DIIS REPORT

DIIS REPORT

Jeppe Teglskov Jacobsen

Kampen for en klar sondring i cyberspace

Kriminalitet, lulz, hacktivisme, spionage, terrorisme, sabotage eller krig?

DIIS Report 2014:09

DIIS · DANSK INSTITUT FOR INTERNATIONALE STUDIER

DIIS • Dansk Institut for Internationale Studier
Østbanegade 117, 2100 København Ø
Tlf: 32 69 87 87
E-mail: diis@diis.dk
Web: www.diis.dk

Layout: Allan Lind Jørgensen
Tryk: Vesterkopi A/S

ISBN:
Print: 978-87-7605-681-0
Pdf: 978-87-7605-682-7

Pris: 50.00 kr. inkl. moms
Trykte eksemplarer kan bestilles på publications@diis.dk
DIIS' publikationer kan downloades gratis på www.diis.dk

Jeppe Teglskov Jacobsen, BA, MSc., videnskabelig assistent, DIIS
jetj@diis,dk

Indhold

Abstract

Blandt politikere, i medierne og i den bredere offentlighed ses cyberspace i stigende grad som et trusselsfyldt domæne. Dette har resulteret i et væld af nye begreber. Denne DIIS-rapport tager udgangspunkt i cyberpræfikset og diskuterer betydningen af de nye (cyber)trusselsbegreber samt de uklarheder, der opstår, når de forskellige begreber benyttes. Rapporten er således først og fremmest et forsøg på at forhindre en unødvendig 'hype' omkring cyberspace, der risikerer at medføre en uhensigtsmæssig allokering af ressourcer samt en militarisering og en underminering af de demokratiske rettigheder.

Ved at inddele cybertruslerne i en række forskellige kategorier, baseret på truslernes strategiske mål, midler, operationelle mål og redskaber, argumenterer rapporten for, at cyberpræfikset hovedsageligt får sin berettigelse på grund af de redskaber der benyttes. Således er cybertruslerne identiske med truslerne i den fysiske verden – blot iblandet andre redskaber. Dermed ikke sagt, at cyberspace ikke bringer nye udfordringer. Rapporten peger netop på, at disse cyberredskaber er kendetegnet ved stor hastighed, lave omkostninger, relativ let tilgængelighed samt høj grad af anonymitet, hvilket har skabt nye muligheder for både stater og ikkestatslige aktører – med juridiske, militære og økonomiske udfordringer til følge. De nye udfordringer ændrer imidlertid ikke ved, at vi, hvis vi ønsker at forstå cybertruslerne, først og fremmest bør søge svarerne 'offline', blandt de mennesker, som er utilfredse med tingenes tilstand.

Indledning

> "[When] it comes to talking about cyber attacks, senior defense leaders have lumped together teenagers defacing public DoD websites, disgruntled soldiers leaking documents, hackers stealing industry secrets, terrorists using YouTube and foreign military agents accessing classified networks to plant worms, as if they were all one and the same, simply because their activities all involved a digital series of 0s and 1s. This is akin to treating the threat posed by a teenager with a bottle rocket, a robber with a revolver, an insurgent with a bomb or a state with a cruise missile as the same simply because they use gunpowder".[1]

Danmark fulgte i 2013 flere andre lande og placerede cyberangreb blandt de største trusler.[2] Ifølge diverse sikkerhedseksperters og efterretningstjenesters vurderinger har de ondsindede og statsfinansierede "hackere" i stigende grad indtaget pladsen som den vigtigste sikkerhedstrussel – en position, der ellers siden den 11. september 2001 har været forbeholdt islamistiske ekstremister. Graver man imidlertid et spadestik dybere i forsøget på at forstå, hvori truslerne fra cyberspace består, mødes man af en del udfordringer, konceptuelle uklarheder og politiske uenigheder.

Forsvarets Efterretningstjeneste vurderede i løbet af 2013, at statsstøttet cyberspionage mod danske virksomheder og cyberangreb mod Danmarks *kritiske infrastruktur* på daværende tidspunkt udgjorde de største udfordringer fra cyberspace.[3] Dette er i tråd med tendensen i USA, hvor cyberspionage – hovedsagelig fra Kina – efter sigende koster den amerikanske stat hundreder af milliarder dollar årligt,[4] og hvor risikoen for cyberterrorangreb mod kritisk infrastruktur spås at kunne gøre en ende på USA's dage som supermagt.[5] Truslen fra kinesiske, russiske og iranske cyberangreb har, især i en amerikansk kontekst, ført til en fornyet interesse for den koldkrigsterminologi, som siden Murens fald ellers var gledet ud af det gængse sikkerhedsvokabularium. Statskrige, afskrækkelsesstrategier og balancering er igen blevet relevante,

[1] Peter W. Singer citeret i Reveron, 2012:11.

[2] Beredskabsstyrelsen, 2013.

[3] Forsvarets Efterretningstjeneste, 2013a; Forsvarets Efterretningstjeneste, 2013b; Lauta et al., 2013.

[4] McAfee & Center for Strategic and International Studies, 2013. I praksis har det vist sig særdeles vanskeligt at måle omkostningerne ved cyberkriminalitet og cyberspionage, hvilket har affødt en del metodiske kritikker – se Anderson et al., 2012.

[5] Panetta, Leon, 2012; Palmer, 2010: 22-24.

men nu påsat et cyberpræfiks. Specielt cyberkrigsbegrebet har vundet indpas blandt politikere, sikkerhedseksperter og i den offentlige debat, hvor både statsstøttet industrispionage, politisk spionage, onlinegruppers sabotage mod diverse virksomheder og statslige institutioners hjemmesider grupperes under betegnelsen cyberkrig.

Til forskel fra USA og Europa vurderer medlemslandene i Shanghai Cooperation Organisation (SCO),[6] at truslerne fra cyberspace i lige så høj grad omfatter både simpel berigelseskriminalitet over internettet og frem for alt den destabiliserende og underminerende indvirkning, som såkaldte terroristers, ekstremisters og separatisters onlinepropaganda kan have på staters sammenhængskraft.[7] Som konsekvens har SCO's medlemslande skærpet indsatsen mod onlineaktivister, der bruger nettet til at sprede deres budskaber. Disse aktivister kategoriseres i stigende grad som *cyberterrorister*.

Mens der er bred enighed om, at der med udbredelsen af cyberspace er fulgt betydelige sikkerhedsudfordringer, har det divergerende syn på cybertruslens præcise karakter modarbejdet muligheden for internationale aftaler. Europæisk og amerikansk mistillid til Kina og Rusland afstedkommet af mistanken om omfattende industrispionage, samt kinesisk og russisk altoverskyggende fokus på intern stabilitet har eksempelvis gjort det vanskeligt at nå til enighed om bindende aftaler i forbindelse med kriminalitetsbekæmpelse eller om retningslinjerne for en afmilitarisering af cyberspace.[8]

Men det er ikke udelukkende forskellene i de politiske prioriteter, der har vanskeliggjort samarbejde. Blandt analytikere, politikere og diverse medier har der været en tendens til, uden nævneværdige forsøg på at definere begreberne, at kategorisere en stor del af aktiviteterne online som enten cyberkrig eller cyberterrorisme. Dette har mudret billedet af, hvad der menes, ikke blot når man bruger ord som cyberterrorisme og cyberkrig, men også ord som cyberkriminalitet, cyberspionage, cybersabotage og onlineaktivisme (hacktivisme). At det netop er de relativt dramatisk ladede begreber som terrorisme og krig, der benyttes, bidrager således til at tegne et faretruende billede af cyberspace som en international arena, hvor man ikke kan stole på andre; hvor betragtelige politiske og økonomiske ressourcer nødvendigvis allokeres til at forebygge fremtidige angreb og opbygge angrebskapabiliteter; og hvor de vestlige værdier om retten til privatliv og demokratisk gennemsigtighed udfordres. Dette gælder også i Danmark.

[6] Den eurasiske, politiske, økonomiske og militære organisation indeholdende Kina, Rusland samt en række tidligere sovjetiske stater og med Indien, Afghanistan, Iran og Pakistan som observatørstater.

[7] InfoSec.ru, 2011; *Russia & India Report*, 2013.

[8] Hathaway & Crootof, 2012: 9-10, 54.

På trods af at Danmark endnu ikke har produceret en officiel cybersikkerhedsstrategi, som EU ellers flere gange har anbefalet,[9] er der sket en del de seneste år. I løbet af sommeren 2013 valgte det danske forsvar frem mod 2016 at opprioritere en offensiv cyberenhed, der har til formål at finde fejl og sårbarheder i fjendens it-systemer[10], og i 2012 blev It- og Telestyrelsen samt de civile og militære cyberberedskabs- og varslingstjenester GovCERT og MILCERT samlet til et Center for Cybersikkerhed under Forsvarets Efterretningstjeneste. Sidstnævnte har senest skabt en del debat i forbindelse med det lovforslag, der skal ligge til grund for centerets aktiviteter.[11] I lyset af Edward Snowdens banebrydende afsløringer om massiv overvågning af borgere i USA og Europa samt om et globalt partnerskab mellem efterretningstjenester[12] er det således ikke faldet i god jord, at Forsvarsministeriet har foreslået yderligere indskrænkning af borgernes mulighed for aktindsigt. Skal borgere, politikere og medier i Danmark have mulighed for på et oplyst grundlag at kunne engagere sig i debatten om cybertrusler og cybersikkerhed, er det vigtigt med en grundig indsigt i, hvad præcis der menes, når de forskellige cyberbegreber benyttes. Dette vil kunne imødegå den hype, der ofte fører unødvendigt gennemgribende politiske indgreb med sig.

På den baggrund forsøger denne rapport at give et overblik over forskelle og ligheder mellem de mest diskuterede cybertrusler samt at klarlægge nogle af de generelle betydningsforskelle og udfordringer, der eksisterer på området. Denne diskussion har til hensigt at samle nogle af de vigtigste trusselsbegreber inden for cyberlitteraturen, hvilket ikke er blevet gjort systematisk eller i en dansk sammenhæng, men fungerer også som en opfordring til politikere, akademikere og medier til at tænke over, hvilke begreber der anvendes til at omtale trusler og fænomener i cyberspace.

Går man – som i det følgende – konceptuelt og systematisk til værks og undersøger betydningen af de hyppigst omtalte cybertrusler med henvisning til fire centrale parametre, nemlig formål, midler, objekt og redskaber, viser det sig, at det eneste, der adskiller de forskellige trusler fra almindelige trusler, er de redskaber, der bruges. Cybertrusler bør derfor i udgangspunktet ses ikke som én samlende og ny trusselskategori, men i stedet blot som forlængelser af eksisterende kategorier som terrorisme, kriminalitet og krig, iblandet nye midler.

[9] Kjær, 2013.
[10] Broberg & Ellegaard, 2013; Crawford & Jacobsen, 2014.
[11] Jacobsen, 2014.
[12] Nyst, 2013.

Mens dette gør det muligt at undgå yderligere hype og forvirring, indeholder cyberspace nogle unikke karakteristika, der medfører nye udfordringer. Eksempelvis giver internettet mulighed for at forblive anonym samt ramme næsten overalt på kloden. Dette har stater, aktivister, virksomheder og kriminelle udnyttet til at indgå nogle uskønne alliancer, der vanskeliggør mulighederne for at samarbejde, skaber juridisk uklarhed i cyberspace og øger militariseringen af internettet. Samtidig gør kompleksiteten af cyberspace, at stater, virksomheder og borgere aldrig vil kunne vide sig fuldstændig sikre, når de agerer i cyberspace. Det har ført til et behov for at genoverveje, i hvilken grad borgere, institutioner og stater bør gøre sig selv afhængige af cyberspace. Konceptuel klarhed er et første skridt både til at imødegå nogle af udfordringerne på internationalt plan, til sagligt at kunne prioritere og målrette indsatsen i en dansk cybersikkerhedskontekst og til at kunne forstå og gentænke, hvordan og hvornår et samfunds sammenhængskraft faktisk er truet.

Denne rapports første afsnit introducerer kort cyberpræfikset, afgrænser dets brug og opstiller de parametre, som de syv cybertrusler kan inddeles efter. Dernæst uddybes cybertruslerne i de følgende syv afsnit, inden tre empirisk drevne afsnit afdækker den forvirring og de udfordringer, der opstår, når statslige og ikkestatslige aktører smelter sammen i cyberspace. Rapporten afsluttes med en konklusion.

Cybertrusler: opdelinger og afgrænsninger

Cyberpræfikset kommer oprindelig fra begrebet *cybernetics* – studiet af kommunikation og kontrol med mennesker og maskiner, som blev introduceret i 1940'erne – men blev først for alvor en del af det offentlige sprogbrug, efter at *cyberspace* blev introduceret i science fiction-litteraturen i midten af 1980'erne.[13] Cyberspace blev her set som en hallucination – en fusion af den menneskelige bevidsthed og maskiner – men har senere fået tilføjet en mindre abstrakt og mere teknisk side, som sætter fokus på (1) de *fysiske* computere, servere og kabler, der gør interaktion mulig[14], (2) det *syntaktiske* lag bestående af de protokoller og formater, der strukturerer den information, som computere sender og modtager, og (3) det *semantiske* lag eller den for almindelige mennesker meningsfyldte information, som en computer indeholder.[15] Cyberpræfikset, sammenholdt med trusselsbegrebet har således i udgangspunktet flere betydninger. En cybertrussel strækker sig fra de mere metafysiske spørgsmål om de nye teknologiers betydning for menneskets erkendelse af tid, rum og mening over nye former for propaganda til de sårbarheder, som samfund, der er afhængige af ledninger og sammenkoblede computere, har skabt, både for så vidt angår fysisk destruktion af computere og i forhold til nye angrebsformer som computerhacking og malware.

I forsøget på at bringe mest mulig klarhed til cybertrusselsbegrebet er det nødvendigt at indsnævre de ovennævnte flertydigheder. Således kan truslerne fra den nye teknologi i cyberspace overordnet opdeles i fire overlappende kategorier. Den første og mest abstrakte kategori relaterer sig til forholdet mellem teknologi og bevidsthed og således til de mere psykologiske og kognitive spørgsmål. Eller sagt på en anden måde: betydningen af nye cyberteknologier for, hvordan vi *er*, hvordan vi udfolder os, og hvordan vi sameksisterer som mennesker og samfund. Denne del af cyberlitteraturen mangler stadig at blive grundigt efterforsket, hvilket dog ikke gør disse spørgsmål mindre relevante. Den anden kategori relaterer sig til de nye computerstyrede våben, der anvender konventionel ammunition såsom missiler eller patroner med henblik på at påføre direkte fysisk skade. I amerikansk Department of Defense-terminologi går denne type af trusler (muligheder) under betegnelsen *cybered* og kan bedst illustreres med nye droner, krigsrobotter eller elektromagnetiske jammere.[16]

[13] Cavelty, 2008: 16, 57.
[14] Bauwens, 1994: 42-48.
[15] Libicki, 2009: 12-13; Betz & Stevens, 2011: 36-38.
[16] Moss, 2013.

Den tredje kategori relaterer sig hovedsagelig til krydsfeltet mellem det syntaktiske og det semantiske lag af cyberspace og kan bedst forstås som truslen fra computer-til-computer-angreb eller sagt på en anden måde: de uautoriserede ændringer af computerkode, der forårsager, at fjendens computere eller netværk forstyrres.[17] Det er denne funktionelle kategori, som oftest associeres med *cyber*præfikset.

Den fjerde og sidste kategori betegnes i militærsammenhæng som informationsoperationer og er mere specifikt brugen af nye internetteknologier og mere traditionelle teknologier som tv og radio til spredning af propaganda med henblik på at ændre befolkningers syn på verden.[18] Sker propagandaen ved, at en stat eller ikkestatslig aktør opretter nye hjemmesider eller onlinemedier, bør dette ikke kategoriseres som et cyberangreb eller en cybertrussel, men som en informationsoperation eller – i en krigssituation – som informationskrigsførelse.

I Rusland ses cybersikkerhed ofte som synonym med denne form for informationssikkerhed og -operationer. I denne rapport foreslås det imidlertid, at sådanne informationskampagner holdes adskilt fra cyberpræfikset. Kun såfremt spredning af propaganda sker gennem uautoriserede ændringer af modpartens hjemmesider og lignende, er der et overlap mellem denne kategori og den forrige, da en sådan cyberaktion kræver, at man gennem *egne* computere tilgår og ændrer i *modpartens* it-systemer. Det er imidlertid vigtigt at holde for øje og anerkende, at Rusland og andre SCO-lande ser onlinepropaganda som en reel udfordring for politisk stabilitet og som en potentiel kilde til etniske, racemæssige eller religiøse uroligheder.

Ethvert forsøg på at introducere, analysere eller diskutere cybertrusler bør anerkende denne forskellighed og forsøge enten at indfange alle fire kategorier eller at afgrænse omfanget til én af kategorierne. I denne rapport afgrænses den generelle forståelse af cyberpræfikset til kun at omfatte de aktiviteter, der indeholder computere og computernetværk både som redskaber og som operationelle objekter – altså den tredje og til dels den fjerde kategori. En sådan afgrænsning forbliver imidlertid funktionel og vælger derfor ikke at diskutere den kognitive og kollektive påvirkning fra og stigende afhængighed af nye informations- og kommunikationsteknologier. Sådanne analyser ville ellers – hvis de blev studeret grundigt – bidrage med vigtig viden om, hvordan samfund hænger sammen, og hvor modstandsdygtige samfund rent faktisk er.

[17] Owens et al. (red.), 2009: 10-11.
[18] Fritz, 2013.

Ligesom cyberbegrebet er trusselsbegrebet også mangeartet og overlappende. Som nævnt indledningsvis tager denne rapport i forsøget på at definere og efterprøve forskelle og overlap fat i seks af de mest omdiskuterede cybertrusler – terrorisme, hacktivisme, spionage, sabotage, kriminalitet og krig – og tilføjer en syvende kategori, lulz, som et eksempel på et unikt onlinefænomen. Den sidstnævnte kategori omfatter en ny form for internetbaserede aktioner, der ikke kan karakteriseres som særlig truende. Når den alligevel inddrages her, er det som en slags dummyvariabel, der skal hjælpe med at forstå de drengestreger, der foregår online, og som ofte fejlagtigt placeres under en af de øvrige mere seriøse trusselskategorier. Derudover er cyberkriminalitet i udgangspunktet en kategori med stort overlap i forhold til de andre trusselsformer, herunder især spionage, sabotage og terrorisme, men bruges snævert i denne rapport såvel som i store dele af litteraturen om cybertrusler som en opsamlingskategori for de kriminelle onlineaktiviteter, der har *simpel* berigelse eller anden form for ulovlig individuel tilfredsstillelse til formål.

I forsøget på at klarlægge og diskutere de forskellige cybertrusler introduceres *fire* parametre. Disse fire parametre er på ingen måde unikke for cybertrusler, og de burde således også kunne appliceres på almindelige trusler, der ikke er relateret til internettets domæne.

Det første parameter er gerningsmandens eller gerningsmændenes *strategiske formål*. Det vil sige den overordnede motivation for et cyberangreb eller en cyberaktivitet – det, de forsøger at opnå. Det andet parameter er *midlerne*. Med midlerne forstås, hvordan gerningsmændene eller gerningsmanden har til hensigt at nå et strategisk mål. Det tredje parameter vedrører *de operationelle mål*, eller hvem eller hvilket objekt gerningsmændene forsøger at ramme. I en cyberkontekst ville dette per definition altid i første omgang være en computer eller et netværk hos enten individer, virksomheder, statslige virksomheder, infrastruktur eller lignende. Det fjerde parameter vedrører de i denne sammenhæng it-specifikke *redskaber*, der bruges til at udføre aktionen mod det operationelle mål. Dette kunne eksempelvis være generiske vira og orme, men også mere sociale indgreb, der har til formål at snyde passwords fra intetanende brugere, og udnyttelsen af sårbarheder og fejl i it-systemer, der muliggør, at en hacker kan ændre i koden eller slette data.

Cyberredskaberne besidder en række karakteristika, der spiller en central rolle i forståelsen af cyberspace som noget nyt og truende: (1) Cyberspace faciliterer anonymitet, hvilket vil sige, at det forbliver relativt nemt at skjule, hvem man er; (2) cyberredskaberne har global rækkevidde, hvilket vil sige, at det potentielt er muligt at

Tabel 1.

	Strategiske formål	*Midler*	*Operationelle mål*	*Redskaber*
Cyber-terrorisme	Politiske eller sociale forandringer	Computerbaseret vold eller destruktion med henblik på at fremkalde frygt i befolkningen eller destabilisere strukturer	It-systemer hos individer (civile/ikkecivile) eller i bygninger og infrastruktur	Vira og orme, social engineering, cracking passwords samt hacking
Hacktivisme	Politiske eller sociale forandringer	Underminering af tillid, spredning af et politisk budskab ved hjælp af ændringer af hjemmeside, frigivelse af fortrolige informationer eller forhindring af adgang	It-systemer hos individer, virksomheder eller statslige institutioner	DDoS, social engineering, cracking passwords, sletning af data, defacement eller hacking
Cyber-spionage	Økonomiske, politiske eller militære fordele og overvågning	Opnåelse af onlineadgang til klassificerede dokumenter (uden at blive opdaget)	It-systemer hos individer/borgere, virksomheder eller statslige institutioner	Vira, orme, social engineering, phishing og cracking passwords
Cyberkrig	Politisk	Den gensidige brug af magt, herunder vold gennem computerkode, med henblik på at få modstanderen til at følge ens vilje	It-systemer hos statslige institutioner eller i vital infrastruktur	Orme, DDoS, installering af backdoors, logic bombs, defacement eller hacking
Cyber-sabotage	Politiske, økonomiske eller militære gevinster	Ødelæggelse og uskadeliggørelse af vital it-infrastruktur med henblik på at opnå taktiske fordele	It-systemer hos virksomheder eller i fjendens vitale infrastruktur	Orme, DDoS, installering af backdoors og logic bombs
Cyber-kriminalitet	Personlige og økonomiske gevinster	Opnåelse af adgang til fortrolige data online, afpresning, fildeling af patenteret eller ulovligt materiale	It-systemer hos individer eller virksomheder	Social engineering, phishing, cracking passwords, identitetstyveri, upload-/download-klienter, vira eller DDoS
Lulz	Morskab (anerkendelse blandt ligesindede)	Chikane og ydmygelse af andre online	It-systemer hos individer, virksomheder eller statslige institutioner	Vira og orme, social engineering, cracking passwords, sletning af data eller hacking

ramme næsten alle steder på kloden, der er i besiddelse af en computer; (3) angreb kan ramme med lynets hast; og (4) cyberredskaber er relativt lettilgængelige og billige.[19] Som det indledende citat samt den resterende del af rapporten diskuterer, kan der være stor forskel på, hvordan cyberredskaberne bruges. Dog sætter disse karakteristika også fokus på en række udfordringer, for så vidt angår internationalt samarbejde om kriminalitetsbekæmpelse, overvågning versus privatliv, juridiske uklarheder om staters brug af cyberangreb mod andre stater, samt statsligt sponsoreret hacktivisme og tyveri af intellektuelle rettigheder.

De syv cybertrusler og fire parametre er opsummeret i tabel 1 og vil i den resterende del af rapporten først blive uddybet og derefter diskuteret i relation til udfordringerne, for så vidt angår forholdet mellem stater og både kriminelle og aktivistiske ikkestatslige aktører, der med cyberspace har indgået en række uskønne alliancer.

[19] Betz & Stevens, 2011: 82-88; Krepinevich, 2012; Denning, 2009: 6-10.

Cyberterrorisme

Professor ved Institut for Forsvarsanalyse på Naval Postgraduate School i Monterey, Californien, Dorothy E. Denning er uden sammenligning den mest citerede forsker, når cyberterrorisme skal defineres. Denning ser cyberterrorisme som en kobling af terrorisme og cyberspace. Terrorisme er i sig selv et vanskeligt og svært definerbart begreb, som ofte både tages for givet og bruges politisk. Dennings tilgang til terrorisme lægger sig i udgangspunktet op ad det amerikanske forsvarsministeriums definition som *den bevidste brug af ulovlig vold eller trusler om ulovlig vold med det formål at indgyde frygt, tvinge eller intimidere regeringer eller samfund i et forsøg på at opnå et mål, der generelt er enten politisk, religiøst eller ideologisk*.[20]

Som nævnt ovenfor er cyberspace også et svært definerbart og omdiskuteret begreb. Men holder man blot fast i, at cyberspace relaterer sig til al computermedieret kommunikation, betyder det, at et terrorangreb eller truslen om et terrorangreb nødvendigvis må være computerbaseret, for så vidt angår både de redskaber, der bruges, og de operationelle mål, der rammes. Ellers giver det ikke mening at koble cyberpræfikset på terrorismebegrebet. Med andre ord ødelægger en cyberterrorist ikke computere eller servere med konventionelle bomber eller fysisk tilstedeværelse, men udfører angrebet *gennem* computernetværk med henblik på at forstyrre, afvise, forringe, ødelægge eller ændre informationer i andre computere eller computernetværk.[21]

Således kan cyberterrorisme ifølge Denning generelt forstås som "ulovlige [cyber] angreb og trusler om [cyber]angreb mod computernetværk og informationerne gemt heri, med henblik på at intimidere eller tvinge en regering eller et folk til at følge et politisk eller socialt mål. Ydermere kan cyberterrorisme kvalificeres ved, at et angreb bør resultere i vold mod personer eller ejendom eller i det mindste forårsager nok skade til at generere frygt. Eksempler kunne være angreb, der fører dødsfald, fysiske kvæstelser, eksplosioner, flystyrt, vandforurening eller alvorlige økonomiske tab med sig. Seriøse angreb mod kritisk infrastruktur ville kunne kategoriseres som cyberterrorisme afhængigt af effekten. Angreb, der forstyrrer ikkeessentielle funktioner, eller som hovedsagelig forårsager økonomiske gener, kan derimod ikke karakteriseres som terror".[22]

[20] U.S. Department of Defense, 2010: 266.
[21] Owens et al. (red.), 2009.
[22] Denning, 2000. Alle citater er oversat af forfatteren.

Udøvelsen af computerbaseret vold og destruktion er imidlertid mere kompleks end som så. Først og fremmest er det vigtigt at understrege, at computerkode ikke i sig selv indeholder en eksplosiv ladning. En cyberterrorist må således ikke blot have forståelse for, hvordan man læser, tilgår og ændrer i computerkode, men skal også være i besiddelse af viden og egenskaber, der gør det muligt at kontrollere det fysiske objekt, som rent faktisk skal forvolde den destruktive handling. Ønsker en cyberterrorist eksempelvis at ødelægge en atomreaktor, er det ikke nok at være en god hacker. Det kræver samtidig, at cyberterroristen forstår, hvordan et atomanlæg fungerer, og hvilken del af computerkoden der styrer de sprængfarlige eller radioaktive processer.

Der findes en række it-tekniske værktøjer, som gør det muligt for en hacker at få uautoriseret adgang til sårbare og usikre computere eller netværk, hvilket dermed også giver cyberterroristen mulighed for at sætte disse ud af kraft. Men virusinficerede eller ødelagte computere kan erstattes relativt hurtigt, og det fører ikke nødvendigvis fatale eller destruktive sekundære effekter med sig – selvom det kan være særdeles omkostningsfuldt for den, der rammes. De fleste it-systemer, der kontrollerer fysiske funktioner, har mulighed for manuel tilsidesættelse, så ønsker cyberterroristen at påføre fysisk skade, kræver det, at den pågældende formår at etablere kontrol over den fysiske funktion, som koden styrer – vel at mærke uden at blive opdaget.[23] Har cyberterroristen samtidig et specifikt mål for øje, og ønsker han eller hun klarhed over omfanget af det planlagte cyberangreb, kræver det mere planlægning og flere it-færdigheder, da et sådant angreb – alt efter it-sikkerhedsniveauet – sandsynligvis skal bryde krypteringer, finde endnu ukendte fejl i kommercielt software[24] og tilgå it-systemer, som ikke befinder sig online. Vanskeligheden ved at udføre et cyberterrorangreb sammenlignet med konventionel terrorisme er sandsynligvis en af de afgørende grunde til, at de ikke-it-kyndige og ikke nødvendigvis særlig ressourcestærke religiøse og yderliggående grupper, som i dag associeres med terrorisme, ikke har brugt cyberredskaber til at indgyde frygt i befolkningen gennem voldelige handlinger.[25]

En potentiel cyberterrorists værktøjskasse kan imidlertid variere i størrelse alt efter målets it-sikkerhedskarakter. Er vitale dele af et samfunds it-infrastruktur blottet for enhver form for sikkerhedsforanstaltninger, er det ikke nødvendigvis vanskeligt for en person med almindelige it-kundskaber at forårsage alvorlig og destabili-

[23] Schneier, 2003.

[24] Disse kaldes zero-day-sårbarheder eller bare "zero-days" og kan defineres som de sårbarheder og fejl i it-systemer og software, som bruges af den angribende part *uden* at være kendt af andre.

[25] Weimann, 2005; Stohl, 2006; Lachow, 2009: 37.

serende skade. I praksis vanskeliggør selv de mindste forbedringer af it-sikkerheden dette betragteligt,[26] hvorfor ethvert cyberangreb, der ønsker at skabe frygt gennem tilvejebringelsen af mere eller mindre tilfældig fysisk skade, skal kunne omgå lukkede, sikrede og krypterede it-systemer. Men benytter man sig af sociale taktikker eller tekniske redskaber til at "cracke" passwords, udnytter man fejl i software, eller identificerer man sårbarheder i måden, hvorpå et it-system er skruet sammen, kan en enkeltperson eller en gruppe af it-kyndige udvikle vira og orme eller slette og ændre i den kode, som styrer diverse it-systemer, hvilket kan koste samfundet betragtelige summer. Dette tydeliggøres hvert år på hackerkonferencen DefCon, hvor dygtige hackere overgår hinanden med hacks af biler, vandforsyninger, pacemakere, køleskabe og lignende.[27] Men ud fra en terrorists perspektiv er spørgsmålet, om sådanne cyberangreb er tilstrækkelig tilfredsstillende, spektakulære og kontrollerede til, at den, der angriber, er sikker på at opnå den ønskede effekt, og at de, der angribes, ikke er i tvivl om, at angrebet faktisk er et cyberterrorangreb og ikke bare en tilfældig ulykke eller drengestreger, der er gået for vidt.[28] Derfor er det måske i virkeligheden ikke så sært, at verden endnu ikke har oplevet et cyberterrorangreb.

Således opsummeret: En cyberterrorist er en person, gruppe eller institution, som bruger eller truer med at bruge forskellige cyberredskaber mod it-systemer i bygninger, i den kritiske infrastruktur eller hos civile og uskyldige borgere med henblik på at fremkalde en tilstrækkelig voldelig effekt, der resulterer i en destabilisering af samfundets eksisterende strukturer og en indpodning af frygt i befolkningen med henblik på i sidste ende at opnå politiske eller sociale forandringer.

[26] Singer & Friedman, 2014: 221.
[27] Kelly, 2013.
[28] Conway, 2011.

Hacktivisme

Hacktivisme er fusionen af hacking og aktivisme. En hacker er oprindelig blot en person med passion for computeralgoritmer, diverse kodesprog og operativsystemer, der frem for alt så computerprogrammering som en hobby. Hacking handlede om æstetik og om med en computer at skabe noget nyt og smukt. Dette billede har imidlertid ændret sig drastisk. "Hack" betyder i dag flere ting. I programmeringsverdenen er et "hack" en hurtig og ikke specielt elegant løsning på en fejl (bug) eller en modificering af software eller hardware på ens egen computer.[29] Det er dog it-sikkerhedsverdenens opfattelse af "hack", der er blevet den dominerende i dag. Her ses "hack" – som for eksempel i "hacktivisme" – som et forsøg på i al hemmelighed enten at bryde ind i andres computere og computernetværk (cracke) eller at forhindre adgangen til disse netværk.[30] Da aktivisme samtidig forstås som et direkte og energisk forsøg på gennem demonstrationer, kampagner, strejker, civil ulydighed eller lignende at skabe politiske eller sociale ændringer, skal "hacktivisme" først og fremmest ses som forsøget på at opnå disse strategiske mål ved hjælp af *virtuelle* blokader eller *virtuelle* indbrud i computere.

Set fra et computerteknisk perspektiv er virtuelle blokader, oftest i form af "distributed denial of service"-angreb (DDoS-angreb) – hvormed man oversvømmer hjemmesider med data, indtil de pågældende hjemmesider og servere ikke længere er tilgængelige – hverken et egentligt "hack" eller et "crack", da man ikke skal have de store programmeringsmæssige færdigheder eller behøver at tilgå andre computere eller netværk. DDoS-angreb kan således mest af alt sammenlignes med en demonstration eller en lockout, der forhindrer adgangen til en bestemt ydelse. DDoS-software, der sender en stor mængde forespørgsler af sted til en given hjemmeside, kan hurtigt og nemt downloades online, og de mere ambitiøse aktivister kan erhverve sig et stort netværk af allerede hackede computere – de såkaldte botnets eller zombiecomputere – som de mod betaling kan få lov at kontrollere i en periode.

DDoS-angreb, der gør hjemmesider utilgængelige, viser sig dog kun sjældent at være længerevarende, og ofte er legitime internetbrugere – selvom de ikke er blevet hacket – faktisk selv skyld i, at en hjemmeside ikke kan tilgås. Dette sker eksempelvis, når danskerne én gang om året strømmer til SKAT's hjemmeside i forsøget

[29] Coleman, 2013a.
[30] Denning, 2001.

på finde ud af, om de skal betale til eller have penge tilbage fra SKAT. Her kan der ofte gå dage, før man kan tilgå sine personlige oplysninger. Ligeledes kan tekniske fejl og inkompetence resultere i, at hjemmesider ikke er tilgængelige. Dette oplevede danskerne, da firmaet bag NemID, Nets, ikke kunne håndtere en ny opdatering af Java – programmet som gør, at man kan indtaste de fire unikke cifre på sit nøglekort. Disse udfordringer har indtil nu vist sig at være væsentlig mere omkostningsfulde end de cyberprotester, som Danmark har oplevet.

Modsat cyberterrorister forsøger hacktivisterne ikke at skabe frygt eller kaos. De forsøger at demonstrere deres utilfredshed samt skabe opmærksomhed omkring deres sag ved at ramme beslutningstagerne, private virksomheder eller statslige institutioner *direkte*, og ikke som cyberterroristerne ved at forårsage skade på tilfældige civile. Allerede under NATO's intervention i Kosovo i 1999 oplevede man eksempler på hacktivisme, da civile "hackergrupper" på begge sider spammede henholdsvis NATO's servere og den serbiske regering med e-mails i tusindvis. De brød samtidig passwords, hvilket gav dem mulighed for at skrive og ændre opsætningen på diverse nyhedsmediers hjemmesider – også kaldt defacements.[31] Lignende hændelser har fundet sted i løbet af konflikten mellem Ukraine og Rusland i 2014.[32] Eksempelvis formåede proukrainske hackere at få adgang til Ruslands største nyhedsside www.rt.com og ændre ordet "russer" til ordet "nazist", mens Janukovitj-støtter på den anden side af konflikten formåede at gøre ukrainske regeringshjemmesider og NATO's hjemmeside utilgængelige.

Ligeledes oplevede man en stor onlinemobilisering, da Scientology i 2008 forsøgte at forhindre udbredelsen af en penibel video af Tom Cruise. Dette førte til flere ugers DDoS-angreb på Scientologyhjemmesider i protest mod forsøg på censur på internettet – en operation der fik navnet Chanology.[33] Mange af angrebene mod Scientology havde imidlertid også en ikkepolitisk karakter og bar præg af at være udført for morskabens skyld, hvilket manifesterede sig i en strøm af ubetalte pizzabestillinger, telefonfis og faxede nøgenbilleder (se lulz-afsnittet nedenfor). Angrebene på Scientology var også for alvor begyndelsen på onlinefænomenet Anonymous, som siden da har udgjort en interessant hybrid af lulz og hacktivisme. Hacktivismedelen af Anonymous og af flere udbrydergrupper med lignende agenda såsom Telecomix blev især tydelige under de arabiske revolter i vinteren og

[31] Denning, 2001: 240-242.
[32] Jacobsen, 2014.
[33] Olson, 2013: 60-89.

foråret 2011, da tunesiske og egyptiske regeringer forsøgte at lukke adgangen til internettet. Her muliggjorde hackere ved hjælp af ekstern adgang og vejledninger, at tunesiske og egyptiske aktivister kunne bevare et talerør til resten af verden.[34] Anonymous har ydermere taget æren for en række hacks mod og efterfølgende lækager fra Assadregimets blodige kamp i Syrien.[35]

Kort fortalt kan en hacktivist således opsummeres som en person, hvis strategiske formål er at skabe politiske og sociale forandringer ved at underminere folks tillid til staten eller virksomheder, hvilket sker gennem forskellige cyberaktiviteter såsom "denial of service"-angreb, "defacements" rettet mod staters, virksomheders eller individers hjemmesider og it-systemer eller ved at frigive fortrolige, ofte kompromitterende informationer.

[34] Olson, 2013: 141-144; Fein, 2013.
[35] Greenwood.

Cyberspionage (og cyberovervågning)

Internettet giver mulighed for at tilgå og dele store mængder information og samtidig forblive anonym. Dette har skabt særdeles fordelagtige vilkår for spionage. Spionage er ofte defineret som det at spionere eller gøre brug af spioner med henblik på at skaffe sig information om en udenlandsk regerings eller et konkurrerende firmas planer og aktiviteter.[36] Regeringer kan ligeledes spionere på egne befolkninger ved hjælp af mere eller mindre systematiske overvågningsprogrammer. Begge dele er i den seneste tid blevet aktualiseret i en cyberkontekst.

Cyberspionage eller cyberudnyttelse – forstået som brugen af computer- og informationsteknologi til indsamling af informationer om individer, virksomheder eller stater, der ellers kan betragtes som hemmelige eller fortrolige, uden tilladelse fra indehaveren af denne information – har således fået et ansigt gennem whistlebloweren Edward Snowdens offentliggørelser af NSA's systematiske overvågning af både USA's allierede og landets egne borgere. Disse dokumenter har ført til en fundamental ændring i synet på cybertruslen: fra ekstern spionage til internt brud på privatlivets fred, genereret af en stat eller gruppe af stater, som i udgangspunktet burde forventes at beskytte denne rettighed. Cyberspionagedebatten indbefatter imidlertid stadigvæk også de mange beskyldninger mod det stats- og virksomhedsdrevne tyveri af intellektuelle rettigheder. Den uautoriserede adgang til amerikanske virksomheders data er således blevet karakteriseret som den største overførsel af rigdom i historien og som cyberangreb, der truer USA's nationale sikkerhed.[37]

Men egentlig opfylder cyberspionage eller -overvågning ikke betingelserne for et cyber*angreb*, da cyberspionerne ikke har til hensigt at ødelægge, forstyrre eller ændre informationer i de computere eller netværk, som de har fået uautoriseret adgang til. Cyberspionage er således ikke instrumentel, forstået på den måde at overvågningen ikke nødvendigvis skal bruges til noget eller har et klart mål for øje. Kun såfremt de indsamlede data rent faktisk kan omsættes til forståelig og brugbar viden om f.eks. svagheder i fjendens it-infrastruktur, en konkurrerende virksomheds nye opfindelse eller økonomiske status eller et terrorangreb i svøb, får cyberspionage/-overvågning et egentligt formål. Dog udgør den manglende klarhed omkring motiverne bag cyberspionage også en øget risiko for yderligere

[36] *Merriam-Webster Online Dictionary*, 2014.
[37] Rogin, 2012.

eskalering, da uautoriseret adgang til vitale computersystemer kan øge det politiske pres for præventive indgreb.

Tager man udgangspunkt i en række cyberspionagesager, viser der sig nogle udfordringer med hensyn til kategoriseringen og dermed håndteringen af denne ikke-instrumentelle form for udnyttelse. Først og fremmest er det vanskeligt på baggrund af de it-redskaber, der bruges, at afgøre, om hensigten er et cyberangreb eller cyberspionage. På den ene side behøver succesfuld spionage meget lig cyberterrorisme ikke nødvendigvis at være specielt sofistikeret. Alt efter hvilket mål gerningsmanden eller gerningsmændene har udvalgt, kan social engineering – en overbevisende e-mail med et korrumperet link, eller en inficeret PowerPoint-fil – være rigeligt til at skaffe sig adgang til en anden persons computer.

På den anden side kan den specifikke spionageoperation være ekstremt sofistikeret og foregå over en lang årrække. Blandt de mest komplekse malware, der nogensinde er fundet, er de tre formodentlig amerikansk- eller israelskudviklede spionageorme Duqu, Flame og Gause, som henholdsvis og blandt mange andre ting gav afsenderen fjernadgang til de inficerede it-systemer, gav mulighed for at optage og sende lyd tilbage til afsenderen samt skabte et redskab til at monitorere transaktioner fra en række libanesiske banker.[38] Og uanset om det er en sofistikeret eller simpel cyberoperation, forplumrer cyberspionage billedet, så det bliver svært at skelne mellem det kriminelle og det politiske og mellem det interne og det eksterne. Det er umuligt at vide, om den inficerede fil har simpel berigelseskriminalitet for øje, eller om den giver en potentiel fjende adgang til at installere bagdøre i vital infrastruktur, som ville kunne tilgås i en eventuel krigssituation.

Et andet kendt eksempel på cyberspionage er den række af formodede kinesiske cyberoperationer med tilnavnet Titan Rain, der startede i 2003 og downloadede, hvad der menes at være mellem ti og tyve terabyte datamateriale fra NIPRNet – Pentagons ikkeklassificerede netværk.[39] Tyve terabyte udgør betydelige mængder information, svarende til små 75 kilometer i printet form, og det kræver i sig selv en del arbejde at håndtere. Hermed relaterer cyberspionage sig til fænomenet *big data*. Udfordringen ved big data er, (1) at man ikke kan være sikker på, om man har den rette og nødvendige information, (2) at man mangler redskaber til at dekryptere, analysere og forstå al informationen, og (3) at man risikerer at miste den menneskelige del af efterret-

[38] Rid, 2012: 93-99.
[39] Rid, 2012: 85-86.

ningsarbejdet. Sidstnævnte har i amerikansk overvågningssammenhæng givet anledning til en del pudsige historier om eksempelvis danske turister, der uden officiel begrundelse nægtes indrejse til USA.[40] Chefen for NSA, Keith Alexander, gjorde sig ligeledes uheldigt bemærket, da hans kroneksempel på, hvordan indsamling af store mængder kommunikationsdata kunne bruges til at kortlægge terroristers netværk, ved nærmere eftersyn viste, at de centrale noder, der knyttede terroristerne sammen, ikke var bagmændene, men pizzeriaer.[41] Det mest bemærkelsesværdige eksempel var imidlertid historien om seks FBI-agenter, der som følge af NSA's generelle monitorering af Googlesøgninger bankede på døren hos familien Catalano, efter sigende på baggrund af onlinesøgninger på trykkogere og rygsække.[42]

Som det ser ud i øjeblikket, foregår cyberspionage i en væsentlig større målstok end traditionel spionage. Det skyldes først og fremmest, at cyberspionage og cyberovervågning forbliver både nemmere og hurtigere samt forbundet med færre risici. Det er simpelthen belejligt for både virksomheder og statslige efterretningstjenester at indsamle alle de data, som borgere og virksomheder både frivilligt og ufrivilligt gør tilgængelige via internettet. Og det er ligeledes belejligt for disse efterretningstjenester og virksomheder at modarbejde bedre kryptering og bedre it-sikkerhed generelt, da dette ellers ville gøre det vanskeligere at få mening ud af de indsamlede informationer – om denne mening så har marketing eller borgernes sikkerhed for øje. Det store spørgsmål vedrørende både cyberspionage og cyberovervågning forbliver således, om den kvantitative forøgelse i indsamlingen af data kan omsættes til en kvalitativ forbedring af efterretningerne, og i så fald om denne forbedring kan stå mål med de medfølgende brud på borgerrettighederne. På bagkant af Snowdens lækage har NSA endnu ikke formået at overbevise befolkningen om, at den store indsamling og overvågning af metadata samt den mindre gennemsigtighed og indskrænkning af borgernes retssikkerhed faktisk har forhindret terrorangreb.

Men selvom offentlighedens øgede bevågenhed omkring den masseovervågning, der foregår gennem cyberspace, måske også fører til en øget kontrol med nationale efterretningstjenester, vil cyberindustrispionage efter alt at dømme fortsætte. Det er simpelthen stadig en god forretning at investere ressourcer i at stjæle andres opfindelser, budgetter eller forhandlingsstrategidokumenter ved hjælp af cyberredskaber.

[40] Gonzales, 2010; Skjoldager & Reenberg, 2013.
[41] Harris, 2013.
[42] Gabbatt, 2013.

Opsummerende har cyberspionage ligesom konventionel spionage til formål – gennem indsamling af klassificerede data og private informationer – at opnå enten økonomiske, strategiske eller politiske gevinster, men i cyberspace forfølges dette gennem målrettede eller generiske cyberoperationer mod eller overvågning af individers, virksomheders eller staters it-systemer, hvilket sker ved hjælp af en række it-tekniske redskaber, som strækker sig fra simpel social engineering til de mest komplekse orme. Cyberovervågning inkluderer ydermere åbne informationer, som borgere eksempelvis lægger på sociale medier, eller som bliver indsamlet via teleselskabers monitorering af ind- og udgående opkald og sms.

Cyberkrig

Den nok mest indflydelsesrige amerikanske cyberkrigsforsker John Arquilla er ikke i tvivl: "Cyberkrig er kommet, og kommet for at blive".[43] Denne udtalelse var en direkte respons til en anden prominent cyberkrigsforsker, Thomas Rid, som i en meget refereret bog, *Cyber War Will Not Take Place*, påstod det stik modsatte.[44] Modsætningen mellem de to understreger meget godt den nuværende debat i cyberkrigslitteraturen, som går ind til roden af, hvad *krig* egentlig er.

Den førstnævnte gruppe af forskere tager sig sjældent tid til at diskutere definitionen af cyberkrig, hvilket har resulteret i en bred forståelse af krigsbegrebet, der omfatter cyberspionageoperationer mod virksomheder, defacements af hjemmesider og sletning af data[45]. De få forskere i denne gruppe, der imidlertid tager sig tid til at overveje begrebet, baserer ofte deres analyser på en forståelse af cyberkrig, som USA's tidligere nationale sikkerhedskoordinator Richard A. Clarke definerer som "de aktioner, en nationalstat udfører med henblik på at trænge ind i en anden nations computere eller netværk i forsøget på at forårsage skade eller forstyrrelser"[46]. Da nationalstatsfokusset har været omdiskuteret og kritiseret i krigslitteraturen i et par årtier,[47] har nogle forskere valgt at udvide cyberkrigsdefinitionen til at dække mere end statsaktørers politiske interesser, således at ikkestatslige aktørers religiøse, kulturelle og økonomiske mål også inkluderes i forståelse af cyberkrig.[48] De mere skeptiske cyberkrigsforskere fastholder, at en sådan definition og dertilhørende analyser er for upræcise, empirisk fejlagtige og overser krigens altid politiske, instrumentelle og fysiske karakter.[49] Disse forskere baserer deres analyser på det faktum, at krigens natur – selvom den forstås i en cyberkontekst – ikke har ændret sig, siden Napoleon kæmpede sig vej gennem Europa i det 19. århundrede. Således kan der i en cyberkrig altid tilskrives et politisk formål, hvilket vil sige en stats eller gruppes interaktion omkring, beslutning om og forsøg på at tilkæmpe sig magt over nogen eller noget. Inkluderer man imidlertid i definitionen af krig individuel berigelseskriminalitet eller udelukkende religiøse overvejelser, mudrer man unødvendigt billedet af, hvad krig er vis-à-vis andre trusler.

[43] Arquilla, 2012; Arquilla & Ronfeldt, 1993: 141-165; McConnell, 2010.
[44] Rid, 2012.
[45] Mazanec, 2009; Jenik, 2009; Sale, 2012.
[46] Clarke & Knake, 2010.
[47] Van Creveld, 1991.
[48] Cornish et al., 2011.
[49] Rid, 2011: 5-32; Gartzke, kommende publikation; Lawson, 2011; Jacobsen, 2014.

De skeptiske cyberkrigsforskere understreger yderligere, at en krig altid er den gensidige brug af magt, herunder vold,[50] hvilket i en cyberkrigskontekst vil sige, at to eller flere sider i en konflikt angriber hinanden med cyberredskaber såsom orme, vira og DDoS-angreb eller gennem præinstallerede bagdøre og logiske bomber,[51] indtil fjenden er nedkæmpet, eller de politiske mål er nået. Med andre ord er en krig *aldrig* ét enkelt angreb. Følger man således denne forståelse af cyberkrig, må det nødvendigvis betyde, at it-systemerne i vital infrastruktur og statslige institutioner altid er militærets primære operationelle mål i udkæmpelsen af cyberkrigens slag. Såfremt konventionelle våben i samme eller højere grad bruges, giver det ikke længere mening at karakterisere en konflikt som cyberkrig, når den i lige så høj grad kan ses som en almindelig krig.

Hvorvidt cyberredskaber besidder evnen til at påføre tilstrækkelig skade til at ende en krig, er der ligeledes uenighed om. På den ene side ser en række teoretikere cyberangreb som værende af samme strategiske betydning som atomvåben,[52] mens andre afviser dette som unødvendig hype, der blot bidrager til at militarisere cyberspace endnu mere.[53] Al den usikkerhed, der omgærder denne debat, skyldes først og fremmest, at verden endnu ikke har oplevet en krig, hvori cyberangreb har udgjort det primære redskab. Det eneste eksempel på, at cyberangreb er blevet brugt i forbindelse med en intervention, var i sommeren 2008 i forbindelse med Rusland-Georgien-konflikten.

De cyberredskaber, der blev brugt i denne konflikt, havde hovedsagelig karakter af DDoS-angreb og defacements og blev sporet tilbage til servere tilhørende kriminelle russiske netværk. Kreml afviste ethvert kendskab med reference til, at de ikke havde kontrol med de såkaldte patriotiske hackere eller hacktivister.[54] Cyberangrebene formåede at lukke for den georgiske regerings hjemmesider og nyhedssites, men påvirkede kun kortvarigt den georgiske regerings evne til at kommunikere med omverdenen, da en international koalition bistod Georgien med teknisk assistance.[55] Omvendt svarede den georgiske præsident Mikheil Saakasjvili igen med at censurere russiske hjemmesider.[56] Effekten af cyberangrebene er svær at vurdere, men det

[50] Rid, 2011.
[51] Logic bombs er software gemt i et computersystem, som er præinstalleret til at udløse under givne omstændigheder.
[52] Clemmons & Brown, 1999; Sharma, 2009.
[53] Samaan, 2010; Gartzke, kommende publikation.
[54] Krepinevich, 2012: 23.
[55] Præcis hvor seriøst angrebet var, er der stadig uenighed om i litteraturen. Se Clarke & Knake, 2010; Rid, 2011; Tikk et al., 2008.
[56] Deibert & Rohozinsiki, 2010: 25.

er endnu ikke påstået, at disse angreb var af så afgørende betydning, at de kunne have afløst den fysiske intervention af russiske tropper på de omstridte territorier i Sydossetien og Abkhasien. Den seneste konflikt på Krimhalvøen i foråret 2014 illustrerer ligeledes meget godt, hvordan hackere i en krigssituation stadig ikke kan indtage en flådebase eller andet fysisk territorium – og dermed erstatte soldater på jorden. Dette ser ikke ud til at ændre sig i den nærmeste fremtid.

De manglende eksempler på strategisk og målrettet brug af cyberredskaber i krig har imidlertid affødt en omfattende juridisk diskussion blandt vestlige eksperter i international lov om, hvornår man befinder sig i en krigssituation, eller med andre ord, hvornår et cyberangreb er krigens indledende handling, der retfærdiggør FN's artikel 2 stk. 4 eller artikel 51 vedrørende forbuddet mod staters brug af magt samt retten til selvforsvar[57]. Her findes der bred enighed om, at et cyberangreb *kan* udgøre en krigshandling i sig selv, såfremt *konsekvenserne* er seriøse nok. Præcis hvor seriøse de skal være, er der imidlertid fortsat uenighed om.[58] Værd at bemærke er således, at det mest omfattende juridiske dokument endnu udarbejdet på området, *Tallinn-manualen*[59], hverken når til enighed på dette område eller adresserer de russiske bekymringer om informationssikkerhed og propaganda. Netop usikkerheden og uenigheden om de juridiske retningslinjer sammenholdt med uvidenheden om modstanderens offensive cyberkapabiliteter gør, at cyberangreb i krig stadig befinder sig i en gråzone. Denne usikkerhed kan imidlertid have en dæmpende effekt på lysten til at bruge cyberangreb som krigens indledende handling.

Konflikten på Krim i foråret 2014 illustrerer meget godt denne pointe. Rusland mangler viden om, hvilken cyberkapacitet Ukraine besidder, og hvad ukrainske cyberangreb eventuelt vil kunne betyde for borgere i Moskva og Skt. Petersborg. Det samme gælder for Ukraine i forhold til cyberangreb på vital infrastruktur i Kiev. Og selvom en af konfliktens parter alligevel skulle forsøge sig med et målrettet cyberangreb, gør de manglende juridiske retningslinjer, at intet hindrer et konventionelt militært modsvar og dermed en eskalering af konflikten. Med andre ord forbliver cyberkrigsbegrebet uhensigtsmæssigt, af den simple årsag at en krig udelukkende i cyberspace er og bliver en usandsynlighed.

[57] Schmitt (red.), 2012.

[58] Barkham, 2001; Buchan, 2012; Schmitt, 1999; Schmitt & O'Donnell (red.), 2002; Hathaway & Crootof, 2012; Lin, 2010; Richardson, 2011; Roscini, 2010; Sandvik, 2012; Sharp, 1999.

[59] Schmitt (red.), 2012.

Cyberkrigsdebatten er i dette afsnit forsøgt udfoldet med henblik på at påpege, hvorledes uenighederne bunder i en divergerende forståelse af, hvad krig er. Følger man teoretikerne, der lægger sig op ad den klassiske krigslitteratur, kan cyberkrig opsummeres som den gensidige og instrumentelle brug af magt med henblik på at opnå et politisk mål, hvor den primære anvendelse af vold mod vital infrastrukturs og statslige institutioners it-systemer sker indirekte gennem computerkode og andre cyberredskaber såsom DDoS-angreb. Opfylder en konflikt ikke disse krav, betyder det ikke nødvendigvis – som konflikten i Georgien understregede – at cyberangreb ikke har været brugt eller kan have været operationelt vigtige. Dette diskuteres i det følgende afsnit.

Cybersabotage

"Cyber-sabotage is Easy – So why aren't hackers crashing the grid?". Sådan startede Thomas Rid for nylig en *Foreign Policy*-artikel.[60] Den ellers kritiske cyberkrigsteoretiker havde deltaget i en femdagesøvelse i Idaho arrangeret af det amerikanske Industrial Control Systems Cyber Emergency Response Team. Spørgsmålet opstod, da han med egne øjne oplevede, at en beholder med vand, der skulle forestille giftig væske, som følge af et cyberangreb knustes mod gulvet. Et lignende spørgsmål kunne passende være blevet stillet i relation til spørgsmålet cyberterrorisme. Her kunne nogle af forklaringerne – som det blev diskuteret i cyberterrorisme ovenfor – ligge i det faktum, (1) at cyberangreb sammenlignet med konventionelle terrorangreb ikke har så direkte fysisk og derfor ikke så spektakulær og voldelig effekt; (2) at de grupper af terrorister, som vi frygter i dag, ikke har eller søger særlige it-tekniske færdigheder, men i højere grad drages af den umiddelbare tilfredsstillelse og følelse af fællesskab, som det at holde et fysisk våben blandt ligesindede giver; og (3) at det kan være vanskeligt at afgøre, om et cyberangreb rent faktisk var et angreb eller blot et uheld.

Sabotage derimod har ikke til hensigt at sprede frygt. Den indeholder ikke nødvendigvis en voldelig komponent med henblik på at skade andre mennesker, og der eksisterer ikke et ønske om anerkendelse eller et behov for at blive tilskrevet handlingen. Tværtimod har sabotøren et ønske om anonymitet og målretter udelukkende sine angreb mod ikkemenneskelige mål.

Sabotage fik først for alvor en destruktiv betydning i det 20. århundrede, da begrebet blev associeret med en strejke blandt jernbanearbejdere i Frankrig i 1912, hvor arbejderne forsøgte at afspore togene i protest mod ringe forhold.[61] Sidenhen er begrebet blevet brugt til blandt andet at beskrive de aktiviteter, som modstandsbevægelserne i Anden Verdenskrig benyttede sig af under den tyske besættelse. Således kan sabotage forstås som en "planmæssig ødelæggelse af produktion eller produktionsmidler [herunder rustningsindustrien, militære anlæg og trafikmidler] i den politiske, økonomiske eller militære kamp".[62] I en cyberkontekst har dette ikke ændret sig. Faktisk passer cyberspace og sabotage – eller cybotage[63] – intuitivt set vældig godt

[60] Rid, 2013.
[61] Donald, 2008.
[62] Gyldendal, 2009.
[63] Arquilla & Ronfeldt, 2001: 5.

sammen, især den stigende afhængighed af it-infrastruktur, som samfundet oplever i dag, taget i betragtning. Cyberangreb kan forholdsvis gnidningsfrit gøres anonyme, og sammen med deres uundgåelige tekniske og dermed kun indirekte fysiske karakter ligger cyberredskaberne i god forlængelse af sabotørens ønske om anonymt at kunne ødelægge forskellige ting, mekanismer og systemer af central betydning for modstanderens manøvremuligheder.

Tages dette i betragtning, er Rids indledende forundring ikke ubegrundet. Der har dog været eksempler på cybersabotage. I 2000 formåede Vitel Boden, efter i en tremåneders periode 46 gange at have trængt ind i et rensningsanlæg i Maroochy Shire, Queensland, at lukke over en million liter kloakvand ud i lokale parker og åer. Boden, der tidligere havde arbejdet for det firma, der havde installeret rensningsanlæggets it-systemer, havde ikke fået det kommunale job, han havde søgt hos Maroochy Shire Council.[64] Denne form for sabotage blev dog håndteret som en simpel kriminel handling, og Boden fik to år i fængsel.[65]

Sabotage er generelt blevet beskrevet som de svages våben, der først og fremmest har moralsk betydning i kampen mod overmagten, og er altid af overmagten blevet karakteriseret som almindelig kriminalitet. Sabotage bør dog også appliceres i en militær (cyber)kontekst, da den kan bruges til at forstå de angreb, som den stærke stat bruger. Cybersabotageaktioner, der lægger overvågningssystemer ned og lammer kommunikationsnetværk, kan vise sig vitale i en krigssituation, enten selvstændigt eller måske især som en forudgående operation, der øger effekten af et konventionelt militært angreb (en "force multiplier").[66] Israels bombning af en atomreaktor i Dayr al-Zor i Syrien i 2007 illustrerer cybersabotageaktioner som en force multiplier og fremstår måske som det bedste eksempel på, hvad cyberredskaber kan bruges til i en militær sammenhæng. Bombningen er interessant, fordi et forudgående cyberangreb formodentlig havde udnyttet en bagdør i det it-system, der styrede det syriske forsvarsnetværk. Dette gjorde det muligt at sætte det syriske overvågningssystem, der ellers skulle opfange de israelske fly, ud af kraft, mens aktionen fandt sted.[67] Således er det vanskeligt i en krigssituation at opretholde en sondring mellem cyberkrigsførelse – som de cyberaktiviteter, der finder sted i en krig – og cybersabotage.

[64] Slay & Miller, 2007; Rid & McBurney, 2010: 10.
[65] Smith, 2001.
[66] Stone, 2013: 106.
[67] Clarke, & Knake, 2010.

Værd at bemærke er, at Israel og, som rapporten diskuterer senere, USA ikke forblev anonyme. Dette vidner om, at selvom de tekniske analyser ikke giver entydige svar på, hvem der står bag cybersabotagen, kan konteksten og almindelige menneskelige efterretninger hjælpe til med at udpege bagmanden. At Syrien – og senere Iran – ikke svarede igen med seriøse cyberangreb eller konventionel militær gengældelse, skyldes, at dette fra både et taktisk og et strategisk synspunkt ville være det rene selvmord. Både USA og Israel har overlegent militær og vil ikke politisk kunne tolerere at blive angrebet uden at igangsætte en seriøs gengældelsesaktion. Pointen er således, at cybersabotage ikke hovedsagelig er den svage aktørs våben, men faktisk har vist sig mest brugbar for den stærke stat.

Det paradoksale ved denne pointe er imidlertid, at den stærke stats opgradering af offensive cyberkapabiliteter med eksempelvis sabotage (eller spionage) til formål udfordrer disse staters egen cybersikkerhed, hvilket ultimativt øger risikoen for, at ikkestatslige aktører i fremtiden søger mere aktivt at opbygge kapaciteten til at påføre seriøs skade ved hjælp af cyberangreb. Forklaringen ligger i, at ethvert cyberangreb hviler på evnen til at finde programmeringsfejl eller andre sårbarheder i fjendens it-systemer, men at mange af disse it-systemer samtidig gør brug af kommercielle produkter fra f.eks. Microsoft, Siemens og Google, som også bruges i eksempelvis USA og Europa. Identificerer hackere således en fejl i disse it-produkter, som gør det muligt at få uautoriseret adgang til fjendens it-systemer, står de over for et valg: 1) enten at holde fejlen hemmelig med henblik på at udnytte denne adgang i fremtidige cyberangreb og derved bevare en potentiel sårbarhed i statens egen infrastruktur eller 2) at offentliggøre sårbarheden og dermed være med til at øge cybersikkerheden for alle.

Problemet er langtfra hypotetisk. NSA afsatte sammen med en række andre sikkerhedsagenturer i 2013 midler til at erhverve sig viden om nye fejl i it-produkter.[68] Den øgede interesse for cyberangreb som en måde at sabotere fjendens vitale infrastruktur uden at forårsage fysisk vold på civile har fået flere til at se fordelene ved den stærke stats cybersabotage.[69] Men de fordele, der eventuelt måtte være, bør altid sættes i relation til den generelle it-sikkerhed, som man som følge heraf uundgåeligt nedprioriterer.

Cybersabotage kan således kort opsummeres som de angreb, der udføres med cyberredskaber – orme, DDoS, udnyttelse af bagdøre og lignende – med henblik på at ødelægge

[68] Peterson, 2013.
[69] Lewis, 2012: 72.

eller midlertidig uskadeliggøre fjendens vitale infrastruktur i forsøget på at opnå enten politiske, økonomiske eller militære gevinster.

Cyberkriminalitet

Der hersker en del uklarhed, for så vidt angår sondringen mellem cyberkriminalitet og andre former for cybertrusler. Dette har ført til, at de fleste artikler og rapporter om emnet end ikke forsøger at definere begrebet[70]. *Europarådet* undlod for eksempel at definere begrebet, da det vedtog konventionen om cyberkriminalitet i 2004.[71] Europa-Kommissionen har imidlertid foreslået, at cyberkriminalitet er traditionelle former for kriminalitet såsom (1) bedrag eller falskneri begået gennem elektroniske kommunikationsnetværk og informationssystemer, (2) udgivelsen af ulovligt indhold via elektroniske medier (eksempelvis materiale, der viser seksuelt misbrug eller opfordrer til racehad) eller (3) unikke onlinefænomener som DDoS-angreb eller *black-hat hacking*, der hindrer adgang til eller korrumperer data[72].

Afhængigt af nationale lovgivninger samt tolkningen af international lov kan en ulovlig handling i cyberspace således inkludere samtlige cybertrusler, der her diskuteres. Det betyder, at cyberkriminalitet i udgangspunktet er en opsamlingskategori, som indeholder de cybertrusler, der ikke falder ind under de andre kategorier. Denne opsamling af simplere former for cyberkriminalitet adskiller sig ved at være centreret udelukkende om en direkte og personlig tilfredsstillelse, gennem enten økonomiske gevinster, anerkendelse eller seksuel tilfredsstillelse i form af børneporno og lignende, og omfatter forholdsvis simple forsøg på identitetstyveri, phishing, udnyttelse af allerede kendte svagheder hos individer eller virksomheder (low-hanging fruits) eller fildeling af ulovligt materiale.[73] Cyberspionage i form af industrispionage falder også ind under kategorien økonomisk motiveret kriminalitet, men er ofte mere indirekte, baseret på nationalstatslige og sikkerhedspolitiske interesser, mindre instrumentel og sjældent så individualiseret som den simple form for cybersvindel.

At det har været umuligt helt at adskille den simple form for cyberkriminalitet fra andre former for trusler, har haft en direkte effekt på muligheden for at bekæmpe cyberkriminalitet. Ved at tilføje cyberpræfikset vanskeliggøres både bekæmpelsen og efterforskningen af cyberkriminelle. Det hænger frem for alt sammen med cyberspaces transnationale karakter samt muligheden for anonymitet, hvilket har fået

[70] Gordon & Ford, 2006: 13.
[71] Europarådet, 2004.
[72] Europa-Kommissionen, 2007.
[73] For en omfattende indsigt i den simple berigelseskriminalitet online læs Glenny, 2012.

mange it-sikkerhedseksperter til at understrege, at cyberkriminalitet er den farligste kriminalitetstrussel nogensinde.[74] Et overlap mellem de tekniske metoder, der bruges til henholdsvis berigelseskriminalitet, spionage/overvågning, aktivisme og for den sags skyld også cybersabotage, gør ydermere, at der kan være nogle politiske og strategiske årsager til ikke at ville et internationalt samarbejde. Dette illustreres især ved den manglende villighed mellem aktører som Rusland og Kina, hvis forståelse af cybertruslen frem for alt relaterer sig til bekæmpelse af den interne ustabilitet, som et åbent internet kan medføre, og USA og EU, som i stigende grad ser Rusland og Kinas cyberspionage som det største sikkerhedspolitiske problem. Billedet mudres især, når Kina og Rusland beskyldes for at hyre kriminelle hackergrupper til at bryde ind i amerikanske virksomheders it-systemer for at finde militære hemmeligheder og intellektuelle rettigheder.[75] Der mangler således tillid til, at andre lande ikke vil udnytte den åbenhed, som internationalt samarbejde påkræver, til at tilegne sig yderligere viden om it-setuppet hos modparten.

Andre mere håndgribelige udfordringer vedrører national lovgivning. Filippinerne havde eksempelvis ikke juridisk belæg for hverken at udlevere eller at dømme Onel de Guzman, som i 2000 skabte ILOVEYOU-virussen, der efter sigende på globalt plan kostede milliarder af dollar.[76] Motivationen for ILOVEYOU-virussen adskilte sig fra sædvanlige motivationer for cyberkriminalitet. Tilsyneladende havde ILOVEYOU hverken berigelseskriminalitet, terror eller aktivisme for øje, men derimod udelukkende til formål at skaffe Guzman anerkendelse fra det onlinefællesskab, hvori han befandt sig. Begrebet *black-hat hacking* er i høj grad kommet til at karakterisere denne form for kriminalitet, der omfavner uautoriseret adgang til beskyttede it-systemer eller programmering af spektakulære vira med det ene umiddelbare formål at opnå anerkendelse.[77]

Håndteringen af cyberkriminalitet vanskeliggøres for det tredje af, at der endnu ikke foreligger nogen muligheder for blot nogenlunde præcist at måle det samfundsmæssige tab ved cyberkriminalitet. Der er blevet givet forskellige bud. Oftest refereret er en rapport fra det britiske Office of Cyber Security & Information Assurance, der

[74] Blakemore, 2012: 12.

[75] Doherty, 2013.

[76] Brock Jr., 2000.

[77] *Black-hat hacking* står i modsætning til *white-hat hacking*, der indrammer de tilfælde, hvor hackere bliver købt af virksomheder eller stater til at identificere fejl og sårbarheder i disse institutioners egne it-systemer og netværk. En midterkategori udgøres af *grey-hat*-hackere, der hacker uden at have fået tilladelse med det formål at frigive de sårbarheder, som de finder. Sådanne eksempler findes ofte hos hackere, der ønsker at påvise, hvor utilstrækkelig staters it-sikkerhed på nuværende tidspunkt er.

i 2011 fremlagde et beløb, der lød på en årlig omkostning for den britiske økonomi på svimlende 27 milliarder pund.[78] Her udgøres 62 % af tyveri af intellektuelle rettigheder og spionage. Går man rapporten igennem, viser det sig imidlertid, at tallene er baseret på det rene gætværk, da "andelen af stjålne intellektuelle rettigheder ikke på nuværende tidspunkt kan måles med nogen form for sikkerhed", og da "det er vanskeligt at afgøre, hvilken andel af industrispionagen der skyldes cyberkriminalitet".[79] De astronomiske tal er dog med til at presse politikere til at bruge flere penge på cybersikkerhed, hvilket paradoksalt nok ifølge rapportens målemetoder blot indgår i det samlede tabstal for cyberkriminalitet – som en yderligere udgift!

Skal man forsøge at opsummere cyberkriminalitet som noget separat i forhold til de andre former for cybertrusler, kan man sige, at simpel cyberkriminalitet har individuelle økonomiske gevinster eller personlig tilfredsstillelse til formål. Den kriminelle aktivitet er oftest rettet mod it-systemer hos individer og virksomheder med henblik på at opnå adgang til fortrolige data eller at dele ulovligt materiale. Med hensyn til de it-redskaber, der bruges, er der næsten ingen grænser for kreativiteten, og de cyberkriminelle er oftest først med de nyeste teknikker inden for alt fra phishing, cracking og social engineering til sofistikerede orme og vira.

[78] Detica & The Office of Cyber-Security and Information Assurance in the Cabinet Office, 2011.

[79] Detica & The Office of Cyber-Security and Information Assurance in the Cabinet Office, 2011: 16 (citater oversat af forfatteren); Anderson et al., 2012.

Lulz

De seks første trusler gennemgået ovenfor har alle været sammenkoblinger af forskellige virkelige trusler og cyberspace. *Lulz* er et fænomen, der er opstået med internettets udbredelse, og bruges i rapporten som et eksempel på en kategori, der indfanger de drengestreger, der finder sted i cyberspace. *Lulz* er egentlig bare en videreudvikling af den kendte forkortelse "lol" ("laughing out loud") og bruges som motivation for en handling. Altså at man gør noget online for sjov med henblik på at få et godt grin. Begrebet indeholder imidlertid også en social dimension, da man helst skal dele sine *pranks* ("drengestreger") med sine ligesindede online – jo mere skandaløs og ydmygende en aktion er, desto mere anerkendelse modtager man. Umiddelbart synes *lulz* og trusler at ligge langt fra hinanden og bør da heller ikke i udgangspunktet kobles. Grunden til, at diskussionen af begrebet er relevant, er imidlertid, at der i stigende grad er kommet fokus på internetfænomenet Anonymous. Uden kendskab til og forståelse for begrebet *lulz* er der en vis sandsynlighed for, at man misforstår, miskategoriserer og simplificerer de onlineaktivister, som Anonymous de seneste år har repræsenteret.[80]

Ét sted at starte, når man skal forsøge at forstå *lulz*-delen af Anonymous, er på hjemmesiden 4chan.org, hvor begrebet *lulz* har sin oprindelse. 4chan.org, eller nærmere bestemt /b/-tråden på 4chan.org, er af den satiriske wiki *Encyclopedia Dramatica* blevet kaldt "internettets røvhul" – en hjemmeside, hvor det absurde, det væmmelige og det ydmygende går hånd i hånd med morskaben.[81] Det er på denne hjemmeside, hvor al kommunikation er anonym, at begreber som "trolling" og "doxing" er opstået.[82] Og det var i 2007, da *Fox News* kaldte 4chan "internettets hademaskine", at Anonymous for første gang, i en spydig svarvideo, blev brugt som en samlende betegnelse for den gruppe af folk, der opholdt sig på nettet med henblik på at have det sjovt og gøre grin med andre.[83]

Forsøger man at forstå Anonymous uden denne lulz-del, er det med stor fare for at misforstå fænomenet Anonymous og de folk, der associerer sig med det (Anons). Dermed ikke sagt, at Anons ikke også kan være og er hacktivister og kriminelle, men

[80] Se eksempelvis Woolford & Matusitz, 2011.

[81] Olson, 2013: 26-47.

[82] Trolling er internetslang for et forsøg på at gøre andre folk så sure og ophidsede som muligt, mens doxing er frigivelse af personlige data med henblik på at ydmyge denne person.

[83] Coleman, 2013b: 4-5.

som antropologen Gabriella Coleman understreger, så er langt størstedelen af aktiviteterne "for the lulz" ufarlige og lovlige.[84] Der er imidlertid opstået et klart overlap mellem hacktivisme og lulz blandt Anons. Som allerede nævnt var Chanology, Anonymous' stadig igangværende aktion mod Scientology, karakteriseret ved både et politisk budskab og morskab. Med oprettelsen af LulzSec i 2011 blev sammenhængen mellem de to endnu mere mudret. LulzSec, en udbrydergruppe fra Anonymous, eksisterede i 50 dage, men formåede blandt andet at frigive fortrolige data fra Sony og NATO, udgive opdigtede nyheder på *PBS News* og *The Sun* og lægge det britiske Serious Organised Crime Agency og civ.gov ned ved hjælp af DDoS-angreb – alt sammen, som navnet antyder, "for the lulz". Kendetegnende for disse gråzoner mellem det kriminelle og morskaben er, at de fleste centrale personer, som rent faktisk brød loven, har siddet i fængsel som følge af deres aktiviteter på internettet.

En diskussion af disse eksempler, omend de lyder alvorlige og kan have store økonomiske konsekvenser, sammenholdt med begrebet *lulz* har således til hensigt at påpege, hvorledes en central del af motivationen for størstedelen af Anons operation ikke skal overanalyseres og tales op til meget andet end småkriminelle drengestreger og irritationer. Der er tale om hverken terrorisme eller et forsøg på at omstyrte den nuværende samfundsstruktur – på trods af den floromvundne retorik, som selvudnævnte talsmænd for Anonymous ofte benytter sig af.

Det er vigtigt at have for øje, at de fleste Anons ligesom alle mulige andre mennesker føler sig som en del af et fællesskab, som de ønsker at imponere. At opnå anerkendelse fra ligesindede er en vigtig motivation, som gennemsyrer mange af de onlineaktiviteter, der associeres med Anonymous og andre former for *black-hat hacking*. Det er imidlertid vigtigt at huske på, at Anonymous også indeholder aktivister og hacktivister, der forsøger at mobilisere andre onlinebrugere til at kæmpe for en politisk sag, hvilket gør onlinekollektivet vanskeligt entydigt at definere.

Lulz er et fænomen, der er kommet for at blive. Motiveret af den blotte morskab eller anerkendelse forsøger onlinebrugere at opnå en simpel effekt, nemlig ydmygelse og chikane af andre brugere. Det er således mindre vigtigt, hvem der er tale om, eller hvordan denne ydmygelse finder sted. Præcis hvem målet er, og hvilke midler der bruges, kan være svært at sige. Målet kan variere fra andre onlinebrugere på 4chan eller Facebook til virksomheder og regeringer, og metoderne kan være alt fra provokerende kommentarer over social engineering til vira og udnyttelse af forskellige sårbarheder.

[84] Coleman, 2013b: 13.

Når virksomheder og regeringer rammes, bliver der ofte tilskrevet et politisk budskab. Dette skyldes, at aktionerne drives frem af både aktivister og folk, der ønsker et godt grin. Grænsen mellem lulz og hacktivisme forbliver dog svær at opretholde i praksis, da det politiske budskab ofte medfører øget offentlig bevågenhed. Noget, som både hacktivister og prankstere ønsker.

Cyberforvirring i praksis I: Estland 2007

I det ovenstående er der forsøgt sondret mellem syv forskellige cybertrusler. Disse trusler blev adskilt på fire parametre, *strategiske formål, midler, operationelle mål* og *redskaber*, men som det fremgår af tabel 1, er der en lang række overlap især i de brugte cyberredskaber og i de operationelle mål. I tilfælde af at en stat, en virksomhed eller en person udsættes for et cyberangreb, kan det således være vanskeligt at kategorisere cyberangrebet, medmindre eksempelvis det strategiske formål eller de midler, hvormed dette formål forfølges på den ene eller anden måde er blevet kommunikeret. Cyberaktioners ofte anonyme (eller pseudonyme) karakter gør det ligeledes vanskeligt at verificere, når udtalelser fra selvudnævnte gerningsmænd offentliggøres.

En af de absolut mest refererede begivenheder, der ofte ses som skelsættende for cybertrusselslitteraturen, cyberangrebene i Estland i 2007, understreger meget godt, hvordan en fuldstændig klar sondring mellem disse syv grupper er svær at opretholde i praksis (og i litteraturen).[85] Har man imidlertid indblik i forskellene og ligheder cybertruslerne imellem, er det muligt at diskutere og forstå de forskellige cyberbegivenheder uden at bringe yderligere – unødvendig – hype til den allerede hypede cyberlitteratur.

I forlængelse af den estiske regerings beslutning om at fjerne et sovjetisk mindesmærke fra Anden Verdenskrig fra en central plads i Tallinn udbrød der en række demonstrationer i april 2007. Disse protester blev efterfulgt af tre ugers cyberangreb, der ved hjælp af DDoS-angreb formåede for en kortere periode at lukke for forskellige bankydelser samt forhindre adgangen til og ændre udseendet på en række statslige hjemmesider.[86] Cyberangrebene fik imidlertid ikke den estiske regering til at ændre deres beslutning. Den eneste faktiske betydning, angrebet fik, var – ud over at den ene russiske udvekslingsstuderende fik tildelt en bøde på godt 1.600 euro for at udgive falske nyheder på premierminister Andrus Ansips hjemmeside[87] – at Tallinn fik tildelt NATO Cooperative Cyber Defence Centre of Excellence, at cyberkrigslitteraturen eksploderede, at nationale cyberstrategier blev udarbejdet, og at cybersikkerhedsindustrien for alvor fik vind i sejlene.

[85] Fidler, 2012: 74.

[86] For flere uddybende analyser af begivenhederne i Estland se Rid, 2012: 6-7, 31-32; Geers, 2011: 84-86; Schreier, 2012: 109-110; Glenny, 2012: 223-244.

[87] Shackelford, 2009: 208.

Ud fra de ovennævnte sondringer synes det ikke vanskeligt at konkludere, at cyberaktionerne var en form for "hacktivisme", men da man ikke kunne finde frem til de individer, der stod bag, samtidig med at Rusland undlod at assistere det estiske politis efterforskning,[88] begyndte spekulationer om, hvem der stod bag og med hvilket formål, at florere. Var angrebet et "proof of concept" for den russiske regering, som havde til hensigt at teste sine offensive cyberkapabiliteter?[89] I så fald ville de begyndende diskussioner om cyberkrig og cybersabotage ikke være ubegrundede, og det til trods for at Estland ikke officielt påkaldte sig NATO's "én for alle, alle for én"-artikel 5. Eller var det, som Stephen Herzog har beskrevet det, et cyberterrorangreb, der forsøgte at skabe frygt og skræmme esterne og deres regering til at vende tilbage til Ruslands politiske og sociale indflydelsessfære?[90] Ud fra det internationale fokus på cyberangrebene i Estland og den frygt for yderligere og mere ødelæggende fremtidige angreb, der blev genereret, er en sådan karakteristik måske ikke helt ved siden af. Dog tyder det manglende klart udtrykte politiske budskab, fraværet af et voldeligt udtryk i angrebene og den manglende destabiliserende effekt på, at det ikke var en terrorgruppe, der stod bag.

Ruslands formodede tætte samarbejde med eller accept af kendte cyberkriminelle grupper som Russian Business Network (RBN), hvis servere efter sigende havde en finger med i spillet i cyberangrebene på Estland, mudrer billedet yderligere.[91] RBN er en hosting service, der ikke stiller nogen spørgsmål, hvilket vil sige, at den accepterer alt fra børneporno til spam. Og RBN har ligeledes et af verdens største botnets (for hire), som er blevet sporet til angrebene i Estland (og Georgien), samtidig med at disse har været brugt til kriminelle handlinger som DDoS-afpresning.[92] Cyberkriminalitet kan ikke adskilles fuldstændig fra begivenhederne i Estland, hvad enten det var hacktivister, der lejede botnets og sendte dem mod den estiske regerings hjemmesider, eller det var den russiske stat, der brugte kriminelle som et dække til at forfølge et politisk mål – nemlig mindre europæisering af Estland.

Det eneste, der med nogenlunde sikkerhed kan afvises, er, at cyberangrebene på Estland var en form for cyberspionage, da cyberspionage netop har til formål at indhente elektroniske data, *uden* at det bliver opdaget. Kun såfremt cyberangrebene var en

[88] Shackelford, 2009: 208.
[89] Krepinevich, 2012.
[90] Herzog, 2011.
[91] Klimburg, 2011: 50; Clarke & Knake, 2010: 15; Mshvidobadze, 2011; Carr, 2010: 118-119.
[92] Amit, 2010.

afledningsmanøvre for indhentningen af fortrolige data fra Estland, kan angrebene siges at være tilknyttet cyberspionageaktiviteter. Dette er dog en af de få konspirationsteorier, der endnu ikke har været i spil.

Lulz er heller ikke blevet diskuteret i forbindelse med angrebene, men det kan langtfra afvises, at en del af aktiviteterne var motiveret af "the lulz" og drevet af et ønske om at opnå anerkendelse blandt ligesindede online. Ændringer af hjemmesider med henblik på at få politikere eller andre offentlige personligheder til at fremstå tåbelige er en meget brugt taktik, som også fandt sted i Estland. Samtidig kan der i både Rusland, Estland og andre østeuropæiske lande findes onlinebrugere, der associerer sig med Anonymous og dermed også med den mere useriøse del af fænomenet, hvis aktiviteter kan tilskrives behovet for anerkendelse gennem morskab og ydmygelser. Netop med hensyn til behovet for anerkendelse blandt ligesindede kan der drages en parallel til de DDoS-angreb, som blev iværksat under Anonymousbanneret på PayPal og MasterCard. Parmy Olson har fint beskrevet, hvorledes de få Anons med store botnets modtog respekt – næsten lige meget hvad disse blev brugt til.[93]

Insisterer man imidlertid på at placere casen Estland i en af de ovennævnte kategorier, må man holde fast i, at cyberangrebene – omend de førte en del irritation med sig – ikke resulterede i, end ikke var tæt på at resultere i og ikke medførte nogen trussel om fysisk skade eller vold. Cyberangrebene har kun øget cybersikkerheden, således at et lignende angreb på større og mere kendte hjemmesider som Amazon og Google ifølge cybersikkerhedseksperterne Gary McGraw og Nathaniel Fick ville fejle på det skammeligste – af den simple grund, at det i omfang langtfra ville være potent nok.[94] Der var ingen enkeltperson, der tjente penge eller var motiveret af at tjene penge på netop de cyberangreb, der ramte Estland (ud over de it-sikkerhedsfirmaer og forskere, der blev ansat ved NATO Cooperative Cyber Defence Centre of Excellence bagefter), og ingen fortrolige data blev lækket eller frigivet. På trods af at det i praksis kan være vanskeligt klart at kategorisere et cyberangreb, mens et sådant finder sted, så gør en klar sondring mellem de forskellige typer af cybertrusler, at begivenheder i Estland mest af alt – på baggrund af kontekst og effekten – bør karakteriseres som en protest eller demonstration, eller i cyberjargon: hacktivisme.

[93] Olson, 2013: 119-121.
[94] McGraw & Fick, 2013.

Cyberforvirring i praksis II: Stuxnet 2010 & Shamoon 2012

Begivenhederne i Estland i 2007 fik som sagt stor betydning for synet på cyberspace som et forum for virkelige og seriøse trusler. Måske mere skelsættende var det, da offentligheden i 2010 fik nys om, at en computerorm ved navn Stuxnet havde forårsaget fysisk destruktion af ca. 1000 centrifuger på det iranske atomanlæg i Natanz. Stuxnet, viste det sig, efter at it-ekspert Ralph Langner havde gennemanalyseret ormen, var en af de mest komplekse malware, som verden endnu havde set. Den formåede at ramme et specifikt it-system fysisk adskilt fra internettet, hvilket betød, at ormen sandsynligvis blev overført via usb-nøgle. Den præprogrammerede orm, som dermed ikke kunne kontrolleres af afsenderen, efter at den var frigivet, foldede sig herefter ud inde på det lukkede netværk. Stuxnet udnyttede fire på daværende tidspunkt ukendte fejl i Windowsoperativsystemet, benyttede sig af to stjålne verificeringscertifikater for at omgå antivirussoftware og udnyttede, at it-systemet ikke havde ændret default password. Samtidig var Stuxnet også målrettet mod det Siemens Industrial Control System, som blev brugt i Natanz, var præprogrammeret til over flere måneder at ændre hastigheder på atomcentrifugerne og indeholdt kode, der satte it-alarmklokkerne ud af kraft. For at udvikle og teste ormen krævedes der indgående kendskab til fremstillingen af atomenergi samt tid, penge og it-viden.[95]

Kompleksiteten sammenholdt med det specifikke mål – atomanlægget i Natanz – har gjort, at diskussionerne om, hvad Stuxnet er, hovedsagelig har centreret sig om forholdet mellem cyberkrig og cybersabotage. Det giver ikke specielt meget mening at diskutere kriminalitet, hacktivisme eller *lulz* i relation til Stuxnet, og Iran selv kategoriserede angrebet som et eksempel på et statssponsoreret cyberterrorangreb.[96] Og selvom der helt bestemt har gået væsentlige cyberspionageaktiviteter forud for cyberangrebet, hvilket de relaterede Duqu- og Flameorme vidner om,[97] indeholdt Stuxnet en såkaldt payload, dvs. computerkode, der har til hensigt at påføre skade, hvorfor det heller ikke giver nogen mening at karakterisere aktionen som spionage.

På trods af den manglende klarhed over afsenderen tog spekulationerne om cyberkrig for alvor fart og har på mange måder ændret måden, hvorpå vi forestiller os

[95] Langner, 2011; Langner, 2013; Nachenberg, 2012; McGraw, 2013.
[96] Vahidi, 2011.
[97] Bencsáth et al., 2011.

fremtidens krige.[98] Michael Gross fra *Vanity Fair* kaldte Stuxnet "the Hiroshima of cyber-war",[99] Farwell & Rohozinski så med Stuxnet starten på en cyberkrig,[100] mens andre pludselig for alvor diskuterede, hvad den nye realitet var efter Stuxnet, for så vidt angår, både hvordan vi skal forstå krig, og hvordan vi skal håndtere cyberkrigsførelse under international lov. Holder man imidlertid fast i forsøget på at definere, hvad cyberangrebet på Iran bedst kan karakteriseres som, er det ikke cyberkrig, der ligger ligefor.

Usikkerheden omkring afsenderen, den meget specifikke destruktion af centrifuger og det manglende iranske forsøg på gengældelse burde, på baggrund af ovenstående diskussion af krigsbegrebet, få de fleste til at afvise angrebet som en krig. Derimod passer Stuxnet særdeles godt som en sabotageaktion,[101] da afsenderen på den ene side nøjedes med at ødelægge hardware i stedet for at påføre fysisk vold mod mennesker og på den anden side forblev anonym indtil 2012, hvor David E. Sanger i bogen *Confront and Conceal* beviste, hvad de fleste havde gættet om USA's og Israels involvering.[102] Netop Sangers bog syntes også at støtte tanken om cybersabotage, da det blev grundigt beskrevet, hvorledes Stuxnet var en del af en flerårig amerikansk operation, *Olympic Games*, der havde til hensigt at forhindre Iran i at få atombomben, *uden* at man behøvede at gå i krig, og som samtidig skulle være så usynlig, at de iranske videnskabsmænd end ikke vidste, at de var under angreb.[103] Det er imidlertid stadigvæk omgærdet med en del spekulation, hvad det skyldes, at Stuxnetormen pludselig begyndte uhensigtsmæssigt at sprede sig. Sanger tilskriver det dårlig testning[104], mens Langner spekulerer i, at det kunne skyldes et bevidst amerikansk ønske om at vise verden, hvad deres cyberkapabiliteter indbefattede – altså en traditionel afskrækkelsesstrategi.[105]

Forstår man Stuxnet som en cybersabotageaktion, vidner det ydermere om, at sabotage, set med militære briller, ikke blot bør associeres med den svage part. USA og Israels anonyme cyberangreb på Iran kan derimod forstås som et forsøg på at opnå politiske, økonomiske og militære gevinster uden at skulle stå til ansvar for eller be-

[98] Denning, 2012.
[99] Gross, 2011.
[100] Farwell & Rohozinski, 2011.
[101] Rid, 2012: 16-20.
[102] Sanger, 2012.
[103] Sanger, 2012: 202-205.
[104] Sanger, 2012: 204.
[105] Langner, 2013.

høve at diskutere den del af international lov, der forbyder stater at intervenere i andre stater. Samtidig undgik USA og Israel de civile tab, der uundgåeligt ville finde sted, hvis de havde valgt at bombe de iranske atomfaciliteter.[106] Cybersabotage er dermed det cyberbegreb, der kommer tættest på at karakterisere Natanzangrebet.

Cyberkrigsdebatten, der omgav Stuxnet, fik ny næring i august 2012, da den store saudiske olieproducent Aramco blev ramt af en virus, Shamoon, der til billedet af brændende amerikanske flag slettede data på omkring 30.000 af firmaets computere og tvang Aramco offline i to uger.[107] En på daværende tidspunkt ukendt gruppe, *The Cutting Sword of Justice*, tog æren for virussen, med beskeden om, at de bekæmpede de regeringer, der stod bag uretfærdigheden og grusomheden i Mellemøsten.[108] Næsten samtidig blev flere store amerikanske banker, herunder Capital One og BB&T Corp., hacket af en anden gruppe, *The Qassam Cyber Fighters*, i et forsøg på at gengælde *Innocence of Muslims*-videoen.[109] Da Iran blev sat i forbindelse med begge grupper, begyndte spekulationen om cyberkrig mellem USA og Iran at florere.[110] Men befandt vi os nu i en cyberkrig?

Hverken Shamoon eller angrebene på de amerikanske banker formåede eller havde til hensigt at påføre fysisk skade. Ingen af angrebene resulterede i andet end irritation og økonomiske tab. Og der var ingen klare beviser for, at angrebene var gengældelse for Stuxnet. Tager man udgangspunkt i de sondringer, som er blevet introduceret tidligere i rapporten, befinder vi os således ikke i en cyberkrig. Godt nok eksisterer der klare politiske uenigheder mellem Iran og USA, men ingen af landene virker interesseret i at starte en krig. Semianonyme cyberangreb gennem diverse selvudnævnte cyberhære kan bestemt bruges til at sabotere og irritere politiske modstandere og giver stater en hensigtsmæssig mulighed for at benægte kendskab til cyberaktionerne. Men skal de påståede iransksponsorerede cyberangreb karakteriseres som andet end onlineprotest (hacktivisme) eller cybersabotage, bør der være klare økonomiske motiver (cyberkriminalitet), klare militær-instrumentelle motiver (cyberkrig) eller et klart ønske om at indgyde frygt i befolkningen (cyberterrorisme).

[106] Barzashka har dog sat spørgsmålstegn ved effekten af Stuxnet, idet hun påpeger, at mængden af fungerende centrifuger faktisk steg i perioden, hvor Stuxnet hærgede. Se Barzashka, 2013.
[107] Pearlroth, 2012.
[108] Bronk & Tikk-Ringas, 2013: 88.
[109] RT, 2012.
[110] Joshi, 2013.

Cyberforvirring i praksis III: Coca-Cola 2009 & Google 2010

Eksempler som Shamoonvirussen, The Qassam Cyber Fighters og for den sags skyld også cyberangrebene i Estland slører forholdet mellem stater og ikkestatslige aktører. Vanskelighederne forbundet med at håndtere disse muligvis statsstøttede aktivister, der efter alt at dømme sidder sikkert beskyttede bag firewalls langt fra de stater, hvor deres angreb rammer, stiller skarpt på, at truslerne fra cyberspace indeholder en række konceptuelle, juridiske og militære udfordringer. Desværre stopper udfordringerne, for så vidt angår den ugennemsigtige relation mellem statslige og ikkestatslige aktører, ikke ved politisk aktivisme, men indeholder også en økonomisk dimension. Denne dimension diskuteres i en amerikansk og europæisk kontekst ofte i relation til beskyldningerne om statsstøttede kinesiske spionageoperationer, hvor man for at få adgang til intellektuelle rettigheder og centrale økonomiske informationer bryder ind i virksomheder.

En række eksempler hives ofte frem for at underbygge, at cyberspionage udgør en trussel. Eksempelvis formåede hackere at opnå uautoriseret adgang til Coca-Colas netværk i 2009, netop som læskedrikgiganten lå i forhandlinger om et 2,4 milliarder dollar stort opkøb af den kinesiske pendant, Huiyuan Juice Group.[111] Kort tid efter brød forhandlingerne, der ellers blot blev set som en formalitet, sammen.[112] Flere rapporter og artikler pegede – trods officielle kinesiske protester[113] – i retning af den kinesiske efterretningstjeneste, eller mere præcist i retning af en statsfinansieret hackergruppe, *Comment Crew* / *APT1*, der efter sigende fra en militærejet bygning i Shanghai havde opnået viden om Coca-Colas økonomiske situation og forhandlingsstrategi.[114] Offentliggørelse af disse rapporter, der gentagne gange pegede på den kinesiske stat som primus motor for cyberspionage, har resulteret i, at amerikanske politikere karakteriserer cyberspionage som den største overførsel af rigdom i historien[115] og som den største nationale sikkerhedstrussel.[116]

[111] Elgin et al., 2012.
[112] Wong, 2008.
[113] BBC, 2013.
[114] Sanger et al., 2013; Feaklin, 2013; Mandiant, 2013.
[115] Keith Alexander i Rogin, 2012.
[116] Rogers, 2013.

Mens Coca-Cola undlod at offentliggøre it-sikkerhedsbruddene, sandsynligvis i et forsøg på ikke at miste tillid fra aktionærer, ansatte og diverse kontrolinstanser, valgte Google en mere åben strategi, da de i starten af 2010 opdagede, at hackere havde opnået adgang til fortrolige dokumenter.[117] Disse hacks skete i en periode med uenigheder om, hvorvidt Google overhovedet skulle operere i Kina på grund af kinesisk censurering, og hvor Google i en periode havde omdirigeret alle kinesiske Google-søgninger gennem Hongkong.[118] Samtidig viste et teknisk Google-NSA-samarbejde, at hackernes ip-adresser kunne spores til to kinesiske skoler, Shanghai Jiaotong-universitetet og Lanxiang-handelsskolen.[119] Dette beviste i udgangspunktet ikke noget som helst, da de forskellige hacks kunne have været udført både af ivrige studerende, der ønskede at teste deres færdigheder, og af en hvilken som helst anden udefrakommende person, der havde kapret nogle af skolernes ip-adresser. Angrebet blev imidlertid set i en større kontekst af cyberspionage mod menneskerettighedsaktivister i Kina og mod 34 andre amerikanske teknologivirksomheder, herunder Adobe, Symantec og Yahoo!, og fik derfor tilnavnet Operation Aurora.[120]

Coca-Cola- og Googleeksemplet peger på flere udfordringer. For det første gør det faktum, at anonymitet er relativt let opnåeligt i cyberspace, og at cyberspionage sjældent efterlader nogen spor, at det kan være vanskeligt at afgøre, hvorvidt et hack er iværksat for at opnå kendskab til og udnytte virksomheders hemmeligheder og intellektuelle rettigheder, eller om der blot er tale om relativt harmløse individers forsøg på at opnå anerkendelse fra ligesindede. Dernæst gør karakteren af spionage, at det er vanskeligt at vurdere omkostningerne ved tab af data.

For det andet vidner synet på cyberspionage, især fra Kina som den største sikkerhedstrussel, om en generel ændring i de nationale trusselsvurderinger – fra at være domineret af ikkestatslige aktørers terrorplaner mod Vesten til nu igen at fokusere på statsaktører. Netop det stigende fokus på kinesisk cyberspionage – modsat fransk eller israelsk – passer godt ind i en generel amerikansk mistro til Kina både militær- og sikkerhedspolitisk i relation til øget kinesisk oprustning og geostrategisk indflydelse i regionen, ideologisk i forhold til det divergerende kinesiske syn på menneskerettigheder og demokrati og økonomisk i forhold til en konkurrent, der truer de amerikanske job og derfor underminerer det amerikanske hegemoni. Det stigende fokus

[117] Drummond, 2010.
[118] O'Hara, 2010: 260-264; Helft & Barboza, 2010.
[119] Markoff & Barboza, 2010.
[120] Kurtz, 2010.

på og sikkerhedsliggørelsen af kinesisk cyberspionage og intellektuelle rettigheder er således med til at konsolidere nye statslige fjendebilleder i international politik.[121]

Dette har ført til den tredje udfordring. Indtil nu har USA forsøgt at håndtere problemet med cyberspionage gennem tre politikområder: (1) håndhævelse af intellektuelle rettigheder, (2) frivillige etiske spilleregler for virksomheder, (3) opbygning af internationale normer.[122] Fælles for de tre indsatsområder er, at ingen af dem stiller krav til eller regulerer private virksomheder og deres it-sikkerhedsstandarder, men nøjes med at tilskynde til bedre koordination mellem det offentlige og det private, mere samarbejde med allierede og eksisterende institutioner og mere åbenhed både politisk og økonomisk.

Internt kan dette føre til, hvad Dowdy kalder et sikkerheds-økonomisk kompleks, hvor regeringen har vedkendt sig et ansvar med henblik på blot at informere og oplyse private virksomheder om cyberspionagetruslens alvor. Med en reel viden om truslens seriøsitet vil virksomheder efterspørge og investere i cybersikkerhedsprodukter, hvilket firmaer med ekspertise inden for it-sikkerhed vil kunne tilbyde. Disse firmaer vil således kunne optimere deres produkter og forbedre deres evaluering af truslens karakter og dernæst slutte cirklen ved at videreformidle dette til regeringen.[123] Fortsætter man denne markedstænkning, møder man udfordringen. Cybersikkerhedsindustrien har ingen interesse i at udrydde cybertruslen, men har derimod interesse i at overdrive den, da dette vil betyde flere indtægter.[124] Og i en situation, hvor stater og deres samarbejde med private virksomheder er genopstået som den primære nationale sikkerhedstrussel, fører overdrivelser ikke blot til en militarisering af cyberspace og mistillid stater imellem, men mindsker også villigheden til at investere i produkter fra, udvikle produkter i samarbejde med eller udlicitere arbejdsopgaver til andre lande. Alt sammen på grund af mistillid og risikoen for præinstallerede bagdøre[125] eller "spioner i kaffemaskiner".[126]

Dette vil promovere mere lukkethed og mindske samhandel og innovation, hvilket ikke blot står lodret i modsætning til det åbne og ideologiske amerikanske frihan-

[121] Read, 2014.
[122] Read, 2014; Obama, 2010; Obama, 2011a; Obama, 2011b; Obama, 2013.
[123] Dowdy, 2012.
[124] Deibert, 2013: 195-216
[125] Clarke & Knake, 2010: 233.
[126] O'Hara & Shadbolt, 2008.

delsregime, som har eksisteret siden Anden Verdenskrig,[127] men også underminerer det amerikanske forsøg på at forsvare den nuværende frivillige, ekspertdrevne, non-profit- og bottom-up-baserede styring af internettet og dets protokoller og adresser mod mere multilateral eller balkaniseret styring.[128]

[127] Layne, 2006; Kiggins, 2013.
[128] Mueller, 2010; Kiggins, 2014.

Konklusion

Denne rapport har forsøgt at bidrage med en introduktion til nogle af de mest diskuterede trusselsbegreber inden for cyberlitteraturen. På nuværende tidspunkt, og som det blev illustreret med begivenhederne i Estland i 2007, hersker der en del forvirring omkring cybertruslerne, og der opstilles ofte en del faretruende scenarier om et cyber-9/11 og cyber-Pearl Harbor, som for enhver pris skal forhindres. I et forsøg på at undgå en unødvendig allokering af ressourcer eller en underminering af de demokratiske rettigheder og den sociale tillid, som Danmark er kendt for, peger rapporten på, at truslen fra cyberterrorisme, onlineaktivisme, cyberspionage, cyberkrig, cybersabotage og cyberkriminalitet er motiveret af de samme strategiske mål, er rettet mod de samme operationelle mål og gør brug af samme midler som disse truslers ikkecyberrelaterede pendant.

Det betyder, at man for at forstå eksempelvis cyberterrorisme eller mangel på samme bør starte med at forsøge at forstå den konventionelle terrorismes ønske om gennem angreb på civile og ikkecivile mål at skabe frygt og destabilisering for derved at opnå sociale eller politiske forandringer. Med andre ord bør en diskussion af cybertruslen starte *uden for* cyberspace med at besvare en række velkendte spørgsmål: Hvem ønsker at udøve terror og aktivisme i Danmark og hvorfor? Hvem begår simple berigelseskriminelle handlinger og hvorfor? Hvem ønsker at gå i krig mod Danmark og hvorfor? Hvem ønsker at spionere og hvorfor? Cybertrusler skal således i udgangspunktet ikke ses som en ny og unik kategori, men bør forstås som en forlængelse og videreudvikling af allerede kendte trusler. Læren er derfor, at cyberbegivenheder, når de faktisk finder sted, kan hjælpe os til at forstå den politiske kontekst, vi befinder os i. Sådanne analyser bør ikke obstrueres af yderligere hype om katastrofale fremtidige scenarier.

Det mest afgørende, der retfærdiggør brugen af et cyberpræfiks, relaterer sig til de it-redskaber, der benyttes. Netop cyberpræfikset blev i starten af rapporten diskuteret med henblik på at afgrænse brugen af dette præfiks til kun at omfatte de angreb og operationer, der relaterer sig til computer-til-computer-aktiviteter. Det vil sige, de aktiviteter, der gør brug af eksempelvis computerkode til uautoriseret at tilgå, forstyrre eller ødelægge data i andre computere. It-redskaberne er ydermere kendetegnede ved deres store hastighed, store rækkevidde, lave omkostninger, lette tilgængelighed og høje grad af anonymitet. Disse karakteristika har resulteret i en række nye udfordringer, som diskuteredes i rapportens tre sidste afsnit specielt med fokus

på forholdet mellem stater og ikkestatslige aktører. Både politisk og økonomisk ser det ud til, at stater har udnyttet den anonymitet og den globale rækkevidde, som cyberspace tilbyder, til at udføre politisk aktivisme og økonomisk spionage enten ved hjælp af eller til fordel for ikkestatslige aktører.

Det tyder på, at cyberspace er på vej mod at blive overtaget af statslige aktører, der i stigende grad ser hinanden som økonomiske og politiske modstandere. Dette kan ændre karakteren af det dynamiske internet, vi kender i dag. Fortsætter cyberspace med at blive set som et domæne, der frem for alt genererer trusler og farer, fordrer det kun mere oprustning, mere overvågning, mere kontrol og mere mistillid fra borger til stat og staterne imellem.

Forsøger man som denne rapport at separere cybertruslerne og i stedet se dem som velkendte udfordringer tilført andre og nye midler, kan man undgå yderligere militarisering af og konfrontation i cyberspace. Ser man eksempelvis på simpel cyberkriminalitet som intet andet end almindelig kriminalitet tilført en ny it-dimension, og undgår man at gøre den til et militært eller ideologisk spørgsmål mellem Vesten på den ene side og Kina, Rusland og Iran på den anden, er der intet til hinder for, at lande kan samarbejde om international kriminalitetsbekæmpelse. Afstår USA og Europa fra at karakterisere proiransk eller prorussisk aktivisme eller kinesisk spionage over internettet som cyberkrig, vil det pludselig give mere mening at sikre sig, at virksomheder og almindelige borgere kender til basale it-sikkerhedsforanstaltninger frem for at investere i nyt offensivt cyberudstyr i en tro på, at cybervåben er de nye masseødelæggelsesvåben, der skal afskrække den genopfundne "statsfjende". Husker man, at bag enhver cybertrussel fra terrorisme, ikkestatslig sabotage eller lækager sidder virkelige mennesker, der sandsynligvis har adgang til og viden om vitale it-systemer, kan man ved at fokusere indsatsen (1) mod "insideren" og (2) mod overholdelsen af de mest basale "IT best practices" forbedre både beskyttelsen af den kritiske digitale infrastruktur og den generelle it-sikkerhed markant.

Vi har endnu ikke oplevet cyberangreb på kritisk infrastruktur med store kaskadeeffekter til følge. Og alt imens flere stater inklusive Danmark har iværksat omfattende store cyberøvelser med deltage fra både det private og offentlige og afsat penge til yderligere forskning i kritisk informations- og kommunikationsteknisk infrastrukturbeskyttelse, forbliver det uhyre vanskeligt at forudsige, hvorvidt sådanne seriøse cyberangreb overhovedet er sandsynlige, og hvilken effekt disse vil få. I forsøget på at undgå endnu mere spekulation bør fremtidig forskning på om-

rådet i stedet rette sig mod en dybere forståelse af ændringerne i forholdet mellem individ, civilsamfund, stat og sikkerhed i en tidsalder, hvor mere og mere interaktion foregår online.

Ordliste

ANONS – Personer, der identificerer sig som en del af Anonymous.

APT (Advanced Persistent Threat) – En gruppe, eksempelvis en udenlandsk regering, der har både kapacitet til og et ønske om målrettet og vedvarende at ramme eller spionere mod et specifikt mål.

BAGDØR – Mulighed for at tilgå et system uden om den normale autentificering.

BIG DATA – Indsamling, opbevaring og analyse af enorme mængder af computerdata.

BOTNET – Et netværk af computere, der fjernstyres af en uautoriseret bruger, oftest uden computerejernes vidende. Et botnet kontrolleres ofte af en eller flere computere, som muliggør, at eksempelvis hjemmesider kan gøres utilgængelige på grund af for meget trafik. En computer i et botnet kaldes ofte en bot eller en zombie.

BUG – En fejl eller defekt i et it-program eller -system, der producerer forkerte eller utilsigtede resultater.

BLACK HAT – En hacker, der tilgår it-systemer uden om de autoriserede verificeringsmekanismer med henblik på, ofte for egen vindings skyld, ulovligt at påføre skade på disse systemer.

CERT – Computer Emergency Response Team eller CSIRT (Computer Security Incident Response Team). En ofte statsligt forankret enhed, der har til formål at håndtere cyberangreb, når de sker, samt forebygge angreb og forbedre modstandsdygtigheden.

COMPUTERKODE – Enhver form for computersprog, som gør det basale computersprog af nuller og ettaller mere forståeligt.

CRACKE (PASSWORDS) – En proces, hvormed man forsøger at få adgang til passwords, der er gemt i et computersystem. En måde at gøre dette på er eksempelvis at gætte.

DDoS (Distributed Denial of Service) – En type af cyberangreb, hvor en stor mængde computere på samme tid forsøger at tilgå en hjemmeside, server eller router med henblik på at gøre denne utilgængelig på grund af for meget trafik. Botnets bruges ofte til at udføre disse angreb.

DEFACEMENT – En ændring af en hjemmesides visuelle fremstilling.

DOXING – At lække fortrolige persondata såsom cpr-numre eller lignende.

FIREWALL – Software, der blokerer uautoriseret adgang til en computer eller netværk.

GREY HAT – En hacker, der tilgår it-systemer uden om de autoriserede verificeringsmekanismer med det ene formål at underrette systemets ejere om fejl og sårbarheder.

IP-ADRESSE – Internetprotokollen, der fastsætter et id-nummer til en specifik computer i et netværk.

IP SPOOFING – Et forsøg på at ændre ip-adresse med det formål at hemmeligholde afsenderens identitet eller at foregive at være en anden.

ISP (Internet Service Provider) – Internetudbyder. Teknisk set en computer, der tilknytter individuelle computere til internettet.

LOGIC BOMB – En fil, som er programmeret til at udløse en ondsindet handling under givne omstændigheder.

LULZ – En videreudvikling og flertalsform af forkortelsen "lol" ("laughing out loud"). Betyder enten morskab/sjov, eller at man gør noget for den blotte morskabs skyld.

LUKKET SYSTEM – Et it-system, der ikke har direkte adgang til internettet.

MALWARE – Ondsindet software, der får computere eller netværk til at gøre noget, som ejeren eller brugeren ikke ønsker. Virus, orme og logic bombs er eksempler på malware.

MAN-IN-THE-MIDDLE-ANGREB – Den angribende part etablerer en uafhængig forbindelse mellem to ofre og får dem til at tro, at de kommunikerer direkte med hinanden.

NIPRNET – Det amerikanske forsvarsministeriums ikkeklassificerede netværk. SIPRNet er det klassificerede.

PAYLOAD – Computerkode i et ondsindet stykke software, som er designet til at gøre mere end bare sprede sig til andre computere. Dette kunne være at slette filer, installere bagdøre eller ændre i måden, hvorpå industrielle computere fungerer.

PHISHING – Et forsøg på at opnå viden om brugernavne, passwords eller finansielle data ved at udgive sig for at være en troværdig kilde (hjemmeside, vedhæftning eller e-mailadresse). Dette kaldes spear phishing, hvis forsøget er rettet mod et bestemt mål.

PRISM – USA's overvågnings- og dataminingprogram styret af NSA.

ORM – Et ondsindet stykke software, der gennem en intetanende brugers netværk sender kopier af sig selv til andre brugere.

REMOTE-ACCESS TOOL (RAT) – Et stykke software, der gør det muligt at fjernstyre et system.

ROOTKIT – Et stykke software, der muliggør fortsat adgang til et it-system uden administratoren af systemets vidende.

SERVER – En computer, som ofte tilgås af andre computere med henblik på at interagere med informationen, der er gemt på denne (hjemmesider eller e-mails). Servere opererer ofte uden konstant menneskelig monitorering. Routere, der dirigerer internettrafikken, er en type af servere.

SNIFFER – Et stykke software, der bliver brugt til at observere og optage trafikken på et netværk.

SOCIAL ENGINEERING – Den psykologiske manipulation af personer med henblik på at få disse til at udføre opgaver eller afsløre hemmelige informationer.

STEGANOGRAFI – En teknik til at gemme en fil i en anden fil. Eksempelvis en .pdf- eller tekstfil i en billedfil.

STUXNET – En sofistikeret computerorm, der var designet til at kompromittere Siemens' industrielle kontrolsystemer på et atomanlæg i Iran med henblik på at ødelægge de centrifuger, der berigede uran.

SQL INJECTION – Et angreb, der indsætter kode i databaser, der bruger det mest udbredte databaseprogrammeringssprog Structured Query Language (SQL). Dette bruges ofte til at opnå uautoriseret adgang til en administratorfunktion på en hjemmeside.

TERABYTE – 1.000.000.000.000 bytes. Forkortes TB.

TROJAN HORSE – Et stykke software, der udgiver sig for at udføre en ønskelig funktion, men som i virkeligheden skader brugeren, når den installeres.

TROLLING – Internetslang for et forsøg på at gøre andre folk så sure og ophidsede som muligt.

VIRUS – Et ondsindet stykke software (malware), der spreder sig selv ved at koble sig på et allerede eksisterende software.

WHITE HAT – En hacker, der bliver betalt af en virksomhed eller regeringer for at tilgå disses it-systemer uden om de autoriserede verificeringsmekanismer med henblik på at teste og forbedre sikkerheden. Også kendt som etisk hacker.

ZERO-DAY EXPLOIT – En it-sikkerhedsfejl eller -sårbarhed, der, før den er blevet udnyttet og brugt, ikke er kendt af målet for angrebet eller producenten af det software, hvori sårbarheden eksisterer.

Litteraturliste

Amit, Iftach (2010): "Cyber) [Crime|War] – Connecting the dots", præsentation, DefCon 18. (http://www.youtube.com/watch?v=qzyz1MtkaQ4)) [8. jan. 2014]

Anderson, Ross, Chris Barton, Rainer Boehme, Richard Clayton, Michael J.G. van Eeten, Michael Levi, Tyler Moore & Steven Savage (2012): *Measuring the Cost of Cybercrime*, 11th Workshop on the Economics of Information Security, 26. juni 2012, Berlin. (http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf)) [8. jan. 2014]

Arquilla, John & David Ronfeldt (1993): "Cyberwar is Coming!", *Comparative Strategy,* 12:2, s. 141-165.

Arquilla, John & David Ronfeldt (2001): "The Advent of Netwar (revisited)", i John Arquilla & David Ronfeldt (red.): *Networks and Netwars: The future of Terror, Crime and Militancy,* Santa Monica: RAND Coorporation.

Arquilla, John (2012): "Cyberwar is already upon us", *Foreign Policy*, marts/april. (http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us)) [8. jan. 2014]

Barkham, Jason (2001): "Information Warfare and International Law on the Use of Force", *International law and Politics* 34, s. 57-113.

Barzashka, Ivanka (2013): "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme", *The RUSI Journal*, 158:2, s. 48-56.

Bauwens, Michel (1994): "What is Cyberspace?", *Internet Liberation*, april, s. 42-48 .

BBC (2013): "China condemns hacking report by US firm Mandiant", BBC Asia, 20. feb. 2013. (http://www.bbc.co.uk/news/world-us-canada-21515259)) [8. jan. 2014]

Bencsáth, Boldizsár, Gábor Pék, Levente Buttyán & Márk Féleguházi (2011): "Duqu: A Stuxnet-like malware found in the wild", teknisk rapport, Laboratory of Cryptography and System Security (CrySyS). (http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf)) [8. jan. 2014]

Beredskabsstyrelsen (2013): *Nationalt Risikobillede (NRB)*, 9. april 2013 (http://newspublicator.dk/e10/parker/pm/b2884e90e2b652c1/ot143954/download/53a44e_nationalt_risikobillede_nrb_.pdf) [8. jan. 2014]

Betz, David J. & Tim Stevens (2011): *Cyberspace and the State – towards a strategy for cyber-power,* Oxon: Routledge.

Blakemore, Brian (2012): "Cyberspace, Cyber Crime and Cyber Terrorism", i Imran Awan & Brian Blakemore (red.): *Policing Cyber Hate, Cyber Threats and Cyber Terrorism*, Farnham: Ashgate, s. 5-20.

Broberg, Mads B. & Carsten Ellegaard (2013): "Danmark ruster sig til at angribe i cyberspace", *Jyllands-Posten*, 6. juni 2013. (http://*Jyllands-Posten*.dk/indland/krimi/ECE5701029/danmark-ruster-sig-til-at-angribe-i-cyberspace/) [14. april 2014]

Brock Jr., Jack L. (2000): "Critical Infrastructure Protection: 'ILOVEYOU' Computer Virus Highlights Need for Improved Alert and Coordination Capabilities", erklæring til The Subcommittee on Financial Institutions, Committee on Banking, Housing and Urban Affairs, Senatet, 19. maj 2000. (http://www.gao.gov/archive/2000/ai00181t.pdf) [8. jan. 2014]

Bronk, Christopher & Eneken Tikk-Ringas (2013): "The Cyber Attack on Saudi Aramco", *Global Politics and Strategy*, 55:2, s. 81-96.

Buchan, Russell (2012): "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", *Journal of Conflict & Security Law*, 17:2, s. 212-227.

Carr, Jeffrey (2010): *Inside Cyber Warfare: Mapping the Cyber Underwold*, Sebastopol, Californien: O'Reilly Media.

Cavelty, Myriam Dunn (2008): *Cyber-Security and Threat Politics – US efforts to secure the information age*, Oxon: Routledge.

Clarke, Richard A. & Robert K. Knake (2010): *Cyber War – The Next Threat to National Security and What to do About it*, New York: HarperCollins.

Clemmons, Byard Q. & Gary D. Brown (1999): "Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction", *Military Review*, 79:5.

Coleman, Gabriella (2013a): *Coding Freedom – The Ethics and Aesthetics of hacking*, Princeton: Princeton University Press.

Coleman, Gabriella (2013b): "Anonymous in Context: The Politics and Power behind the Mask", *Internet Governance Papers* 3, september.

Conway, Maura (2011): "Against Cyberterrorism: Why cyber-based terrorist attacks are unlikely to occur, *Viewpoints*, 54:2.

Cornish, Paul, David Livingstone, Dave Clemente & Claire Yorke (2010): "On Cyber Warfare", *Chatham House Report*, november. (http://www.chathamhouse.org/publications/papers/view/109508) [8. jan. 2014]

Europarådet (2004): *Convention on Cybercrime*. (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm) [8. jan. 2014]

Crawford, Julie & Jeppe T. Jacobsen (2014): "Mandagsanalyse: Skal vi forsvare eller angribe?", *Politiken*, 6. jan. 2014. (http://www.diis.dk/files/_Staff/jetj/Skal%20vi%20forsvare%20eller%20angribe.pdf) [21. april 2014]

Deibert, Ronald & Rafal Rohozinsiki (2010): "Control and Subversion in Russian Cyberspace", i Ronald Deibert, John Palfrey, Rafal Rohozinski & Jonathan Zittrain (red.): *Access Controlled – The Shaping of Power, Rights, and Rules in Cyberspace* Cambridge, Massachusetts: The MIT Press.

Deibert, Ronald (2013): *Black Code – Surveillance, Privacy and the Dark Side of the Internet*, Toronto: McClelland & Steward.

Denning, Dorothy E. (2000): "Cyberterrorism: The Logic Bomb versus the Truck Bomb", *Global Dialogue*, 2:4.

Denning, Dorothy E. (2001): "Activism, Hacktivism, and Counterterrorism: The Internet as a tool for influencing foreign policy", i John Arquilla & David Ronfeldt (red.): *Networks and Netwars: The future of Terror, Crime and Militancy,* Santa Monica: RAND Coorporation.

Denning, Dorothy E. (2009): "Barrier of Entry – Are They Lower for Cyber Warfare?", *IO Journal*, april, s. 6-10.

Denning, Dorothy, E. (2012): "Stuxnet: What has changed?", *Future Internet* 4, s. 672-687.

Detica & The Office of Cyber-Security and Information Assurance in the Cabinet Office (2011): *The Cost of Cyber Crime*, Detica-rapport. (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf) [8. jan. 2014]

Doherty, Stephen (2013): *Hidden Lynx – Professional Hackers for Hire*, Symantec – Security Response, 17. september. (http://www.wired.com/images_blogs/threatlevel/2013/09/hidden_lynx_final.pdf) [8. jan. 2014]

Donald, Graeme (2008): *Sticklers, Sideburns & Bikinis: The Military Origins of Everyday Words and Phrases*, Oxford: Osprey Publishing.

Dowdy, John (2012): "The Cybersecurity Threat to U.S. Growth and Prosperity", i Joseph Nye, Nicholas Burns & Jonathon Price: *Securing Cyberspace – A New Domain for National Security*, Washington D.C.: Brookings Institute Press.

Drummond, David (2010): "A New Approach to China", Official Google Blog, 12. jan. 2010. (http://googleblog.blogspot.dk/2010/01/new-approach-to-china.html) [8. jan. 2014]

Elgin, Ben, Lawrence, Dune & Michael Riley (2012): "Coke Gets Hacked And Doesn't Tell Anyone", *Bloomberg*, 5. nov. 2012. (http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html) [8. jan. 2014]

Europa-Kommissionen (2007): "Communication: Towards a general policy on the fight against cyber crime", 22. maj 2007.

Farwell, James P. & Rafal Rohozinski (2011): "Stuxnet and the Future of Cyber War", *Survival*, 53:1, s. 23-40.

Feaklin, Tobias (2013): "Enter the Cyber Dragon – Understanding Chinese intelligence agencies' cyber capabilities", *Australian Strategic Policy Institute Special Report* 50.

Fein, Peter (2013): "Datalove in a Time of Cyberwar", Google Ideas-seminaret "Conflict in a Connected World", 20-22. okt. 2013. (http://www.google.com/ideas/events/conflict-in-a-connected-world-2013/videos/) [8. jan. 2014]

Fidler, David P. (2012): "*Inter arma silent leges* Redux? The Law of Armed Conflict and Cyber Conflict", i Derek S. Reveron (red.): *Cyberspace and National Security*, Washington D.C.: Georgetown University Press, s. 71-88.

Forsvarets Efterretningstjeneste – Center for Cybersikkerhed (2013a): Cybertruslen mod kritisk infrastruktur, november. (http://fe-ddis.dk/cfcs/CFCS Documents/CFCS_Trusselvurdering_Nov_2013.pdf) [8. jan. 2014]

Forsvarets Efterretningstjeneste (2013b): Efterretningsmæssig risikovurdering 2013 – En aktuel vurdering af forhold i udlandet af betydning for Danmarks sikkerhed.(http://fe-ddis.dk/SiteCollectionDocuments/FE/EfterretningsmaessigeRisikovurderinger/Risikovurdering2013.pdf) [8. jan. 2014]

Fritz, Jason (2013): "*The Semantics of Cyber Warfare* 网络战的语义", East Asian Security Symposium and Conference, Beijing, november.

Gabbatt, Adam (2013): "New York woman visited by police after researching pressure cookers online", *The Guardian*, 1. aug. 2013. (http://www.theguardian.com/world/2013/aug/01/new-york-police-terrorism-pressure-cooker) [8. jan. 2014]

Gartzke, Erik (kommende publikation): "The Myth of Cyberwar – Bringing War on the Internet Back Down to Earth". (http://dss.ucsd.edu/~egartzke/papers/cyberwar_12062012.pdf) [8. jan. 2014]

Geers, Kenneth (2011): *Strategic Cyber Security,* Tallinn: CCD COE Publication.

Glenny, Misha (2012): *Dark Market,* London: Vintage.

Gonzales, Michael J. (2010): "Volbeat-guitarist nægtet indrejse til USA", *Gaffa*, 16. aug. 2010. (http://gaffa.dk/nyhed/42102) [8. jan. 2014]

Gordon, Sara & Richard Ford (2006): "On the definition and classification of cybercrime", *Journal in Computer Virology,* 2:1, s. 13-20.

Greenwood, Phoebe (2012): "Hackers leak Assad's astonishing office emails", *The Telegraph*, 7. feb. 2012. (http://www.telegraph.co.uk/news/worldnews/middleeast/syria/9067118/Anonymous-hackers-leak-Syrias-Bashar-al-Assads-astonishing-office-emails-discussing-Barbara-Walters.html) [8. jan. 2014]

Gross, Michael J. (2011): "A Declaration of Cyber-War", *Vanity Fair*, april. (http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104) [8. jan. 2014]

Gyldendal (2009): "Sabotage", Gyldendal Online. (http://www.denstoredanske.dk/Samfund,_jura_og_politik/Milit%C3%A6r/Strategi,_taktik,_udrustning_og_efterretning/sabotage) [8. jan. 2014]

Harris, Shane (2013): "The Cowboys of the NSA", *Foreign Policy*, 9. sep. 2013. (http://www.foreignpolicy.com/articles/2013/09/08/the_cowboy_of_the_nsa_keith_alexander?page=full) [8. jan. 2014]

Hathaway, Oona A. & Rebecca Crootof (2012): "The Law of Cyber-Attack", *Faculty Scholarship Series*, paper 3852.

Helft, Miguel & Daniel Barboza (2010): "Google Shuts China Site in Dispute Over Censorship", *The New York Times*, 22. marts 2010.(http://www.nytimes.com/2010/03/23/technology/23google.html) [8. jan. 2014]

Herzog, Stephen (2011): "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security*, 4:2, s. 49-60.

InfoSOC.ru (2011): "SCO responds to cyber challenges", 9. juni 2011. (http://infoshos.ru/en/?idn=8349) [8. jan. 2014]

Jacobsen, Jeppe T. (2014): "Cyberkrigen har endnu ikke nået Ukraine", *Jyllands-Posten*, 28. marts 2014. (http://www.diis.dk/hjem/nyheder/2014/hvorfor+er+der+ikke+cyberkrig+i+ukraine) [14. april 2014]

Jacobsen, Jeppe T. (2014): "Nyt lovforslag om it-sikkerhed mangler gode argumenter", *Information*, 17. marts 2014. (http://www.information.dk/491365) [14. april 2014]

Jacobsen, Jeppe T. (2014): "The cyberwar mirage and the utility of cyberattacks in war", *DIIS Working Paper*.

Jenik, Aviram (2009): "Cyberwar in Estonia and the Middle East", *Network Security* 4.

Joshi, Shashank (2013): "Iran, the Mossad and the power of cyber-warfare", *The Telegraph*, 3. okt. 2013. (http://blogs.telegraph.co.uk/news/shashankjoshi/100239562/iran-the-mossad-and-the-power-of-cyber-warfare/) [8. jan. 2014]

Kelly, Heather (2013): "The five scariest hacks we saw last week", CNN, 5. aug. 2013. (http://edition.cnn.com/2013/08/05/tech/mobile/five-hacks/) [8. jan. 2014]

Kiggins, Ryan D. (2013): "Open for Expansion: US Policy and the Purpose for the Internet in the Post-Cold War Era", *International Studies Perspectives*, s. 1-20.

Kiggins, Ryan D. (2014): "US Leadership in Cyberspace: Transnational Cyber Security and Global Governance", i Jan-Frederik Kremer & Benedikt Müller: *Cyberspace and International Relations – Theory, Prospect and Challenges*, Heidelberg: Springer.

Kjær, Jacob S. (2013): "Danmark bagud på it-sikkerhed i Europa", *Politiken*, 22. dec. 2013. (http://politiken.dk/indland/ECE2166430/danmark-bagud-paa-it-sikkerhed-i-europa/) [14. april 2014]

Klimburg, Alexander (2011): "Mobilising Cyber Power", *Survival*, 53:1, s. 41-60.

Krepinevich, Andrew F. (2012): "Cyber Warfare: A 'Nuclear Option'?", papir fra Center for Strategic Budgetary Assessments. (http://www.csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/) [8. jan. 2014]

Kurtz, George (2010): "Operation 'Aurora' Hit Google, Others", McAfee Blog Archive. (http://www.mckeay.net/2010/01/) [8. jan. 2014]

Lachow, Irving (2009): "Cyber Terrorism: Menace or Myth?", i Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz (red.): *Cyberpower and National Security*, Washington D.C.: National Defence University Press & Potomac Books, inc., s. 437-464.

Langner, Ralph (2011): "Cracking Stuxnet, a 21st-century cyber weapon", TED Talks. (http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html) [8. jan. 2014]

Langner, Ralph (2013): "Stuxnet's Secret Twin", *Foreign Policy*, 19. nov. 2013. (http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack) [8. jan. 2014]

Lauta, Kristian C., Hoffman, Rune & Lars B. Struwe (2013): "Cyberwarfares udfordringer af begrebet kritisk infrastruktur", rapport fra Center for Militære Studier, november. (http://cms.polsci.ku.dk/cms/cyberwarfare/Cyberwarfare.pdf) [8. jan. 2014]

Lawson, Sean (2011): "Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History", *Working Paper*, 11:01, Fairfax, Virginia: Mercatus Center.

Layne, Christopher (2006): *The Peace of Illusions: American Grand Strategy from 1940 to the Present*, Ithaca, New York: Cornell University Press.

Lewis, James (2012): "In Defense of Stuxnet", *Military and Strategic Affairs,* 4:3, s. 65-76.

Libicki, Martin C. (2009): *Cyberdeterrence and Cyberwar,* Santa Monica: RAND Corporation.

Lin, Herbert S. (2010): "Offensive Cyber Operations and the Use of Force", *Journal of National Security Law and Policy* 4, s. 63-86.

Mandiant (2013): "APT1: Exposing One of China's Cyber Espionage Units", rapport fra Mandiant Intelligence Center.

Markoff, John & David Barboza (2010): "2 China Schools Said to Be Tied to Online Attacks", *The New York Times*, 18. feb. 2010. (http://www.nytimes.com/2010/02/19/technology/19china.html) [8. jan. 2014]

Mazanec, Brian M. (2009): "The Art of (Cyber) War", *The Journal of International Security Affairs* 19.

McAfee & Center for Strategic and International Studies (2013): *The Economic Impact of Cyber Crime and Cyber Espionage*, rapport. (http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf) [8. jan. 2014]

McConnell, Mike (2010): "Mike McConnell on how to win the cyber-war we're losing", *Washington Post*, 28. feb. 2010. (http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html) [8. jan. 2014]

McGraw, Gary & Nathaniel Fick (2013): "Separating the Threat from the Hype: What Washington Needs to Know About Cyber Security", i *Amsterdam's Cyber Future: Security and Prosperity in the Information Age Volume I and II*, Washington D.C.: Center for New American Society.

McGraw, Gary (2013): "Cyber War is Inevitable (Unless We Build Security In)", *Journal of Strategic Studies*, 36:1, s. 109-119.

Merriam-Webster Online Dictionary (2014): "espionage". (http://www.merriam-webster.com/dictionary/espionage) [8. jan. 2014]

Moss, Kenneth B. (2013): "Ambiguity and Accountability in War: The Challenge of Cyber and Unmanned Systems", præsentation på Dansk Institut for Internationale Studier, 20. juni 2013.

Mshvidobadze, Khatuna (2011): "The Battlefield on Your Laptop", Radio Free Europe/Radio Liberty, Georgian Security Analysis Center, 21. marts 2011.

Mueller, Milton L. (2010): *Networks and States – The Global Politics of Internet Governance*, Cambridge, Massachusetts: MIT Press.

Nachenberg, Carey (2012): "Dissecting Stuxnet", præsentation på Stanford University. (http://www.youtube.com/watch?v=DDH4m6M-ZIU) [8. jan. 2014]

Nyst, Carly (2013): "The Five Eyes Fact Sheet", *Privacy International*, 27. nov. 2013. (https://www.privacyinternational.org/blog/the-five-eyes-fact-sheet) [14. april 2014]

Obama, Barack H. (2010): *2010 Joint Strategic Plan on Intellectual Property Enforcement,* Washington D.C.: US Government Printing Office.

Obama, Barack H. (2011a): *Administration's White Paper on Intellectual Property Enforcement,* Washington D.C.: US Government Printing Office.

Obama, Barack H. (2011b): *International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World,* Washington D.C.: US Government Printing Office.

Obama, Barack H. (2013): *2013 Joint Strategic Plan on Intellectual Property Enforcement,* Washington D.C.: US Government Printing Office.

O'Hara, Gerald (2010): "Cyber-Espionage: A Growing Threat to the American Economy", *CommLaw Conspectus*, 19:1, s. 241-275.

O'Hara, Kieron & Nigel Shadbolt (2008): *The Spy in the Coffee Machine – The End of Privacy As We Know It*, Oxford: Oneworld.

Olson, Parmy (2013): *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency*, London: Random House.

Owens, William A., Kenneth W. Dam & Herbert S. Lin (red.) (2009): *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington D.C.: The National Academies Press.

Palmer, Shelly (2010): Cyber-terrorism vs. Cyber-Warfare, *The Entertainment and Sports Lawyer*, 28:1, s. 22-24.

Panetta, Leon (2012): "Cyberattacks Could Become as Destructive as 9/11", *BloombergBusinessweek*, 12. okt. 2012. (http://businessweek.com/news/2012-10-12/cyberattacks-could-become-as-destructive-as-9-11-panetta) [8. jan. 2014]

Perlroth, Nicole (2012): "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back", *The New York Times*, 23. okt. 2012. (http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=0) [8. jan. 2014]

Peterson, Andrea (2013): "Why everyone is less secure when NSA doesn't help fix security flaws", *Washington Post*, 4. okt. 2013. (http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws/) [14. april 2014]

Read, Oliver (2014): "How the 2010 Attack on Google Changed the US Government's threat perception of Economic Cyber Espionage", i Jan-Frederik Kremer & Benedikt Müller: *Cyberspace and International Relations – Theory, Prospect and Challenges*, Heidelberg: Springer.

Reveron, Derek S. (2012): "An Introduction to National Security and Cyberspace", i Derek S. Reveron (red.): *Cyberspace and National Security*, Washington D.C.: Georgetown University Press.

Richardson, John (2011): "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield", *The John Marshal Journal of Information Technology & Privacy Law*, 29:1, s. 1-27.

Rid, Thomas & Peter McBurney (2010): "Cyber-Weapons", *The RUSI Journal*, 157:1.

Rid, Thomas (2011): "Cyber War Will Not Take Place", *Journal of Strategic Studies*, 35:1.

Rid, Thomas (2012): *Cyber War Will Not Take Place*, London: Hurst & Company.

Rid, Thomas (2013): "Cyber-Sabotage is Easy", *Foreign Policy*, 23. juli 2013.

(http://www.foreignpolicy.com/articles/2013/07/23/cyber_sabotage_is_easy_i_know_i_did_it) [8. jan. 2014]

Rogers, Mike (2013): "Representative Mike Rogers on Cyber Attacks", præsentation på International Institute for Strategic Studies, Washington D.C. (http://www.c-spanvideo.org/program/314114-1) [8. jan. 2014]

Rogin, Josh (2012): "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history'", *Foreign Policy*, 9. juli 2012. (http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history) [8. jan. 2014]

Roscini, Marco (2010): "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", *Max Planck Yearbook of United Nations Law* 14, s. 85-130.

RT (2012): "Cyberwar Speeds Up: US Blames Iran for renewed attacks on American banks", *Russia Today*, 18. okt. 2012. (http://rt.com/usa/us-cyber-iran-banks-731/) [8. jan. 2014]

Russia & India Report (2013): "SCO Members to cooperate in war on cyber terrorism", 2. april 2013. (http://indrus.in/world/2013/04/02/sco_members_to_cooperate_in_war_on_cyber_terrorism_23429.html) [8. jan. 2014]

Sale, Richard (2012): "Iran behind Shamoon Attack", *Industrial Safety and Security Source*, 15. okt. 2012. (http://www.isssource.com/iran-behind-shamoon-attack/) [8. jan. 2014]

Samaan, Jean-Loup (2010): "Cyber Command: The Rift in US Military Strategy", *The RUSI* Journal, 155:6.

Sandvik, Kristin B. (2012): "Cyberwar as an Issue of International Law", *PRIO Policy Brief* 4.

Sanger, David (2012): *Confront and Conceal – Obama's Secret Wars and Surprising Use of American Power*, New York: Random House.

Sanger, David E., David Barboza & Nicole Perlroth (2013): "Chinese Army Unit is Seen as Tied to Hacking Against U.S.", *The New York Times*, 18. feb. 2013. (http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all) [8.jan. 2014]

Schmitt, Michael N. & Brian T. O'Donnell (red.) (2002): "Computer Network Attacks and International Law", *International Law Studies* 76.

Schmitt, Michael N. (1999): "Computer Network Attacks and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law* 7: 884-937.

Schmitt, Michael N. (red.) (2012): *Tallinn Manual on International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press.

Schneier, Bruce (2003): "The Risk of Cyberterrorism", *Crypto-Gram Newsletter*, 15. juni 2003. (https://www.schneier.com/crypto-gram-0306.html#1) [8. jan. 2014]

Schreier, Fred (2012): "On Cyberwarfare", *DCAF Horizon 2015 Working Paper* 7.

Shackelford, Scott J. (2009): "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law*, 27:1.

Sharma, Amit (2009): "Cyber Wars: A Paradigm Shift from Means to Ends", i Christian Czosseck & Kenneth Geers: *The Virtual Battlefield: Perspectives on Cyber Warfare*, Amsterdam: IOS Press.

Sharp Sr., Walter G. (1999): *Cyberspace and the Use of Force*, Fall Church: Aegis Research Corporation.

Sheldon, John B. (2011): "Deciphering Cyberpower – Strategic Purpose in Peace and War", *Strategic Studies Quarterly,* Summer.

Singer, Peter W. & Allan Friedman (2014): *Cybersecurity and Cyberwar – What Everyone Needs to Know*, New York: Oxford University Press.

Skjoldager, Morten & Simon Reenberg (2013): "Overvågning: Ung dansk turist får nej til at rejse ind i USA", *Politiken*, 19. aug. 2013. (http://politiken.dk/indland/ECE2052634/overvaagning-ung-dansk-turist-faar-nej-til-at-rejse-ind-i-usa/) [8. jan. 2014]

Slay, Jill & Michael Miller (2007): "Lessons Learned from the Maroochy Water Breach", *Critical Infrastructure Protection, IFIP International Federation for Information Processing* 253, s. 73-82.

Smith, Tony (2001): "Hacker jailed for revenge sewage attacks", *The Register*, 31. okt. 2001. (http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/) [8. jan. 2014]

Stohl, Michael (2006): "Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?", *Crime Law & Social Change* 46, s. 223-238.

Stone, John (2013): "Cyber War Will Take Place!", *Journal of Strategic Studies*, 36:1, s. 101-108.

Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm & Liis Vihul (2008): "Cyber Attacks Against Georgia: Legal Lessons Identified", rapport fra NATO Cooperative Cyber Defence Centre of Excellence, Tallinn. (http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf) [21. apr. 2014]

U.S. Department of Defense (2010): *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, (As Amended Through 15 December 2013).*

Vahidi, Ahmad (2011): "Iran: Stuxnet worm, computer terrorism", *Press TV*. (http://edition.presstv.ir/detail.fa/146567.html) [8. jan. 2014]

Van Creveld, Martin (1991): *The Transformation of War*, New York: The Free Press.

Weimann, Gabrielle (2005): "Cyberterrorism: The Sum of All Fears?", *Studies in Conflict & Terrorism,* 28:2, s. 129-149.

Wong, Stephanie (2008): "Coca-Cola to Buy China's Huiyuan for $2.3 Billion (Update4)", Bloomberg, 3. sep. 2008. (http://www.bloomberg.com/apps/news?pid=newsarchive&refer=home&sid=atnR.K6weMFM) [8. jan. 2014]

Woolford, Thomas & Jonathan Matusitz (2011): "The Memetic Engineering of Anonymous, the Cyberterrorist Group", *International Journal of Cyber Warfare and Terrorism*, 1:4, s. 1-9.