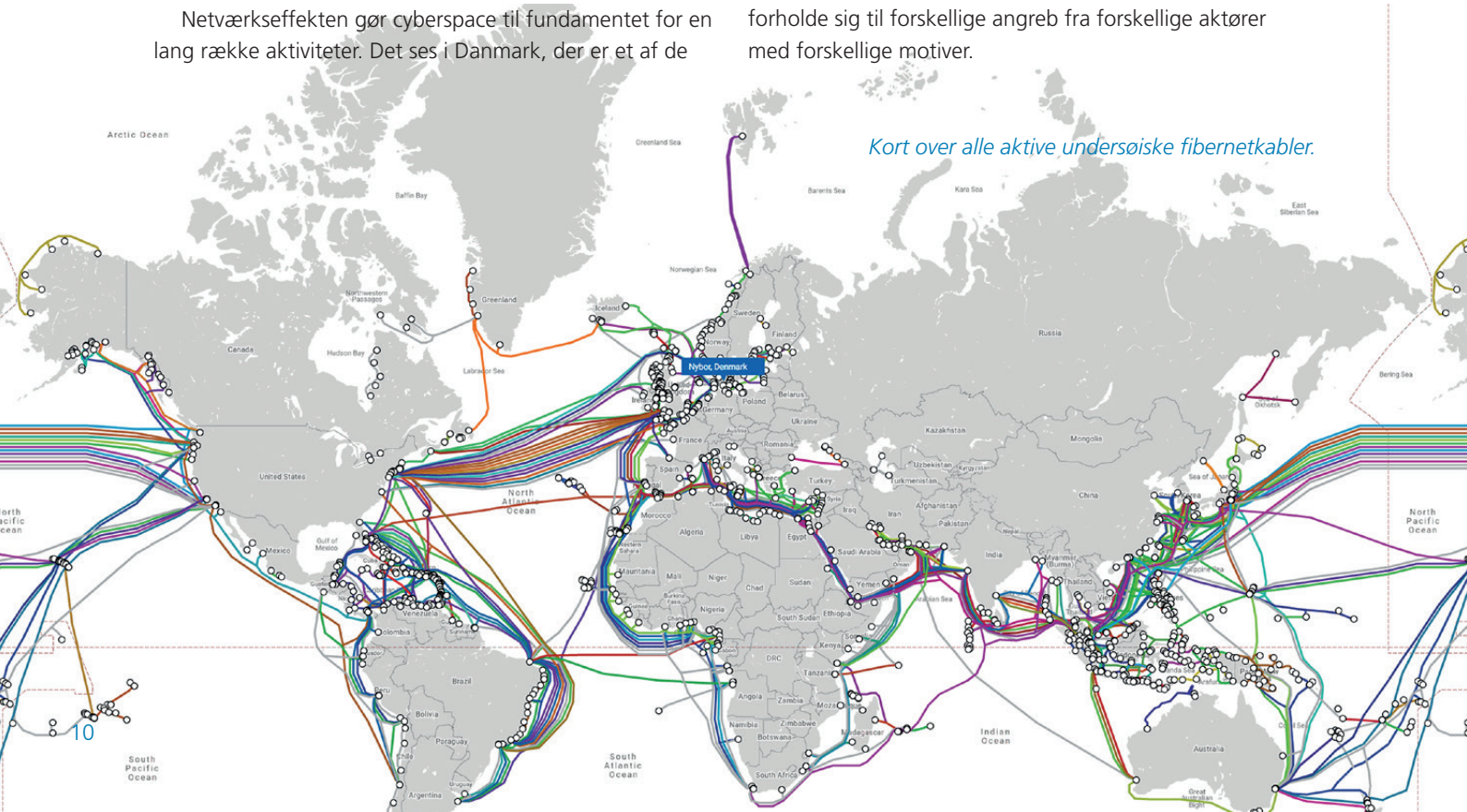
Cyberspace er global og menneskeskabt infrastruktur, der transporterer data og øger menneskers evne til at interagere på tværs af afstande. Det sker gennem et *åbent, globalt netværk* – i daglig tale internettet.[7]

Internettets åbenhed øger internettets værdi gennem såkaldt *netværkseffekt*. Netværkseffekt betyder, at værdien af at anvende et netværk afhænger af antallet af brugere. Det er illustreret i figur 1, som viser, hvordan flere forbindelser skaber mere indhold og forbundethed og udvider netværkets infrastruktur. Den globale internettrafik er således gået fra 100 gigabyte om dagen i 1992 til 46.600 gigabyte i sekundet i 2017.

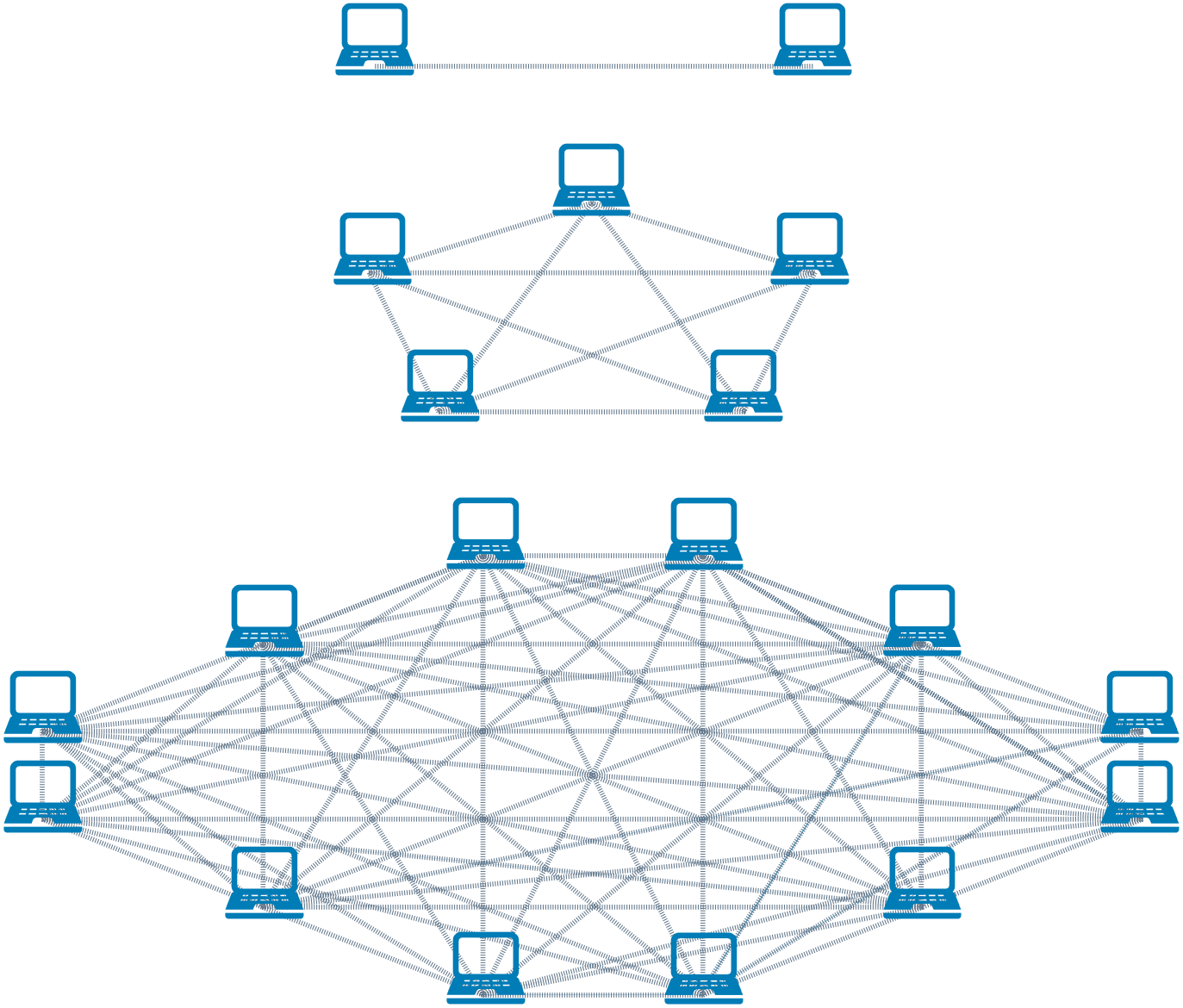
Netværkseffekten gør cyberspace til fundamentet for en lang række aktiviteter. Det ses i Danmark, der er et af de mest digitaliserede lande i verden, hvor cyberspace udgør infrastrukturen for de fleste samfundsfunktioner.[8]

Det globale netværks gevinster modbalanceres af *netværkssårbarheder*. Digitaliseringens dybde skaber mål for aktører, der kan få adgang til følsomme systemer og data. Digitaliseringens bredde betyder, at netværkssårbarhederne kan få forskellige konsekvenser for fysisk, økonomisk og samfundsmæssig sikkerhed.

Internettets åbenhed medfører, at en bred vifte af statslige og ikke-statslige aktører opererer i cyberspace og udnytter netværkssårbarheder til egen vinding. Cyberspace er også et *rum for konkurrence og konflikt*, hvor stater skal forholde sig til forskellige angreb fra forskellige aktører med forskellige motiver.



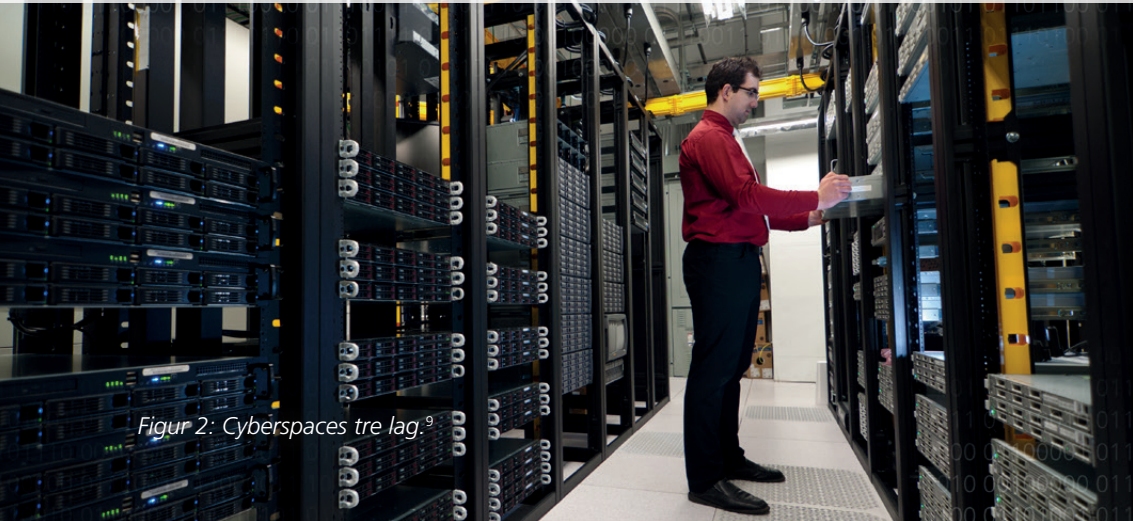
Kort over alle aktive undersøiske fibernetkabler.



Figur 1: Netværkseffekten

Cyberpersonalaget

Det logiske lag



Det fysiske lag

Figur 2: Cyberspaces tre lag.[9]

Tabel 1: Udviklingen i den globale internettrafik [10]

Cyberspace er menneskeskabt. Private aktører driver, udvikler og ejer det meste af cyberspace. Det gælder også mange af de systemer, der driver vigtige samfundsfunktioner såsom telenettet. Angreb mod private systemer kan altså få konsekvenser for stater og samfund. Det skaber en *offentlig-privat problematik* i cyberspace, der udfordrer grænsen mellem offentlige og private systemer og skaber uklar ansvarsfordeling for systemernes sikkerhed mellem offentlige og private aktører.

Arkitekturen for cyberspace kan opdeles i tre lag. *Cyberspaces tre lag* beskriver, hvordan cyberspace både er forbundet til den fysiske verden og er sin egen verden baseret på menneskeskabte regler og logikker. Kombinationen af det fysiske og det menneskeskabte er vigtig for at forstå, hvilke effekter der kan skabes i og gennem cyberspace og hvordan.

Cyberspace har et *fysisk lag*, der er geografisk og underlagt nationale myndigheder. Det fysiske lag er kontaktfladen til cyberspace og består af komponenter som servere og computere. De er sårbare over for både fysiske påvirkninger og angreb gennem cyberspace. Det er gennem det fysiske lag, cyberangreb skaber effekter i den fysiske verden.

Cyberspaces *logiske lag* består af *logisk* programmeret kode, der driver systemerne i cyberspace og gør, at applikationer og programmer fungerer. Det er altså gennem det logiske lag, at handlinger udføres i cyberspace. Indholdet af det logiske lag kan kun påvirkes virtuelt.

Personalaget omfatter aktørers (både menneskelige aktørers og maskiners) repræsentation i cyberspace og deres forhold til hinanden. Det er eksempelvis mailkonti og andre brugerprofiler, der anvendes på forskellige platforme i cyberspace. Repræsentationer i personalaget er unikke profiler, men kan bruges af alle, der besidder den information, som er nødvendig for at bruge dem.

Afskrækkelse i cyberspace?

Cyberspace er både infrastruktur og kamprum på samme tid. Derfor er afhængighed og sårbarhed to vedvarende betingelser for afskrækkelse i cyberspace. Cyberspaces forskellige funktioner er også årsagen til den store diversitet i cyberangreb, der tjener forskellige formål, udføres af forskellige aktører og antager forskellige former.

Det gør det svært at isolere, hvad der skal være mål for afskrækkelse i cyberspace. Figur 3 viser, hvad der potentielt kan være mål for afskrækkelse i cyberspace. Y-aksen beskriver niveauet fra fred til konflikt, som cyberangreb udfolder sig i. X-aksen beskriver forskellige mål for cyberangreb gående fra civile og kommercielle systemer (private aktører) til offentlige og militære systemer (statslige aktører). Ved at opstille de to dimensioner viser figuren mangfoldigheden af cybertrusler. Diversiteten af cybertrusler gør, at der er forskellige logikker for deres modforanstaltninger. Nogle trusler er alvorlige angreb, der imødegås med afskrækkelse for at undgå dem (cyberkrig), andre er mindre alvorlige angreb, der imødegås med afskrækkelse for at minimere dem (cyberspionage) og andre angreb er slet ikke mål for militær afskrækkelse (cyberkriminalitet). De tre felter, som er markeret på figuren med stiplede linjer, markerer snitfladerne for de forskellige logikker, som er på spil.

Størstedelen af de cyberangreb der foretages i Danmark er rettet mod danske private aktører. Det kan eksempelvis være for at få adgang til en virksomheds systemer for at foretage finansiel afpresning. Sådan cyberkriminalitet udføres som regel af ikke-statslige aktører og skader cyberspaces værdi som infrastruktur. Cyberkriminalitet er i udgangspunktet en politiopgave, der håndteres som anden kriminalitet. Det er illustreret i nederste felt, der omfatter niveauet mellem fred og gråzonen og private aktører. Det amerikanske justitsministerium og FBI's stigende involvering i amerikansk afskrækkelsesstrategi skaber dog tvivl om, hvor grænsen går mellem politiopgaver og militær afskrækkelse.

Angreb mod visse privatejede systemer er alligevel et nationalt sikkerhedsanliggende. Disse systemer kendetegnes som kritisk infrastruktur. Angreb mod det fysiske lag af den kritiske infrastruktur som automatiserede industrisystemer (styrings-, regulerings- og overvågningsanlæg eller SRO-anlæg) kan forårsage enorm fysisk skade. Angreb mod et vandrensningsanlægs styresystem kan eksempelvis forurene hele byers drikkevand.[11] Angreb mod det logiske lag med virtuelle skader er også alvorlige. Nedbrud i eksempelvis teleselskabers systemer kan bremse kommunikation i samfundet. Det afspejles i figuren ved, at cyberkrigslogikken rækker ind i arealet for kommercielle systemer.

Cybertruslen mod offentlige og militære systemer tager ofte form af cyberspionage, hvor aktører skaber adgang til netværk og i skjul indsamler information. Det kaldes Computer Network Exploitation (CNE). Fordi det er svært

HVAD SKAL AFVÆRGES VED AFSKRÆKKELSE?

Type af angreb: Er det kun angreb fra statslige aktører, der ødelægger militære eller andre fortrolige systemer, eller også mere udbredt cyberkriminalitet, der skal afværges?

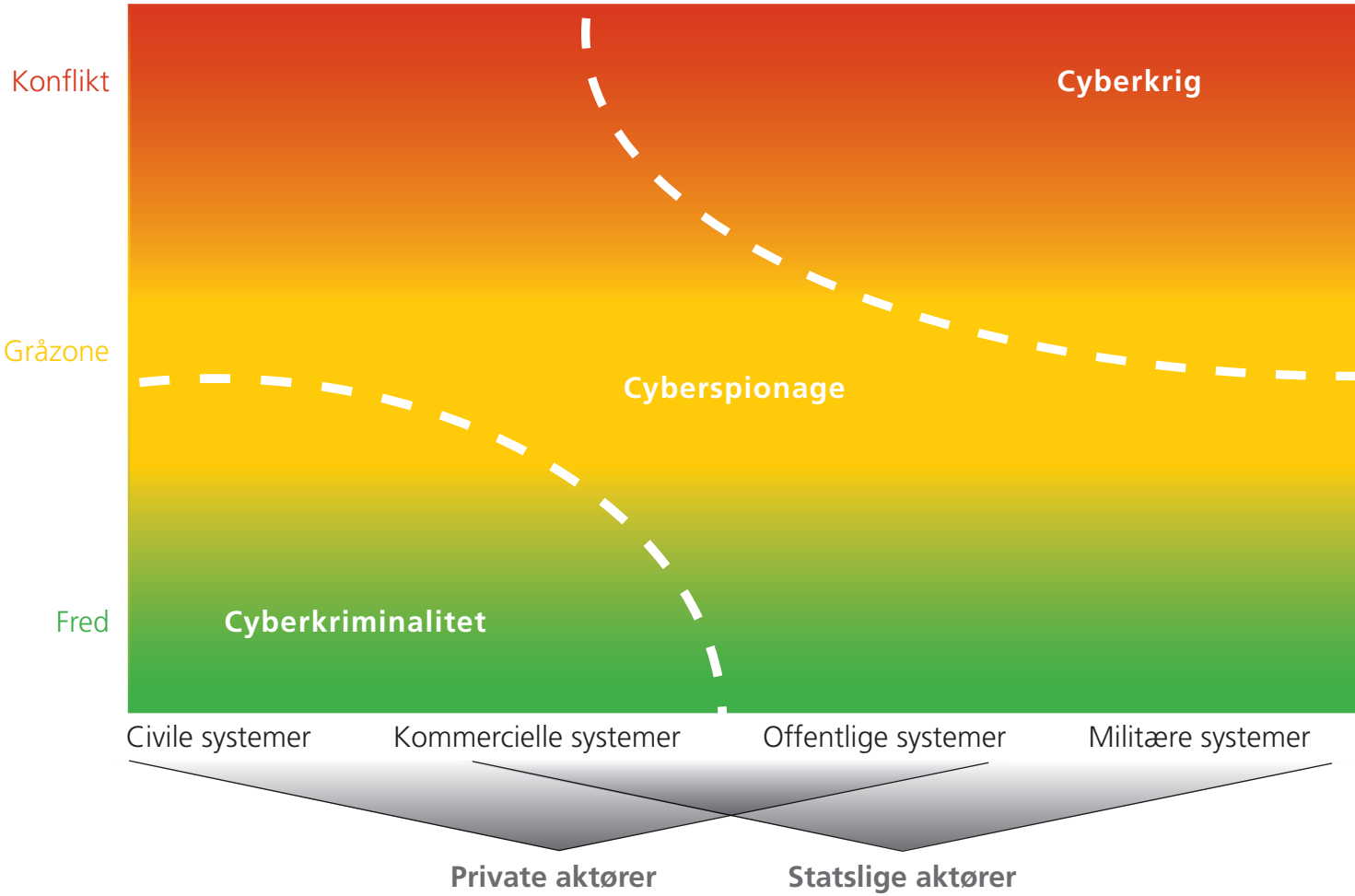
Effekter: Er det kun angreb, der skaber fysiske skader gennem det fysiske lag af cyberspace, eller også angreb, der udelukkende har virtuelle effekter i det logiske lag, der skal afværges?

at forhindre og bliver accepteret i en vis grad på linje med almindelig spionage, ligger det i feltet over cyberkriminalitet, men er heller ikke cyberkrig.

Cyberspionage er ofte et mål i sig selv, men i få tilfælde går det forud for angreb – Computer Network Attack (CNA). CNA er cyberkrigshandlinger, der målrettet ødelægger indhold i det logiske lag, ofte for at skabe kaskadeeffekter med hensyn til fysisk ødelæggelse. Det øverste felt markerer derfor, at stater har en særlig interesse i at afværge angreb mod offentlige og militære systemer samt kritisk infrastruktur.

Det er altså uklart, hvilke angreb der skal afværges, hvornår de skal afværges, og hvem der har ansvaret for det. Men hvad er rammerne for det?

Figur 3: Truslerne fra cyberspace



Hvordan?

3

UDFORDRINGER FOR AFSKRÆKKELSE I CYBERSPACE

Selv hvis der er enighed om, hvor staters ansvar for afskrækkelse begynder og ender, udfordrer tre ting afskrækkelse i cyberspace: 1) Afskrækkelse ved nægtelse kan ikke beskytte stater i cyberspace; 2) det er svært at identificere den angribende part; 3) gengældelsesangreb er svære at begrænse.

1) FORSVAR ER IKKE NOK

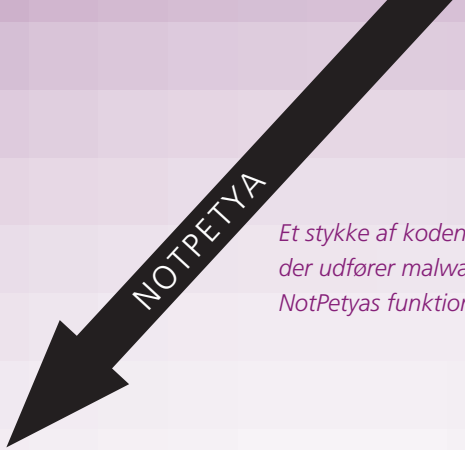
Cyberspaces korte historie viser, at afskrækkelse ved nægtelse og passivt forsvar (systemer der beskytter mod sårbarheder – som firewalls) er utilstrækkeligt til at stoppe angreb. Derfor har stater behov for at undersøge mulighederne for den anden form for afskrækkelse, nemlig afskrækkelse gennem straf.

Cybervåben udvikler sig hastigt. Malware (kode designet til at udrette skade på et mål) kan videreudvikles med nye egenskaber. Det var eksempelvis tilfældet for NotPetya-malwaren, der var en udvikling af den velkendte Petya-malware fra året før.

Det betyder, at passivt forsvar i cyberspace konstant skal udvikles og tilpasses. Tilpasningen sker i forhold til, at flere ting bliver koblet på nettet og dermed åbner flere flanker for angreb, men også i forhold til at holde systemer opdaterede i forhold til kendte sårbarhedsproblemer (patching).

Visse angreb er næsten umulige at undgå. På grund af de store ressourcer og lange tidshorisonter, som statslige aktører kan operere med, vil deres højt sofistikerede operationer altid være i stand til at bryde ind i systemer uden for eller gennem cyberspace. Cyberkriminalitet er også svært at forsvare sig mod. Det skyldes mængden af angreb (der bliver sendt op til 3,4 milliarder phishing mails om dagen), der ofte snyder brugeren til selv at installere malware, hvilket ingen firewall kan forhindre.

Passivt forsvar besværliggøres yderligere af cyberspaces hemmelige natur. Viden om adgangspunkter til beskyttede systemer bliver ikke altid delt, fordi der er interesse hos staternes efterretningstjenester i at beholde og eventuelt bruge den.



Et stykke af koden, der udfører malwaren NotPetyas funktioner.

```
seg000:96D4 C8 16 00 00          enter   16h, 0
seg000:96D8 57                   push    di
seg000:96D9 56                   push    si
seg000:96DA C6 46 EF 31          mov     byte ptr [bp+sigma+1], '1' ; -1nvalid s3ct-id
seg000:96DE C6 46 F0 6E          mov     byte ptr [bp+sigma+2], 'n'
seg000:96E2 C6 46 F1 76          mov     byte ptr [bp+sigma+3], 'v'
seg000:96E6 C6 46 F2 61          mov     byte ptr [bp+sigma+4], 'a'
seg000:96EA C6 46 F3 6C          mov     byte ptr [bp+sigma+5], 'l'
seg000:96EE C6 46 F5 64          mov     byte ptr [bp+sigma+7], 'd'
seg000:96F2 C6 46 F6 20          mov     byte ptr [bp+sigma+8], ' '
seg000:96F6 C6 46 F7 73          mov     byte ptr [bp+sigma+9], 's'
seg000:96FA C6 46 F8 33          mov     byte ptr [bp+sigma+0Ah], '3'
seg000:96FE C6 46 F9 63          mov     byte ptr [bp+sigma+0Bh], 'c'
seg000:9702 C6 46 FA 74          mov     byte ptr [bp+sigma+0Ch], 't'
seg000:9706 B0 2D                mov     al, '-'
seg000:9708 88 46 EE             mov     byte ptr [bp+sigma], al
seg000:970B 88 46 FB             mov     byte ptr [bp+sigma+0Dh], al
seg000:970E B0 69                mov     al, 'i'
seg000:9710 88 46 F4             mov     byte ptr [bp+sigma+6], al
seg000:9713 88 46 FC             mov     byte ptr [bp+sigma+0Eh], al
seg000:9716 C6 46 FD 64          mov     byte ptr [bp+sigma+0Fh], 'd'
seg000:971A 33 FF                xor     di, di
seg000:971C
```

2) ATTRIBUTION: HVEM HAR GJORT DET?

Attribution betyder at placere ansvar. Inden for en kort tidshorisont er det teknisk udfordrende at efterforske, hvem der står bag et cyberangreb. Derfor er det svært at vide, hvem der skal straffes. Det udfordrer præmisserne for afskrækkelse og sænker barrieren for, at aktører gennemfører angreb. Succesfuld attribution har derfor en afskrækkende effekt, da det nægter modstandere gevinsten ved anonymitet.

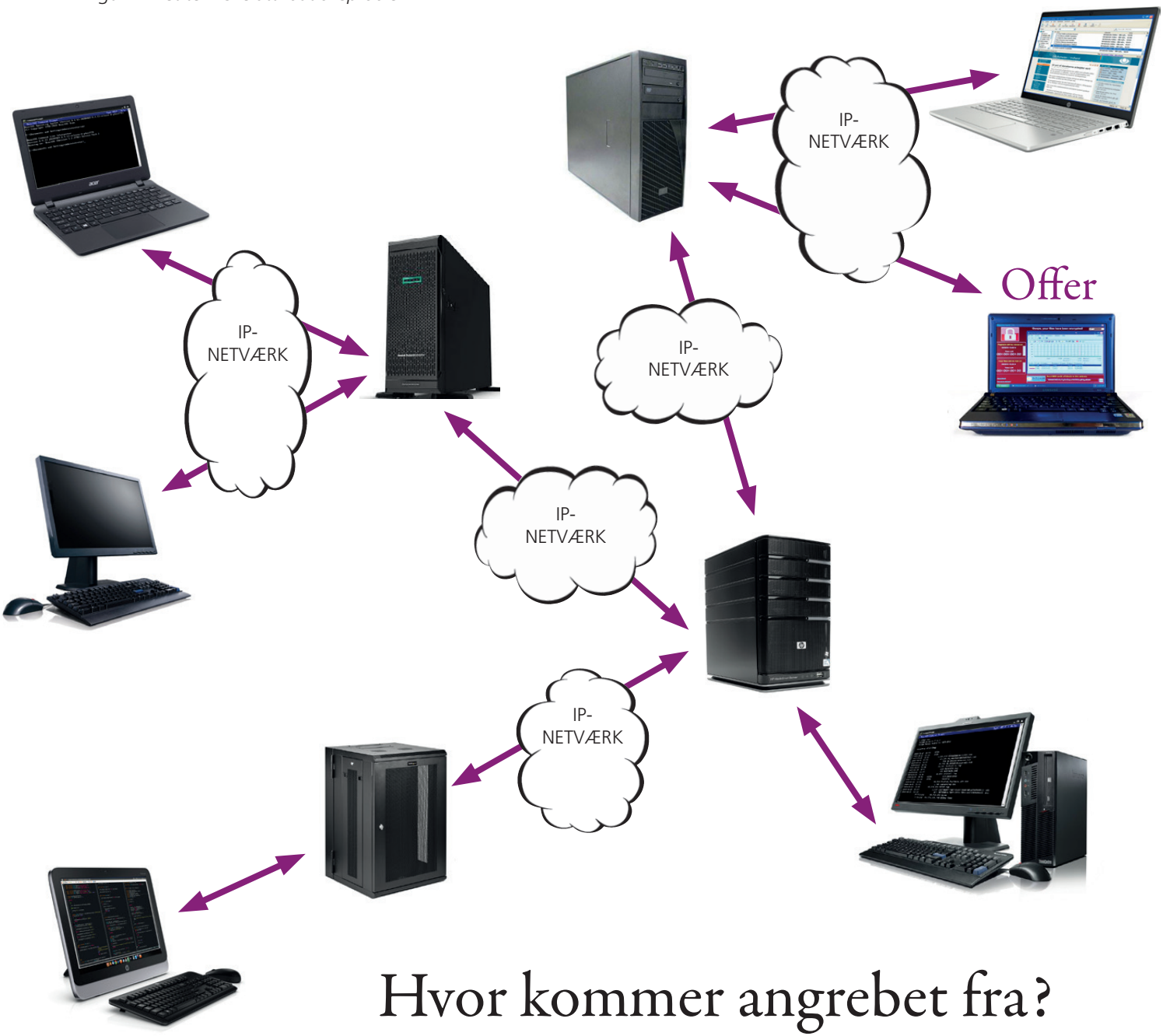
Attribution kan tilskrives computeren, som angrebet er udført fra, personen bag maskinen eller den ansvarlige part for angrebet. Udfordringerne for de to første trin er primært tekniske og efterretningsmæssige. Her er målet at isolere, hvem der gjorde det. Som vist i figur 4 kan et angreb sløres, ved at det bliver udført gennem flere netværk og computere. Derfor er det teknisk udfordrende at finde angrebets udgangspunkt. Efter at have fundet computeren bag angrebet kræver det efterretningsmæssig viden at placere en person bag computeren på tidspunktet for angrebet.

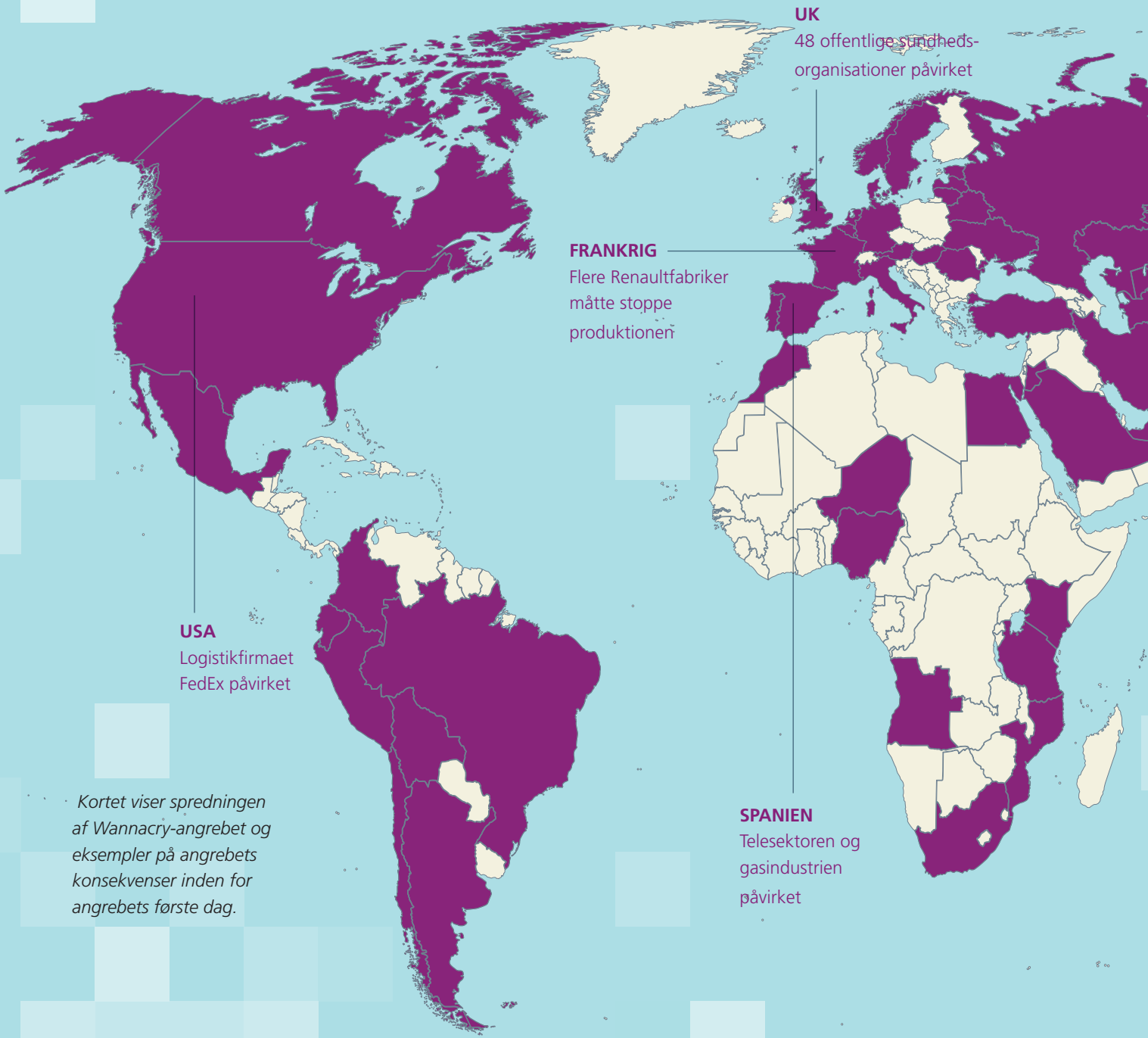
Det sidste trin handler om at placere ansvaret for angrebet. Det er ofte et politisk spørgsmål – især når en regering eller et land udpeges som ansvarlig. Attributionsudfordringen er altså mere end bare teknik. Den politiske ansvarsplacering besværliggøres samtidig af, at tekniske beviser sjældent er "en rygende pistol" i cyberspace, og at angribende stater kan distancere sig fra angrebet ved at anvende private hackergrupper og overtagede systemer i andre lande.

OFFENTLIG-PRIVAT SAMARBEJDE

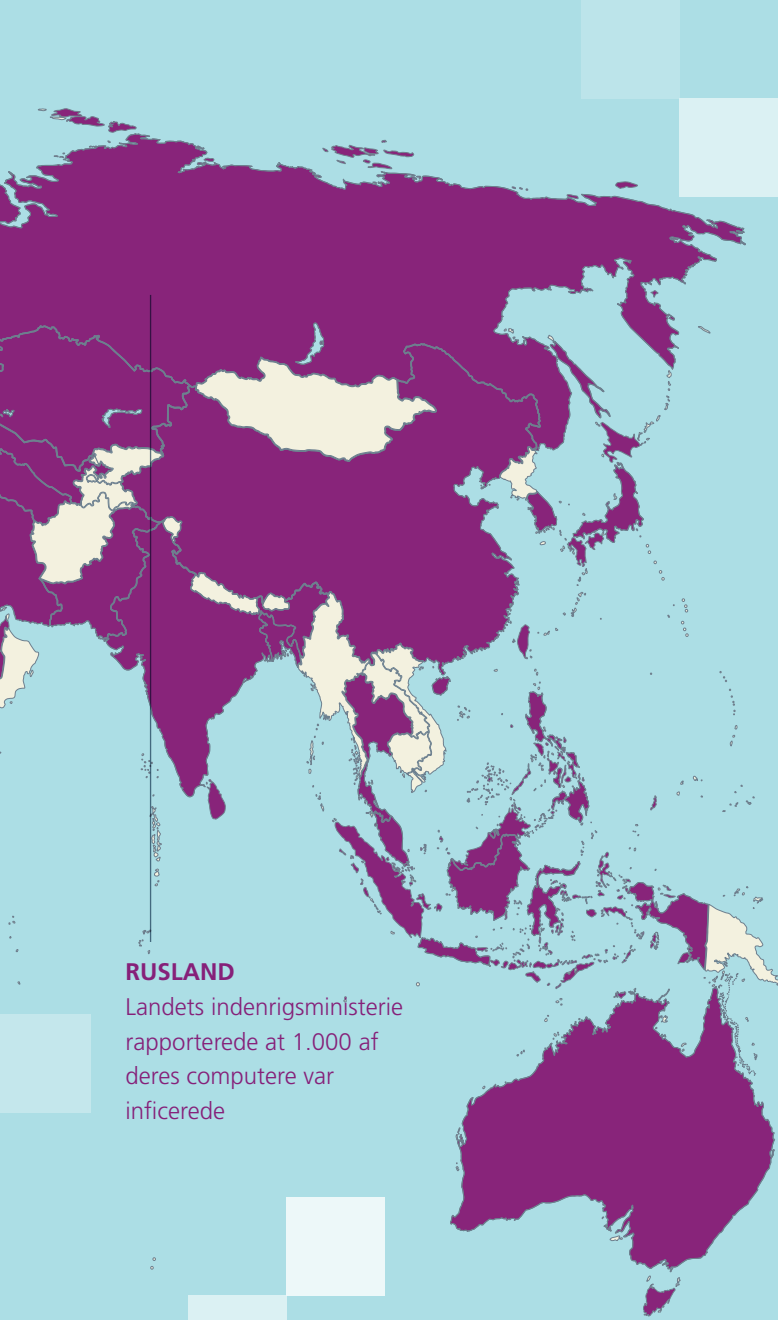
Det er i høj grad private aktører inden for IT-sikkerhedsindustrien, der besidder ekspertisen til at overvåge cyberspace og attribuere angreb. Derfor udgør offentlig-privat samarbejde en central indsats i forbindelse med at afklare attributionsspørgsmål.

Figur 4: Det tekniske attributionsproblem





Kortet viser spredningen af Wannacry-angrebet og eksempler på angrebets konsekvenser inden for angrebets første dag.



3) GENGÆLDELSE ER SVÆRT

Det er svært at forudsige konsekvenserne af gengældelsesangreb i cyberspace på grund af sprednings-, skade- og risikoudfordringer.

1. Ligesom biologiske våben er CNA et uforudsigeligt middel, der er besværligt at begrænse. Forbundetheden i cyberspace gør, at CNA kan sprede sig til mål, der ikke var planlagt og dermed inficere og potentielt ødelægge systemer uden for operationens politiske mandat. Kortet på denne side viser eksempelvis, hvor hurtigt angrebet WannaCry spredte sig på en dag. Selv meget avancerede og specifikke CNA'er har vist sig ikke at kunne begrænses til målet for angrebet. Det var eksempelvis tilfældet ved Stuxnet-ormen, som var specielt designet til at ødelægge en bestemt slags atomcentrifuger i et bestemt iransk atomanlæg. Alligevel spredte ormen sig til computere i blandt andet Indonesien, Indien og USA.[12]

2. Det er svært at forudsige effekterne af CNA. Effekten af CNA er proportional med den ramte aktørs afhængighed af cyberspace, netværkets sikkerhedsniveau, og hvor afhængigt det samlede netværk er af det målrettede system. Hvis der er mange IT- systemer, hvis drift er afhængig af det ramte mål, bliver det svært at forudsige, hvorvidt angrebet vil forhindre civile aktører eller aktører i andre lande i almindelig brug af cyberspace.

3. Endelig er det uklart, fordi militær afskrækkelse i cyberspace er nyt, hvad der retfærdiggør et gengældelsesangreb, og hvad et legitimt modsvar består af. Det skyldes, at der endnu ikke er underliggende normer for legitim statslig adfærd i cyberspace. Uvisheden omkring de fælles spilleregler skaber usikkerhed omkring, hvornår et gengældelsesangreb er proportionalt, og hvordan en modstander vil reagere på det.

På trods af disse udfordringer vil stater alligevel forholde sig til, hvordan de i praksis kan straffe, i forsøget på at blive mere sikre i cyberspace, når de ikke blot kan forlade sig på forsvar.

To strategier for afskrækkelse i cyberspace

Afskrækkelse ved straf i cyberspace kan følge to forskellige strategier. Den første er at afskrække cybermodstandere gennem cyberangreb. Det kaldes vertikal eskalation Det er i høj grad blevet en del af den amerikanske cyberkommandos strategi. Det ses eksempelvis i officielle udmeldinger om, at amerikanske cyberenheder har installeret malware i det russiske energinet for at afskrække russisk CNO-aktivitet mod USA.

Vertikal eskalation er svært, fordi attributionsproblemet skaber tvivl om det rette mål for gengældelsesangrebet, og spredningss- og skadeudfordringer gør det svært at sikre et proportionalt gengældelsesangreb. Attribution skaber også tvivl om den afskrækkende parts egen identitet og gør dermed signaleringen uklar. Som vist i det amerikanske eksempel må stater derfor officielt påtage sig ansvaret for CNA-angreb. Det gør truslen om straf mindre nyttig, da modstanderens mulighed for at opdage og begrænse angrebet øges. Afskrækkelse ved straf gennem CNO-aktivitet er altså mere nyttig, når straffen realiseres, frem for når man truer med at gøre det, og det øger risikoen for eskalation.

Den anden strategi baserer sig på at flytte straffen fra cyberspace til fysiske domæner, hvor konventionelle militære redskaber kan anvendes, og dermed omgå de tekniske udfordringer for afskrækkelse i cyberspace. Det kaldes horisontal eskalation.

Det var eksempelvis tilfældet ved israelske forsvarsstyrkers bombeangreb på en bygning i Gaza i 2019, som angiveligt husede en Hamas-hackergruppe. Det horisontale skift behøver ikke at blive gennemført med militære instrumenter. EU har eksempelvis udviklet en fælles responsramme, Cyber Diplomatic Toolbox (CDT), der skal signalere evne og vilje til at foretage økonomiske sanktioner mod aktører, der udfører eller planlægger cyberangreb mod EU og dets medlemsstater.

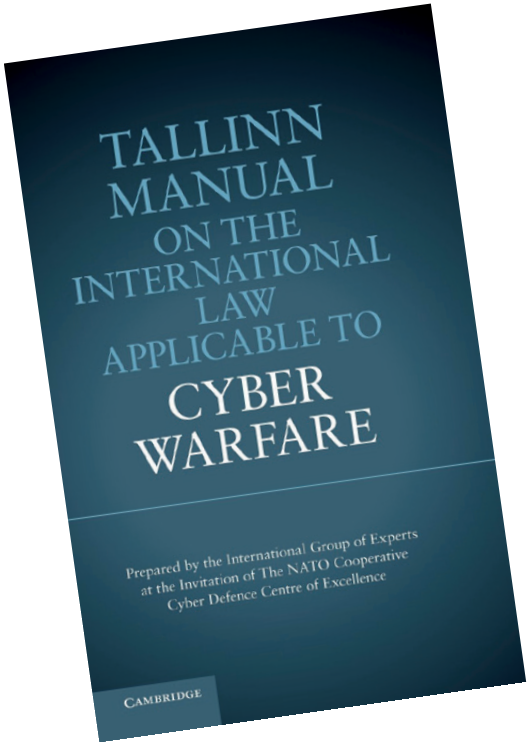
Horisontal eskalation åbner op for andre problemer. Ved at skifte til konventionelle militære instrumenter kan situationen nemmere krydse tærsklen til væbnet konflikt. Omvendt har ikke-militære optioner måske ikke samme afskrækkende effekt som en ødelæggende militær straf.

Logoet for den amerikanske Cyberkommando, der planlægger, koordinerer og udfører amerikanske militære cyberspace-operationer.

Danmarks sikkerhedsudfordringer

Danmarks sikkerhedsudfordringer i cyberspace rækker ud over udfordringerne for afskrækkelse: Der gælder andre spilleregler for operationer i cyberspace; Danmark kan ikke på samme måde dække sig bag sine allierede; og den høje grad af digitalisering gør Danmark ekstraordinært sårbar.

Sikkerhedsudfordringerne eksisterer i et nyt og anderledes strategisk rum, som bliver belyst af følgende tre punkter.



Tallinnmanualen (2013) udgør et af de tidligste forsøg på at fastslå folkerettens anvendelse i cyberkonflikter. Den blev skrevet af internationale eksperter inviteret af NATO Cooperative Cyber Defence Centre of Excellence

1. Hvad kan Danmark gøre alene i cyberspace, og hvor aktiv vil Danmark være for at forsvare sig selv? I geopolitiske termer er Danmark en småstat, der sjældent handler alene, men i cyberspace kan Danmark blive en lille, men robust cybermagt. Relativt små investeringer i CNA-kapaciteter kan give store offensive egenskaber. Det fordrer en politisk dialog om et ambitionsniveau for, hvad Danmark kan og vil gøre i cyberspace for at forsvare danske interesser. Det hænger også sammen med strategiske overvejelser bag dansk afskrækkelse: Hvor bredt et omfang af handlinger i cyberspace skal Danmark forholde sig til, og hvor proaktiv skal afskrækkelsen være?

2. Hvordan kan Danmark være en nyttig allieret i cyberspace? Siden NATO-topmødet i 2018 har Danmark valgt at tilbyde nationale cyberkapabiliteter til indsættelse inden for rammen af NATO. CNA kan altså nyttiggøre Danmark for dets kerneallierede. CNA kræver ikke "støvler på jorden", hvilket reducerer faren mod danske soldaters liv, men fungerer CNA-bidrag så på samme måde som konventionelle militærbidrag i alliancelogikken? CNA-bidrag risikerer også at gøre Danmark til mål for gengældelsesangreb i et kamprum, hvor NATO's modstandere er mere villige til at gå i clinch med militæralliancens medlemmer, og hvor Danmark kan stå mere alene. Alliancepolitiske logikker og risici og deres sammenhæng i cyberspace er uklare, hvilket lægger op til en politisk diskussion af, i hvilken grad og med hvilke forventninger Danmark kan placere sig i cyberfrontlinjen for sine allierede.

3. I hvor høj grad vil og kan Danmark bidrage til den internationale normdannelse? Udviklingen af fælles internationale normer og tillidsskabende foranstaltninger foregår i flere internationale fora (eksempelvis FN, EU, NATO og

OSCE) og er i småstaten Danmarks interesse. Det bidrager eksempelvis til at værne mod Danmarks store netværkssårbarheder ved at tabuisere angreb mod civile mål og kritisk infrastruktur i fredstid. Anvendelsen af CNA risikerer at spænde ben for den diplomatiske indsats om tilbageholdenhed i cyberspace på grund af risikoen for uforudsete følgeskader. Det skaber uklare betingelser for, hvornår CNA bør aktiveres, og hvordan risikoen for følgeskader fra CNO-operationer skal håndteres.

Både på et operationelt og på et strategisk plan er betingelserne for, hvordan Danmark kan agere militært, altså ikke de samme i cyberspace som uden for cyberspace. Danske beslutningstagere kan derfor ikke forlade sig på sædvanlige danske sikkerhedsstrategier eller de forhold og antagelser, der bliver taget for givet i andre sikkerhedspolitiske sammenhænge.

De tre punkter viser to underliggende betingelser for en dansk position i den uafklarede strategiske debat om militært engagement i cyberspace. Hvor fremadlænet skal Danmark være i cyberspace? Og i hvilken grad vil og kan Danmark handle sammen med sine allierede?

At definere en dansk position for militær handlen i cyberspace er derfor en politisk-strategisk udfordring, som mange offentlige aktører er med til at definere i praksis. Afskrækkelse er en væsentlig del af det, men det handler også om at balancere de tre anderledes betingelser for det strategiske rum og diskutere mere eller mindre røde linjer for truslerne i cyberspace. Det nødvendiggør en politisk-strategisk diskussion af mål, midler, risici og politisk ambitionsniveau, der erkender de fundamentalt anderledes dynamikker sammenlignet med traditionel dansk forsvars- og sikkerhedspolitik samt de mange uvisheder, en dansk position baseres på.

Læs mere om afskrækkelse i cyberspace:

Jacquelyn Schneider, "Deterrence in and through cyberspace", I: Cross-domain deterrence in an era of complexity, Jon R. Linsay & Erik Gartzke, Oxford: Oxford University Press 2019.

Tobias Liebetrau, Offensive Cybermidler i Europa: I Gråzonen mellem angreb, spionage og forsvar, Center for Militære Studier 2020.

Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace", International Security, 41: 3 (vinter 2016/17), s. 44–71.

US Joint Staff, Updated doctrine for Cyberspace Operations (Joint Publication 3-12), 8. juni 2018.

Forsvarsakademiet, "Værnsfælles doktrin for militære cyberspaceoperationer", september 2019.

Billedkilder

Side 3 / 4: Soldater som firmahold i Counterstrike til Copenhagen Games. *Forsvarsgalleriet / Kristian Brøndum*

Side 4: Berlingske Tidende 2019, "Hård kritik af ny lov om cybersikkerhed:
'Helt og aldeles uacceptabelt i et demokratisk samfund'"
BT august 2018, "Supervirus lagde Mærsk ned i dagevis og kostede milliarder"
Ekstra Bladet oktober 2015: "Massiv hacker-bølge kidnapper danskeres data"
Kristeligt-dagblad oktober 2018, "Data fra 29 millioner facebookbrugere endte hos hackere"

Side 6: Karikaturtegning af President John F. Kennedy og Sovjetunionens generalsekretær Nikita Khrusjtjov fra den engelsk avis Daily Mail, 1962. *Tegnet af Leslie Gilbert Illingworth*

Side 9: Atombomben Atombomberne over Nagasaki,1945. *Wikimedia Commons*

Side 10: Kort over alle aktive undersøiske fibernetkabler. *Google*

Side 8: Illustration over netværkseffekt i simple telefonnetværk. *Signs & Wonders*

Side 12: Cyberspaces tre lag. Illustrationen baseret på den amerikanske cyberdoktrin fra 2018.
Shutterstock (stockfour / metamorworks). Fotocollage af Signs & Wonders

Side 17: Del af kildekoden for NotPetya-malwaren.
http://blog.ptsecurity.com/2017/06/notpetya-and-petya-compared-any-hope.html

Side 20: Kortlægning af de 99 ramte lande af WannaCry-malwareen inden for den første dag af angrebet.

Side 14: U.S. Army solday bærer United States Cyber Command patch under øvelsen "Cyber Guard 2015". The two-week "Cyber Guard 2015" i Suffolk, Virginia. *Marvin Lynchard, Department of Defense / Alamy*

Side 16: Tallinn Manual on the International Law Applicable to Cyber Warfare.
https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE

Noter

1. Se eksempelvis for dybere gennemgang: Tobias Liebetrau, Dansk offensiv cybermagt mellem angreb, spionage og forsvar: en komparativ analyse på tværs af Europa. Center for Militære Studier, 2020.

2. Forsvarets Efterretningstjeneste, Efterretningsmæssig Risikovurdering 2018: (København: Forsvarets Efterretningstjeneste, 2018), s. 11.

3. Forsvarsministeriet, "Offensive Cybereffekter", februar 2019: https://fmn.dk/temaer/nato/Documents/2018/Faktaark-cyber-effekter.pdf

4. Forsvarsakademiet, "Værnsfælles doktrin for militære cyberspaceoperationer", september 2019

5. Afskrækkelsesteorien er en bred og nuanceret akademisk tradition, og det er kun de mest grundlæggende logikker og argumenter, som inddrages her. For klassiske introduktioner til afskrækkelse, se f.eks. Bernard Brodie, "The Anatomy of Deterrence", World Politics, 11:2 (1959), 173-191; Thomas Schelling, "The Role of Deterrence in Total Disarmament", Foreign Affairs, 40:3 (1961), 392-406. For nyere perspektiver på afskrækkelse og afskrækkelsesteorien i dag, se f.eks. Freedman, Deterrence; Jeffrey W. Knopf, "The Fourth Wave in Deterrence Research", Contemporary Security Policy, 31:1 (2010), 1-33; Patrick M. Morgan, "The State of Deterrence in International Politics Today", Contemporary Security Policy, 33:1 (2012), 85-107; T.V. Paul, Patrick M. Morgan & James J. Wirtz (red.), Complex Deterrence: Strategy in the Global Age, Chicago: The University of Chicago Press, 2009.

6. Tekstboksen er fra CMS-rapporten Orden og afskrækkelse: Vestens håndtering af Rusland efter annekteringen af Krim af Henrik Breitenbauch, Niels Byrjalsen, Mark Winther og Mikkel Broen Jakobsen, Center for Militære Studier, juni 2017.

7. Mark Raymond, "Managing Decentralized Cyber Governance", I: Gary Schaub Jr. Understanding Cyber Security: Emerging Governance & Strategy New York, Rowman & Littlefield, 2018, s. 26-27.

8. Vurderet på baggrund af Europa-Kommissionen, "The Digital Economy and Society Index", september 2019: https://ec.europa.eu/digital-single-market/en/desi

9. Se den amerikanske cyberdoktrin for en nærmere beskrivelse af cyberspaces tre lag: US Joint Chiefs of Staff, Updated doctrine for Cyberspace Operations (Joint Publication 3-12), 8. juni 2018, s. vii-viii.

10. Cisco "Cisco Visual Networking Index: Forecast and Trends, 2017–2022, White Paper" Cisco VNI, 2018: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

11. Andy Greenberg, Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, 2019, New York: Random House USA Inc, 1-368.

12. Symantec, "W32.Stuxnet", januar 2020: https://www.symantec.com/security-center/writeup/2010-071400-3123-99