politica, 47. årg. nr. 3 2015, 404-423

Jeppe Teglskov Jacobsen

Terrorisme i cyberspace: udfordringer ved organisering og udførelse af politisk vold online

Internettet præsenteres ofte som et farligt redskab i hænderne på terrorister. Det er dog ikke nødvendigvis sandheden. Artiklen trækker på indsigter fra studier af sunniekstremistiske grupper, Anders B. Breivik og Anonymous og diskuterer terroristers anvendelse af internettet i organiseringen og udførelsen af terrorisme. Jeg vil argumentere for, at det anarkiske og anonyme internet fører mistillid og fragmentering med sig, hvilket gør det sværere for grupper at opretholde en fælles strategi og det fælles fjendebillede. Artiklen styrker derfor fortællingen om, at det hovedsageligt er ekskluderede og socialt marginaliserede enspændere, der ender med at planlægge voldshandlinger i isolation bag computerskærmen. I forlængelse heraf vil jeg pege på, at hovedparten af potentielle terrorister drages af fysisk interaktion, våben og eksplosioner – og ikke udviklingen af komplekse cybervåben.

Islamisk Stats gruopvækkende halshugningsvideoer og fejringer af terrorangrebet på *Charlie Hebdo* har nok en gang placeret terroristers brug af internettet højt på den politiske dagsorden. Zoomer man ind på cyberspace, fremstår terrortruslen som en palet af nye og uhåndgribelige udfordringer. Internettet kan bruges til spredning af propaganda, radikalisering, rekruttering, finansiering, organisering og endda udførelse af terrorangreb. Samtidig fremstår cyberspace med sin globale, øjeblikkelige, anonyme og tilgængelige karakter som et oplagt våben for terroristen – og hermed som en bekymring i politiarbejdet (Verton, 2003; Wikotorowicz, 2005; Weimann, 2004, 2006, 2010; Matusitz, 2008; Clarke and Knake, 2010; Brunst, 2010; McFarlane, 2010; Thompson, 2011; Helfstein, 2012; Holt, 2012; Hua og Bapna, 2012; Ogun, 2012; Wilson, 2014).

Det har naturligt ført til et væld af både nationale og internationale initiativer, strategier og resolutioner til bekæmpelse og forebyggelse af onlineradikalisering, terroristers kriminelle onlineadfærd og cyberterrorisme (Cabinet Office, 2010; UNODC, 2012; EU Cybersecurity Strategy, 2013; Rådet for den Europæiske Union, 2015; Kirkhope og Tannock, 2015; Regeringen 2014). Den omfattende allokering af ressourcer til terrorismebekæmpelse på og fra internettet og cyberspace er dog også blevet kritiseret for ikke at stå mål med den faktiske trussel.[1] Flere forskere peger på, at indflydelsen fra virtuel interaktion og voldeligt onlinemateriale på rekruttering og radikalisering er stærkt overvurderet (McCants, 2008; Hoskins og O'Loughlin, 2009; Lenning et al., 2010; Kenney, 2010; Borum, 2011; Hegghammer, 2013; Gemmerli, 2014; Archetti, 2015). Dog har de politikker, der skal bekæmpe organisering af terrorisme online, forebygge radikalisering af soloterrorister i cyberspace samt forhindre udførelse af cyberterrorisme, ikke været genstand for samme grad af kritisk refleksion.[2]

Jeg vil forsøge at bidrage til en sådan refleksion. Det er således ikke min hensigt at vurdere, hvad der virker eller ikke virker for personer og grupper, der ønsker at organisere og udføre terrorisme online.[3] Derimod forsøger jeg – ved at sammenholde en række cases med cyberspaces tekniske karakteristika – at påpege, at anvendelsen af internettet ikke partout vil føre mere terrorisme med sig.[4] Det følgende bør derfor læses som et forsøg på at stimulere kritisk tænkning for dermed at undgå forhastede konklusioner om internettets indbyggede farer.

Artiklen er struktureret i forhold til tre typer aktører (gruppe-, solo- og onlineaktører) og tre korresponderende typer terrorangreb, hvori cyberspace spiller en rolle. Den første type er de mere velorganiserede sunniekstremistiske grupper såsom al-Qaida og Islamisk Stat (IS), som kan udnytte den forbedrede adgang til internettet til nemmere at organisere store terrorangreb i stil med 9/11 (Hoffman, 2006; Awan, 2007; Thompson, 2011; Gertz, 2014).[5] Den anden type er ensomme ulve som Anders B. Breivik, der vælger at planlægge soloangreb i fysisk isolation i det anonyme cyberspace (Pantucci, 2011; Thompson, 2011; Spaaij, 2010; Helfstein, 2012). Til sidst trækker artiklen på en tredje type aktører, de mere computerkyndige onlinegrupperinger. Her tages udgangspunkt i Anonymous, som ved hjælp af onlineaktioner har formået at igangsætte diskussioner om fremtidige cyberterrorangreb (Woolford og Matusitz, 2013; Redins, 2012; Molfino, 2012: 79; Walsh, 2012: 233; Holt, 2012). Anonymous er imidlertid en flygtig og mangeartet størrelse (Coleman, 2014; Olson, 2013; Kushner, 2014), hvorfor jeg primært vil inddrage de mere teknisk kompetente udbrydergrupper LulzSec og AntiSec. Det gøres i forsøget på at vise, hvorledes cyberspace og dets karakteristika ikke nødvendigvis er så tiltrækkende for onlinegrupper, som ønsker at organisere (cyber)terrorisme.[6]

Kombineres indsigterne med eksempler fra jihadfora, peger artiklen på, at det anonyme og mistillidsskabende internet og den ukontrollerbare og individualistiske brug af sociale medier kan vanskeliggøre målrettede politiske projekter – og dermed også de velorganiserede terrorangreb kendt fra bin Laden-æraen. Jeg foreslår dernæst, særligt på baggrund af Anders B. Breivik, at ensomme ulve ikke nødvendigvis *vælger* at organisere soloterrorangreb i fysisk isolation på internettet grundet et ønske om taktisk diskretion, men derimod

på baggrund af ensomhed og social marginalisering.[7] Sidst tager jeg udgangspunkt i de tre aktørtypers it-færdigheder og forholdet mellem konventionelle våben og cybervåben.[8] Her tyder meget på, at den tekniske kompleksitet, omkostningerne og vanskelighederne ved at frembringe destruktive og visuelle effekter gør cyberterrorisme mindre attraktiv end konventionelle våben.

Artiklen falder i tre dele. De to første afsnit vedrører hovedsageligt organisering, og den tredje udførelsen af terrorisme. Første afsnit diskuterer internettets betydning for voldelige politiske grupper online såvel som offline. Andet afsnit undersøger bevæggrunden for soloterroristers fysiske isolation bag computerskærmen. Tredje afsnit påpeger en række ulemper ved brugen af cybervåben.

Terrorgrupper: Skaber det sociale internet enighed og tillid?

Al-Qaidas angreb den 11. september udgør det mest betydningsfulde terrorangreb i nyere tid, og frygten for en gentagelse optager stadig politikere, kommentatorer og forskere (Mueller, 2013; Gertz, 2014). Ifølge *9/11 Commission Report* kostede angrebene på World Trade Center og Pentagon al-Qaida ca. 500.000 dollars og tog godt og vel to år at forberede. Angrebene var orkestreret af ledende al-Qaida-medlemmer, der ned til mindste detalje besluttede, hvem der skulle involveres, hvordan træningen skulle foregå, og hvordan operationen skulle udføres (The 9/11 Commission Report, 2004: 151-173).

Den øgede adgang til informations- og kommunikationsteknologier spillede her en rolle. Det blev muligt at kommunikere over fax og satellittelefoner, at overføre penge via globalt forbundne banksystemer og gemme planer på computere (Behnke, 2004: 307). Det seneste årti har gjort stadig flere teknologier og onlineforbindelser tilgængelige, og det virker plausibelt, at grupper såsom al-Qaida vil have evnen til at udnytte disse nye teknologier (Coll and Glasser, 2005). Men til trods for, at internettet fremstår som et vigtigt redskab i organiseringen af store og spektakulære terrorangreb, kan internettets sociale karakter lige så vel forpurre gruppers ideologiske og hierarkisk-organisatoriske sammenhængskraft.

Hvad er rigtig jihad?

Den lille gruppe af elitære ideologer, som i de tidlige år kæmpede om at definere al-Qaida, og som kontrollerede træningslejre i Afghanistan (Wright, 2006), ser ud til at have stadig vanskeligere ved at definere, hvad al-Qaida er og burde være. En del af forklaringen skal findes i, at de ideologiske, religiøse og strategiske diskussioner i stigende grad finder sted online, hvor tilhængere – høj som lav – frit kan bidrage med individuelle fortolkninger af, hvad sunniekstremisme er.

Vanskelighederne ved at opretholde fysiske træningslejre grundet systematiske droneangreb har fået al-Qaida på den arabiske halvø (AQAP) til i blandt andet onlinemagasinet *Inspire* at opfordre støtter til selv at organisere og udføre terrorangreb (AQAP, 2010). Mens opfordringen kan forøge risici for mindre og ikke særlig velorganiserede terrorangreb, gør den samtidig angreb i stil med 9/11 mindre sandsynlige. Det er blevet vanskeligt, hvis ikke umuligt, at kontrollere, hvem der tilslutter sig, hvad der bliver skrevet på diverse jihadfora og i sidste ende, hvilken retning sunniekstremismen bevæger sig i.

En onlinedebat på et jihadforum om "den perfekte terrorist" illustrerer denne pointe. Et indlæg i kølvandet på al-Qaida-videoen *Du har kun ansvaret for dig selv* modtog en del positiv omtale for at foreslå, at jihadistiske salafister skulle klæde sig som vesterlændinge og følge vestlig kultur for derved at forblive under radaren. Ideologerne, der administrerede hjemmesiden, så pointen om en fuldstændig assimilation som et *for* radikalt skridt og følte sig nødsaget til at fjerne de mest kontroversielle dele af indlægget. Ligeledes pointerede AQAP, at støtter, selv når de planlagde terrorisme, skulle følge ledernes ord og instrukser om at følge islams kald uden at lade sig opsluge af vestlig kultur (Hemmingsen, 2011: 32-33).

Et andet eksempel relaterer sig til den somaliske al-Qaida-affilierede gruppe al-Shabaab. Gruppens selvudnævnte engelsktalende onlinepropagandist, Omar Hammami, uploadede en YouTube-video, hvori han erklærede, at hans kritiske syn på al-Shabaabs strategi og fortolkning af Sharia havde fået ham til at frygte for sit liv. Diskussionerne omkring videoen blev imidlertid censureret i forsøget på at imødegå intern fragmentering, og lederskabet følte sig nødsaget til at fordømme enhver dødstrussel mod Hammami (Zelin, 2013: 11-12). Hammami blev myrdet under ét år efter udtalelserne, men på daværende tidspunkt havde hans kritik allerede udmøntet sig i en intern fragmentering, der havde flyttet al-Shabaabs fokus over på den interne magtkamp (Hansen, 2013).

Eksemplerne viser, at lederne af sunniekstremistiske grupperinger har vanskeligt ved at kontrollere støtters brug af internettet. Enhver kan tilslutte sig en onlinegruppering med en hvilken som helst fortolkning af, hvad sunniekstremisme er. Men med den interne uenighed om politisk retning og et manglende hierarki internt i organisationen mudres billedet af den politiske ven og fjende og derfor også af den politiske kamp, hvilket i sidste ende kan vanskeliggøre organiseringen af et storstilet terrorangreb.

Denne pointe kan også tydeliggøres ved at kaste et blik på de *foreign fighters*, der rejser til Syrien eller Irak for at slutte sig til ekstremistiske fraktioner. Alt imens de kæmper på jorden, bruger de sociale medier som en social, onlinedag-

bog, der skal bevidne oplevelser, heltedåd og vigtigheden af netop deres kamp. Disse kæmpere bidrager med individuelle fortolkninger af krigshandlingerne og af det sunniekstremistiske projekt. Beretningerne på sociale medier, hvor nogle bliver delt vidt og bredt, mens andre går i glemmebogen, skaber både for omverdenen og grupperingerne selv uklarhed i forhold til, hvorfor og hvordan der kæmpes.

IS har i et forsøg på at forhindre intern fragmentering oprettet mediecentre med topstyrret meningsmonopol både online og offline (RwB, 2014). Whistleblowere som fx #wikibaghdady, der lækker informationer om IS-lederen al-Baghdadi og dennes forhold til Baathpartiet, er derfor en irritation for IS-lederskabet (Speri, 2014). Om det også er undergravende for den interne sammenhængskraft, må tiden vise.

Den ikke helt så brugbare anonymitet

Selvom internettet også kan være en irritation for større politiske grupperinger, muliggør det stadig, at enkeltindivider, som ellers tidligere ikke havde muligheden for at mødes, kan finde sammen. For onlinefænomenet Anonymous, hvis tilhængere (Anons) varierer i tekniske færdigheder og politisk interesse og inkluderer hackere, nørder, spasmagere, aktivister og seksuelle afvigere (Kushner, 2014; Coleman, 2014),[9] har onlinechatfora som Internet Relay Chat skabt muligheden for anonymt at skrive i forskellige offentlige chatrum eller oprette private rum. I teorien betyder den anonyme, lederløse og ofte spontane form for mobilisering, at politiet får vanskeligt ved at forhindre operationer i at tage form, herunder at identificere deltagere.

Men selv for mindre onlinegrupperinger er internettet ikke nødvendigvis et ideelt redskab, når terrorisme skal organiseres. Det skyldes paradoksalt nok den anonymitet, som ofte udråbes som internettets største aktiv (Weimann, 2004; Knake, 2010; Holt, 2012; Benson, 2014: 298-299). Onlineoperationer og hacktivisme udført af nogle af de dygtigste af Anonymous' udbrydergrupperinger, LulzSec og AntiSec, viser netop, at flygtigheden og anonymiteten online er mulig at overkomme. Størstedelen af gruppernes medlemmer er fængslet, hvilket primært skyldes internettets sociale karakter. Medlemmerne havde opnået idolstatus online og var ikke villige til at miste deres pseudonymer, da det uundgåeligt ville betyde tab af denne status (Olson, 2013). Det blev således muligt for politiet at indsamle data på pseudonymerne og vente på de fejl, der muliggjorde fysisk identifikation.

En yderligere grund til, at anonyme onlinegrupperinger ikke nødvendigvis er ideelle terrorister, relaterer sig til tillid. Onlinefællesskaber baseret på pseudonymer og anonymitet er ikke ideelle platforme for opbygning af tillid, da de samtidig betyder, at det er nemmere og mindre risikofyldt at være en anonym stikker. Hector "Sabu" Monsegur – en af stifterne af LulzSec – viste sig eksempelvis at være FBI-informant. Da nyheden blev offentlig, blev mistilliden, som altid eksisterer i et anonymt fællesskab, afløst af paranoia, som siden har hæmmet seriøse samarbejder (Coleman, 2013: 11).

Jeg har indtil nu vist, hvorfor internettet ikke nødvendigvis er brugbart i organisering af terrorisme. Et stort terrorangreb, der planlægges af få strateger, er vanskeligt at organisere på onlineplatforme. Det skyldes, at internettet – sammenlignet med hierarkiske træningslejre eller uddannelsesplatforme – giver mulighed for, at individuelle sympatisører deltager på lige fod og ofte med modsatrettede fortolkninger af den politiske kamp. Derudover følger mistillid ofte af anonyme onlinemiljøer, hvilket igen gør koordineret og voldelig politisk handling vanskelig. Frygten for stikkere og overvågning er endnu mere udtalt online.

På trods af at terrorgrupperinger ikke nødvendigvis styrkes med internettet som et organiseringsværktøj, kan individer, som rationelt vælger anonymitet i cyberspace, forblive usynlige, indtil et terrorangreb igangsættes (Spaaij, 2010: 16; Weimann, 2012; Jones, 2012). Men er fysisk isolation online virkelig mere attraktivt end offline interaktion med ligesindede?

Soloterrorisme: hvorfor vælge fysisk isolation online?

Internettet var vigtigt for Breivik i organiseringen og måske endda også for udførelsen af angrebene den 22. juni 2011. Breivik fandt manualer, købte produkter og mødte ideologisk ligesindede online. Ifølge hans manifest finansierede han sine aktiviteter og øvede sine skydeegenskaber online (Pantucci, 2011: 36; Ravndal, 2012: 179). Olsen (2014: 18) har ydermere påpeget, at computerspils ofte nøgterne tone i beskrivelsen af mål og missioner også afspejles i Breiviks egen udvælgelse af mål. Men for Breivik fandtes intet alternativ til internettet. Der var ingen mulighed for at møde ligesindede offline – ingen mulighed for at organisere angreb. Kun ved én enkelt lejlighed påstår Breivik at have rejst til London for at møde andre "Tempelriddere", hvorefter disse blev enige om at afskære alt kontakt. "Enmandshære" var essentielle for operationel succes, hedder det sig i Brieviks Manifest (Pantucci, 2011: 31-33). Hvis dette er sandt, er frygten for ensomme ulve, der udelukkende af hensyn til operationel succes vælger fysisk isolation, reel.

Flere analytikere har imidlertid påpeget, at "Tempelridderne" med al sandsynlighed er en fiktion (Syse, 2014; Melle, 2013; Sandberg, 2013). Breivik selv beskriver både gruppen som reelt eksisterende og som en hypotetisk og fiktiv gruppe (2011: 776). Det er umuligt kategorisk at afvise eksistensen af "Tem-

pelridderne" og Breivik som en "sole cell commander", men noget tyder på, at Breivik konstruerede disse fantasier i forsøget på at romantisere sin operationelle ensomhed.

Faktisk tyder meget på, at Breiviks afsondrede liv skyldes ensomhed og manglende sociale egenskaber. De, der kender ham, beskriver ham som ensom og genert (Sandberg, 2013: 71), og Borchgevink (2013: 90) pointerer, at Breivik gennem sine skoleår "kæmpede for at forstå det sociale spil". Breiviks manifest og retssagen imod ham beretter om en ustabil opvækst med et anstrengt forhold til sin far, en mor med psykiske problemer og om flere dårlige oplevelser med muslimske bekendte (Breivik, 2011: 1377-1414; Seierstad, 2013). Breivik bliver ydermere karakteriseret som oprørsk og sardonisk, som en følelsesforladt narcissist, patologisk løgner og en suicidial sociopat (Melle, 2013; Syse, 2014).

Selvom Breivik har forsøgt at portrættere sig selv som intelligent, kompetent og succesfuld, vidner hans livshistorie om mange nederlag. Han blev erklæret uegnet til militæret, han mislykkedes med en karriere i det norske Fremskridtspartiet, han gik konkurs med sit firma og hans skriftlige udkast til artikler blev afvist (Pantucci, 2011; Ravndal, 2013: 177).

Derudover står Breiviks ihærdige forsøg på at fremstille sin manglende sociale interaktion som en opofrelse for et større mål og som et forsøg på at gå under jorden i skærende kontrast til hans faktiske forsøg på at mødes med de personer, han følte sig ideologisk forbundet med. Flere gange forsøgte han at mødes med sit idol, Fjordman, men blev konsekvent afvist (Breivik, 2011: 1405).

Breivik er ikke den eneste ensomme ulv, for hvem operationel isolation er et resultat af social marginalisering. Roshonara Choudhry, som forsøgte at dræbe den britiske MP Stephen Timms, understregede selv, at grunden til, at hun søgte mod den AQAP-affilierede Anwar al-Awlakis onlineprædikener, var, at hun ikke havde nogen at tale med, og at ingen rigtig forstod hende (Dodd, 2010). Ligeledes udførte Fort Hood-skyderen Nidal Hasan først sin aktion efter, at al-Awlaki – med hvem han havde en noget ensidig emailkorrespondance – ignorerede hans gentagne og indtrængende bøn om religiøs vejledning og hans tilbud om at bidrage til kampen for islam (FBI, 2012: 41-62). Breivik, Choudhry og Hasan er – trods forskellig ideologi – fælles om at kæmpe alene. Her virker isolationen online som den eneste reelle mulighed.

Når individer har muligheden for at mødes, træne og kæmpe side om side med ligesindede, virker det som om, at det foretrækkes (Bigo et al., 2014). Personerne bag London-bomberne, den hollandske Hofstad Gruppe og de fransk-algeriske gerningsmænd bag *Charlie Hebdo*-angrebet indgik i fysiske fællesskaber og rejste for at mødes med veletablerede terrororganisationer i Afghanistan og Pakistan (Nesser, 2008; Stenersen, 2008; Ritzau, 2015).

Det store antal foreign fighters, som er rejst til Syrien eller Irak for at gøre en forskel, understreger, at der er et (fysisk) socialt aspekt i den voldelige aktivisme. For størstedelen af individer med voldelige tendenser er det sociale kammeratskab en meget vigtig årsag til, at de drages mod felten (Bigo et al., 2014: 16).

Det betyder ikke, at isolerede skyderier udført af forstyrrede, voldelige enkeltpersoner, der påberåber sig en ideologi, ikke vil finde sted – som Bruxelles-skyderen Mehdi Nemmouche eller Omar al-Hussein (Saunders, 2014; Thyssen, 2015). Det ovenstående foreslår blot, at fremtidige soloterrorister ikke hovedsageligt er produkter af rationelle kalkuler baseret på ønsket om taktisk diskretion online, men i stedet er et resultat af social marginalisering. Ønsker forskere og politiet at forstå ensomme ulve, er det hverken tilstrækkeligt at analysere brugen af internettet eller en bestemt ideologi. De bør også kigge indad på den øgede individualisering og fremmedgørelse i samfundet (Pisoiu, 2013: 64; Böckler, Seeger og Heitmeyer, 2011).

Soloterrorister kan gemme sig i det anonyme cyberspace indtil udførelsen af en terroraktion. Men i planlægningsøjemed er internettet ikke nødvendigvis en katalysator for terroristen. Som ovenstående eksempler har illustreret, er det hovedsageligt sociale afvigere, der søger mod internettet i forberedelsen af soloterrorisme. For det voldelige individ fremstår det fysisk domæne med dets kammeratskab, fysiske træning og interaktion stadig særdeles attraktivt. Dette argument er også relevant i det følgende afsnit, der viser, hvorfor cyberterrorisme ikke bør frygtes i den nærmeste fremtid.

Cyberterrorismens tiltrækningskraft: våbenliggørelsen af internettet

Cyberterrorisme defineres på mange måder i den akademiske litteratur (Chen, Jarvis og Macdonald, 2014). Cyberterrorisme separeres først og fremmest fra terroristers sociale aktiviteter online i organisering af og kommunikationen om terrorhandlinger (Singer og Friedman, 2014). Cyberterrorisme er sammenkoblingen af cyberspace og terrorisme og refererer til selve udførelsen af terrorhandlingen (Lachow, 2009). For at retfærdiggøre cyberpræfikset må cyberterrorisme nødvendigvis også være udført gennem et computernetværk (Denning, 2000, 2007). Således foreslår jeg, at cyberterrorisme udelukkende forstås som den politisk motiverede brug af computerkode og netværkstrafik med henblik på at generere frygt gennem en ødelæggelse eller forstyrrelse af computere eller computernetværk, der i sidste ende skader civile. Med udgangspunkt i denne

definition vil jeg nu diskutere cybervåbens tiltrækning for personer, der ønsker at udføre terrorisme.

Ressourcemæssige og tekniske begrænsninger

Tidligere NSA-chef, Keith Alexander frygter, at onlineaktivister besidder evner til at lukke for det amerikanske elektricitetsnetværk (Smith, 2012), og tidligere FBI-chef, Robert Mueller understregede, at terrorister har udvist interesse for at tilegne sig hackingegenskaber eller hyre sådanne kapaciteter (FBI, 2010). Men der findes gode argumenter for, at et cyberterrorangreb *ikke* er nærtforestående.

For det første argumenterer Conway (2014: 100) for, at planlægningen af cyberterrorisme rettet mod eksempelvis en dæmning – med fysisk skade til følge – sandsynligvis koster den angribende millioner af dollars. Det er betydeligt mere end planlægningen og udførelsen af 9/11. Det alvorligste cyberangreb, som faktisk formåede at påføre fysisk skade, var den amerikansk-israelske Stuxnet-orm rettet mod det iranske atomprogram. Udarbejdelsen af ormen krævede en fuld funktionsdygtig kopi af it-infrastrukturen på atomanlægget og indgående kendskab til nukleare processer (Sanger, 2012: 202-205). Det bidrager til, at prisen for at udføre et målrettet cyberangreb stiger relativt til eksempelvis at sprænge en bilbombe.

Lindsey (2013: 389) peger ydermere på den høje tekniske kompleksitet ved alvorlige cyberangreb, og ifølge it-sikkerhedsguruen Chris Wysopal har selv de dygtigste amatører eller hacktivister i eksempelvis Anonymous ikke imponeret mange i it-sikkerhedsindustrien (Mansfield-Devine, 2011b).[10] Anons og hackere, der støtter IS, bruger relativt simple hackingteknikker og udvælger deres mål baseret på allerede kendte sårbarheder (Mansfield-Devine, 2011a; 2011b; Deibert, 2013: 222-225; Marcus 2015). Disse sårbarheder har hovedsageligt givet adgang til at redigere indhold på hjemmesider eller lække hemmeligstemplede dokumenter. Førstnævnte svarer i it-sikkerhedsverdenen til graffiti, mens sidstnævnte potentielt kan have alvorligere konsekvenser. Dog har Anons, når det kommer til lækager, ikke kunnet måle sig med "insiderne" Edward Snowden og Chelsea Manning. De mest spektakulære Anon-lækager, LulzSecs hack på Sony og NATO, var både ydmygende og dyre for de to organisationer, men konsekvenserne relativt få og forbigående. Det skyldes efter al sandsynlighed, at hackernes ikke kunne få adgang til mere data (Mansfield-Devine, 2011a; 2011b; Olson, 2013).

Den til dato mest prominente, selvudnævnte onlineterrorist, Younis Tsouli eller Irhabi007, er et godt eksempel på, at der er store forskelle på at redigere indhold på hjemmesider, opfordre til vold gennem YouTube-videoer og snyde

med kreditkort online og så den faktiske gennemførelse af voldelige handlinger ved hjælp af hacking. Tsouli administrerede al-Qaida hjemmesider fra sin fars diplomatlejlighed i London. Men havde han besiddet den tekniske kapacitet til at forstyrre samfundsvigtige funktioner gennem cyberangreb, havde han nok ikke begrænset sig til spredning af onlinepropaganda. Faktisk er der intet i Tsoulis historie, der indikerer, at han overhovedet evnede at udføre vold (July 7th People's Independent Inquiry Forum, 2009).

At verden endnu ikke har oplevet cyberterrorisme betyder ikke, at der ikke findes enheder med færdighederne til at skabe ødelæggende cybervåben. Men disse er drevet af økonomiske incitamenter eller indgår som en del af konventionelle militære kapabiliteter (Deibert, 2013: 148-187). Skulle terrororganisationer forsøge at *crowdsource* eller hyre hackere, er det forbundet med store risici, da sandsynligheden for at blive opdaget, når terrorister bevæger sig udenfor den betroede indercirkel, er markant større.

Terrorister kan udnytte det store marked for køb af endnu ukendte it-sårbarheder (Deibert, 2013: 195-216; Kibar, 2014), men selv med adgang til disse kræver et cyberangreb med stor effekt mere end blot kendskab til it-sårbarheder og programmeringsfærdigheder. Det kræver også teknisk viden om de funktioner, processer og maskiner, terroristen ønsker at påvirke eller ødelægge (Jacobsen, 2014: 9-10). Det skyldes, at computerkode ikke indeholder en eksplosiv ladning, hvorfor fysisk skade nødvendigvis skal forårsages indirekte gennem den angrebne computer (Rid og McBurney, 2012: 9). Kendskab til de ikke nødvendigvis computertekniske processer, som computeren styrer, er således essentiel for, at processerne kan ændres eller stoppes gennem en ændring i computerkoden med en fysisk effekt til følge. Sammenlignes et sådant cyberangreb med en selvmordsbombe eller en bilbombe, er det ikke sært, at sidstnævnte er mere attraktive. Breiviks simple bilbombe i regeringskvarteret i Oslo kostede eksempelvis Norge op mod $100 millioner dollars i genopbyggelsesomkostninger (Sandelson og Smith, 2013).

Cyberterroristens visuelle begrænsning

Terrorangrebets spektakulære og gruopvækkende visuelle karakter er også essentielt for terroristen (Conway, 2014: 114-115). Hvis ingen ved, at et terrorangreb har fundet sted, eller hvorfor det har fundet sted, har terroristen svært ved at etablere den ønskede effekt, nemlig frygten. Terrorgrupper tager derfor ofte direkte eller indirekte ansvaret for et terrorangreb og er samtidig afhængige af, at medierne rapporterer om angrebet.

Cyberangreb er derfor problematiske for terrorister. Det oftest fremstillede *worst case*-scenarium, en omfattende strømafbrydelse, fører hverken til en eks-

plosion eller et særlig medievenligt billede. Når afbrydelsen indtræffer, er det svært at vide, om hændelsen er et uheld eller ej, og de påvirkede har ingen mulighed for at finde ud af det, mens strømafbrydelsen finder sted. En strømafbrydelse genererer af ovenstående grund ikke nødvendigvis frygt.

Cyberterroristens visuelle begrænsning kan også forstås i relation til terroristen selv. Crone (2014) påpeger, at den voldelige handling skal have speciel visuel udformning hos forskellige militante subkulturer. For den sunniekstremistiske terrorist skal den visuelle udformning eksempelvis være den selvmordsbombende martyr, håndteringen af en Kalashnikov og halshugningen af vandtro. Det er de ultimative billeder af voldelig jihadisme, som bliver delt som "selfies" og i YouTube-videoer. Noget lignende ser vi i den narcissistiske selvoptagethed, som Breivik præsenterede i sine ridderlignende selvportrætter (Behnke, 2014). Imitationen af en voldelig eller ridderlig idealfigur står i skærende kontrast til diskussionen på diverse Anon chatfora, hvor tilskyndelsen til vold medfører eksklusion.

Anons har imidlertid udført en række DDoS-angreb[11] (Olson, 2013). Men at tale om DDoS-angreb som et eksempel på cyberterrorisme er kontroversielt. I udgangspunktet har DDoS-angreb ikke noget med hacking at gøre. Det fører hverken til fysisk eller funktionel skade og gør blot et system langsommere (Rid, 2012). Sådanne angreb er irriterende, kan koste mange penge og gør vitale funktioner midlertidigt utilgængelige. Men langt størstedelen af de oplevede DDoS-angreb – som dem udført af pro-russiske grupperinger mod Estland i 2007 – ville have fejlet mod populære hjemmesider som Amazon og Google (McGraw og Fick, 2011: 44). Dette skyldes, at højere it-sikkerhedsstandarder, større servere og tekniske modsvar gør succesfulde DDoS-angreb vanskeligere at udføre.

Det betyder dog ikke, at alvorlige DDoS-angreb er utænkelige. Forstyrrelser i datatrafikken – selvom den er ikke-voldelig – er en ny taktik, som bør tages seriøs. Effekten af et DDoS-angreb er imidlertid uforudsigeligt. Det er ikke nær så attraktivt for individer, der ønsker at forårsage frygt gennem vold, at give sig i kast med angreb, hvor effekten er både tilfældig og usikker. For de ikke-voldelige Anons er DDoS-angreb blot en virtuel protest og bør ikke blive frygtet, som var det et kommende terrorangreb.

Konklusion

Gennem analyser af voldelig sunniekstremisme, Anders B. Breivik og Anonymous har jeg peget på en række dynamikker, som nuancerer forståelsen af cyberspaces og internettets potentialer for organisering og udførelse af terrorisme. Her kan tre pointer fremhæves.

Internettets sociale, anarkiske og mistillidsfulde natur kan vanskeliggøre hierarkisk politisk kontrol i terrorgrupperinger og dermed også organisering af storstilede terrorangreb. Internettet – i særdeleshed onlinefora – har gjort det muligt for ellers marginaliserede ekstremister at interagere med ligesindede, men disse foras anonyme og lettilgængelige karakter har samtidig gjort det svært at opretholde en hierarkisk styring kendt fra bin Laden-æraen. Individer kan i stigende grad bidrage med egne fortolkninger af, hvordan det politiske projekt bør udleves. Selv for mindre grupperinger er det anonyme internet en kilde til mistillid, hvilket kan gøre terrorplanlægning mindre attraktiv online.

Soloterrorister søger hovedsageligt mod cyberspace, når de er forhindrede i at interagere og samarbejde offline. Individer med voldelige tilbøjeligheder fravælger fysisk isolation online og rejser, hvis muligt, til kamppladsen i eksempelvis Syrien eller Irak. Er man tiltrukket af muligheden for at udøve vold, kan computerskærmen, musen og keyboardet ikke konkurrere med socialt kammeratskab og fysisk interaktion.

Cyberterrorisme er ikke så attraktiv som konventionel terrorisme. Et voldeligt, politisk motiveret cyberangreb, der har til hensigt at indgyde frygt gennem brugen af og målrettet mod computere og computernetværk, er vanskeligere at udføre end et konventionelt angreb. Sammenlignet med en bombe er omkostningerne ved at udarbejde, teste eller påføre et stykke software med en eksplosiv ladning store. Cyberangreb kan medføre forstyrrelser af vigtige funktioner, men angrebene mangler tilstrækkelig visuel effekt til at generere frygt. Derudover udgør hackeren med en mus og et keyboard ikke et symbol på vold, som voldelige individer kan spejle sig i.

Noter

1. Cyberspace og internettet er ikke identisk. Cyberspace kan bredt forstås som alle netværk, hvor data – ofte automatisk – udveksles ved hjælp af og på tværs af computere (se Betz og Stevens, 2011: 36-38). Internettet er det største netværk, men stadig blot ét af de mange computernetværk i cyberspace, kendetegnet ved især sin store grad af social interaktion. Cyberangreb er således ikke nødvendigvis ensbetydende med, at et stykke malware har befundet sig på internettet (eksempelvis Stuxnet før 2010, se Langner, 2013).
2. Der er selvsagt undtagelser: Bensons (2014) kvantitative studie af, hvorfor politiarbejdet faktisk har en fordel i cyberspace; Conways (2014) *reality check* af sandsynligheden for cyberterrorisme; samt Stohls (2006), Dunn Caveltys (2008) og Deiberts (2013) kritiske framing-analyser af de interesser, der ligger bag fokuset på terroristers onlineadfærd.

3. Når forskningen ikke er præget af stærke konklusioner vedrørende terroristers brug af internettet, skyldes det blandt andet vanskelighederne ved at indsamle og fortolke empiri fra internettet. Gemmerli (2015) påpeger eksempelvis, hvorledes nettet er spækket med evigt foranderlige pseudonymer og multifacetterede identiteter, som ikke nødvendigvis afspejles i handlinger/holdninger udenfor de lukkede, semilukkede eller åbne onlinefora. Dette gør enhver systematisk empiriindsamling vanskelig, hvorfor det kan være problematisk at konkludere og generalisere ud over de konkrete cases.
4. Artiklen undersøger udelukkende internettet og cyberspace i relation til terrorisme forstået som den politisk motiverede, *fysiske* vold mod civile med henblik på at skabe frygt i en befolkning.
5. Med "organisering" menes *ikke* brugen af onlinebanking eller flybooking. Artiklen orienterer sig derimod mod onlineaktiviteter vedrørende organiseringen og koordineringen af hvor, hvordan og hvornår et angreb skal finde sted.
6. Inddragelsen af LulzSec og AntiSec i relation til diskussionen af (cyber)terrorisme er ikke ensbetydende med, at Anonymous bekender sig til terrorisme som strategi. Det gør de ikke (Coleman, 2014). Derimod virker eksemplerne fra LulzSec ogAntiSec som en illustration af, at amatørhackere og hacktivitster – selv hvis de ville – har vanskeligt ved for alvor at våbenliggøre cyberspace.
7. Enhver analyse af soloterrorisme udfordres af et begrænset antal cases. Artiklen anerkender generaliseringsudfordringerne, men tillader sig at påpege, at Breivikcasen – når den relateres til andre ensomme ulve og det større antal foreign fighters, som søger mod fysiske fællesskaber – peger i retning af, at fremtidige undersøgelser af relationen mellem cyberspace og soleterrorisme bør have for øje, at internettet ikke nødvendigvis udgør et rationelt, taktisk redskab.
8. Inspireret af Thomas Rid (2012: 37) defineres cybervåben som en computerkode, der kan bruges til at forårsage eller true med at forårsage fysisk, funktionel eller mental skade på strukturer, systemer eller levende individer. Artiklen inddrager dog ikke "mental skade" som en del af diskussionen om våbenliggørelsen af computerkoder.
9. Anonymous er per definition umulige at karakterisere. Alle, der kalder sig Anonymous, er Anonymous, og intet afholder en politisk motiveret voldsudøver fra at kalde sig Anonymous. Colemans (2014) omfattende studier af Anonymous' mange ansigter viser dog, at politisk vold ikke indgår som en del af Anonymous' oprindelige selvforståelse.
10. Her inddrages Anonymous-udbrydergrupperne *ikke* som "terrorgrupper", men som en illustration af de mest it-kyndige aktivister.
11. *Distributed-Denial-of-Service* (DDoS) er en oversvømmelsen af en server med trafik i forsøget på at gøre den midlertidig utilgængelig.

Litteratur

AQAP (2010). Special Issue. *Inspire*, november.

Archetti, Cristina (2015). Terrorism, communication and new media: explaining radicalization in the digital age. *Perspectives on Terrorism* 9 (1): 49-59.

Awan, Akil (2007). Radicalization on the Internet? *RUSI Journal* 152 (3): 76-81.

Behnke, Andreas (2004). Terrorising the political: 9/11 within the context of the globalisation of violence. *Millennium* 33: 279-312.

Behnke, Andreas (2014). Dressed to kill: the sartorial code of Anders Behring Breivik, i Sue Malvern og Gabriel Koureas (red.), *Terrorist Transgressions. Gender and the Visual Culture of the Terrorist*. London: I.B. Tauris.

Benson, David (2014). Why the Internet is not increasing terrorism. *Security Studies* 23 (2): 293-328.

Betz, David og Tim Stevens (2011). *Cyberspace and the State – towards a Strategy for Cyber-power*. Oxon: Routledge.

Bigo, Didier, Laurent Bonelli, Emmanuel-Pierre Guittet og Francesco Ragazzi (2014). *Preventing and countering youth radicalisation in the EU*. LIBE committee study, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/509977/IPOL-LIBE_ET(2014)509977_EN.pdf (5. marts 2015).

Borchgrevink, Aage (2013). *A Norwegian Tragedy*. Cambridge: Polity.

Borum, Randy (2011). Radicalization into violent extremism II. *Journal of Strategic Security* 4(4) : 36-62.

Breivik, Anders (2011). *2083 – A European Declaration of Independence*, http://publicintelligence.net/anders-behring-breiviks-complete-manifesto-2083-a-european-declaration-of-independence/ (5. marts 2015).

Brunst, Phillip (2010). Terrorism and the Internet: new threats posed by cyberterrorism and terrorist use of the Internet, i Philip Brunst (red.), *A War on Terror?* Heidelberg: Springer.

Böckler, Nils, Thorsten Seeger og Wilhelm Heitmeyer (2011). School shootings: a double loss of control, i Wilhelm Heitmeyer, Heinz-Gerhard Haupt, Andrea Kirschner og Stefan Malthaner (red.), *Control of Violence*. New York: Springer.

Cabinet Office (2010). *The National Security Strategy*. London: Crown Copyright.

Chen, Thomas, Lee Jarvis og Stuart Macdonald (red.) (2014). *Cyberterrorism – Understanding, Assessment, and Response*. New York: Springer.

Clarke, Richard og Robert Knake (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins.

Coleman, Gabriella (2013). Anonymous in context: the politics and power behind the mask, *Internet Governance Papers*.

Coleman, Gabriella (2014). *Hackers, Hoaxer, Whistleblower, Spy. The Many Faces of Anonymous*. London/New York: Verso.

Coll, Steve og Susan Glasser (2005). Terrorists turn to the web as base of operations. *Washington Post*, 7. august, http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html (5. marts 2015).

Conway, Maura (2014). Reality check: assessing the (un)likelihood of cyberterrorism, i Thomas Chen, Lee Jarvis og Stuart Macdonald (red.), *Cyberterrorism – Understanding, Assessment, and Response*. New York/Heidelberg: Springer.

Crone, Manni (2014). Religion and violence: governing muslim militancy through aesthetic assemblages. *Millennium* 43(1): 291-307.

Deibert, Ronald J. (2013). *Black Code: Surveillance, Privacy and the Dark Side of the Internet*. Toronto: Signal.

Denning, Dorothy (2000). Cyberterrorism: the logic bombs versus the truck bomb. *Global Dialogue* 4(2).

Denning, Dorothy (2007). A view of cyberterrorism five years later, i Kenneth Himma (red.) *Internet Security: Hacking, Counterhacking, and Society*. Sudbury: Jones and Bartlett.

Dodd, Vikram (2010). Roshonara Choudhry: police interview extracts, *Guardian*, 3. november, http://www.theguardian.com/uk/2010/nov/03/roshonara-choudhry-police-interview (5. marts 2015).

Dunn Cavelty, Myriam (2008). Cyber-terror – looming threat or phantom menace? *Journal of Information Technology & Politics* 4 (1): 19-36.

EU Cybersecurity Strategy (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Bruxelles, 7. februar.

FBI (2010). The cyber threat – using intelligence to predict and prevent. *FBI.gov*, 3. april, http://www.fbi.gov/news/stories/2010/march/cyberintel030410 (5. marts 2015).

FBI (2012). *Final Report on the William H. Webster Commission on the Federal Bureau of Investigation, Counterterrorism Intelligence*. http://www.fbi.gov/news/pressrel/press-releases/final-report-of-the-william-h.-webster-commission (5. marts 2015).

Gemmerli, Tobias (2014). *Online-radikalisering: et uafklaret begreb. Litteraturreview af definitioner og tilgange inden for online-radikalisering* (del 1 af 3), DIIS Rapport 7, København: DIIS.

Gemmerli, Tobias (2015). *Online-radikalisering: forebyggelse på internettet*. DIIS Rapport 3, København: DIIS.

Gertz, Bill (2014). Al-Qaida targeting U.S. infrastructure for digital 9/11. *The Washington–Free Beacon*, 25. juli, http://freebeacon.com/national-security/al-Qaida-targeting-u-s-infrastructure-for-digital-911/ (5. marts 2015).

Hansen, Stig Jarle (2013). *Al-Shabaab in Somalia: The History and Ideology of a Militant Islamist Group, 2005*-2012. New York: Oxford University Press.

Hegghammer, Thomas (2013). The recruiter's dilemma: signalling and rebel recruitment tactics. *Journal of Peace Research* 50 (3): 3-16.

Helfstein, Scott (2012). *Edge of Radicalization: Individuals, Networks and Ideas in Violent Extremism, Countering Terrorism Center*, https://www.ctc.usma.edu/posts/edges-of-radicalization-ideas-individuals-and-networks-in-violent-extremism (5. marts 2015).

Hemmingsen, Ann-Sophie (2011). Individualismens terrorisme, i Lars Erslev Andersen, Manni Crone, Peter Hansen, Ann-Sophie Hemmingsen, Ulla Holm, Søren Hove og Leila Stockmarr (red.), *Ti år efter 11. september 2011 – tilbageblik, status og aktuelle tendenser*. København: DIIS.

Hoffman, Bruce (2006). The use of the Internet by Islamic extremists. Testimony presented to the House Permanent Select Committee on Intelligence, 4. maj.

Holt, Thomas (2012). Exploring the intersections of technology crime, and terror. *Terrorism and Political Violence* 24 (2): 337-354.

Hoskins, Andrew og Ben O'Loughlin (2009). Media and the myth of radicalization. *Media, War & Conflict* 2 (2): 107-110.

Hua, Jian og Sanjay Bapna (2012). How can we deter cyber terrorism? *Information Security Journal* 21: 102-114.

Jacobsen, Jeppe T. (2014). Clausewitz and the utility of cyberattacks in war. *International Journal of Cyber Warfare and Terrorism* 4(4): 1-16.

Jones, Bryony (2012). French attacks could inspire next generation of terrorists. *CNN*, 22. marts, http://edition.cnn.com/2012/03/21/world/europe/lone-wolf-future-of-terrrorists/index.html (5. marts 2015).

July 7th People's Independent Inquiry Forum (2009). Waseem Mughal and Younis Tsouli incl., http://z13.invisionfree.com/julyseventh/ar/t1770.htm (5. marts 2015).

Kenney, Michael (2010). Beyond the Internet: metis, techne, and the limitations of online artifacts for Islamist terrorists. *Terrorism and Political Violence* 22 (2): 177-197.

Kibar, Omar (2014). Virushandlerne. *Weekendavisen*, 9. maj.

Kirkhope, Timothy og Charles Tannock (2015). Motion for a resolution, European Parliament – Plenary Sitting, 4. februar, B8-0126/2015.

Knake, Robert (2010). Untangling attribution: moving beyond accountability in cyberspace. Prepared statement, Council for Foreign Relations.

Kushner, David (2014). The masked avengers: How Anonymous incited online vigilantism from Tunisia to Ferguson. *New Yorker*, 8. september.

Lachow, Irving (2009). Cyber terrorism: menace or myth?, i Franklin Kramer, Stuart Starr og Larry Wentz (red.), *Cyberpower and National Security*. Washington DC: National Defense University Press.

Langner, Ralph (2013). Stuxnet's secret twin. *Foreign Policy*, 19. november.

Lenning, Christopher, Krestina Amon, Heidi Brummert og Nicholas Lennings (2010). Grooming for terror: the Internet and young people. *Psychiatry, Psychology and Law* 17 (3): 424-437.

Lindsey, Jon (2013). Stuxnet and the limit of cyber warfare. *Security Studies* 22(3): 365-404.

Mansfield-Devine, Steve (2011a). Anonymous: serious threat or mere annoyance. *Network Security* 12 (1): 1-10.

Mansfield-Devine, Steve (2011b). Hacktivism: assessing the damage. *Network Security* 12 (8): 1-13.

Marcus, Jonathan (2015). US Centcom Twitter account hacked by pro-IS group. *BBC*, 12. januar, http://www.bbc.com/news/world-us-canada-30785232 (5. marts 2015).

Matusitz, Jonathan (2008). Cyberterrorism: postmodern state of chaos. *Information Security Journal* 17: 179-187.

McCant, Will (2008). More on online recruitment. *Jihadica*, 18. september og 14. oktober, http://www.jihadica.com/?cat=89 (5. marts 2015).

McFarlane, Bruce (2010). Online violent radicalisation (OVeR): Challenges facing law enforcement agencies and policy stakeholders, conference paper, http://artsonline.monash.edu.au/radicalisation/files/2013/03/conference-2010-online-violent-radicalisation-bm.pdf (5. marts 2015).

McGraw, Gary og Nathaniel Fick (2011). Separating the threat from the hype: what Washington needs to know about cyber security, kapitel 3 i Kristin M. Lord og Travis Sharp (red.), *America's Cyber Future: Security and Prosperity in the Information Age*. Washington DC: Center for a New American Security.

Melle, Ingrid (2013). The Breivik case and what psychiatrists can learn from it. *World Psychiatry* 12 (1): 16-21.

Molfino, Emily (2012). VIEWPOINT: Cyberterrorism: Cyber "Pearl Harbor" is Imminent, i Sean Costigan og Jake Perry (red.), *Cyberspaces and Global Affairs*. Farnham: Ashgate Publishing Limited.

Mueller, Robert (2013). FBI Director fears 9/11-style attack on US. *SkyNews*, 23. august, http://news.sky.com/story/1132290/fbi-director-fears-9-11-style-attack-on-us (5. marts 2015).

Nesser, Petter (2008). How did Europe's global jihadis obtain training for their militant causes? *Terrorism and Political Violence* 20 (2): 234-256.

Ogun, Mehmet (2012). Terrorist use of the Internet. *Journal of Applied Security Research* 7 (2): 203-217.

Olsen, Jon (2014). Trusselsbilledet – fra dommedagsprofeter til ensomme ulve, i Lars Erslev Andersen (red.), *Terrorisme og trusselsvurderinger*. København: DIIS.

Olson, Parmy (2013). *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous and the Global Cyber Insurgency*. London: RandomHouse.

Pantucci, Raffaello (2011). What have we learned about lone wolves from Anders Behring Breivik? *Perspectives on Terrorism* 5 (5-6): 27-42.

Pisoiu, Daniela (2013). Theoretische Ansätze zur Erklärung individueller Radikalisierungsprozesse: eine kritische Beurteilung und Überblick der Kontroversen. *Journal EXIT-Deutschland* 1: 41-87.

Ravndal, Jacob (2013). Anders Behring Breivik's use of the Internet and social media. *Journal EXIT-Deutschland* 2: 172-185.

Redins, Larisa (2012). Understanding cyberterrorism. *Risk Management* 59 (8): 32-35.

Regeringen (2014). Forebyggelse af ekstremisme og radikaliseringen – Regeringens handlingsplan.

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

Rid, Thomas og Peter McBurney (2012). Cyber-weapons. *RUSI Journal* 157(1): 6-13.

Ritzau (2015). Efterforskningskilder: Terrormistænkt trænede med al-Qaeda i Yemen. *Politiken*, 9. januar, http://politiken.dk/udland/int_europa/ECE2505758/efterforskningskilderterrormistaenkt-traenede-med-al-qaeda-i-yemen/ (5. marts 2015).

RwB, Reports without Borders (2014). Areas controlled by Islamic State are news "black holes", 23. oktober, http://en.rsf.org/iraq-areas-controlled-by-islamic-state-23-10-2014,47147.html (5. marts 2015).

Rådet for den Europæiske Union (2015). *Council Conclusions on Cyber Diplomacy*, 6122/15, Bruxelles, 11. februar.

Sandberg, Sveinung (2013). Are self-narratives strategic or determined, unified or fragmented? *Acta Sociologica* 56: 69-83.

Sandelson, Michael og Lyndsey Smith (2013). Oslo government headquarters building fate due to new review. *The Foreigner*, 20. september, http://theforeigner.no/pages/news/oslo-government-headquarters-building-fate-due-for-new-review/ (5. marts 2015).

Sanger, David (2012). *Confront and Conceal*. New York: RandomHouse.

Saunders, Doug (2014). When troubled young men turn to terror, is it ideology or pathology? *The Global and Mail*, 24. oktober, http://www.theglobeandmail.com/news/national/lone-wolf-ideology-or-pathology/article21293910/ (5. marts 2015).

Seierstad, Åsne (2013). *En av oss – en fortelling om Norge*. Oslo: Kagge.

Singer, Peter og Allan Friedman (2014). *Cybersecurity and Cyberwar – What Everyone Needs To Know*. Oxford: Oxford University Press.

Smith, Graham (2012). Hacking group Anonymous could shut down the entire U.S. power grid, head of national security warns. *DailyMail*, 22. februar, http://www.

dailymail.co.uk/news/article-2104832/Hacking-group-Anonymous-shut-entire-U-S-power-grid-head-national-security-warns.html (5. marts 2015).
Spaaij, Ramon (2010). The enigma of lone wolf terrorism. *Studies in Conflict & Terrorism* 33 (9): 854-870.
Speri, Alice (2014). Now even ISIS has its own whistleblower, 20. juni, https://news.vice.com/article/now-even-isis-has-its-very-own-whistleblower (5. marts 2015).
Stenersen, Anne (2008). The Internet: a virtual training camp? *Terrorism and Political Violence* 20(2): 215-233.
Stohl, Michael (2006). Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot game? *Crime, Law and Social Change* 46: 223-238.
Syse, Aslak (2014). Breivik – the Norwegian terrorist case. *Behavioural Science and Law* 32: 389-407.
The 9/11 Commission Report (2004). National Commission on Terrorist Attacks Upon the United States. Washington DC: Government Printing Office.
Thompson, Robin (2011). Radicalization and the use of social media. *Journal of Strategic Studies* 4 (4): 167-190.
Thyssen, Ole (2015). Var Omar El-Hussein blot morder, eller var han terrorist? *Politiken*, 18. februar.
UNODC (2012). *The Use of the Internet for Terrorist Purposes*. Publishing and Library Section, UN Office at Vienna.
Verton, Dan (2003). *Black Ice – The Invisible Threat of Cyber-Terrorism*. Emeryville: McGill-Hill Companies.
Walsh, Eddie (2012). VIEWPOINT: an alternative perspective on cyber anarchy for policy-makers, i Sean Costigan og Jake Perry (red.), *Cyberspaces and Global Affairs*. Farnham: Ashgate Publishing Limited.
Weimann, Gabriel (2004). *Cyberterrorism: How Real is the Threat?* United States Institute of Peace Special Report.
Weimann, Gabriel (2006). *Terror on the Internet*. Washington DC: The Endowment of the United States Institute for Peace.
Weimann, Gabriel (2010). Terror on Facebook, Twitter and Youtube. *Brown Journal of World Affairs* 16 (2): 45-54.
Weimann, Gabriel (2012). Lone wolves in cyberspace. *Journal of Terrorism Research* 3 (2): 76-90.
Wikotorowicz, Q. (2005). *The State of Global Jihad Online – A Qualitative, Quantitative, and Cross-Lingual Analysis*. Oxford: Rowman & Littlefield.
Wilson, Clay (2014). Cyber threats to critical information infrastructure, i Thomas Chen, Lee Jarvis og Stuart Macdonald (red.), *Cyberterrorism – Understanding, Assessment, and Response*. New York/Heidelberg: Springer.

Woolford, Thomas og Jonathan Matusitz (2013). Cyberterrorism group Anonymous at the forefront of research. *Extremist Project*, 13. februar, http://extremisproject.org/2013/02/cyberterrorism-group-anonymous-at-forefront-of-research (5. marts 2015).
Wright, Lawrence (2006). *The Looming Tower – Al-Qaida and the Road to 9/11*. New York: Alfred A. Knopf.
Zelin, Aaron (2013). The state of global Jihad online. *New American Foundation*, januar, http://www.newamerica.net/sites/newamerica.net/files/policydocs/Zelin_Global%20Jihad%20Online_NAF.pdf (5. marts 2015).