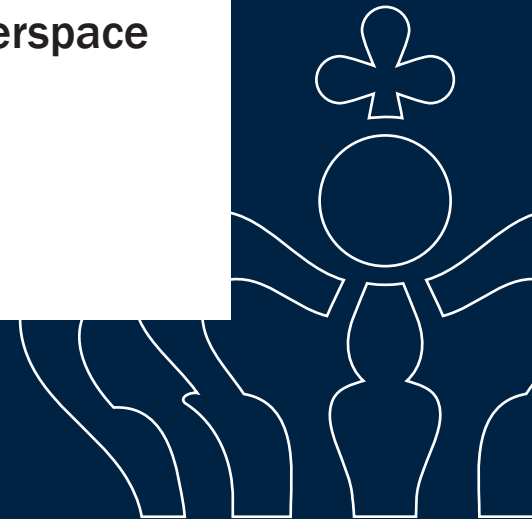


Kinas kapabiliteter i cyberspace

Strategisk afskrækkelse?

Af Magnus Hjortdal, forskningsmedarbejder,
Institut for Strategi

Brief



Kinas kapabiliteter i cyberspace Strategisk afskrækkelse?

**Af Magnus Hjortdal, forskningsmedarbejder,
Institut for Strategi**

Magnus Hjortdal er forskningsmedarbejder ved Institut for Strategi. Hans primære fokusområder er Kinas udenrigs- og sikkerhedspolitik og Kinas forhold til USA.

Magnus Hjortdal kan kontaktes på ifs-s-01@fak.dk

Institut for Strategi - www.fak.dk/fsmo/ifs
Fakultet for Strategi og Militære Operationer

Forsvarsakademiet Ryvangs Allé 1 2100 København Ø www.fak.dk



Forsvarsakademiet

Forsvarsakademiet er dansk forsvars internationale videncenter, og vi forsker i et bredt felt af militære emner. Vores forskningsmæssige prioriteringer, deriblandt overordnede emner og ressourcefordeling, fastsættes af chefen for Forsvarsakademiet. Chefen støttes i det arbejde af et forskningsråd.

Forsvarsakademiets forskning skal oplyse og udfordre brugerne, hvad enten de er i forsvaret eller i det omkringliggende samfund. Det kan kun opnås, hvis den enkelte medarbejder har frihed til at tilrettelægge sine forskningsprojekter og til at drage sine egne konklusioner. Det er et princip, som hyldes ved Forsvarsakademiet.

God fornøjelse ved læsning af Forsvarsakademiets publikationer!

© Forsvarsakademiet

København januar 2010

Forsvarsakademiet

Institut for Strategi

Svanemøllens Kaserne

Postboks 2521

2100 København Ø

Tlf.: 3915 1210

Fax: 3915 1504

Redaktør: Institutchef Nicolas T. Veicherts.

ifs-01@fak.dk, tlf.: 3915 1210

Grafisk Design: Bysted

ISBN: 9788791421891

Udkommer kun i elektronisk form

Forsvarsakademiets forlag

Indhold

| | |
|--|----|
| Resumé..... | 4 |
| Indledning | 5 |
| Cyberspace og Kina | 7 |
| Kinas tanker og evner i cyberspace..... | 8 |
| Aggressive og omfattende angreb fra Kina | 8 |
| Eksempler på den totale afskrækkelse..... | 9 |
| USA's el-net og en luftbase | 10 |
| Joint Strike Fighter, Pentagon og Merkel | 10 |
| Google var blot en lille del af et større angreb..... | 11 |
| Kina svarer igen | 12 |
| Konklusion og perspektiver: Kina som cybermagt og supermagt... | 13 |
| Efterskrift: Krigen kommer aldrig..... | 14 |
| Litteraturliste | 15 |

Resumé

Briefet præsenterer tre årsager til at stater anvender deres evner i cyberspace på en offensiv måde, og viser at cyberspace er – og vil blive ved med at være – et afgørende element i Kinas strategi for opstigningen i det internationale system. De tre årsager er: 1) afskrækkelse via infiltration, 2) militær-teknologisk spionage, samt 3) industrispionage for økonomisk vinding.

Briefet dokumenterer, at Kina har en større interesse i at anvende cyberspace på en offensiv måde, end andre aktører på området som fx USA. Det skyldes, at Kina har mere at vinde ved at spionere og afskrække bl.a. USA via cyberspace. Herudover dokumenteres det, at Kina udvikler sig kraftigt på området, hvilket ligger i forlængelse af Kinas traditionelle strategiske tænkning og den nuværende kinesiske debat.

Endvidere fremdrager briefet en del eksempler på offensive aktioner i cyberspace, hvor Kina beskyldes for at stå bag. Der har bl.a. været cyberangreb på et atomvåben-laboratorium, forsvarsministerier (herunder Joint Strike Fighter-kampflyet og en luftbase), det amerikanske el-net, samt den nylige Google-sag, som har vist sig at være en lille del af et omfattende angreb.

Der er dog også argumenter, der nuancerer billedet af Kina som en offensiv aktør i cyberspace. Nogle mener, at Kina selv er udsat for ligeså mange angreb fra andre stater, og yderligere har visse aktører i USA og Vesten en interesse i at overvurdere Kinas evner i cyberspace for at sikre deres budgetter.

Endeligt konkluderer briefet, at Kina *kan* benytte cyberspace til at afskrække USA, og på et senere tidspunkt bruge det til at blive en reel supermagt på det teknologiske og militære område. Den kinesiske opstigning vil dog ikke skabe nogen åben krig med USA, som nogle frygter, da forholdet er baseret på gensidig afskrækkelse.

Indledning¹

“In today’s information age, the People’s Republic of China has replaced and even improved upon KGB methods of industrial espionage to the point that the People’s Republic of China now presents one of the most capable threats to U.S. technology leadership and by extension its national security”

Dan Verton, ekspert i cyberkrig
(Verton 2008: 4)

Læser kineserne med på vores e-mails? Kan de kopiere vigtige oplysninger fra vores computere? Debatten i mange medier tilskriver, at man bør tænke sådan. Derfor vil dette brief bidrage til mere oplysning om, hvad Kina i cyberspace egentlig er for en størrelse.

Formålet med dette brief er, at beskrive de kinesiske evner i cyberspace, samt forklare og undersøge, hvorfor Kina opretholder og anvender en aggressiv cyberkapabilitet, og hvorfor USA frygter disse kapabiliteter.

Indledningsvis vil jeg forklare, hvorfor cyberspace er en vigtig dimension i dagens udenrigs- og sikkerhedspolitik. Herefter gennemgår jeg de kinesiske evner på området, og forklarer via udvalgte eksempler, hvorfor USA føler sig skræmt. Endelig trækker jeg de kinesiske evner i cyberspace op på et strategisk niveau, hvori det argumenteres, at Kinas udbygning af dets evner i cyberspace kan sikre dets opstigning til en status som supermagt på længere sigt.

Cyberspace er afgørende for moderne krigsførelse. Det gælder både på det rent operative niveau, hvor soldaterne er dybt afhængige af cyberspace, men også på det strategiske niveau, hvor svagheder og styrker i cyberspace kan benyttes til at afskrække og præge den strategiske magtbalance.

Dette brief opererer med tre årsager til at stater søger at opretholde og anvende en aggressiv cyberkapabilitet:²

- 1) afskrækkelse af andre stater via infiltration af kritisk infrastruktur.
- 2) opnå viden via spionage i cyberspace, der vil give stater mulighed for at springe flere militære udviklingstrin over.
- 3) økonomiske hensyn, hvor teknologiske fremskridt eksempelvis opnås via industrispionage (her kan det foregå udenom officielle institutioner).

(1) En tak til Peter J.B. Gottlieb, Ditte Tøfting-Kristiansen, Andreas Andersen, Sigge Aaberg Kærn og Emma Knudsen for kommentarer samt korrekturlæsning.

(2) Herhjemme skriver Forsvarets Efterretningstjeneste (FE 2009: 19) i den årlige åbne risikovurdering, at “[t]ruslen fra spionage fortsat [kommer] fra visse udenlandske efterretningstjenester, der har interesse i dansk forsvar, forsvarets internationale engagement samt NATO og det europæiske forsvarssamarbejde”. Herudover betoner FE, at ”Spionagen fortsat [sker] gennem en bred vifte af metoder, spændende fra brug af åbne kilder som f.eks. internettet til den hemmelige virksomhed, hvor man forsøger at udnytte andre personer til at skaffe sig oplysninger. Der er ingen indikationer på, at den efterretningsmæssige trussel vil aftage (FE 2009: 19).”

En analyse af Kinas statslige evner i cyberspace er yderst relevant som analysesubjekt, da Kina har mere nytte af at have offensive evner i cyberspace end de fleste statslige aktører. Jeg skal dog understrege, at formålet med dette brief ikke er at udstille Kina som klassens frække dreng, der som den eneste bryder reglerne for god adfærd.

Vesten og USA må ligeledes forventes at foretage mange af de samme handlinger, som Kina beskyldes for. En analyse af de amerikanske evner er dog ikke fokus her, da USA eksempelvis ikke har ligeså meget at vinde ved at opretholde en aggressiv cyberkapabilitet. Det kan ses med baggrund i de tre årsager til, at stater søger at opretholde og anvende en aggressiv cyberkapabilitet. Hvad angår den første årsag, så behøver USA ikke at afskrække andre stater via cyberspace. Amerikanerne klarer det fint uden. I relation til den anden årsag, er realiteterne i dag, at USA's militærteknologi er second to none, så det er ikke nødvendigt at spionere voldsomt for at opnå viden om andre staters militære teknologi. Når man ser på den tredje årsag vedr. de økonomiske hensyn står det klart, at industrispionage giver mindre mening for USA, da det teknologiske niveau i USA er blandt de mest udviklede i verden.

Kina har derimod, koblet til den første årsag, en interesse i at undgå at Vesten og USA kan udsætte Kina for politisk og militær pression. Derudover har Kina for det andet en interesse i opnå hurtig militær udvikling, da Kina stadig halter langt bagefter Vesten og USA. Og endelig er Kinas generelle teknologiske niveau for det tredje også stadig et stykke efter USA, hvilket vil gøre incitamentet til industrispionage for økonomisk vindings skyld større.

Derfor er det særligt interessant at se på Kinas evner indenfor cyberspace, men man skal stadig huske på, at andre statslige aktører benytter sig af de samme teknikker. Forskellen er blot, at incitamentene er mindre for Vesten og USA til at benytte cyberspace offensivt.

Cyberkapabiliteter er ikke et emne, hvor stater åbent fortæller om deres evner. Det skyldes, at det sjældent kan betale sig at offentliggøre, at man har spioneret eller lagt andre staters netværk ned. Usikkerheden om det reelle niveau kan afskrække USA og andre stater yderligere, da stater ud fra en klassisk militær logik må forberede sig på det værste, når de ikke kender det fulde niveau for Kinas kapabiliteter i cyberspace. Alligevel skrives der om det vitale i at have evner på området (State Council 2009: 8-11), og selvom stater ikke selv direkte udtaler sig om deres egne offensive evner i cyberspace, afholder det dem ikke fra at omtale og analysere andre staters evner og optioner på området (Office of The Secretary of Defense 2009: 17, 24).

Derudover kan stater også ved at agere meget aggressivt forøge risikoen for at blive beskyldt for at have udført cyberangreb, hvilket i sig selv og for sig selv på paradoksalt vis kan gavne et land som fx Kina. Det skyldes, at det afskrækkende element i besiddelsen af avancerede cyberkapabiliteter aldrig vil komme til udtryk, hvis ingen andre end en selv kender til det. Med andre ord, hvis Nordkorea var den eneste stat i verden, der vidste at de havde en atombombe, men resten af verden var overbevist om, at det ikke var tilfældet, så bliver det afskrækkende element i Nordkoreas atomvåbenprogram udvandet. Strategien omkring at afskrække bliver med andre ord tvedelt og på sin vis modsætningsfuld. Det er en balancegang mellem på den

ene side at skjule det maksimale niveau for evnerne, men på den anden side også kommunikere og vise, at der eksisterer et tilpas højt niveau, så andre stater føler sig afskrækket.

Cyberspace og Kina

I Kinas militære strategi nævnes cyberkapabiliteter som et område Folkets Befrielseshær (Kinas militær), skal investere i og benytte sig af i stor stil via en målrettet fokusering på området (Chen 2009: 19). Den amerikanske forsvarsminister, Robert Gates, har da også erklæret, at Kinas udvikling på cyber-området i stigende grad bekymrer ham (Lin 2009: 14).

Stort set alle digitale og militære systemer kan angribes via cyberspace. Derfor er det essentielt at udvikle dette område, hvis man ønsker at udfordre den amerikanske unipolaritet. Det interessante spørgsmål bliver derfor, om Kina opbygger kapabiliteter i cyberspace til at afskrække USA?³

Men hvorfor er det, at stater frygter Kinas styrke indenfor cyberspace? Hvad er årsagen til det? For det første kan det siges, at Folkets Befrielseshær bruger stigende ressourcer på at udvikle sig indenfor nye kamppladser som det ydre rum og cyberspace (Miller 2008: 2-3).

For det andet har Folkets Befrielseshær etableret "*information warfare*"⁴ kapabiliteter, med særligt fokus på cyberkrig, der også skal bruges i fredstid (Cheung 2009: 34).

Og for det tredje advokerer strateger fra Folkets Befrielseshær for brugen af virus og hackerangreb, der kan paralisere og overraske modstandere (Cheung 2009: 35).

Begreber indenfor krig i cyberspace

Den overordnede NATO-term er Computer Network Operations (CNO).

Under CNO kan der identificeres tre elementer (Mulvenon 2009: 257-259):

- 1) Det kan opdeles i Computer Network Exploitation (CNE), hvor det søges at indhente oplysninger om et system, til brug for senere angreb.
- 2) Computer Network Attack (CNA), hvor man søger at ødelægge systemer.
- 3) Computer Network Defense (CND), der refererer til eget forsvar imod angreb.

Sammenhængen mellem de tre er, at man ikke kan lave effektivt CNA uden også at have CNE og CND og omvendt.

I Kina går CNO og rumkapabiliteter under én samlet betegnelse, *informationization/informatization*, hvor CNO udgør cyber-delen af det kinesiske begreb (State Council 2009: 7).

(3) Herudover kan det også fremadrettet være yderst interessant at undersøge, hvordan andre aktører som de øvrige større vestlige lande og Danmark skal forholde sig til de kinesiske evner på cyberområdet.

(4) *Information Warfare*: Kort sagt al krig, der kan føres igennem, mod og via informationsteknologi (Berkowitz 1997: 175-177).

Kinas tanker og evner i cyberspace

Kinesiske militærstrateger beskriver cyberkapabiliteter som en kraftfuld *asymmetrisk* mulighed i en *afskrækkende* strategi (Mulvenon 2009: 257). Analytikere anslår, at et "important theme in Chinese writings on CNO is the use of computer network attack as the spearpoint of deterrence" (Mulvenon 2009: 257). Det bevirker, at man herved gør omkostningerne for store for fjenden, hvilket kinesiske analytikere vurderer som essentielt indenfor afskrækkelse (Thomas 2009: 468; Mulvenon 2009: 258). Det kan grundlæggende tolkes som om, at denne asymmetriske afskrækkelsesstrategi mod en militær overmagt (her USA) er nødvendig, for at en stat med supermagtspotentiale (her Kina) kan skabe sig mulighed for en militær og politisk opstigning i det internationale system (Thomas 2009: 469, 475).

Det siges yderligere, at "most significant, computer network attack is characterized as a pre-emption weapon to be used under the rubric of the rising Chinese strategy of [...] gaining mastery before the enemy has struck" (Mulvenon 2009: 259).

Derfor har Kina også som andre stater, der søger en lignende kapacitet, rekrutteret massivt blandt hackermiljøer internt i Kina (Northrop Grumman 2009: 7; Mulvenon 2009: 277-278).

Aggressive og omfattende angreb fra Kina

Kina anses som en trussel for USA i cyberspace (og i rummet), og det er Kinas brug af asymmetriske kapabiliteter, særligt cyberkrig, der kan ødelægge eksempelvis den amerikanske økonomi (USCC 2009: 167-183; Office of The Secretary of Defense 2009: 20).⁵ Analytikere siger, at "China could well have the most extensive and aggressive cyberwarfare capability in the world", og at det er drevet af "Beijing's desire for global-power status" (Stratfor: 2. marts 2009). Disse betragtninger kommer ikke ud af ingenting, men som en konsekvens af, at den kinesiske autoritative skrivning på området betoner cyberkrig som et oplagt asymmetrisk instrument til at balancere USA's magt, særligt i tilfælde af åben konflikt, men også som afskrækkelse (Qiao og Wang 1999: 29, 47, 211-212).

Generelt er Kina meget aktive på området (Verton 2008: 5-7), og det tyder på et højt kapabilitetsniveau at de eksempelvis kan infiltrere computere i 103 lande for at holde et vågent øje med bl.a. eksiltibetaneres kamp for et frit Tibet (NY Times: 28. marts 2009).

Dette kan sammenholdes med det faktum, at amerikanske sikkerhedsekspertter kalder USA's forsvar mod cyberangreb for "pinligt ringe", og en "dampmaskine, der er løbet tør for damp" (BBC News: 29. april 2009), samt at der allokeres mange ressourcer til det kinesiske cyberprogram (NY Times: 27. april 2009).

På trods af dette, bliver risikoen for kinesiske cyberangreb dog taget alvorligt. Chefen for det amerikanske sikkerhedsministerium, Department of Homeland Se-

(5) Men også andre vestlige lande må på samme måde føle sig udsatte, hvis det skulle komme til en konflikt.

curity, har udtalt, at cyberangreb er på linie med angrebene 11. september 2001, og at "[w]e take threats to the cyber world as seriously as we take threats from the material world" (BBC News: 8. april 2008).

Sagt om Kinas cyberkapabiliteter

"Critical U.S. infrastructure is vulnerable to malicious cyber activity. Chinese military doctrine calls for exploiting these vulnerabilities in the case of a conflict"

The U.S.-China Economic and Security Review Commission 2009
(USCC 2009: 181)

"[The Chinese government] resolutely oppose[s] any crime, including hacking, that destroys the Internet or computer network [...] some people overseas with Cold War mentality are indulged in fabricating the sheer lies of the so-called cyberspies in China"

Wang Baodung, talsmand for den kinesiske ambassade i Washington
(Wall Street Journal: 8. april 2009)

At der er god grund til at tage det alvorligt, vidner et cyberangreb på et amerikansk atomvåben-laboratorium om, hvor det ikke vides med sikkerhed, hvad meget data, der blev downloadet (NY Times: 9. november 2007). I værste fald kan angrebene, der kunne spores til Kina og præges af at være udført af statslige organisationer, have resulteret i overgivelse af amerikansk teknologi indenfor atomvåben.

Derudover sagde chefen for den engelske indenrigsefterretningstjeneste, MI5, i december 2007, at de var under cyberangreb fra "Chinese state organizations" (NY Times: 2. december 2007), og CNO er et område i kraftig vækst for Folkets Befrielseshær, men det er ikke klart, hvordan den reelle kapacitet fungerer og hvad den præcist er underlagt (Miller 2008: 3).⁶

Eksempler på den totale afskrækkelse

Kinas offensive evner indenfor angreb via cyberspace identificeres i rapporteringer fra analytikere og forsvarsministerier, der beskriver, at Kina holdt en militær øvelse så tidligt som i 2005, hvor der målrettet blev trænet i at hacke fjendtlige netværk (Jane's Defence Weekly: 19. september 2008; SCMP: 5. september 2007).

Næstformanden for den amerikanske generalstab, general James Cartwright har sagt, at et kinesisk cyberangreb i fuld skala potentielt kan have samme effekt som et masseødelæggelsesvåben (Jane's Defence Weekly: 19. september 2008). Og cyberangreb sammenlignes også allerede med atomvåben, mens det diskuteres

(6) Dette mener jeg, på trods af at en amerikansk rapport har påpeget konkrete steder, hvor Kinas enheder til cyberkrigsførelse bør være placeret (USCC 2009: 172-176).

livligt, om de samme dynamikker⁷ fra atomvåben har medført kan gøre sig gældende i en ny kontekst (NY Times: 27. april 2009).

En vestlig ekspert siger yderligere med tydelig reference til Kina: "Let's say an emerging superpower would dedicate 20.000, 30.000, 40.000 people and then unleash that force at some point, I would say we would not be ready" (Jane's Defence Weekly: 19. september 2008).

USA's el-net og en luftbase

Det er dog væsentligt, at cyberkapabiliteter først begynder at antage en reel afskrækkende virkning, når en stat viser deres evner overfor omverdenen. Det skete, da det gik op for USA, at deres el-net var blevet hacket, og at store dele kunne slukkes, når hackeren ønskede det (Wall Street Journal: 8. april 2009). Angrebet blev sporet til Kina, og chefen for kontraefterretning i USA sagde, at "[w]e have seen Chinese network operations inside certain of our electricity grids" (NY Times: 27. april 2009). At amerikanerne ikke er i stand til at varetage sikkerheden på deres elektriske net er kritisk for dem, men det viser samtidig, at de har alvorlige problemer med at modstå et ambitiøst kinesisk cyber-program. USA er i øjeblikket bagud i forhold til Kina, hvad angår uddannelsen af ingeniører, der kan bruges til cyber-relaterede funktioner (Jane's Intelligence Digest: 5. maj 2009).

Herudover har en amerikansk luftbase været nødsaget til at slukke for deres net og lukke for start og landing i en periode på grund af massive virus-angreb sporet til Kina (NY Times: 27. april 2009). Hvordan det står til med sikkerheden i andre vestlige lande kan man gisne om, men niveauet er næppe væsentligt højere end i USA.

Joint Strike Fighter, Pentagon og Merkel

På sin vis kan man sige, at det er regulær afskrækkelse at vide, at Kina har haft evnen til at tænde og slukke for strømmen og lukke luftbaser, og man må overveje, om der mon er andet, de er i stand til, men som endnu ikke er blevet opdaget? Der har i 2009 været et elektronisk indbrud i Joint Strike Fighter-programmet (kampfly), og store mængder data blev kopieret (Stratfor: 21. april 2009). Angrebet kan ifølge nuværende og tidligere ansatte i Pentagon spores til Kina (BBC News: 22. april 2009; Stratfor: 21. april 2009; Wall Street Journal: 21. april 2009). Det *kan* medføre, at det bliver nemt for eksempelvis Kina at forsvare sig imod flyet (som mange vestlige lande, inklusiv Danmark forventes at anskaffe), og hvis de havde fået fat i mere data, havde de måske endda kunne kopiere dele af flyet (Wall Street Journal: 21. april 2009). Det er yderligere blevet beskrevet, hvordan den amerikanske chef for kontraefterretning har udtalt, at "our networks are being mapped" med henvisning

(7) Såsom "Mutually Assured Destruction" (MAD), der bevirkede gensidig afskrækkelse imellem USA og Sovjet under den kolde krig. Kineserne bruger i forvejen en pendant til MAD indenfor deres strategi for deres rumkapabiliteter, hvori de omtaler en "space balance of force" (Krepon 2008: 174).

til den amerikanske kontrol over flytrafikken, og advarede yderligere om en situation hvor "a fighter pilot can't trust his radar" (Wall Street Journal: 21. april 2009).

Det bør nævnes, at Pentagon allerede har haft en "computer security incident", hvorefter USB-penne blev forbudt. Videre er det relevant at vide, at Kina er verdens største producent af USB-penne (Stratfor: 2. marts 2009). Det skyldes, at visse iagttagere i uformelle sammenhænge taler om, hvilke muligheder det ville give en stat at have lagt programmer ind på samtlige USB-penne, landet producerede. På den måde kunne de melde tilbage til en central, hvor informationer om indholdet på de computere, der brugte pågældende lands USB-penne ville komme flyvende. Det er naturligvis et paranoidt tankeeksperiment, men illustrerer udmærket hvilken frygt og alvorlighed begreber som statslig cyberkrig og hacking fører med sig.

Herudover er den tyske kansler Angela Merkels kontor blevet hacket og meget sensitiv data kopieret. Det vurderes, at statslige aktører må være bag, og det blev sporet til Kina (Times Online: 27. august 2007). At det kan lade sig gøre, at bryde ind i Angela Merkels computer har store implikationer for alvorligheden af Kinas evner i cyberspace.

Google var blot en lille del af et større angreb

Herudover er det i forbindelse med massive hackerangreb på kunder med mail-konti hos firmaet Google (Reuters: 13. januar 2010), blevet afsløret, at angrebene (der muligvis får Google til at trække sig ud af samarbejdet omkring censurering) blot var en lille del af et større cyberangreb på minimum 34 amerikanske firmaer og institutioner med tilknytning til den amerikanske administration, herunder leverandører til Pentagon (Washington Post: 14. januar 2010; NY Times: 18. januar 2010). Disse fandt alle sted i december, men er først kommet til offentlighedens kendskab nu. Samtidig bekræftes rygter om, at udenlandske journalister i Kina også har fået hacket deres mailkonto og private mails er blevet videresendt. Det er bl.a. gået ud over en journalist fra det velansete Associated Press (Associated Press: 19. januar 2010). I en rapport, der identificerer hvor angrebene i december er kommet fra, erklærer eksperter fra VeriSign iDefense uden tøven, at den kinesiske regering står bag (Ars Technica: 14. januar 2010). Samtidig er en klassificeret FBI-rapport blevet lækket, hvoraf det fremgår, at Kina har udviklet en "cyber-hær" bestående af 30.000 militære cyberspioner, samt 150.000 spioner hyret fra den private sektor. Det nævnes, at deres mission er at stjæle amerikanske militære og teknologiske hemmeligheder (The Daily Beast: 13. januar 2010), hvilket også i stigende grad bliver beskrevet i bekymrede vendinger af højtstående personer fra den amerikanske hær, såsom den øverstbefalende for U.S. Pacific Command, admiral Robert Willard (DefenseNews: 13. januar 2010).

En af de mest anerkendte eksperter på området, James A. Lewis, havde denne kontante analyse af angrebene: "This is a big espionage program aimed at getting high-tech information and politically sensitive information – the high-tech information to jump-start China's economy and the political information to ensure the survival of the regime [...] This is what China's leadership is after. This reflects China's national priorities" (Washington Post: 14. januar 2010).

På baggrund af disse talrige eksempler, må det siges at de kinesiske evner indenfor cyberspace have en afskrækkende effekt.

Kina svarer igen

Der kan identificeres en række argumenter til forsvar for Kina, som kort oplystes her:

- 1) *Hvem angriber egentlig hvem?* Kinas egne netværk fremstår ubeskyttede, og andre lande kan udføre angreb igennem Kina, hvilket mistænkeliggør landet (Associated Press: 6. september 2007). IT-ekspert Steve Armstrong siger videre: "It's too easy to blame China [...] In fact, legitimate countries are bouncing their attacks through China. It's very easy to do, so why not? [...] My evil opinion is that some western governments are already doing this" (BBC News: 25. april 2008).
- 2) *Aktører i USA har interesse i at overdrive Kinas evner.* For at sikre sin eksistensberettigelse og øgede budgetter, er der flere aktører i USA, der kan have en interesse i at fremstille Kina som en trussel mod USA's sikkerhed. Både Pentagon, navngivne politikere og efterretningstjenesterne beskyldes ofte for at agere som under den kolde krig og bidrage til en konfliktpræget udvikling i forholdet mellem Kina og USA (AFP: 3. marts 2008; China Daily: 23. april 2009).
- 3) *Kina foreslår globalt samarbejde om hacking* (Wall Street Journal: 8. april 2009). Det lyder jo i og for sig fint, men som det er beskrevet tidligere, har visse stater for meget at vinde ved at benytte sig af cyberangreb, hvilket vil besværliggøre samarbejdet. Og i øvrigt er det yderst svært at se hvordan og hvem, der i givet fald skulle håndhæve et sådant samarbejde?
- 4) Det er yderligere muligt, at forestille sig at der er en *anarkisk ledet struktur indenfor CNO i Kina*. Altså, at den centrale ledelse ikke kan kontrollere, hvem der foretager angreb. Amerikanske rapporter indikerer dette (USCC 2008: 164), og den situation er i virkeligheden lidt skræmmende, hvis det forholder sig sådan. Kritiske røster siger derimod sige, at det blot er en måde, hvorpå man fra kinesisk side benytter sig af hackere udenfor militæret og regeringsapparatet til at udføre angreb (The Daily Beast: 13. januar 2010).
- 5) *Kina benægter at militære hackere findes i landet* (NY Times: 28. marts 2009). Det ville andre lande muligvis også gøre, men det ændrer ikke på det faktum, at kineserne må have nogen med forstand på IT i Folkets Befrielseshær. Hvorvidt disse personer med IT-forstand på et højt niveau benyttes til at udføre cyberangreb er et andet spørgsmål. Men ud fra materialet i dette brief understøtter flere kilder, at der også fra Folkets Befrielseshær anvendes hackere til at spionere.

Desuden er der, på trods af de ovenstående argumenter til forsvar for Kina, en grundlæggende forståelse af vigtigheden af cyberkrig i Folkets Befrielseshærs strategiske tænkning (Thomas 2009: 467-469). Denne form for asymmetriske

strategi er længe internt blevet debatteret. (Associated Press: 6. september 2007; The Economist: 6. september 2007; Office of The Secretary of Defense 2009: 52-53), og i en opsigtsvækkende bog, skrevet af to kinesiske oberster kaldet *Unrestricted Warfare*, siges det, at "[i]n the information age, the influence exerted by a nuclear bomb is perhaps less than the influence exerted by a hacker" (Qiao og Wang 1999: 47).

Konklusion og perspektiver: Kina som cybermagt og supermagt

I forordet til den australske hvidbog for deres fremtidige forsvar kaldet *Defending Australia in the Asia Pacific Century: Force 2030*, skriver den australske forsvarsminister, Joel Fitzgibbon, at "[c]yber warfare has emerged as a serious threat to critical infrastructure [and] the biggest changes to our outlook over the period have been the rise of China [...] [T]he beginning of the end of the so-called unipolar moment; the almost two-decade-long period in which the pre-eminence of our principal ally, the United States, was without question" (Australian Department of Defence 2009: 9). Det unipolære øjeblik, hvor USA kunne sikre alle sine allieredes sikkerhed er under forandring, og Kinas egenskaber indenfor cyberkrig er et vigtigt element i denne forandring.

For at imødegå dette har USA nu lanceret en ny "Cyber Command" og udpeget en "Cyber Czar" til at koordinere de statslige beredskaber (Wall Street Journal: 22. april 2009; CBS News: 21. december 2009).⁸ Alligevel er det yderst vanskeligt, at imødegå de kinesiske evner indenfor feltet. Derfor vil amerikanske forsøg på en opprioritering af deres cyberkapabiliteter sandsynligvis først få indflydelse på lidt længere sigt, hvis overhovedet. Men i takt med dette vil også kineserne forsøge at undgå at deres afskrækkende evner neutraliseres.

Briefet har sandsynliggjort, at den kinesiske oprustning på cyberområdet vil fortsætte. Der er grundlæggende meget at vinde for opstigende stater ved at have en offensiv og aggressiv cyberkapabilitet. Det skyldes primært at det er svært direkte at bevise, når stater står bag. Selv stater er vel uskyldige indtil det modsatte er bevist.

Generelt kan det derfor fastslås, at Kina afskrækker USA via deres cyberkapabiliteter, hvilket på længere sigt vil give mulighed for yderligere kinesisk ekspansion på det politisk-militære område, så Kina en dag kan fremstå som en reel supermagt, både på det økonomiske, teknologiske og militære område.

(8) Og herhjemme i Danmark skal vi ifølge den seneste Forsvarskommission opbygge vores militære evne indenfor CNO (Forsvarskommissionen 2009: 101)

Efterskrift: Krigen kommer aldrig

Men dermed ikke sagt, at der vil opstå reelle militære konflikter imellem to de aktører. Det er ikke sandsynligt, på grund af den gensidige afhængighed, der eksisterer på det økonomiske område. Derudover er Kina nu også en position, hvor USA føler sig skræmt af de kinesiske evner, og da Kina stadig generelt er klart militært underlegne i forhold til USA, er forholdet på det militære område karakteriseret af en gensidig afskrækkelse. At basere et forhold på gensidig afskrækkelse er naturligvis ikke optimalt, men på den anden side vælger man jo ikke altid sin partner.

Litteraturliste

- Ars Technica (14. januar 2010), "Researchers identify command servers behind Google attack", lokaliseret den 14. januar 2010 på <http://arstechnica.com/security/news/2010/01/researchers-identify-command-servers-behind-google-attack.ars>.
- AFP (3. marts 2008), "China Tells U.S. to End Cold War Mentality", lokaliseret den 20. oktober 2009 på <http://www.defensenews.com/story.php?i=3402950>.
- Associated Press (6. september 2007), "China denies cyber spying charges, but claims highlight pursuit of unconventional strategies", lokaliseret den 20. oktober 2009 på <http://www.theage.com.au/news/TECHNOLOGY/China-denies-cyber-spying-charges-but-claims-highlight-pursuit-of-unconventional-strategies/2007/09/06/1188783328617.html>.
- Associated Press (19. januar 2010), "Foreign reporters' Google e-mail hacked in China", lokaliseret den 19. januar 2010 på <http://www.scmp.com/portal/site/SCMP/menuitem.2af62ecb329d3d7733492d9253a0a0a0/?vgnnextoid=a37d228dda446210VgnVCM100000360a0a0aRCRD&ss=China&s=News>.
- Australian Department of Defence (2009), *Defending Australia in the Asia Pacific Century: Force 2030 - Defence White Paper*.
- BBC News (8. april 2008), "Cyber risk 'equals 9/11 impact'", lokaliseret den 20. oktober 2009 på <http://news.bbc.co.uk/2/hi/technology/7335930.stm>.
- BBC News (25. april 2008), "Hackers warn high street chains", lokaliseret den 20. oktober 2009 på <http://news.bbc.co.uk/2/hi/7366995.stm>
- BBC News (22. april 2009), "New 'Cyber Command' for US military", lokaliseret den 20. oktober 2009 på http://news.bbc.co.uk/newsbeat/hi/technology/newsid_8012000/8012141.stm.
- BBC News (29. april 2009), "US cybersecurity 'embarrassing'", lokaliseret den 20. oktober 2009 på <http://news.bbc.co.uk/2/hi/technology/8023793.stm>.
- Berkowitz, Bruce D. (1997), "Wartime in the Information Age", i: Arquilla, John og David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, CA: RAND Corporation.
- CBS News (21. december 2009), "Obama Taps Cyber Security Exec as New Czar", lokaliseret den 6. januar 2010 på <http://www.cbsnews.com/stories/2009/12/21/politics/main6008388.shtml>.
- Chen, Zhou (2009), "A Review of China's Military Strategy", *China Armed Forces*, Vol. 1, No 1., Beijing: Beijing Daily Printing Co, pp. 12-21.
- Cheung, Tai Ming (2009), "Dragon on the Horizon: China's Defense Industrial Renaissance", *Journal of Strategic Studies*, vol. 32, no. 1, pp. 29-66.
- China Daily (23. april 2009), "'Cold War mentality' drives US cyber plan", lokaliseret

den 30. april 2009 på http://www.chinadaily.com.cn/world/2009-04/23/content_7707135.htm.

DefenseNews (13. januar 2010), "Chinese Buildup Of Cyber, Space Tools Worries U.S.", lokaliseret den 14. januar 2010 på <http://www.defensenews.com/story.php?i=4452407&c=ASI&s=SEA>.

Forsvarskommissionen af 2008 (2009), *Dansk forsvar – Globalt engagement. Beretning fra Forsvarskommissionen af 2008, hovedbind*, København: Forsvarsministeriet.

Jane's Defence Weekly (19. september 2008), "War and PC: cyberwarfare", lokaliseret den 20. oktober 2009 på <http://search.janes.com.ez-fak.minimeta.minibib.dk/Search/printFriendlyView.do?docId=/content1/janesdata/mags/jdw/history/jdw2008/jdw37840.htm@current>.

Jane's Intelligence Digest (5. maj 2009), "Cyber spies assault US power grid", lokaliseret den 20. oktober 2009 på <http://search.janes.com.ez-fak.minimeta.minibib.dk/Search/printFriendlyView.do?docId=/content1/janesdata/mags/jiwk/history/jid2009/jid70585.htm@current>.

Lin, Cheng-yi (2009), "China's 2008 Defense White Paper: The view from Taiwan", *China Brief*, Vol. IX, Issue 3, pp. 11-14.

Miller, Marc (2008), *PLA Missions Beyond Taiwan*, Colloquium Brief, Carlisle, PA: Strategic Studies Institute, U.S. Army War College.

Mulvenon, James (2009), "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability", i: Kamphausen, Roy, David Lai og Andrew Scobell (eds.), *Beyond the Strait: PLA Missions Other Than Taiwan*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, pp. 253-286.

Northrop Grumman (2009), *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, report prepared for The US-China Economic and Security Review Commission (USCC), McLean, Virginia: Northrop Grumman Corporation, Information Systems Sector.

NY Times (9. november 2007), "Cyber attack on U.S. nuclear arms lab linked to China", lokaliseret den 20. oktober 2009 på <http://www.nytimes.com/2007/12/09/world/americas/09iht-hack.1.8653712.html>.

NY Times (2. december 2007), "Spy Chief in Britain accuses China of cyber crime", lokaliseret den 20. oktober 2009 på <http://www.nytimes.com/2007/12/02/world/europe/02iht-cyber.1.8557238.html>.

NY Times (28. marts 2009), "Vast Spy System Loots Computers in 103 Countries", lokaliseret den 20. oktober 2009 på <http://www.nytimes.com/2009/03/29/technology/29spy.html>.

NY Times (27. april 2009), "U.S. Steps Up Effort on Digital Defenses", lokaliseret den 20. oktober 2009 på <http://www.nytimes.com/2009/04/28/us/28cyber.html>.

- NY Times (18. januar 2010), "The Lock That Says 'Pick Me'", lokaliseret den 18. januar 2010 på <http://www.nytimes.com/2010/01/18/technology/internet/18defend.html?ref=internet>.
- Office of The Secretary of Defense (2009), *Annual Report to Congress: Military power of the People's Republic of China 2009*, Washington: U.S. Department of Defense.
- Qiao, Liang og Xiangsui Wang (1999), *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House, lokaliseret den 20. december 2008 på <http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf>.
- Reuters (13. januar 2010), "US, Google and China clash over internet censorship", lokaliseret den 15. januar 2010 på <http://www.scmp.com/portal/site/SCMP/menuitem.2af62ecb329d3d7733492d9253a0a0a0/?vgnnextoid=88ca7468f6526210VgnVCM100000360a0a0aRCRD&ss=China&s=News>.
- SCMP, South China Morning Post (5. september 2007), "Chinese hackers attack British parliament", lokaliseret den 27. september 2009 på <http://archive.scmp.com/showarticles.php>.
- State Council (2009), *China's National Defense in 2008*, Information Office of the State Council of the People's Republic of China, Beijing: Foreign Languages Press.
- Stratfor (2. marts 2009), "China: Pushing Ahead of the Cyberwarfare Pack", lokaliseret den 20. oktober 2009 på http://www.stratfor.com/memberships/132785/analysis/20090225_china_pushing_ahead_cyberwarfare_pack.
- Stratfor (21. april 2009), "U.S.: Cyberspies Attack Joint Strike Fighter Project – Report", lokaliseret den 20. oktober 2009 på http://www.stratfor.com/sitrep/20090421_u_s_cyberspies_attack_joint_strike_fighter_project_report.
- The Daily Beast (13. januar 2010), "China's Secret Cyberterrorism", lokaliseret den 14. januar 2010 på <http://www.thedailybeast.com/blogs-and-stories/2010-01-13/chinas-secret-cyber-terrorism/>.
- The Economist (6. september 2007), "Beware the Trojan panda", lokaliseret den 20. oktober 2009 på http://www.economist.com/world/international/displaystory.cfm?story_id=9769319.
- Thomas, Timothy L. (2009), "Nation-state Cyber Strategies: Examples from China and Russia", i: Kramer, Franklin D., Stuart H. Starr og Larry K. Wentz (eds.), *Cyberpower and National Security*, Dulles, Virginia: Potomac Books, Inc. og NDU Press, pp. 465-488.
- Times Online (27. august 2007), "China accused of hacking into heart of Merkel administration", lokaliseret den 20. oktober 2009 på <http://www.timesonline.co.uk/tol/news/world/europe/article2332130.ece>.

-
- USCC, U.S.-China Economic and Security Review Commission (2008), *2008 Report to Congress of the U.S.-China Economic and Security Review Commission*, Washington: U.S. Government Printing Office.
- USCC, U.S.-China Economic and Security Review Commission (2009), *2009 Report to Congress of the U.S.-China Economic and Security Review Commission*, Washington: U.S. Government Printing Office.
- Verton, Dan (2008), "The Evolution of Espionage: Beijing's Red Spider Web", *China Brief*, Vol. VIII, Issue 15, pp. 4-7.
- Wall Street Journal (8. april 2009), "Electricity Grid in U.S. Penetrated By Spies", lokaliseret den 20. oktober 2009 på <http://online.wsj.com/article/SB123914805204099085.html>.
- Wall Street Journal (21. april 2009), "Computer Spies Breach Fighter-Jet Project", lokaliseret den 20. oktober 2009 på <http://online.wsj.com/article/SB124027491029837401.html>.
- Wall Street Journal (22. april 2009), "New Military Command to Focus on Cybersecurity", lokaliseret den 20. oktober 2009 på <http://online.wsj.com/article/SB124035738674441033.html>.
- Washington Post (14. januar 2010), "Google China cyberattack part of spy campaign", lokaliseret den 15. januar 2009 på http://www.msnbc.msn.com/id/34855470/ns/technology_and_science-washington_post/.