DIIS REPORT 2015: 03

ONLINE-RADIKALISERING

Forebyggelse på internettet

Denne rapport er skrevet af Tobias Gemmerli og udgivet af DIIS.

Tobias Gemmeri, videnskabelig assistent på DIIS

DIIS · Dansk Institut for Internationale Studier
Østbanegade 117, København Ø
Telefon 32 69 87 87
Email: diis@diis.dk
www.diis.dk

Layout: Lone Ravnkilde & Viki Rachlitz
Forsideillustration: Pawel Kuczynski
Trykt i Danmark af Eurographic Danmark
ISBN 978-87-7605-741-1 (pdf)
ISBN 978-87-7605-742-8 (Print)

DIIS publikationer kan downloades gratis eller bestilles fra www.diis.dk

Indhold

ABSTRACT

Radikaliseringsforebyggelsens søgen efter terrorister in spe har de seneste år taget stadig mere avancerede metoder i brug. Den ekstremistiske propagandas udbredelse på internettet har medført en række bløde og hårde forebyggelsestiltag. Senest er kvantitative analyser af de præradikaliserede unges færden på internettet også begyndt at vinde frem. De kvantitative metoder kan bistå myndighederne i den direkte terrorbekæmpelse, men de har også til hensigt at pege forebyggelsesindsatsen i retning af de mest radikaliseringssårbare unge og dermed styrke 'den tidlige indsats'.

Metoderne beskrives ofte som en teknologisk avanceret forlængelse af allerede eksisterende forebyggelsestilgange såsom censur, overvågning og forskellige former for modnarrativer. Men metoderne fremhæves også som en ny teknologi, der skal gøre det muligt for myndighederne at finde frem til de behandlingsegnede og radikaliseringstruede sårbare unge. De kvantitative tilgange fortrænger dog, deres højt avancerede algoritmer til trods, en række ubesvarede spørgsmål i radikaliseringsteorien og bygger videre på en uholdbar forestilling om 'profilering' af terrorister eller radikaliserede unge.

Rapporten kaster et kritisk lys på denne nye forebyggelseslitteratur ved først kort at gennemgå den eksisterende online-forebyggelse for dernæst at gennemgå de beregningsmæssige og kvantitative tilgange. Afslutningsvist betragter rapporten litteraturen gennem et kritisk radikaliseringsteoretisk prisme.

Rapporten bygger videre på Gemmerlis øvrige rapporter om online-radikalisering. For en mere tilbundsgående analyse og diskussion af litteraturens definitoriske spørgsmål og antagelser henvises til Gemmerli 2014a. For en gennemgang af de gennerelle skillelinjer i litteraturen om online-radikalisering henvises til Gemmerli 2014b.

Forkortelser og ordforklaringer

AFFECT ANALYSIS	Indholdsanalyse rettet mod at analysere og ekstrahere tendenserne i følelsesmæssige udbrud og holdninger på fx sociale medier.
ALIAS MATCHING	Computerprogrammer, der er i stand til at genkende ligheder i forskellige brugerprofilers tekstopdateringer og derved koble forskellige konti til samme bruger.
ALGORITME-CENSUR	Søgemaskine-algoritmer (computerkoder), der rangerer søgeresultaterne ud fra en skjult prioritering af politisk korrekt indhold.
AUTHOR RECOGNITION	Se alias matching.
AVE	Against Violent Extremism network er et Google ideas-baseret netværk under ledelse af Institute for Strategic Dialogue (ISD), der vha. nye teknologier arbejder på at påvirke alle former for voldelig ekstremisme.
BAG OF WORDS	Begreb fra indholdsanalysen. En ordliste anvendt af tekstanalyseprogrammer, der automatisk identificerer de mest anvendte ord eller ordpar i store mængder online-tekst for at kunne klassificere tekststykker efter analyserelevant indhold.
BETWEENNESS CENTRALITY	Begreb fra netværksanalysen. Angiver online-aktørers evner til at forbinde klynger af netværk og derved fungere som bro mellem forskellige online-fællesskaber.
DARK WEB	Den del af internettet, der ikke er indekseret eller kortlagt af søgemaskiner.
DATA MINING	Søgning i mønstrer og strukturer i større datamængder.
DATA NUDGING	Nudging er forsøg på med positive og ofte indirekte tilskyndelse at påvirke menneskers adfærd. Data nudging bruges i denne rapport synonymt med algoritme-censur som betegnelse for manipulation af online-indhold, så brugere ubevidst påvirkes til en mere politisk korrekt onlineadfærd.
DDOS-ANGREB	Distributed denial of service-angreb. En hjemmeside eller server oversvømmes af henvendelser, indtil den ikke længere er tilgængelig, eller serveren overbelastes.

DISCRIMINANT WORD LEXICON	Se bag of words.
DNS	Domain Name Server er den internetserver, hvor IP-adressen kobles til et domænenavn.
DNS-HIJACKING	Manipulerer serveren med adressekartoteket, så domænenavnet ikke længere henviser til den rigtige adresse. I stedet kan hijackerne henvise til en fejlside eller en forfalsket klon.
DYNAMISK FILTRERING	Analyserer hele datatrafikken i realtid på udkig efter sortlistede ord for herefter at blokere den ulovlige trafik.
FLAGGING	En slags brugerdrevet censur, hvor brugere af de sociale medier får mulighed for at angive eventuelle brud på brugerbetingelserne til serviceudbyderne, som derefter kan vælge at lukke ned for de indklagede brugerprofiler eller sætte dem i karantæne.
FOI	Totalförsvarets forskninginstitut, Stockholm Universitet.
FREMMEDKRIGERE	Betegnelse for statsborgere, som drager til et andet land for at tilslutte sig oprørs- eller terrorbevægelser i en væbnet kamp med et fremmed lands herskende styre eller andre grupperinger.
GEODÆTISKE STIER (el. geodætiske linjer)	Forbindelserne mellem noder.
HACKTIVISME	Når politiske eller sociale forandringer søges opnået gennem (ofte illegitime) internetdrevne angreb, såsom DDoS.
HYPERLINK	En tekst på en internetside, som ved klik leder brugeren videre til en ny internetside.
ICSR	The International Centre for the Study of Radicalisation and Political Violence (King's College).
INDHOLDSFILTRERING	Se dynamisk filtrering.
IP	Internet Protocol. IP-adresse er et nummer, som computere bruger til at kommunikere med hinanden over internetprotokollen. Alle computere eller netværksenheder skal have deres egen adresse.
ISP	Internet Service Provider (internetudbyder).

ISP-FILTRERING	Den censurerende router (Internet Service Provider) sammenligner IP-adressen med en liste over sortlistede adresser. Adgangen nægtes, hvis IP-adressen står på listen.
KORPUSLINGVISTIK	Tekstanalyseteknikker, som analyserer en tekstsamling (tekstkorpus).
KORRELATION	Et statistisk mål for graden af samvariation mellem to variabler.
LONGITUDINALE	Målinger eller analyser over længere tid.
MORAL DISENGAGEMENT	En teori om en psykologisk proces, hvor individer fraviger deres naturlige eller indre moral eller kontrol, hvorved voldelige handlinger bliver mulige.
NODE	Knudepunkter i et netværk. Fx kan en brugerprofil i et netværk af facebookbrugere betegnes som en node
NODECENTRALITET	Begreb fra netværksanalyse. Angiver online-aktørers popularitet i et netværk – fx hvor mange direkte forbindelser de har til andre aktører i netværket.
NØGLEDATA (seeds)	Ekspertudvalgte noder (fx nøglepersoner) i et netværk, der fungerer som afsæt eller udgangspunkt for en netværksanalyse, der optrevler de ekspertudvalgte noders forbindelser til andre noder.
OFFENSIVE CYBERSTRATEGIER	Finder og udnytter fejl og sårbarheder i fjendens it-systemer.
OPINION MINING	Holdnings- og meningsanalyse i netværk.
METHODS	Forskellige teknikker til indholdsanalyse, der forsøger at uddrage dynamikkerne omkring holdnings- og meningsdannelse i sociale netværk. Analysen kan særligt være rettet mod at lokalisere individer med markante og kontroversielle holdninger til et bestemt emne.
OSINT	Open Source Intelligence. Offentligt tilgængelige informationskilder.
PALANTIR TORCH	Et data mining og netværksanalyseprogram, som blandt andet er udviklet af CIA.
PaVE	People against Violent Extremism. Australsk NGO, som står bag online-kampagnen Walk Away from Violent Extremism (WAVE).
PROFILERING (ifm. radikalisering)	Udkrystallisering af mønstre i adfærd og holdning, som kan siges at karakterisere radikalisering og voldelig ekstremisme.

RADIKALISATOR	Ideen om en radikaliserende agent, som gennem sin påvirkning på unge får dem til at ændre holdning og adfærd.
RELIABILITET (pålidelighed)	Garanteres ved at sikre, at analyser afstedkommer konsistente og gentagelige resultater.
REPRÆSENTATIVITET	Angiver om analysen afdækker en bagvedliggende social realitet og kan styrkes ved at holde analyseresultaterne op mod sammenlignelige studier.
SENTIMENT ANALYSIS	Se opinion mining methods.
SNOWBALLING (el. snowball sampling)	En ikke-probabilistisk teknik til at opbygge et datasæt ved fx at tage udgangspunkt i ekspertudvalgte nøgledata og via linkstrukturen optrevle et netværk.
SPURIØS (el. spuriøs sammenhæng)	Når det, som ligner en sammenhæng mellem to variabler i virkeligheden blot er et sammenfald, der enten skyldes tilfældigheder eller at begge variabler påvirkes af den samme mellemliggende variabel.
TAKEDOWNS	Fjernelse af ekstremistisk indhold fra nettet eller besværliggørelse af tilgangen hertil.
TATA	Think Again Turn Away er en online modnarrativkampagne, som det amerikanske udenrigsministerium står bag.
TEKST-MINING	Se data mining.
THE PIRATE BAY	En svensk fildelingstjeneste, hvor ophavsretsbeskyttet indhold blev delt.
TOR-BROWSERE	En gratis software, der beskytter mod overvågning af internettrafikken.
TROLLING	Når en debattrådsdeltager obstruerer en verserende debattråd ved at overlæsse den med information og hånlige kommentarer.
TÆTHED (density)	Begreb fra netværksanalyse. Statistisk mål for hvor tæt forbundet noderne i et netværk er, dvs. antallet af faktiske forbindelser holdt op mod antallet af mulige forbindelser.
URL-NODER	En URL (Uniform Resource Locator) beskriver adressen for en bestemt ressource eller node på internettet.
VALIDITET	Den statistiske validitet angiver, hvor godt målinger, koncepter og konklusioner stemmer overens med den virkelighed, de forsøger at beskriver.

WARNING BEHAVIOUR	Advarselsadfærd og bekymringssignaler, som angiver 'farligheden' af en bestemt online-bruger.
WAVE	Walk Away from Violent Extremism er en online-kampagne lanceret af den australske NGO People against Violent Extremism (PaVE).
WEB CRAWLING	Se snowballing.
ØKOLOGISK FEJLSLUTNING	Hvis der fejlagtigt sluttes fra et aggregeret niveau (gruppeadfærd) til individniveau (individuel adfærd).

ONLINE-RADIKALISERING OG FOREBYGGELSE

Blodig videopropaganda, meningsudvekslinger med ekstremistiske grupperinger og realtidsopdateringer fra nutidens konfliktzoner. Ekstremister og terrorister erobrer stadig større dele af det åbne internet, og ekstremismens budskaber er blevet en del af unge menneskers online-liv. Den øgede tilgængelighed skaber samtidig bekymring for en tiltagende radikalisering blandt unge internetbrugere med ekstremistisk vold og terror som de ultimative konsekvenser heraf.[1] Animeret af de ekstremistiske grupperingers aktiviteter på sociale medier har diverse forskningsdiscipliner og videnskabelige traditioner derfor budt ind med forskellige forklaringer på den potentielle radikalisering af unge mennesker via de sociale medier.[2] Til trods for den store forskningsmæssige uenighed om såvel radikalisering som internettets indflydelse herpå har mange forskere og policy-skribenter alligevel valgt at sammenstille de to fænomener under betegnelsen online-radikalisering.[3]

Ekstremismens udbredelse på de sociale medier har tilmed skænket forskningsverdenen en hel urskov af empiri, som før ikke var så direkte tilgængelig. Forskere og metodeudviklere er således, den manglende konsensus til trods, begyndt at applicere avancerede beregningsmæssige og kvantitative metoder til sporing, kortlægning og analyse af "cyberekstremisme", "hadpropaganda på nettet" eller "online-radikalisering" – som det kaldes i flæng.[4] Grebet af empiriens forøgede

1 Se eksempel på bekymring og "call to action": Nouri & Whiting (2015: 175).

2 Gemmerli, 2014a; Gemmerli, 2014b.

3 For en mere uddybende diskussion af begrebet online-radikalisering henvises til første og anden rapport i denne serie af litteraturreview af definitioner og tilgange inden for online-radikalisering: Gemmerli (2014a) og Gemmerli (2014b).

4 Correa & Sureka, 2013: 2.

tilgængelighed har en lang række forskere med afsæt i en bred vifte af videnskabelige discipliner fremsat forskellige teknologiske løsninger til håndtering af ekstremismeudfordringen. Spørgsmålet bliver da mere præcist, hvorledes ekstremistisk adfærd på nettet kan monitoreres og informationerne anvendes.[5] Herved er et definitionsproblem (hvad er online-radikalisering?) blevet fortrængt af et operationaliseringsproblem (hvordan kan vi måle sårbare unges radikaliseringsrisiko ud fra deres adfærd på internettet?).[6]

Det teknologiske fix er forlokkende, men det fortrænger væsentlige videnskabelige spørgsmål og risikerer at sende forebyggelsespolitikken ud på et uheldigt sidespor.

De nye beregningsmæssige og kvantitative tilgange til forebyggelse af online-radikalisering beskrives som teknologisk avancerede udvidelser af eksisterende forebyggelsesindsatser såsom censur, overvågning og forskellige former for modnarrativer. Stadig oftere beskrives teknologierne dog også som selvstændige bud på metoder, der skal gøre det muligt for myndighederne mere effektivt at finde frem til radikaliseringstruede og behandlingsegnede sårbare unge.

Fænomenets mange synonymer afslører, at det som oftest er ytringernes ideologiske og antagonistiske markeringer, der lægges til grund for analysernes algoritmer. I jagten på en brugbar operationalisering til anvendelse for de bredspektrede kvantitative tilgange lokker radikaliseringsteoriernes mest simple og monokausale modeller med hurtige svar og lette løsninger. Ideen om forebyggelse ved brug af kvantitative metoder foretager derfor ofte en implicit kobling fra ideologisk radikalisering til voldelig handling.[7] Problemet er dog, at radikaliseringens mange ubekendte elementer blot fortrænges til fordel for komplekse netværksvisualiseringer og avancerede computeralgoritmer. Det teknologiske fix er forlokkende, men det fortrænger væsentlige videnskabelige spørgsmål og risikerer at sende forebyggelsespolitikken ud på et uheldigt sidespor. Den nye tendens inden for forebyggelseslitteraturen stiller derfor forskningen over for en lang række metodiske, etiske og videnskabsteoretiske spørgsmål, som endnu savner et klart svar.

5 Neumann, 2013: 452.

6 Morozov, 2014b: 5.

7 se mere i Gemmerli (2014a).

Ikke desto mindre har den danske radikaliseringsforebyggelse allerede rettet et skarpt blik mod, hvad der foregår på internettet. I en ny handlingsplan til forebyggelse af radikalisering og ekstremisme fra september 2014 introducerer SR-regeringen således en række nye værktøjer til at imødegå problemet med online-radikalisering.[8] Her lægges op til øget monitorering, internationalt samarbejde, online-baseret undervisning i kritisk internetbrug samt online-kampagner, "hvor der bliver sat spørgsmålstegn ved ekstremistisk propaganda og fremstillet andre måder at betragte verden på".[9]

Den nye danske handlingsplan ligger i forlængelse af policy-tendenser andre steder i verden. Det Hvide Hus i Washington nedsatte allerede i februar 2013 en arbejdsgruppe med specifikt fokus på online-radikalisering under ledelse af Quintan Wiktorowicz;[10] forfatteren til den hyppigt citerede Radical Islam Rising (2005) og ophavsmand til en af de første policy-konceptualiseringer af radikaliseringsbegrebet. Senest har Det Hvide Hus lanceret online-kampagnen "Think Again Turn Away"[11] på de sociale medier.

En gammel drøm om at kunne profilere terroristen har nu fået ny næring. Denne gang er det dog den sårbare og radikaliseringstruede normalitetsafviger, som er kommet i fantomtegnernes søgelys.

Ud over en fornyet indsats med modnarrativer i forskellige medier er fokus også skiftet til nye former for censurering af online-indhold, hvor myndighederne indgår i strategiske samarbejder med udbydere af sociale netværkstjenester og inddrager brugerne af disse tjenester som frivilligt værn, der anmelder stødende indhold. Dermed er der åbnet op for en udefinerbar gråzone mellem private udbydere af forskellige netværkstjenester, deres brugere og visse myndigheders ønsker om overvågning og censur af online-indhold.

En RAND EUROPE-rapport om online-radikalisering fra 2013 kom således med følgende anbefaling: "The police and relevant agencies might require closer relationships in the future with companies such as Facebook and Google to assist

8 Regeringen, 2014: 12.

9 ibid.

10 http://www.whitehouse.gov/blog/2013/02/05/working-counter-online-radicalization-violence-united-states

11 https://twitter.com/ThinkAgain_DOS

them in identifying red flags for vulnerable individuals" (Behr et al., 2013: 34). Hvad "røde flag" og "sårbarhed" over for online-radikalisering mere præcist betegner, er endnu et åbent spørgsmål. Men flere forskere fokuserer på de potentielle muligheder for forebyggelse af terrorisme ved mere systematisk at søge efter disse røde flag.[12] En gammel drøm om at kunne profilere terroristen har nu fået ny næring. Denne gang er det dog den sårbare og radikaliseringstruede normalitetsafviger, som er kommet i fantomtegnernes søgelys. Selv en af radikaliseringsbranchens all-stars og leder af The International Centre for the Study of Radicalisation and Political Violence (ICSR), Peter Neumann, har forskningsinteressen rettet mod netop internettets rolle:

> "The importance of extending counterradicalization into cyberspace is beyond question. The use of the Internet to radicalize and recruit homegrown terrorists is perhaps the single most important and dangerous novelty since the terrorist attacks of 11 September 2001.[13] "

Der er altså pres fra flere sider for at imødegå online-radikalisering, og indeværende rapport har således som overordnet formål at skabe overblik over den spirende nye forebyggelseslitteratur. Rapporten søger at besvare spørgsmålene: hvad er de grundlæggende rationaler bag ideen om forebyggelse af online-radikalisering, hvordan bidrager de kvantitative metoder hertil, og hvordan afspejler denne forebyggelsestanke sig i den øvrige litteratur om radikalisering? Rapporten er i udgangspunktet eksplorativ og redegørende, men den tager samtidig afsæt i den kritiske tradition inden for terror- og radikaliseringsforskning. Rapporten lægger således hovedvægten på en teori- og metodeintern diskussion og kritik, men det vil også enkelte steder blive tydeligt, at kritikken delvist har grund i en poststrukturalistisk analysetradition.[14]

12 Holbrook et al., 2013: 203.

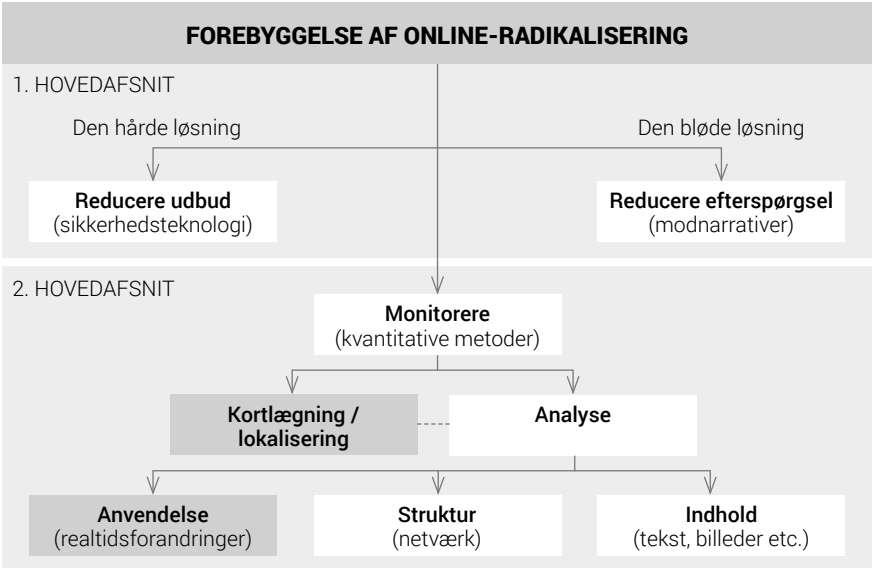
13 Neumann, 2013: 453.

14 Den poststrukturalistiske tradition inden for radikaliserings- og terrorforskning har ofte afsæt i videnskabelige og filosofiske kritikker, der tager fat om teoriernes og politikkernes ontologiske antagelser – altså antagelser om individet, det sociale, volden, samfundet osv. Christel Stormhøj beskriver poststrukturalisme som følgende: "[P]oststrukturalismer [kan] beskrives som 'antifundamentalistiske' tænkemåder, der udvikles gennem dialog mellem forskellige strømninger, og som via differentierede analysestrategier udmøntes i forskellige kritikker af den traditionelle vestlige filosofis og samfundsvidenskabelige tænknings metafysiske grundlag ('fundamenter')" (Stormhøj, 2010: 13). Traditionen er således kendetegnet ved et kritisk indadvendt blik, som forsøger at klarlægge blinde vinkler og potentielle bivirkninger af den førte politik. Denne rapport lægger sig særligt i forlængelse af de radikaldemokratiske samfundskritikker, som de er beskrevet og praktiseret af Ernesto Laclau og Chantal Mouffe (2001 [1985]) m.fl.

Med afsæt i ovenstående spørgsmål gennemgår rapportens del 1 de forskellige eksisterende tilgange til ekstremismen på de sociale medier – fra de 'hårde' sikkerhedsteknologiske løsninger til de 'bløde' modnarrativer. I del 2 dykker rapporten ned i de beregningsmæssige og kvantitative analysemetoder ved at fokusere på henholdsvis netværks- og indholdsanalyse. Del 3 vurderer afslutningsvist den gennemgåede litteratur ud fra en række af radikaliseringsteoriernes videnskabelige grundspørgsmål. Dette gøres først ved kritisk at udkrystallisere og diskutere online-litteraturens radikaliseringsmodel. Endelig diskuteres det, hvorvidt forebyggelsestankens fokus på teknologiske løsninger er ved at føre indsatsen på et vildspor, hvor voldelig ekstremisme og radikalisering betragtes som individuelle kendetegn, der efterlader konkrete og målbare online-spor.

Nedenstående figur er en forsimplet illustration af de forskellige tilgange til forebyggelse af online-radikalisering, som vil blive præsenteret i denne rapport. Rapporten konkluderer, at den nye forebyggelseslitteratur i sin søgen efter metoder til at lokalisere kommende terrorister enten implicit eller eksplicit læner sig op af problematiske forestillinger om at kunne opstille en profil for den radikaliserings sårbare internetadfærd. For ikke at reproducere stereotyper om radikaliserede unge normalitetsafvigere, og for at styrke forståelsen for forebyggelsesindsatsens mange videnskabelige og etiske problemstillinger, opfordrer rapporten til mere forskning på området samt en mådeholden forebyggelsespolitik, der ikke lader sig besnære af det nye teknologiske fix.

Fig. 1: Tilgange til forebyggelse af online-radikalisering



Del 1:

FRA HÅRD TIL BLØD FOREBYGGELSE

Forebyggelse af radikalisering og voldelig ekstremisme er videnskabeligt betragtet endnu et underudforsket felt, der både savner klare metodiske retningslinjer og empirisk evidens. Det er derfor en forudsætning for feltets videre udvikling, at der gøres forskellige forsøg på at klassificere de mulige indsatser, vurdere effekterne heraf og udvikle alternative metoder. Ligeledes må denne udvikling forblive i kritisk dialog med sig selv, hvis metoderne også fremadrettet skal bære både videnskabelig og demokratisk legitimitet. Nedenstående redegørelse og diskussion af en række eksisterende bløde og hårde tilgange til forebyggelse af online-radikalisering skal derfor læses som kritiske bidrag til metodernes videreudvikling samt som en optegning af den bane, de nye beregningsmæssige og kvantitative tilgange har valgt at spille på. Redegørelsen er derfor en nødvendig mellemstation for en præsentation af forskningen inden for beregningsmæssige og kvantitative metoder til forebyggelse af online-radikalisering, og redegørelsen har først og fremmest til hensigt at optegne nogle tendenser, som suppleres med enkelte eksempler.

Helt overordnet kan de eksisterende tilgange til forebyggelse af online-radikalisering inddeles i to hovedgrupper: fra de 'hårdeste' og mest indgribende sikkerheds-teknologiske løsninger til de 'blødeste' former for modnarrativer.[15] Den hårde ende af skalaen har primært fokus på at reducere online-udbuddet af voldelig ekstremistisk propaganda. Disse løsninger kan være overvågning, lukning (takedowns), blokering eller censur af internetsider og brugerprofiler på sociale medier. I den bløde ende af skalaen findes forskellige former for modnarrativer via online-kampagner og lignende, samt den helt tidlige indsats, der skal oplære unge mennesker i en kritisk

15 Hussain & Saltman, 2014: 82.

tilgang til digital kommunikation. Fælles for de bløde tilgange er et ønske om at reducere efterspørgslen efter, og indflydelsen fra, radikalt online-indhold.[16] Mellem disse to yderpunkter – og i forlængelse heraf – vokser en tredje kategori, der kombinerer den mere efterretningsorienterede informationsindsamling og monitorering med en tidligere og mere målrettet forebyggelse. Det er denne tilgangs overordnede hensigt at anvende de forskellige beregningsmæssige og kvantitative metoder, evt. suppleret af fagprofessionel vurdering, til at udpege de sårbare unge, som er i ekstremismens risikogruppe.

Hvordan informationerne dernæst skal anvendes, og med hvilke midler de sårbare unge skal sættes på ret køl, er et andet spørgsmål, som delvist peger tilbage på det eksisterende spektrum af bløde og hårde tiltag såvel som forebyggelsespolitikkens vifte af kriminalpræventive indsatser. Det er blandt andet en udbredt forestilling, at en effektiv blokering af links til ekstremistiske hjemmesider, en forstyrrelse af kommunikationslinjerne mellem ekstremistiske mediebureauer og online-fora kombineret med troværdige modnarrativer vil forhindre ekstremistiske gruppers muligheder for at sprede deres budskaber og formindske ideernes indflydelse.[17]

SIKKERHEDSTEKNOLOGISKE LØSNINGER – REDUKTION AF UDBUD

Alle samfund har implementeret en eller anden form for internetcensur. Det er derfor ikke længere spørgsmålet, om internettet skal kontrolleres, men derimod hvor meget og på hvilke områder kontrollen skal indføres.[18] Hvor nogle lande har 'kulturspecifik' filtrering (fx blokeres indhold relateret til nazisme og holocaust-benægtelse i Frankrig og Tyskland), går andre filtreringstendenser på tværs af hele Europa (fx filtre mod børneporno).[19]

Online-radikalisering bliver på globalt plan forsøgt forebygget eller obstrueret ved brug af en vifte af sikkerhedsteknologiske løsninger.[20] Det mere præcise omfang af lukninger (takedowns) vides ikke med nøjagtighed. De anvendte værktøjer og teknikker rækker længere end blot spærring af adgangen til bestemte informationer. Indsatserne inkluderer alt fra målrettede computervira og strategisk timing af distributed denial-of-service (DDoS) angreb til en restriktiv håndtering af

16 Neumann, 2013.

17 IHS, 2013: 8

18 Bitso et al., 2013: 167.

19 Hussain & Saltman, 2014: 83.

20 Briggs & Feve, 2014: 7.

brugerservicevilkår.[21] Indsatsen foregår således på mange forskellige fronter i en gråzone mellem myndigheder, efterretningstjenester, hacktivister, private internetudbydere og udbydere af sociale medier.

Metoder og tendenser – indsnævring af de virtuelle flaskehalse

Teknikker til internetcensur har udviklet sig dramatisk i de seneste år. Censuren er nu blevet langt mere varieret, manipulerende og usynlig end tidligere, og såvel stater som store multinationale virksomheder har sat overvågning af forskellig karakter højt på agendaen. Den statsligt baserede overvågning muliggøres således gennem forskellige samarbejder med private udbydere, kritiske internetbrugere m.fl.[22] Mange af de udviklede metoder er i udgangspunktet udviklet til at efterforske og forhindre et bredere spekter af stadig mere avanceret og organiseret kriminalitet på internettet. De er ikke udviklet til håndtering af ekstremisme og radikalisering per se. Nedenstående metodegennemgang fokuserer derfor mere specifikt på myndighedernes anvendelse af sikkerhedsteknologiske løsninger inden for forebyggelse af radikalisering og ekstremisme.

Overordnet betragtet består de hårde løsninger af en bred vifte af indgribende tiltag, der kan inddeles i fire kategorier: Lukning af brugerprofiler og hjemmesider, filtrering og manipulation af internetsider og online-indhold, overvågning og monitorering samt data nudging og algoritme-censur.

Metoderne i den første kategori, lukninger, som ofte betegnes ved deres engelske navn, takedowns, forsøger at fjerne problematisk online-indhold og lukke brugerprofiler og hjemmesider for på den måde at forhindre spredningen af informationer, propaganda og hadefulde ytringer, der opfordrer til et ekstremistisk engagement eller udbreder ekstremistiske eller kriminelle ytringer. Traditionelt har myndighederne forsøgt at lukke eksempelvis hjemmesider gennem retskendelser eller via pres på de serviceudbydere, der faciliterer indholdets tilgængelighed på nettet.[23]

21 Bitso et al., 2013: 174; Stevens & Neumann, 2009: 16.

22 Poell, 2014: 192..

23 Bitso et al., 2013: 175; Briggs & Feve, 2014: 8.

Det nyeste skud på stammen over takedown-initiativer er de sociale mediers flagging-funktioner. Det er en slags frivillig brugerdrevet censur, hvor brugere af de sociale medier inddrages i forsøget på at skabe et fælles ansvar om kampen for ekstremismefrie sociale medier.[24] Flagging fungerer ved, at brugere anmelder andre brugere, som forbryder sig mod de sociale mediers ofte restriktive brugerbetingelser. Både Facebook og Twitter stiller denne service til rådighed, og YouTube har med et Trusted Flaggers Program, iværksat af Against Violent Extremism-netværket (AVE),[25] kombineret tidligere ekstremisters forhåndskendskab med nye tekniske sorteringsmuligheder for at forbedre de eksisterende procedurer for takedowns af problematiske videoer.[26] Endelig findes også enkelte eksempler på forsøg på at lukke eller hæmme driften af hjemmesider via cyberangreb med målrettede computervira, DDoS-angreb (hvor en hjemmeside eller server oversvømmes af henvendelser, indtil den ikke længere er tilgængelig) eller antiekstremistisk hacktivisme.[27]

I situationer, hvor de problematiske hjemmesider eller det ulovlige materiale ligger på servere i andre lande, må staten tage andre teknikker i brug – den anden kategori af ovennævnte hårde tilgange. Her ledes online-trafikken gennem en række "virtuelle flaskehalse", hvor online-kommunikationen filtreres og manipuleres.[28] Målet med internetfiltrering er derfor at kontrollere flowet af informationer. Dette er muligt, fordi langt det meste internetkommunikation foregår via et begrænset antal nationale internetudbydere (Internet service provider (ISP)).[29] ISP-filtrering fungerer ved, at den censurerende router (typisk den private internetudbyder) sammenligner den konkrete hjemmesideadresse, som kundens computer forsøger at kontakte, med en oversigt over sortlistede adresser. Såfremt den efterspurgte adresse står opført på listen, nægtes internetkunden adgang til den adspurgte hjemmeside.[30] I enkelte lande er denne liste hemmeligholdt, hvorimod den i andre lande er offentligt tilgængelig.[31,32]

24 Stevens & Neumann, 2009: 31.

25 AVE koordineres af den London-baserede tænketank Institute for Strategic Dialogue (ISD), der samarbejder om arbejdet med Google Ideas, Gen Next Foundation og rehabstudio. Se mere på: http://www.againstviolentextremism.org/

26 Ramalingam, 2014; Saltman & Russell, 2014: 5.

27 Jacobsen, 2014: 17; Stevens & Neumann, 2009: 22; Hussain & Saltman, 2014: 103-104.

28 Hussain & Saltman, 2014: 86-87.

29 Stevens & Neumann, 2009: 16-17.

30 Bitso et al., 2013: 174-175; Hussain & Saltman, 2014: 87.

31 Bitso et al., 2013: 177.

32 For en teknisk uddybning af de forskellige filtreringsløsninger henvises til Bitso et al. (2013: 175).

En anden og mere subtil form for filtrering eller manipulation kaldes "Domain Name Server (DNS) Tampering" eller DNS-hijacking.[33] Her manipuleres serveren med adressekartoteket, så domænenavnet ikke længere henviser til den rigtige adresse. Når den enkelte internetbruger forsøger at gå ind på et bestemt domænenavn, vil han derfor i stedet blive omdirigeret til en fejlside eller en manipuleret klon, der overvåges eller indeholder manipuleret materiale og fejlinformationer.[34] Endelig kan filtrering ske ved at sammenholde hele datatrafikken med sortlistede nøgleord (indholdsfiltrering eller dynamisk filtrering). Denne filtreringsmekanisme vil dog sænke hastigheden på internettrafikken betydeligt.[35]

Overvågning og monitorering af internet-trafik – den tredje kategori – anvendes i stort omfang, hvilket også Edward Snowdens læk af dokumenter fra National Security Agency (NSA) i USA afslørede.[36] I den hjemlige kontekst blev internetlogning af al datatrafik anvendt fra 2007 frem til juni 2014 (jf. det europæiske logningsdirektiv og den danske logningsbekendtgørelse[37]), ligesom der formodentlig stadig gennemføres overvågning og registrering af brugere og netværk.[38] Det præcise omfang vides dog ikke, om end en del af omfanget kom for dagen, da Snowden-lækagerne afslørede Danmarks deltagelse i det såkaldte "9 eyes", der siges at være det andet højeste niveau af informationsdeling med det amerikanske efterretnings-væsen[39]. De beregningsmæssige og kvantitative tilgange til online-radikalisering kan i de fleste tilfælde siges at falde under monitoreringsindsatsen. Monitorering (af offentligt tilgængelige kilder) er i sig selv ganske harmløs. Det er de medfølgende analyser, konklusioner og politikker til gengæld ikke.

De nyeste metoder i kampen mod online-ekstremismen – den fjerde kategori – er forskellige former for data nudging (adfærdsændrende teknologier) og andre sociale teknikker. Et eksempel er indførelsen af ID-verifikation og andre registreringsteknikker under oprettelsen af online-profiler eller ved tilgang til offentlige internetforbindelser.[40] Ideen er herved at anspore til moderation – under antagelsen om, at de fleste vil føle

33 Bitso et al., 2013: 175.

34 Briggs & Feve, 2014: 8.

35 Stevens & Neumann, 2009: 17; Hussain & Saltman, 2014: 89.

36 Gjerding et al., 2014, 19. juni: Snowden-dokumenter afslører dansk partnerskab med NSA.

37 Se logningsbekendtgørelsen her https://www.retsinformation.dk/Forms/R0710.aspx?id=2445

38 Bitso et al., 2013: 175; Briggs & Feve, 2014: 8.

39 Se mere: http://cphpost.dk/news/denmark-is-one-of-the-nsas-9-eyes.7611.html

40 Bitso et al., 2013: 175.

tilskyndelse til at udvise den korrekte adfærd, hvis de registrerer sig ved eget navn og ikke uhindret folder sig ud i leg med identiteter og aliasser. Nudging skal altså appellere til individernes egeninteresse.[41]

Et andet forslag til adfærdsregulering i kampen mod online-radikalisering er at arbejde med det sociale og fysiske rum som påvirkningsfaktor. Offentlige computere kan eksempelvis blive placeret i åbne rum, hvor omgivelserne kan følge internetadfærden. Herved disciplineres den enkelte bruger til kun at betragte socialt acceptabelt indhold.[42] Centralt for begge metoder er naturligvis antagelsen om, at de påvirker den enkeltes internetbrug til i højere grad at bevæge sig inden for 'normen' – at den enkelte bruger således disciplinerer egen online-adfærd. Med andre ord sidestiller tankegangen anonymitet med normløshed.

Den mere skjulte adfærdspåvirkning finder sted gennem en algoritmecensur, hvor den enkeltes internetsøgninger eller nyhedsstrøm manipuleres vha. de stadig mere avancerede sorteringsalgoritmer. Teknikken minder i funktionen om DNS-manipulation. Således vil søgninger på visse nøgleord medføre en prioriteret/manipuleret liste, der fremhæver 'positive' (eller fra statens og søgemaskinernes side ønskede) resultater øverst i søgningen og placerer 'negative' resultater, som fx terrororganisationers mediebureauer, meget længere nede i søgninger.[43]

Det er endnu svært at få det fulde overblik over, hvilke strategier, der bruges hvor, og i hvilket omfang. Takedown-regimer fungerer allerede på ekstremismeområdet i en lang række lande. Med varierende grader af kontrol og lovgivning har Storbritannien, Holland, Frankrig, USA, Tyskland og Australien allerede programmer i funktion. ISP-filtrering og DNS-hijacking er under overvejelse i Australien og EU. Storbritannien og Frankrig[44] anvender allerede ISP-filtrering.[45] Den danske praksis på dette område er stadig ret afgrænset, og endnu er der ingen direkte internetcensur på ekstremisme-området. I Danmark blev blokeringsteknologien i starten indført for at forhindre udbredelse og brug af børneporno, og internetudbyderne følger derfor i dag frivilligt en myndighedsfastlagt sortliste over flere tusinde børneporno-hjemmesider, dvs. hjemmesider med nøgenbilleder af personer, som politiet skønner at være under 18 år.[46]

41 Morozov, 2014b: 198.

42 Royal Canadian Mounted Police, 2011: 21.

43 Stevens & Neumann, 2009: 22; Hussain & Saltman, 2014: 91.

44 Se mere: http://arstechnica.com/tech-policy/2015/02/sites-featuring-terrorism-or-child-pornography-to-be-blocked-in-france/

45 Nouri & Whiting, 2015: 185.

46 Deibert et al., 2010: 329.

Siden indførelsen af DNS-blokering i Danmark har brugen udbredt sig til hjemmesider, hvor der er ophavsretskrænkelser (fx deling af musik og film), overtrædelse af Lægemiddelloven (hvor man kan købe ulovlige eller receptpligtige præparater) og overtrædelse af Spilleloven (online-kasinoer).[47] Blokering sker enten ved frivillighed (internetudbyderen opstiller selv et filter), hvilket er fremgangsmåden ved børneporno, eller ved at domstolene nedlægger fogedforbud. Det sidste var eksempelvis tilfældet, da man i januar 2008 forhindrede danske internetkunders adgang til den svenske fildelingstjeneste The Pirate Bay.[48]

Fordele og ulemper

Censur kan både have fordele og ulemper. Blandt fordelene nævnes evnen til kortvarigt at lamme ekstremistiske miljøer og reagere hurtigt på truslen samt flagging-funktionens decentrale og selvopretholdende karakter. Men de hårde løsninger kan dog også kritiseres for at være en symptombehandling, der stiller samfundet over for en række demokratiske og etiske udfordringer. I tilgift er de omkostningstunge og ineffektive og besværliggør både forskning og efterforskning. Nedenstående afsnit diskuterer kort disse udfordringer og kritikker.

Censur, der fjerner indhold fra de sociale medier, bygger i stigende omfang på andre brugeres indrapportering (flagging), hvilket er både hurtigere og mere fleksibelt end en myndighedsbaseret central censur.

Censur vurderes at have en række fordele. Den generelle takedown-strategi er med til at fjerne ekstremistisk indhold fra nettet og besværliggøre tilgængeligheden af indholdet en smule – om end denne kamp synes at være tabt på forhånd, med mindre man indfører kinesiske principper for åbenhed. Cyberangreb og infiltrering afbryder de forskellige fora og grupperingernes normale funktion og kapacitet ved at lamme et aktivt online-miljø for kortere eller længere tid. Herved forhindres eller vanskeliggøres tilgangen for nye medlemmer eller rekrutter, og miljøernes kreativitet og spontanitet, som før florerede i åbenhed, lider et midlertidigt knæk.[49]

47 Se advokatgruppen: http://www.advokatgruppen.dk/files/5/en_komplet_oversigt_over_eksisterende_blokeringer_af_internetsider_i_danmark.pdf

48 Deibert et al., 2010: 327.

49 Torres-Soriano, 2014: 11.

Censur, der fjerner indhold fra de sociale medier, bygger i stigende omfang på andre brugeres indrapportering (flagging), hvilket er både hurtigere og mere fleksibelt end en myndighedsbaseret central censur.[50] På den måde opnår censuren en norm- og brugervilkårsbaseret sortering, der grundet sin decentrale og selvregulerende karakter kan reagere hurtigere og med større følsomhed over for indhold af stødende og potentiel problematisk karakter. Censur ved hjælp af brugerindrapportering kan herudover potentielt set medvirke til at disciplinere andre brugere og sætte nye grænser for debat og tone på de sociale medier.[51] Frem for at være begrænset af ytringsfriheden er en censur af debatten på de sociale medier underlagt private udbyderes brugervilkårspolitikker, der ofte er meget restriktive og derfor sætter klare normgrænser for ytringernes karakter.

Af rettighedsmæssige, politiske og praktiske årsager er det umuligt helt at fjerne alt voldeligt ekstremistisk indhold fra nettet. De fleste forsøg på at begrænse udbud er omkostningsfulde. Problemet er, at det fjernede indhold altid finder en måde at omgå censuren på, ligesom brugere med meget enkle midler kan omgå de forskellige nationale filtre.

Hacktivisme (udført af patriotiske freelance-hackere) og andre offensive cyberstrategier har også en række fordele, da de kan reagere øjeblikkeligt og udenom retsstatens procedurale langsommelighed. På den ene side kan hjemmesider hurtigt lægges ned, hacktivismen kan anvendes som en parallel efterretningsvirksomhed og de anonyme angreb er ikke direkte koblet til staten, hvilket har fordelen af ikke at forstærke det klassiske fjendebillede. Herudover kan hacktivismen oftest trænge længere ind i online-universerne end den officielle forebyggelse. På den anden side risikerer hacktivismen at forstyrre eller direkte modarbejde fungerende efterretningsvirksomhed, og det kan fremprovokere en endnu mere sikkerhedsbevidst og dark web-orienteret online-ekstremisme, dvs. en onlineekstremisme, der bevæger sig hinsides det offentligt tilgængelige internet ved hjælp af krypteringsværktøjer og lukkede fora.[52] Herudover arbejder hacktivismen uden for retsstatens rum, hvilket risikerer at undergrave tilliden til systemet.

50 Briggs & Feve, 2014: 7.

51 Stevens & Neumann, 2009: 31.

52 Hussain & Saltman, 2014: 103-104; Saltman & Russell, 2014: 6.

Hacktivister kan også tænkes at gå efter indhold eller personer, som ikke direkte er involveret i ulovligheder, hvilket får hacktivismen til i højere grad at ligne politisk forfølgelse og selvtægt.

At forebygge online-radikalisering gennem forsøg på at reducere udbuddet af ekstremistisk online-indhold kritiseres også for at være en konventionel tilgang til et relativt nyt fænomen.[53] Der er således udbredt konsensus blandt forskere om, at en omfattende brug af særligt takedown og filtrering kan have en række utilsigtede effekter, der overgår fordelene ved brugen af disse teknikker. Af rettighedsmæssige, politiske og praktiske årsager er det umuligt helt at fjerne alt voldeligt ekstremistisk indhold fra nettet. De fleste forsøg på at begrænse udbud er omkostningsfulde. Problemet er, at det fjernede indhold altid finder en måde at omgå censuren på, ligesom brugere med meget enkle midler kan omgå de forskellige nationale filtre.[54] Desuden betyder den sideordnede integration af fildelingsløsninger, at man hurtigt kan dele indhold på mange netværk samtidig, hvilket gør delingsmekanismerne endnu mere modstandsdygtig over for censur.[55]

Forsøg på at opløse forskellige facebookgrupper har ført til, at jihadistgrupper nu i stedet optræder som enkeltindivider. Men grundet åbenhedens begrænsninger er de ofte påpasselige med at komme med opfordringer til vold og andre inkriminerende udsagn, ligesom de anvender flere profiler samtidig for derved altid at have netværket intakt, når en profil lukkes.[56] Samtidig fremprovokerer de hårde tilgange en mere kreativ og avanceret mediebrug fra de ekstremistiske netværks side, og de forskellige hindringer risikerer derfor også at presse folk ud i en mere avanceret brug af det ucensurerede 'dark web' via Tor-browsere: en form for kryptering, som gør overvågning og monitorering langt vanskeligere. [57]

Herudover fremhæver enkelte forskere det modsætningsforhold, at oplysnings-grundlaget, som skal informere og forbedre anvendelsen af forskellige (bløde) modnarrativer, bliver af en ringere kvalitet jo mere online-ekstremismen presses ned

53 Nouri & Whiting, 2015: 186.

54 Hussain & Saltman, 2014: 87-89; Dienstbühl & Weber, 2014: 43.

55 Klausen, 2014; Salem et al., 2008: 607.

56 Difraoui, 2012: 73.

57 Hussain & Saltman, 2014: 90; Saltman & Russell, 2014: 11.

i det skjulte. Den omfattende brug af takedown- og filtreringsmekanismer besværliggør med andre ord de forsknings- og efterretningsrelaterede studier af materialet, netværksforbindelserne mv., hvilket kan være et problem for den vidensbaserede forebyggelse og terrorbekæmpelse.[58] De hårde og de bløde tiltag kan fra det perspektiv siges at modarbejde hinanden, og 'filter and remove'-tilgangen synes derfor at være kontraproduktivt i forhold til en mere ideologisk konfronterende og ytringsfrihedsbaseret linje, der handler om at udfordre ekstremismens fortællinger med demokratiske værdier og positive alternative.[59] Desuden har filtrerings- og blokeringstilgangen (særligt ISP- og DNS-filtrering) en tendens til både at gøre internettrafikken langsommere og medføre "over blocking", hvor også lovlige hjemmesider eller lovligt online-indhold blokeres eller fjernes, hvilket kan afstedkomme en række problemer for virksomheder og organisationer.[60]

De hårde og de bløde tiltag kan fra det perspektiv siges at modarbejde hinanden, og 'filter and remove'-tilgangen synes derfor at være kontraproduktivt i forhold til en mere ideologisk konfronterende og ytringsfrihedsbaseret linje, der handler om at udfordre ekstremismens fortællinger med demokratiske værdier og positive alternative.

Retsbaserede hjemmesidelukninger, forskellige blokerings- og filtreringssystemer eller direkte cyberangreb er således kun symptombehandling. De kan have en kortvarig effekt på individuelle hjemmesider, men de vil som regel betyde, at indholdet blot spredes til andre medier eller brugerprofiler. Sammenholdes dette med de sociale mediers dynamiske karakter, bevirker det, at de sikkerhedsteknologiske løsninger praktisk taget bliver til sisyfosarbejde.[61] Selvom det ikke forekommer optimalt at lade eksempelvis jihadistiske sider og brugerprofiler være tilgængelige, argumenterer flere forskere derfor for at vælge den djævel, vi kender og lade internetsiderne forblive tilgængelige.[62]

58 Saltman & Russell, 2014: 8.

59 Hussain & Saltman, 2014: 95; Nouri & Whiting, 2015: 185-186.

60 Neumann, 2013: 439; Stevens & Neumann, 2009: 22; Hussain & Saltman, 2014: 88.

61 Neumann, 2013: 438-441; Neumann & Stevens, 2009: 25-26; Briggs & Feve, 2014: 9; Gartenstein-Ross, 2013; Halverson og Way, 2012: 149; Difraoui, 2012: 70; IHS, 2013: 4; Hussain & Saltman, 2014: 91; Saltman & Russell, 2014: 6.

62 Zelin, 2013: 3.

Ud over de mere tekniske og metodiske vanskeligheder ved brugen af sikkerhedsteknologisk udbudsreduktion stiller tilgangene samfundet over for en række etiske og demokratiske udfordringer. Et af de mest bekymrende aspekter af internetfiltrering er, at den ofte er usynlig for brugerne og således foregår uden for offentlighedens kontrol.[63] Særligt brugen af algoritmer til at frasortere problematisk materiale i internetsøgninger stiller spørgsmål til etikken i udbudsreduktionen. For hvordan og af hvem defineres de kriterier for ekstremistisk indhold, som algoritmen opererer på baggrund af?[64] Som teknologiforsker og censurkritiker Evgeny Morozov bemærker, kan denne form for nudging potentielt set skade demokratiet, og dens anvendelse har derfor en række dystopiske undertoner, vi endnu mangler at forholde os til.[65] Som Morozov også understreger: "Turning something into a nudge by mere technocratic fiat presumes social consensus—over both ends and means—where it may not yet exist".[66]

Retsbaserede hjemmesidelukninger, forskellige blokerings- og filtreringssystemer eller direkte cyberangreb er således kun symptombehandling. De kan have en kortvarig effekt på individuelle hjemmesider, men de vil som regel betyde, at indholdet blot spredes til andre medier eller brugerprofiler. Sammenholdes dette med de sociale mediers dynamiske karakter, bevirker det, at de sikkerhedsteknologiske løsninger praktisk taget bliver til sisyfosarbejde.

Modsat områder som fx pædofili er ekstremisme et udtalt politisk fænomen, der således også deler offentligheden. Offentliggørelse af myndighedernes ekstremismesortlister risikerer at skabe offentlig debat om emnet og derved øge opmærksomheden om terrororganisationer og ekstremistiske strømninger frem for at sænke den.[67] Herudover er effekten af manipulation med søgeresultater relativt begrænset, da de fleste får tips om hjemmesider osv. af andre kilder end søgermaskiner; fx internetfora og sociale netværk.[68]

63 Deibert et al., 2010: xvi; Pariser, 2011.

64 Hussain & Saltman, 2014: 91.

65 Morozov 2014a; Morozov 2014b: 198-199.

66 Morozov, 2014b: 199

67 Stevens & Neumann, 2009: 20..

68 Stevens & Neumann, 2009: 19.

Sociale netværkstjenesters flagging af brugerprofiler og grupper er en anden problematisk tendens – de samfundspædagogiske og normdannende fordele til trods. Flagging-funktionerne gør ganske vist overvågningen mere omkostningseffektiv, men det giver også regimetilhængere og statsmagter et instrument til bekæmpelse af sociale bevægelser.[69] Samtidig betyder det, at ingen har det fulde overblik over censuren og dens konsekvenser. Case-studier viser, at nye navnepolitikker (real name policy) på Facebook, YouTube og Twitter har medført forbud mod anonyme aktivister, fjernelse af aktivistisk, kritisk indhold og overlevering af følsomme oplysninger til myndighederne. Politikken er altså med til at besværliggøre sociale bevægelsers modstand mod repressive regimer.[70] Pres for større kontrol og mere censur af de sociale medier vil med andre ord også have indflydelse på modstandspolitikken i den ikke-demokratiske del af verden. I oktober 2014 har Facebook dog tilnærmet sig dele af denne kritik ved at åbne op for en Facebook-indgang via Tor-browsere, der kan sørge for en delvis anonymisering af internettrafikken.[71] Herved bliver det mere sikkert at bruge Facebook og forblive beskyttet af internettets anonymitet.

Problemerne med de sikkerhedsteknologiske tiltag ligger således ikke blot i de tekniske udfordringer, men handler også i høj grad om utilsigtede demokratiske og sociale følgevirkninger.[72] De målrettede interventioner risikerer at bære brænde til bålet blandt de ekstremistiske grupper og miljøer, der i forvejen føler, at deres ytrings- og forsamlingsfrihed er under pres, samt at de er ofre for dobbelte standarder.[73] Dette peger på et fænomen blandt sociale bevægelser, som David Hess og Brian Martin kalder 'backfire'. Backfire kan ifølge Hess og Martin optræde ved censur, der opfattes som uretfærdigt, og det kan medvirke til at drive dele af en bevægelse eller organisation under jorden.[74] På den måde risikerer censuren at bidrage til konfliktniveauet mellem staten og dens ideologiske fjendegrupperinger. Og kommunikationen i de mere lukkede miljøer risikerer at eskalere konfliktforholdet. Ud fra visse radikaliseringsteoretiske perspektiver er effekten af udbudsreduktion ligeledes tvivlsom, da sammenhængen mellem radikalisering og internettet er langt mere kompliceret, end denne løsning synes at antage, og ingen reelt set ved, om det

69 Poell, 2014: 198.

70 Poell, 2014: 191.

71 Tor er en gratis software, der beskytter mod overvågning af internettrafikken. Læs mere om Tor på https://www.torproject.org og læs om det nye samarbejde med Facebook på https://blog.torproject.org/blog/facebook-hidden-services-and-https-certs

72 Stevens & Neumann, 2009: 28.

73 Nouri & Whiting, 2015: 187.

74 Hess & Martin, 2006.

har nogen effekt.[75] Flere forskere peger derfor i stedet i retning af efterspørgslen. Der er, med Johnny Ryans ord, behov for at stole på den enkelte borger og styrke samfundet således, at informationssamfundets plasticitet kan arbejde til demokratiets og retsstatens fordel:

> "Subversives will persist online, but the more people in society who understand and oppose the violent narratives that threaten their society, the harder it will be for isolated militants to appeal with a consistent message across the wider Internet..[76]"

Neumann foreslår også, at samfundet i stedet bør fokusere på at nedbringe efterspørgslen efter ekstremistisk online-indhold ved at diskreditere, modgå og konfrontere ekstremistiske narrativer eller gennem uddannelse af unge mennesker, så de forbliver skeptiske over for de budskaber, de konfronteres med på sociale medier.[77]

MODNARRATIVER – REDUKTION AF EFTERSPØRGSEL

Modnarrativer (counternarratives) er mange forskellige tilgange under et. De forskellige tilgange tager tankerne om kapacitetsopbygning og modstandskraft et skridt videre og bygger helt overordnet på ideen om at gennemtrænge ekstremismens virtuelle ekkokamre (de ideologiske osteklokker, som visse miljøer lever under på internettet) med alternative narrativer og fakta, der angiveligt svækker ekstremismens tiltrækningskraft.[78] Et narrativ kan groft siges at indeholde tre hovedkomponenter. For det første tager det afsæt i et eksistentielt, politisk eller religiøst anklagepunkt – en grundlæggende konflikt, som individer eller grupper kan sættes i forbindelse

75 Gemmerli, 2014a; Neumann & Stevens, 2009: 15.

76 Ryan, 2007.

77 Neumann, 2013: 433.

78 Neumann, 2013: 447.

med. For det andet indeholder et narrativ en helteskikkelse eller agent og en potentiel løsning på konflikten. For det tredje indeholder et narrativ et løsningsforslag, som motiverer den enkelte til at træde til handling.[79],[80]

Modnarrativer (counternarratives) er mange forskellige tilgange under et. De forskellige tilgange tager tankerne om kapacitetsopbygning og modstandskraft et skridt videre og bygger helt overordnet på ideen om at gennemtrænge ekstremismens virtuelle ekkokamre (de ideologiske osteklokker, som visse miljøer lever under på internettet) med alternative narrativer og fakta, der angiveligt svækker ekstremismens tiltrækningskraft.

I indeværende rapport anvendes modnarrativer både som generel betegnelse for en vifte af forskellige kommunikations- og informationsstrategier og som specifik betegnelse (direkte modnarrativer) for tilgange, der direkte anfægter ideologiske, politiske eller religiøse argumenter.[81] Nedenstående afsnit inkluderer de sondringer og metoder, som den eksisterende policy-litteratur hyppigst henviser til. Det betyder imidlertid ikke, at der ikke findes andre og mere avancerede modnarrativer, som politikken på området endnu mangler at omfavne. Der er, i lyset af den voldelige ekstremismes mange facetter, god grund til kritisk at arbejde med at videreudvikle metoder og teorier.

Metoder og tendenser – "a healthier realm of ideas"

De forskellige typer af modnarrativer forsøger alle at begrænse indflydelsen fra de ekstremistiske fortællinger på internettet. Nedenstående afsnit vil redegøre for de tre overordnede kategorier: direkte modnarrativer, de positive alternativer og uddannelse til kritisk tænkning. Selvom tilgangene deler mange antagelser om ideologier,

79 Quiggin, 2009: 23.

80 Denne beskrivelse minder om David Snow og Robert Benfords frame alignment-teori (1988), som forklarer mobilisering af sociale bevægelser ud fra 'frame alignment', dvs. tilfælde hvor individers opfattelse af virkeligheden, interesser og værdier resonerer med en gruppes/bevægelses aktiviteter, målsætninger og ideologi. Snow og Benford arbejder ud fra en forståelse af, at aktører ikke blot er bærere af ideer, men også selv er med til at konstruere den sociale virkelighed (Snow & Benford, 1988: 198). Dette muliggør en diskursiv konstruktion af en opfattet konflikt (diagnostic frame), der kan anvendes strategisk i forsøget på at fremsætte en taktik til løsning af konflikten (prognostic frame) samt et rationale, der skal mobilisere til handling (motivational frame) (Snow & Benford, 1988: 199).

81 Briggs & Feve, 2014: 13.

sprog og individer, er der også en række forskelle tilgangene imellem, hvilket kort vil blive diskuteret. I forlængelse af denne diskussion præsentes tre forskellige eksempler på modnarrativer på nettet: Think Again Turn Away, Walk Away from Violent Extremism og Abdullah X.

Ifølge Ghaffar Hussain og Erin Marie Saltman fra den britiske antiekstremistiske tænketank Quilliam Foundation, er 'bløde' tiltag, der udvikler modnarrativer og udbreder initiativer, som modsiger internettets ekstremistiske stemmer, en langt mere effektiv måde at udfordre de ekstremistiske ideologier på end de hårde sikkerhedsteknologiske løsninger. For Hussain og Saltman er et af ekstremisme-bekæmpelsens helt store udfordringer, at der findes så meget ekstremistisk materiale på nettet, at ekstremisterne reelt har informationsmonopol på en række områder.[82]

De direkte modnarrativer forsøger at 'vinde argumentet' ved at dekonstruere og delegitimere den ekstremistiske propaganda og derved underminere den intellektuelle ramme, som argumenterne er opsat i.

Det synes at være en bagvedliggende tanke for såvel Hussain og Saltman som for andre fortalere for modnarrativer, at den normalt velfungerende og selvregulerende "ideernes markedsplads" grundet markedsfejl i informationsstrømmen fungerer suboptimalt (dvs. dårligere end man kunne ønske sig), og derfor tillader ekstremisterne at agere under monopollignende forhold. Agenterne på dette marked har med andre ord ikke det fornødne oplysningsgrundlag til at træffe rationelle livsvalg, hvorfor stater og civilsamfundsorganisationer må sørge for at udbedre denne mangel og tale 'de potentielt farlige ideologier' imod.[83] En Quilliam-hvidbog sætter ligeledes denne filosofi i cirkulation og anvender det sproglige billede "a healthier realm of ideas" om det ekstremismefrie internet, som de efterstræber.[84]

En anden grundlæggende tanke for modnarrativerne er, at den ekstremistiske ideologi og fortællingen om ekstremismens fællesskaber har en stor betydning for radikalisering til voldelig ekstremisme. Ph.D. i medier og kultur Anne Aly, der står i

82 Hussain & Saltman, 2014: 7.

83 Saltman & Russell, 2014: 3.

84 Saltman & Russell, 2014: 10.

spidsen for den australsk NGO People against Violent Extremism (PaVE), og herigennem arbejder med modnarrativerne som våben mod ekstremismen, konstruerer således ekstremismeproblemet som en kombination af svage individer og ekstremistiske narrativer: et marked, hvor ekstremistisk udbud møder en efterspørgsel fra fejlinformerede og sårbare unge.[85]

De alternative og multifacetterede tilgange, som Aly fremhæver, fokuserer på at hjælpe sårbare unge med at gennemskue propaganda og misinformation. Viften af forskellige modnarrativer er stor. Helt overordnet kan modnarrativer inddeles i tre kategorier. For det første kan de arbejde med direkte modnarrativer til ekstremismens ideologi og livsstil. For det andet kan de opstille alternative handlingsmuligheder og narrativer samt hjælpe troværdige stemmer med at bryde ekstremismens online-monopol. Og for det tredje kan de arbejde for at opbygge digitale kompetencer og kritiske refleksionsevner hos potentielt sårbare unge.[86]

De direkte modnarrativer forsøger at 'vinde argumentet' ved at dekonstruere og delegitimere den ekstremistiske propaganda og derved underminere den intellektuelle ramme, som argumenterne er opsat i. Således sigter de direkte modnarrativer mod at påvirke adfærden hos dem, der sympatiserer med den voldelige ekstremisme. De direkte modnarrativer kan handle om at latterliggøre ekstremismens budskaber, at udfordre og falsificere den ekstremistiske ideologis politiske eller religiøse påstande, at vise ekstremismens negative konsekvenser, at fremstille diskrepansen mellem ekstremismens grandiose anråb og dens brutale virkelighed samt at betvivle effekterne af den ekstremistiske strategi.[87]

Den mest direkte måde at praktisere modnarrativerne på er ved at konfrontere online-propagandaen med dialog og diskussion der, hvor den opstår. En måde at få narrativerne til at fremstå mindre tiltrækkende på kan eksempelvis være ved at 'genfremstille' narrativerne råt for usødet, så deres kommunikationstekniske branding eller framing dekonstrueres. Dette kan eksempelvis gøres ved at koble ekstremismens skønmalerier til billeder af den brutale virkelighed. Ideen om den direkte og konfronterende tilgang bygger ofte på en grundantagelse om, at den voldelige ekstremismes narrativer er baseret på misinformation og konspirations-teorier, som, når de afsløres som sådan, vil plante en tvivl i de ekstremistiske tankerækker og 'retlede' sympatisørerne fra voldens livsbane.[88]

85 Aly, 2014: 64.

86 Briggs & Feve, 2014: 10-14; PPN, 2011: 9; Busch, 2008: 13-15.

87 Neumann, 2013: 447; Ramalingam, 2014; Briggs & Feve, 2014: 16.

88 Neumann, 2013: 447; Hussain & Saltman, 2014: 109; Aly, 2014: 71.

Netop denne tanke ligger bag teorien i "Edges of Radicalization" af den tidligere West Point Fellow Scott Helfstein. Helfstein understreger dog nødvendigheden af en ihærdig og vedvarende indsats, hvis målsætningen skal lykkes:

> "Countering radical ideology is probably perceived or defined differently across the spectrum of pertinent actors, but it is unlikely that success will come from falsifying an idea or finding the loophole that invalidates an ideology. Rather, it will require a process whereby the ineffective and corrupt nature of the radical ideas must be displayed repeatedly over time. [89] "

På baggrund af blandt andet økonomisk teori og teorier om sociale bevægelser opstiller Helfstein en radikaliseringsmodel med fire faser og lokaliserer den fase, acceptfasen, hvor individer ifølge teorien søger sociale forbindelser for at kunne overskride de normative (moralske) begrænsninger, der ellers er en naturlig hindring for voldelig adfærd, og hvor (moralske) modnarrativer derfor forventes at have størst effekt.[90]

Herudover kan modnarrativer også fokusere på at opstille positive alternativer til ekstremismens budskaber og livsstil.[91] Her er hovedfokus at modgå ekstremismens tiltrækningskraft gennem alternative 'udbud' på identitetsmarkedet. De alternative udbud forsøger således ikke at udfordre ekstremismens narrativer direkte men ønsker i stedet at påvirke de unge, der måtte være sårbare over for budskaberne (uden selv at være blevet aktive tilhængere). I stedet for at anklage ekstremisme-butikken for at sælge et produkt, der ikke holder, hvad det lover, prøver denne tilgang så at sige blot at sælge et bedre og billigere produkt – at udkonkurrere ekstremismen.

Herudover kan de alternative stemmer hjælpe med at samle det stille flertal imod ekstremismen (skabe brede bevægelser omkring budskabet) ved at understrege solidaritet, fælles mål og fælles værdier og derved marginalisere ekstremistisk adfærd og fremtoning.[92] Indenfor modnarrativernes markedsmetafor svarer dette altså til at skabe en 'bandwagon-effekt' – at skabe følelsesmæssige og sociale købemotiver, der får folk til at kopiere andre folks købeadfærd.

89 Helfstein, 2012: 3.

90 Helfstein, 2012: 3-4.

91 Neumann, 2013: 447.

92 Briggs & Feve, 2014: 15; Ramalingam, 2014.

Forskellene i den strategiske brug af narrativer peger på, hvad Rachel Briggs og Sebatian Feve fra Institute for Strategic Dialogue i deres policy-papir om online-ekstremisme kalder strategisk kommunikation. Myndigheder skal således navigere udenom en række politiske, økonomiske og bureaukratiske udfordringer. Og de skal balancere mellem ønsket om at formidle fakta samtidig med, at de skal kunne tale til følelserne i deres målgruppe. Herudover advarer Briggs og Feve om faren ved et 'say do gap'. Det solgte produkt skal holde, hvad det lover. Myndigheder eller regeringer vil således blive målt på, hvad de gør, og ikke hvad de siger. En diskrepans mellem de to elementer vil blot være til ekstremisternes fordel.[93] Samme problemstilling om say do gap gør sig for øvrigt gældende for ekstremisterne.

Flere undersøgelser antyder, at besiddelse af evnen til kritisk tænkning og skepsis over for informationers sandhedsværdi gør unge mennesker mindre voldelige uanset radikaliteten af deres ideologiske tankesæt.

Hussains og Saltman argumenterer i den forbindelse for etableringen af kommunikationsinitiativer på de sociale medier, som klarlægger regeringens politikker og fremstiller propagandaens falskhed.[94] Men de advarer også om, at modnarrativer ikke alene kan udføres som ren akademisk eller bureaukratisk begrebsgymnastik fremført af veluddannede mennesker med en ikke-aktivistisk og værdineutral baggrund. Modnarrativerne må ifølge Quilliam-forfatterne, grundet det følelsesmæssige aspekt, fremføres af følelsesmæssigt engagerede mennesker, som er bekendt med ekstremismens metoder, men har et brændende ønske om at forsvare visse fundamentale demokratiske værdier.[95] Forfatterne foreslår derfor centrale finansierings- og træningsmekanismer for græsrodsorganisationer, så de får mulighed for mere massivt at spille ind med modnarrativer online.[96] I det tidligere omtalte Quilliam-hvidbog argumenterer forfatterne for, at monitoreringsindsatsen er meget effektiv, hvis den varetages af NGO'er og tænketanke.[97],[98]

93 Briggs & Feve, 2014: 15.

94 Hussain & Saltman, 2014: 8.

95 Hussain & Saltman, 2014: 111.

96 Hussain & Saltman, 2014: 8; Saltman & Russell, 2014: 2.

97 Saltman & Russell, 2014: 8.

98 Værd at bemærke er måske, at denne anbefaling kommer fra en NGO, der i udgangspunktet består af tidligere ekstremister, og som i høj grad lever af at producere modnarrativer og overvåge ekstremister.

Flere undersøgelser antyder, at besiddelse af evnen til kritisk tænkning og skepsis over for informationers sandhedsværdi gør unge mennesker mindre voldelige uanset radikaliteten af deres ideologiske tankesæt.[99] Dette peger endvidere på, at klassiske dannelsesidealer kombineret med gode digitale kundskaber og forståelse for internettets funktionsmåder kan virke forebyggende på unges engagement med voldelig ekstremisme. Forebyggelsen af online-radikalisering skal således øge evnen til at tilgå, forstå og producere online-kommunikation i en række forskellige kontekster.[100] Christoph Busch argumenterer derfor for en 'demokratipædagogik', der arbejder med at forbedre unge menneskers mediekompetencer; dvs. forståelse for de forskellige digitale mediers funktioner, færdigheder til omgangen med nye medier samt analytiske og refleksive mediekritiske kundskaber.[101]

Dette peger også på, at modnarrativer i den bredeste forståelse ikke nødvendigvis behøver at foregå online. Tiltag, som opbygger digitale færdigheder og en kritisk forståelse offline, vil nødvendigvis også have en effekt online.[102] Med Ryans ord: "A counternarrative to avert the next generation of violent radicals could perhaps be as broad and non-specific to the radicalization problem as a school curriculum that instills a sense of citizenship".[103] Modnarrativer, der skal sættes ind tidligt i den digitale dannelse, bør derfor satse på langsigtsperspektivet og opbygge et stærkt demokratisk samfund af digitalt indfødte fremfor at fokusere på den korte banes imperativ om at handle i lyset af truslen fra online-ekstremismen og den potentielle online-radikalisering.[104]

Mere konkret peger Briggs og Feve på, at de kritiske færdigheder koncentrerer sig om tre hovedområder. For det første bør unge mennesker generelt uddannes i at forstå propagandaens teknikker online og have større kildekritisk kendskab. For det andet bør unge mennesker oplæres i mere generelt at forstå internettets opbygning, samt hvordan fx søgeresultater genereres (hvilket peger tilbage på et kritisk engagement med brugen af algoritmecensur). For det tredje peger Briggs og Feve på, at særligt de mest sårbare skal lære at forstå og dekonstruere ekstremistiske

99 Briggs & Feve, 2014: 10-11; Rieger et al., 2013; Saltman & Russell, 2014: 11.

100 Stevens & Neumann, 2009: 37.

101 Busch, 2008: 13-15.

102 Ryan, 2007.

103 Ryan, 2007.

104 Ryan, 2007.

narrativer – lære hvordan man gennemskuer ekstremismens løgne.[105] Hussain og Saltman fremhæver i lighed hermed behovet for at udforme de forskellige uddannelsestiltag som oplysningskampagner, der advarer unge mennesker om farerne ved ekstremistisk propaganda på nettet.[106] Dette kan, som Royal Canadian Mounted Police eksempelvis foreslår, foregå gennem oplæg, der omhandler forskellige scenarier for online-adfærd, og hvad der er den korrekte respons ("what to do if…"), når den enkelte konfronteres med ekstremismen.[107]

Modnarrativer, der skal sættes ind tidligt i den digitale dannelse, bør derfor satse på langsigtsperspektivet og opbygge et stærkt demokratisk samfund af digitalt indfødte fremfor at fokusere på den korte banes imperativ om at handle i lyset af truslen fra online-ekstremismen og den potentielle online-radikalisering.

Hussain og Saltman præsenterer selv en række konkrete eksempler på modnarrativer, og diskuterer såvel fordele som ulemper ved disse.[108] Et eksempel på et nyt initiativ, som forsøger at spille på flere tilgange, og som har fået en del (også kritisk) medieomtale[109],[110], er initiativet Think Again Turn Away (TATA), som det amerikanske udenrigsministerium står bag. TATA er tænkt som et initiativ, der skal være med til at vinde 'hearts and minds' og modgå terrorgruppers indflydelse på amerikanske unge. Her anvendes terrororganisationers og ekstremisters strategiske fejltagelser samt beretninger fra afhoppere til at fremstille den voldelige ekstremisme som en fejlslagen strategi. TATA breder sig i film og billeder over de fleste sociale medier, men de har især et aktivt korps af Twitterbrugere, som mikroblogger om jihadistiske netværks fejlinformation og manipulation, og som responderer direkte på den jihadistiske propaganda.[111] Dette kan fx foregå gennem kritik af anvendelse af billedmateriale, som stammer fra en anden sammenhæng end den oplyste. Det kan også foregå gennem modkampagner om den amerikanske strategi i Mellemøsten eller ved direkte at latterliggøre den ekstremistiske propaganda. Kampagnen har særligt fået omtale for en kontroversiel video, "Welcome to the "Islamic State" land

105 Briggs & Feve, 2014: 11.

106 Hussain & Saltman, 2014: 96.

107 Royal Canadian Mounted Police, 2011: 21.

108 Hussain & Saltman, 2014.

109 For en kritik af TATA, se: http://www.nydailynews.com/news/politics/state-department-embarrassing-turn-twitter-campaign-legitimizes-terrorists-expert-article-1.1941990

110 Kritik fra Rita Katz (direktør for SITE Intelligence Group): http://time.com/3387065/isis-twitter-war-state-department/

(ISIL/ISIS)", der i sarkastiske vendinger fortæller om alle fordelene ved at blive fremmedkriger for den Islamiske Stat i Syrien og Irak. TATA-kampagnens slogan på dens officielle Tumblr-side (Tumblr er et socialt fotodelingsmedie) er "some truths about terrorism". Dette slogan beskriver tydeligt den bagvedliggende forståelse af ekstremistisk ideologi som en realitetsforvrængning, der kan rystes væk med de rette modnarrativer og gennem en korrekt fremstilling af 'fakta'. Denne forståelse ligger i god forlængelse af West Point Fellow Scott Helfsteins teorier om radikalisering og ekstremistisk propaganda, og den ræsonnerer til lige med dele af Quintan Wiktorowicz' radikaliseringsteori.

Kampagnen fokuserer derfor primært på følelser og alternativer frem for, som TATA, at køre meget på humor og kontraideologisk fakta-checking.

Et andet eksempel på en kampagne på de sociale medier er det australske Walk Away from Violent Extremism (WAVE). WAVE er modsat TATA ikke myndighedsbaseret men iværksat af den før omtalte NGO, People against Violent Extremism (PaVE). PaVE er den første australske NGO, der specifikt fokuserer på voldelig ekstremisme i alle dens former. En af organisationens grundlæggere, Anne Aly, beskriver organisationen som et ikke-religiøst og ikke-politisk nationalt netværk af mennesker, som dedikeret kæmper for at afskaffe den voldelige ekstremisme.[112] WAVE-kampagnen tager udgangspunkt i en "social marketing approach" og bevæger sig på flere platforme med både film og billeder. Kampagnen har tre fokusområder: For det første lanceres en interaktiv hjemmeside (, som endnu ikke kører), for det andet køres en opmærksomhedskampagne eller online-plakatkampagne på flere sociale medier og for det tredje følges op med en videokampagne, der skal forsøge at ramme "de søgende unge" på udkig efter ekstremistisk propaganda.[113] Formålet med kampagnen er således blandt andet at forbedre viden og opmærksomhed om voldelig ekstremisme; at udvikle modnarrativer, som deles gennem online-platforme; og at udvikle en modstandsdygtighed over for radikal og ekstremistisk indflydelse på unge mennesker (baseret på teorien om 'moral disengagement').[114] Kampagnen fokuserer derfor primært på følelser og alternativer frem for, som TATA, at køre

111 Hussain & Saltman, 2014: 110.

112 Aly, 2014: 66.

113 Aly, 2014: 67-68.

114 Aly, 2014: 69.

meget på humor og kontraideologisk fakta-checking. Alys forståelse af moralens betydning og narrativernes virkning har dog stadig en række indbyggede vanskeligheder, hvilket næste underafsnit vil komme ind på.

Et sidste eksempel, som kort skal nævnes, er det britisk-baserede Abdullah X,[115] der producerer en tegneseriekampagne (video), hvor man følger den unge Abdullahs kamp for at finde identitet, anerkendelse og den rette fortolkning af islam. Narrativet fokuserer således på tanker om islam og voldelig jihad, hvor religiøse og politiske argumenter er centrale. Abdullah X er efter sigende et uafhængigt projekt startet af en tidligere ekstremist. Afsenderen forbliver dog indtil videre anonym, hvilket måske kan have en positiv betydning for tegneseriens modtagelse. Som næste afsnit vil komme ind på, er budskabets afsender ikke uvæsentlig, hvis det skal have nogen chance for at gennembryde ekstremismens diskursive forsvarsværker. Abdullah X kører med sin tegneserieform en klar visuel stil, som spiller på visuel politisk/religiøs identitet i både form og følelser. Abdullah X udmærker sig således ved at formulere en fælles ramme, hvor flere modnarrativer fungerer samtidig. Herudover har projektet forsøgt at holde sig økonomisk og ideologisk uafhængig. Spørgsmålet er dog, hvorvidt den positive medieomtale ikke for længst har ødelagt ambitionen om uafhængighed? Desuden bærer Abdullahs monologer præg af en kontra-ideologisk opstemthed – modnarrativer af ideologer for ideologer. Spørgsmålet bliver, om Abdullah X ikke netop heri, og i en generel dystopisk tone om livet på kanten af samfundsnormaliteten, kommer til at forstærke sin egen visuelle og følelsesmæssige modstandsidentitet?

Fordele og ulemper

Som i tilfældet med de 'hårde' løsninger til bekæmpelse af online-radikalisering kan modnarrativer siges at have flere fordele og ulemper. Dog synes der blandt forskere og tænketanksaktivister – modsat den manglende akademiske tilslutning til de hårde løsninger, hvor effekten er usikker og bivirkningerne potentielt store – at være større konsensus om en tiltro til fordelene ved de bløde forebyggelsesstrategier. Fokus på 'efterspørgselsreduktion' anses således generelt for at være bedre for samfundets sammenhængskraft og mindre problematisk i forhold til de demokratiske frihedsrettigheder. Særligt fokus på kritisk dannelse kan have en række positivt afsmittende effekter på andre områder i samfundet. Nedenstående underafsnit kommer først kort omkring et par af fordelsperspektiverne. Herefter diskuterer afsnittet problematiske selvmodsigelser tilgangene imellem. Her vil foregående underafsnits eksemplificeringer også blive inddraget.

115 Følg Abdullah X på: http://www.abdullahx.com/

Vurderingen af fordelene ved at anvende modnarrativer kobler sig til antagelser om ideologiens effekt på mennesker, og modnarrativerne kan derfor ikke vurderes adskilt herfra. Hvis modnarrativerne således arbejder ud fra en antagelse om rationelle aktører på et marked af ideologier, består fordelene i modnarrativernes evne til at præsentere fakta og aflive myter, sådan som eksempelvis det amerikanske initiativ TATA ofte gør det.

Fokus på 'efterspørgselsreduktion' anses således generelt for at være bedre for samfundets sammenhængskraft og mindre problematisk i forhold til de demokratiske frihedsrettigheder. Særligt fokus på kritisk dannelse kan have en række positivt afsmittende effekter på andre områder i samfundet.

Blandt tilhængere af de mere direkte og konfronterende modnarrativer nævnes derfor strategisk præcision og evnen til gentagne gange at falsificere "de radikale ideers ineffektive og korrupte natur" som vigtige fordele.[116] Men som Helfstein også påpeger, handler forebyggelse og bekæmpelse af voldelig ekstremisme ikke blot om at indfange og falsificere dens ideologi, på samme måde som Vesten, ifølge Helfstein, falsificerede kommunismen. Under antagelsen om, at modnarrativerne formår at tale til den rationelle aktør, er det samtidig en fordel at kunne forstå de sociale, adfærdsmæssige og biologiske årsager til, at ideologien overhovedet har et resonansrum, så modnarrativerne strategisk kan indsættes der, hvor de har størst effekt, og hvor de afskrækker folk fra at bevæge sig over den normative (moralske) tærskel til den voldelige ekstremisme. Denne indsats fordrer, at modnarrativerne er vedholdende og fortsætter modstandsarbejdet som en vagthund, der ikke vil stoppe med at gø.[117]

Andre tilgange tager imidlertid afsæt i en anden forståelse af narrativernes funktion. Arbejder modnarrativerne således med blikket på sårbare og følende individer, fremstår positive alternativer som det rette valg, hvilket er, hvad det australske WAVE sigter mod. Denne tilgang kan tilmed potentielt virke i en tidlig forebyggelse, hvor de ideologiske komponenter endnu ikke er så tydelige.

116 Helfstein, 2012: 3.

117 Helfstein, 2012: 66.

Modnarrativerne handler i dette perspektiv ikke om at vinde et argument eller at 'overbevise' målgruppen om rigtigheden af 'vores' virkelighedsforståelse. Modnarrativerne handler om gradvist at lede folk i 'den rigtige retning', hvorfor menneskelige følelser er vigtigere end faktuelle beviser.[118] Det effektfulde mod-narrativ skal (som en trojansk hest) via følelser plante en spire af tvivl, der kan få lov at vokse og nedbryde de ekstremistiske forsvarsværker indefra. Vidhya Ramalingam (2014) fra Institute for Strategic Dialogue beskriver denne tvivl som stykker af information, der ikke direkte underminerer ekstremistiske narrativer, men som bevirker, at den enkelte begynder at stille kritiske spørgsmål – og begynder at revurdere sin offer- eller krænkelsesfortælling.

Det effektfulde modnarrativ skal (som en trojansk hest) via følelser plante en spire af tvivl, der kan få lov at vokse og nedbryde de ekstremistiske forsvarsværker indefra.

Men for at den trojanske hest overhovedet skal have en chance for at komme inden for murene, må afsenderen ikke være synlig og hensigten ikke være klar, hvilket er et af de største problemer for regeringsstyrede indsatser som den amerikanske TATA.[119] Det er også et af problemerne ved den positive medieomtale af Abdullah X. Alene denne positive omtale i vestlige medier kan medføre, at modtagergruppen afviser initiativet som et stykke vestligt propaganda. Frontpersonalet, der har den daglige omgang med unge mennesker i risikogruppen, har derfor en større chance for at plante tvivl hos de sårbare unge eller dem, der allerede abonnerer på ekstremistiske ideer. Og endnu mere effektfuldt bliver det ifølge denne logik, hvis tvivlens stemme udgår fra de ekstremistiske miljøers indre – evt. i form af exitberetninger fra frafaldne ekstremister. Her bevæger modnarrativerne sig altså fra at være et kontraideologisk projekt til at være et (mere subversivt) projekt om oplysning og (kritisk) dannelse.

Den kritiske dannelse er den mest fundamentale af de narrative strategier. Her kobles generel viden og oplysning til den kritiske sans (tvivlens nådegave) for herved at gøre unge mennesker mere skeptiske over for simple sandhedsudsagn. Men strategien bærer som sådan ikke nogen narrativ struktur. Netop narrativet kan hurtigt blive et problem for den kritiske dannelse. Her støder de forskellige narrative

118 Briggs & Feve, 2014: 19.

119 Saltman & Russell, 2014: 8.

strategier således på interne modsætninger og ulemper. Hvis forsøget på at lære de unge at forholde sig kritisk til informationer, billeder og indtryk på internettet specifikt retter fokus mod en bestemt fremmed ideologi, risikerer forsøget på kritisk dannelse hurtigt at få karakter af de direkte modnarrativer, hvilket har fået kritik fra flere kanter.

Den strategiske kommunikation, som de direkte modnarrativer ofte er udtryk for, bliver således ofte beskyldt for at anvende alt for simple antagelser om kommunikationens rum, hvor problemstillingen ofte reduceres til et spørgsmål om udbud og efterspørgsel eller sandt og falsk.

De direkte modnarrativer, som eksempelvis Scott Helfstein beskriver dem, handler om at demonstrere ideologiens 'falske' grundlag (at falsificere den ekstremistiske propaganda) og vise de unge mennesker, hvordan virkeligheden i 'virkeligheden' tager sig ud. Ifølge tankegangen er nogle narrativer korrekte eller sande gengivelser af virkeligheden, mens andre er forkerte eller falske. Dette får også Hussain og Saltman til at foreslå, at modnarrativer bør adressere teologiske argumenter og kontekstualisere ekstremisternes brug af referencer til skriftsteder for herved at underminere deres teologiske troværdighed.[120] Tilgangen anerkender med andre ord ikke, at virkeligheden er politisk kontingent, og at den moderne medievirkelighed altid betinger en bestemt vinkling eller fordrejning af indholdet – uanset hvem afsenderen er. Den strategiske kommunikation, som de direkte modnarrativer ofte er udtryk for, bliver således ofte beskyldt for at anvende alt for simple antagelser om kommunikationens rum, hvor problemstillingen ofte reduceres til et spørgsmål om udbud og efterspørgsel eller sandt og falsk.[121] Den kritiske dannelse, derimod, handler om at lære at betvivle sandhedsudsagn og de autoriteter, som fremfører dem. Den første tilgang postulerer altså en anden sandhed. Den anden tilgang vægter kritikken af sandhedsudsigelser. De to forskellige tilgange synes derfor umiddelbart uforenelige.

At konfrontere ekstremistiske narrativer direkte og på individuelt niveau indbefatter også andre risici. Det kan eksempelvis presse ekstremistiske grupper eller individer ud i en defensiv position, der blot genbekræfter fjendskabet og styrker troen på egne

120 Hussain & Saltman, 2014: 109.

121 Archetti, 2015: 50.

argumenter. Herudover risikerer modnarrativerne at blive uskønne 'cut and paste'-konstruktioner, som ikke taler til den medievante og gaming-orienterede ungdom. Fakta og debattråds-trolling (hvor man obstruerer en verserende debattråd ved at overlæsse den med information og hånlige kommentarer) er i det perspektiv ikke solide medieredskaber i mødet med de normalitetsskeptiske unge. Strategierne må i stedet gøre brug af følelser, ny teknologi, kulturelle referencer osv.[122]

Et alt for konfronterende modnarrativ med en åbenlys afsender risikerer endog at blive genstand for strategiske mod-modnarrativer, hvor ekstremistiske grupper eller individer anvender kommunikationen til egen fordel. Dette ses eksempelvis ved det amerikanske TATA. En yndlingsbeskæftigelse blandt visse grupper af kvindelige støtter af Islamisk Stat er således at replicere på TATA's opdateringer.[123] Herudover kan den medfølgende italesættelse kaste unødvendig opmærksomhed på netop de ekstremistiske grupper, hvilket for nogle vil virke dragende.[124] TATA er således fra flere side blevet kritiseret for i visse tilfælde at oppiske en debat og stille en talerstol til rådighed for den ekstremistiske propaganda.[125]

Et andet problem ved at lægge for meget vægt på logiske og rationelle argumenter er, at det overser de aspekter af det sociale, hvor ideologien har sin dybeste forankring – i følelser, fantasier og begærsrelationer. Et eksempel herpå kunne være traileren til Islamisk Stats spillefilmsdokumentar Flames of War fra september 2014. Traileren er næsten blottet for ideologisk indhold, men til gengæld lover den spænding med visuelle effekter og actionsekvenser i slow-motion. Det er tydeligt ud fra sådanne videoer, at det ideologisk-politiske narrativ er underordnet det taktisk-ideologisk-visuelle indhold: krigsæstetikken. I det hele taget ligner videoen mere en Hollywood-filmtrailer eller reklamen for et nyt computerspil, end hvad vi normalt opfatter som et radikalt islamistisk propagandafremstød.

Den ofte anvendte forståelsesramme for modnarrativer, som placerer narrativerne ude på 'ideernes markedsplads' bygger også på en række problematiske antagelser, der netop overser alle de ofte ubevidste følelsesmæssige, kontekstuelle og dynamiske processer, som radikalisering indbefatter. Ideernes markedsplads bærer reminiscenser af den økonomiske tænkning, som metaforen udspringer af. Tilgangen har en blind tro til miljøet og individets rationelle kerne som det, der skal stimulere den korrekte brug af information. I situationer hvor individet afviger fra sin

122 Ramalingam, 2014.

123 Klausen, 2014.

124 Briggs & Feve, 2014: 19.

125 Katz, 2014.

moralske grundindstilling og tilslutter sig den voldelige ekstremisme, skyldes det således en markedsfejl på ideernes markedsplads (hvor moralens pejlemærker sættes op). Og en fejl, som derfor kan korrigeres gennem modnarrativer, der højner oplysningsgrundlaget og guider til den korrekte fortolkning af virkeligheden.

Et alt for konfronterende modnarrativ med en åbenlys afsender risikerer endog at blive genstand for strategiske mod-modnarrativer, hvor ekstremistiske grupper eller individer anvender kommunikationen til egen fordel.

Fokus på denne korrekthed i narrativernes konstruktion gør også de forskellige indsatser blinde over for finansiering- og afsenderparadokset. Forestillingen bygger til dels på, at narrativerne skal leveres af alternative autoritative stemmer, der kan hjælpe til at affeje volden som legitim metode.[126] Problemet er dog, at online-ekstremismen og radikaliseringsfænomenet i høj grad også er baseret på et oprør mod autoriteter, hvorfor det autoritetsbaserede modnarrativ blot risikerer at bekræfte og måske også forstærke oprørstrangen. Er de alternative stemmer oven i købet økonomisk eller ideologisk koblet til staten, vil det, som nævnt, blot bestyrke mistanken og mistilliden. Dette beskriver også paradokset i, fra statens side, aktivt at støtte forskellige modnarrativer fremført af civilsamfundsorganisationer. Den direkte støtte risikerer med Tim Stevens og Peter Neumanns ord at blive et 'kiss of death' for troværdigheden af de uafhængige initiativer".[127]

Hussain og Saltman præsenterer en række eksempler på, hvad de mener, er succesfulde modnarrativer; herunder det Google Ideas baserede Against Violent Extremism (AVE). Forfatterne fremhæver, hvorledes AVE ved brug af personlige videoberetninger fra reformerede ekstremister på en effektfuld måde kan promovere visse modnarrativer og igangsætte en tiltrængt diskussion om ekstremismerelaterede emner. Tydeligt imponerede over indholdet bemærker forfatterne med undren, at videoerne har et meget lavt kliktal – er blevet set af meget få mennesker – fra færre end 100 visninger til 16.000 visninger for det mest populære interview med en tidligere canadisk supremacist.[128]

126 Hussain & Saltman, 2014: 97-98.

127 Stevens & Neumann, 2009: 43.

128 Hussain & Saltman, 2014: 101-102; Saltman & Russell, 2014: 9.

Det manglende kliktal viser en fundamental problemstilling for de internetbaserede modnarrativer. Da det er frivilligt, om den enkelte ønsker at se indholdet, og da de fleste i forvejen kæmper med at navigere i et kaotisk informationshav, er det tvivlsomt, om de normalitetsskeptiske unge vil vælge at betragte de sindrigt konstruerede modnarrativer. Videoer som disse kan måske med fordel bruges i eksempelvis folkeskoleundervisning (selvom dette heller ikke er uden risiko), men de vil finde meget lidt relevans for den egentlige målgruppe på nettet. Disse er i langt højere grad motiverede ud fra andre elementer og søger først og fremmest at få bekræftet egne ideer og radikale inklinationer.

Netop problemet med at ramme den rigtige målgruppe er et metodisk spørgsmål, som kalder på teknologisk assistance. Målgruppesegmentering blandt modnarrativer er endnu et underudforsket felt.[129] Ifølge Anne Aly handler det for de australske modnarrativer om at identificere alle sårbare unge, som er i ekstremismens risikogruppe, og overbevise dem om at "gå væk" fra ekstremismen.[130] Teknologien skal hjælpe os med at udpege den rigtige målgruppe og de rigtige individer. Herudover skal teknologien – som i Helfsteins tilfælde – hjælpe med at lokalisere den radikaliseringsfase, som er bedst egnet til en intervention. Helfstein definerer denne fase som værende 'acceptfasen', hvor de personlige omkostninger ved at overskride den naturligt forekommende normbarriere mellem ikke-vold og vold er størst.[131] Samme antagelse om "normative constraints on violent action" findes hos Anne Aly i form af en almindelig moralsk barriere for vold, som under indflydelse fra ekstremismen overskrides i en proces, hun kalder "moral disengagement".

Problemet er altså, at de mange antagelser om menneskers moralske natur og kommunikationens effekt ikke har blik for radikaliseringens meget individuelle og kontekstuelle karakter. Archetti kommer derfor med denne hårde dom over den strategiske kommunikation og de direkte modnarrativer:

129 Briggs & Feve, 2014: 19.

130 Anne Aly i et interview i The Guardian: http://www.theguardian.com/world/2014/aug/20/countering-violent-extremism-program-funding-not-renewed-in-budget

131 Helfstein, 2012: 3-4.

> "[B]ecause any individual interprets incoming information according to a personal narrative that is rooted in one's network of relationships at any given time, targeting extremists with the "right" message is, to put it bluntly, a waste of time.[132] "

Modnarrativernes implicitte radikaliseringsmodeller og antagelser om individet vil komme under yderligere kritisk behandling i rapportens del 3. Men først rettes fokus i del 2 på den tililende teknologiske assistance.

132 Archetti, 2015: 56.

Del 2:

KVANTITATIVE METODER TIL MONITORERING OG FOREBYGGELSE

> "Monitoring extremist and terrorist trends online, particularly using social media as a tool for visualising networks, has been crucial in recent surveillance as well as counter-terrorism and counter-extremism initiatives. Not taking down extremist content that does not breach counter-terrorism legislation is a valuable way for governmental and non-governmental practitioners to build a more accurate picture of the radicalisation process to improve strategies to tackle it.[133] "

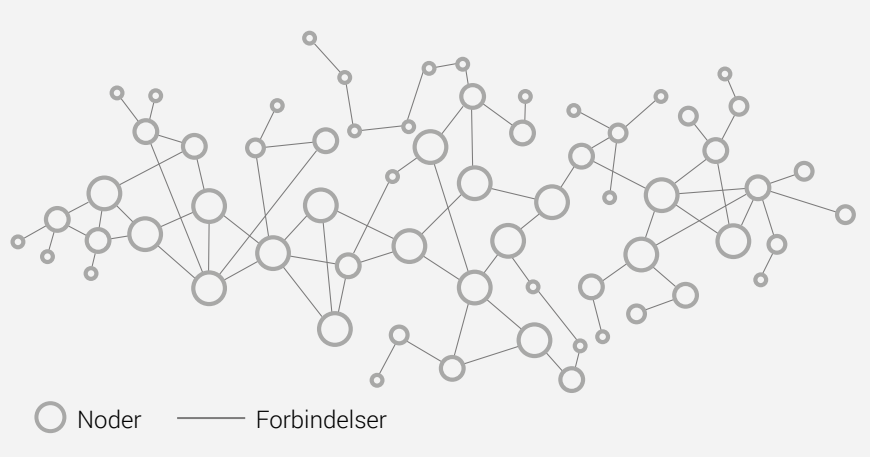
De beregningsmæssige og kvantitative metoder, som anvendes til monitorering og forebyggelse af online-radikalisering, placerer sig et sted i feltet mellem bløde og hårde tilgange – og i forlængelse af allerede eksisterende forebyggelsestiltag. Det er dog samtidig klart, at en alt for hård tilgang besværliggør arbejdet med open source intelligence (OSINT), da empirien derved fjernes fra nettet, og netværkets strukturer og dynamikker påvirkes, hvilket Saltman og Russell delvist er inde på i ovenstående citat.

Når de sociale mediers netværk og indhold analyseres med forskellige beregningsmæssige og kvantitative metoder, reduceres netværkets elementer typisk til en epistemologisk ramme bestående af to hovedelementer: noder og forbindelser. Denne reduktion udspringer af måden, netværksteorien definerer netværk på. Netværksanalyse har således fokus på relationerne mellem forskellige entiteter, hvor disse relationer deles op i en mængde noder (knudepunkter) og forbindelserne

133 Saltman & Russell, 2014: 8.

mellem disse noder (links). Netværk kan derfor i udgangspunktet være alt fra terrororganisationer til kognitive tankesystemer.[134] I radikaliseringsøjemed bliver disse dog ofte til netværk af radikale ideologier, radikalisatorer, grupperinger, sårbare unge osv.

Fig. 2: Tilgange til forebyggelse af online-radikalisering



De forskellige forsøg på at applicere beregningsmæssige og kvantitative tilgange til studiet af radikalisering kan groft opdeles i to faser. I den første fase, dataindsamling, anvendes metoder til (automatisk) sporing eller kortlægning af radikalt, hadefuldt eller ekstremistisk indhold og ekstremistiske netværk på internettet. I den anden fase, dataanalyse, anvendes metoder og modeller til egentlige analyser af det kortlagte materiale.

Dataindsamlingsdelen handler om at ekstrahere store mængder information ved brug af forskellige sorteringssystemer (disse kaldes ofte for web crawling- og data mining-teknikker), der optrevler netværkets forbindelser, samt forskellige tekst-klassifikationsprincipper, der sørger for at frasortere den 'harmløse' information. Analysedelen forsøger dernæst at få en dybere indsigt i ekstremistiske netværks funktion og sammensætning samt en indsigt i gruppers og individers brug af internettet. Via avancerede algoritmer analyseres indholdet i håbet om at kunne forklare adfærdsmæssige, strukturelle og sproglige karakteristika ved netværket.[135] I sidste instans ønsker tilgangene at kunne forklare og forudsige den potentielle online-radikalisering samt udpege radikaliseringstruede sårbare unge.

134 Cioffi-Revilla, 2010: 261; Lomborg, 2012: 6.

135 Correa & Sureka, 2013: 8-10; Cohen et al., 2014: 250; Ressler, 2006: 4; Cioffi-Revilla, 2010: 259.

Ud over sondringen mellem dataindsamling og dataanalyse er der forskel på, hvilke elementer dataindsamling og -analyse vælger at fokusere på. Overordnet kan teknikkerne inddeles efter indhold, struktur og anvendelse.[136] Indholdskortlægning- og analyse kan fx pege på informationer i tekst, video, lyd, metadata og hyperlinks, og foregår således med en hovedvægt på noderne. Struktur- eller linkanalyse kan i modsætning hertil modellere, visualisere og analysere forbindelserne mellem netværkets noder, hvilket fortæller lidt om de forskellige knudepunkters placering i forhold til hinanden. Mere konkret kan analysen opspore fællesskaber og fællesskabsforbindelser, finde centrale ledere samt klarlægge bestemte karakteristika for netværket.[137] Forskellen mellem netværks- og indholdsanalyse er dog en ren analytisk sondring. De er naturligvis afhængige af hinanden under selve dataindsamlingen, og i praksis (især i terror- og radikaliseringsforskning) anvendes de to tilgange ofte synkront.[138]

Fig. 3: Typologi over beregningsmæssige og kvantitative tilgange

	DATAINDSAMLING	DATAANALYSE	EPISTEMOLOGISK FOKUS
Indhold	Content mining	Tekst, lyd, video, metadata, hyperlinks • Holdningsdannelse • Tendenser og popularitet	Noderne: -Indholdets radikalitet
Struktur	Web link mining	Social netværksanalyse • Fællesskaber • Forbindelser mellem fællesskaber • Centrale ledere	Forbindelserne: -Knudepunkters placering og vigtighed
Anvendelse	Flow	?	Dynamiske skift i brugen

Endelig er det også muligt at analysere brugen af nettet, dvs. søgninger, klik, bevægelser mm. Der findes også beregningsmæssige simulationsmodeller, som fokuserer på systemdynamikker eller agentbaseret modellering. De kan potentielt anvendes til at simulere 'alternative' udviklinger inden for (kommunikationen i) terrornetværk m.m. Hertil kommer, at de beregningsmæssige simulationsmodeller

136 Correa & Sureka, 2013: 9.

137 Correa & Sureka, 2013: 13; Kaschesky et al., 2011: 318.

138 Bermingham et al., 2009; Gloor et al., 2009.

er mere realtidsfølsomme og mere avancerede end de simple netværksanalyser.[139] Disse værktøjer står dog endnu over for at blive færdigudviklet på terror- og radikaliseringsområdet, hvorfor indeværende redegørelse vil nøjes med at uddybe henholdsvis netværksanalysen (fx linkanalyse) og indholdsanalysen (fx analyser af holdningstilkendegivelser).

Litteraturen inden for området er en blandet landhandel med varierende metoder og teknologier. Somme tider er målgruppen eksplicit defineret, men oftest forbliver denne del uklar, da fokus i første omgang ligger på det rent metodiske. Men der er (i princippet) forskel på, om indsatsen retter sig mod at lokalisere de sårbare og radikaliseringstruede unge, som er genstand for terrorgruppers radikaliserings- og rekrutteringsbestræbelser (radikaliseringsforebyggelse), eller om indsatsen fokuserer på allerede aktive voldelige ekstremister (terrorbekæmpelse). Og der er forskel på, om indsatsen er rettet imod at lokalisere og kortlægge individer (noder) eller radikale miljøer (netværk).

Fig. 4: Analysernes forskellige målgrupper

	RADIKALISERINGSFOREBYGGELSE	TERRORBEKÆMPELSE
Netværk	**grupper/miljøer**, som er genstand for terrornetværks radikaliserings- og rekrutteringsbestræbelser	• terrorgrupper og miljøer • fx Islamisk Stat (i Irak og Syrien)
Noder	**individer**, som er genstand for terrornetværks radikaliserings- og rekrutteringsbestræbelser	• terrorister og terrorplanlæggere • fx Anders Behring Breivik

Herudover kan anvendelsen af beregningsmæssige og kvantitative metoder have forskellige intentioner. Skal analyserne kun sigte mod at undersøge og monitorere internetekstremismen, eller skal de også anvendes til direkte at forebygge radikalisering og bekæmpe terror?[140] Det første er en nødvendig forundersøgelse af det sidste, men kortlægning og undersøgelse af ekstreme miljøer og verserende diskurser fortæller ikke nødvendigvis meget om radikaliseringsproblemet.

139 Cioffi-Revilla, 2010: 264.

140 Neumann, 2011: 7.

Grundet en ofte uklar eller mangelende sondring mellem individer og miljøer før eller efter radikalisering, indeholder nedenstående gennemgang artikler fra forskellige lejre. Der er ofte en glidende overgang mellem efterretningsvirksomhed og socialpolitik – mellem antiterror og radikaliseringsforebyggelse – inden for dette forskningsområde.

Første afsnit i denne del 2 beskæftiger sig med netværksanalysen. Andet afsnit beskæftiger sig med indholdsanalysen. Begge afsnit starter ud med at gennemgå generelle principper, metoder og eksempler, hvorefter fokus skifter til en kritisk gennemgang af de metodiske problemstillinger, tilgangene står overfor i studiet af radikalisering og ekstremisme på sociale medier.

NETVÆRKSANALYSE

Netværksanalyser undersøger helt overordnet, hvorledes forskellige strukturer af noder og forbindelser er konstrueret, hvordan de udvikler sig, og hvordan de påvirker adfærden i eller omkring netværket.[141] Netværksanalyse kan derfor ifølge en del terroreksperter bidrage med vigtig viden om terrororganisationers unikke karakter i alt fra rekrutterings- og ekspansionsstrategi til den netværksinterne diffusion af radikale ideer.[142] Det er således en udbredt forestilling, at netværksanalysen kan kaste mere lys på, hvorledes sociale online-netværk og udbredelsen af radikale ideer er med til at radikalisere unge mennesker.[143]

Netværksanalysen forsøger med andre ord at forstå betydningen af (digitale) forbindelser mellem mennesker. I sin mest simple form fokuserer analysen på elementer som 'likes', 'følgere' eller 'delt indhold'. Analyser af sociale medier kan derfor bidrage med vigtig viden om, hvilke noder (hvem) i de ekstremistiske miljøer og terrornetværk, som er involveret i rekruttering og propagandaudbredelse på de sociale medier, samt hvilke mekanismer denne informationsdeling er karakteriseret ved. Og når de forskellige netværksanalyser kombineres med indholdsanalyser, kan de, ifølge blandt andre Peter Neumann, blive vægtige redskaber til opstilling af modeller, som skal forudsige internetinspirerede terroraktioner.[144] Det er under alle omstændigheder ofte med det håb, de forskellige nye teknologier introduceres.

141 Helfstein, 2012: 37.

142 Ressler, 2006: 1.

143 Cioffi-Revilla, 2010: 262.

144 Neumann, 2013: 451.

Indeværende afsnit om netværksanalyser er opdelt i to underafsnit. Første underafsnit redegør for netværksanalysens metoder og centrale principper fulgt op af nogle eksempler på metodens anvendelsesmuligheder. Andet underafsnit udfolder diskussionen af de metodiske og analysemæssige problemstillinger som medfølger, når netværksanalysen appliceres på terror- og radikaliseringsforskning.

Metoder og eksempler

Netværksanalysen kortlægger noder og forbindelser gennem forskellige halv- og helautomatiske teknikker. Som regel tager kortlægningen af netværkets hyperlinks eller sociale forbindelser afsæt i en række nøgledata (seeds), dvs. URL-noder/IP-adresser, brugernavne, e-mailadresser, osv. – fx et velkendt jihadiforum eller brugerprofilen for en berygtet foreign fighter. Disse nøgledata er autoritativt givet ud fra kilder med ekspertise på området og fungerer som node-afsæt for snowballing eller optrevling af link-strukturen.[145] Denne proces kaldes også ofte for web crawling og er baseret på avancerede computeralgoritmer, der detekterer visse tendenser og optrevler de forbindelser, det omkringliggende netværk består af.[146] I princippet svarer denne proces lidt til at surfe på internettet bortset fra, at web crawler-programmet minutiøst åbner alle links for at kortlægge, hvor de fører hen.

Netværksanalysen kan dernæst måle styrken af netværkets forbindelser gennem forskellige mål af nodecentralitet (popularitet), samt mål for netværkets karakter, fx tæthed. Dette giver en fornemmelse for netværkets størrelse samt centrale og indflydelsesrige aktører. Analysen interesserer sig ofte særligt for aktører med høj centralitet, da de vurderes at være indflydelsesrige. Særlig interesse har aktører med høj betweenness centrality. Dette er aktører, der kobler flest geodætiske stier (forbindelser) og således forbinder klynger af netværk, dvs. de fungerer som informationsbro mellem forskellige domæner eller fællesskaber.[147] Et godt eksempel på en node eller aktør med høj betweenness centrality er de tidligere omtalte online-jihadister, som forbinder netværk af fremmedkrigere og terrororganisationer i Mellemøsten med netværk af sympatisører i Vesten.

Kvantitative analyser bør forholde sig til klassiske positivistiske validitetskriterier som repræsentativitet, reliabilitet (pålidelighed) og gentagelighed. Validiteten sikres i første omgang ved at indsamle data korrekt – dvs. at få en datagengivelse, som

145 Correa & Sureka, 2013: 15.

146 Brynielsson et al., 2012: 199; Gloor et al., 2009: 215.

147 Bermingham et al, 2009: 5; Gloor et al., 2009: 217; Klausen, 2014.

svarer til det oprindelige system. Om denne repræsentativitet så dækker en antaget virkelighed bag de sociale netværk, må vurderes og antages ud fra anden forskning. Datagengivelsen skal ikke nødvendigvis indeholde alle de samme informationer, men den skal dog bevare en vis konsistens af både noder og indhold. Ved sociale medier betyder dette, at såvel venskabsforbindelser som beskeder og opdateringer ideelt set skal være tilgængelige, hvilket stiller store krav til beregningssystemernes kapacitet og regnekraft. Fungerer denne dataindsamling optimalt, vil en anden forsker, under uændrede forhold, kunne finde frem til samme data og påvise de samme tendenser. Forskningens reliabilitet (pålidelighed) garanteres ved at sikre, at data mining og dataanalyse afstedkommer konsistente og gentagelige resultater over tid. Dette betyder at både 'lagring' og data mining må vedblive at indhente sammenlignelige data. De sociale mediers omskiftelige karakter taget i betragtning kan reliabiliteten blive en stor udfordring. Der kan både ske ændringer i platformenes funktionsmåde, ligesom brugerne over tid kan emigrere til andre platforme.[148]

Det er således en udbredt forestilling, at netværksanalysen kan kaste mere lys på, hvorledes sociale online-netværk og udbredelsen af radikale ideer er med til at radikalisere unge mennesker.

Disse kriterier sætter andre af netværksanalysens egenskaber under pres og implicerer videnskabelige antagelser om, at fænomenet er konstant. Men et af netværksanalysens helt store styrkeområder er netop, at det er et øjebliksbillede af fænomener i stadig forandring. Forskellene mellem to stillbilleder af netværket viser lidt af det flow og de tendenser, som karakteriserer netværket. En styrke ved netværksanalysen er således, at det med tiden bliver muligt at beskrive bevægelserne – analyseperspektivet skifter fra objekt til flow, som dernæst kan visualiseres og anskueliggøres på forskellig vis.[149] Ligesom to tilfældige billeder fra en fodboldkamp siger meget mindre om kampens udvikling og konsekvenser end en film over hele forløbet, lige så lidt siger to tilfældige tværsnit af sociale netværk sammenlignet med dokumentation af udviklingen over tid. Men netop denne longitudinale analyseproces stiller store krav til de indsamlede datas kvalitet. Alt afhænger dog naturligvis af, hvilke analyser man ønsker at foretage.

148 Falkenberg, 2012: 18-19.

149 Markham, 2012: 48.

Analyserne kan endvidere anskueliggøre sociale netværk gennem grafer og diagrammer, der bl.a. visualiserer og klarlægge forbindelserne mellem noderne. Analysernes visuelle karakter gør resultaterne lettere at afkode og fortolke for forskere uden indgående kendskab til de anvendte beregningsteknikker. Analyserne siger dog meget lidt om nodeindholdets kvaliteter og netværksegenskaberne på det semantiske niveau.[150] Her bliver en supplerende indholdsanalyse nødvendig.

Blandt nogle forskere i radikalisering og ekstremisme er netværksanalysen også blevet populær, fordi den giver indblik i den radikale ideologis udbredelse og dermed peger tilbage på ekstremismens centrale online-aktører. Scott Helfstein betragter eksempelvis den digitale ideologiske propagandaudbredelse som et flow af informationer mellem individer, der påvirker en proces, han kalder netværks-radikalisering. Hertil skal ifølge Helfstein lægges, at de sociale netværk faciliterer den operationelle planlægning, mobilisering og udførelse af terrorplots.[151] Helfsteins teknologiske løsningsforslag er at analysere sig frem til, hvornår de radikaliserede unge mennesker træder ind i tredje fase (af Helfsteins fire-fase-model), hvor det er mest effektfuldt fra myndighedernes side at intervenere.[152]

Blandt nogle forskere i radikalisering og ekstremisme er netværksanalysen også blevet populær, fordi den giver indblik i den radikale ideologis udbredelse og dermed peger tilbage på ekstremismens centrale online-aktører.

Netværksanalysen gør det muligt at opdage og visualisere implicitte fællesskaber og centrale skikkelser eller organisationer i netværket.[153] Dette gør det lettere for både forebyggelse og terrorbekæmpelse at være mere målgruppefokuseret samt at få et øget kendskab til målgruppen. Herudover kan analysen redegøre for andre topologiske karakteristika: om relationerne mellem individer eller organisationer bygger på forskelle eller ligheder; om netværket er konflikt- eller konsensusskabende; om det er centraliseret eller opdelt.[154] Ved at finde svar på disse spørgsmål formår netværksanalysen at føje mere substans til radikaliseringsmodellernes meso-niveau og derved forbinde radikaliseringsmodellernes mikro- og makro-niveau.[155]

150 Lomborg, 2012: 6.
151 Helfstein, 2012: 37.
152 Helfstein, 2012: 4.
153 Correa & Sureka, 2013: 19.
154 Caiani & Wagemann, 2009: 70.
155 Caiani & Wagemann, 2009: 69.

Et godt eksempel på denne berigelse af ekstremismeforskningens mesoniveau er en britisk rapport om foreign fighters fra 2014: "#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks". Her har en gruppe forskere fra "The International Center for the Study of Radicalisation and Political Violence" (ICSR) ved Kings College i London i et år fulgt en række britiske foreign fighter-profiler på Facebook og Twitter.[156] Forskergruppen bruger i første omgang netværksanalysen til deskriptivt at analysere individer relateret til terror og voldelig ekstremisme i udlandet. Fokusgruppen for undersøgelsen er med andre ord den voldelige ekstremismes fortrop, og rapporten synes hverken at interessere sig synderligt for forebyggelse eller policy-løsninger. At forskningsinteressen er rettet mod den skarpe ende af spektret ses også ved, at radikalisering som fænomen kun nævnes i spekulative og vagt formulerede vendinger to steder i rapporten.

Til at indsamle data (og analysere dem via netværksanalyse) har forskergruppen blandt andet anvendt et af de nyeste skud på stammen over data mining-programmer, Palantir Torch, som er udviklet med støtte fra blandt andre CIA. Databasens nøgledata bestående af 190 profiler på Facebook og Twitter (heraf 121 unikke profiler), er dog fundet ved manuel snowballing over 12 måneder. Den manuelle og ekspertdrevne udvælgelsesmetode virker således bedst til udpegning af små sæt af noder, som gemmer sig i en større population af brugerprofiler.

Den indsamlede data, kombineret med en grundig kvalitativ metode og en stor mængde online-interviews, har indtil videre udartet sig i én rapport. Ved at betragte og kvalitativt udvælge unikke fremmedkriger-konti har forskergruppen været i stand til at erkende mønstre i informationsspredningen for særligt fremmedkrigere tilknyttet de to konkurrerende sunni-ekstremistiske terrorgrupper Jabhat al-Nusrah og Islamisk Stat.[157]

Rapporten finder blandt andet, at krigerne i Syrien har udpræget realtids-kontakt med hinanden såvel som med den hjemlige diaspora. Denne kontakt finder ofte sted via en lille gruppe meget aktive nyhedsdistributører, som ofte ikke er direkte tilknyttet nogen grupper, men som sympatiserer med og deler informationer fra de forskellige organisationer. Distributører kommer derved til at forbinde forskellige fællesskaber. Herudover lokaliserer rapporten en ny klasse religiøse autoriteter, som taler flydende

156 Carter et al., 2014.

157 Carter et al., 2014: 1.

engelsk, og som gør sig bemærket ved at være behændige i brugen af sociale medier. Rapporten udpeger her særligt to centrale prædikanter: amerikaneren Ahmad Musa Jibril og australieren Musa Cerantonio.[158]

Vha. netværksanalysen fastslår forskergruppen også, at der øjensynligt findes mange online-jihadister, der, som den berygtede Irhabi 007 (Younis Tsouli), ikke praktiserer en aktiv voldelig ekstremisme uden for online-virkeligheden.[159] Herudover finder gruppen, at de sociale mediers åbenhed har medført dissens og diskussionslyst blandt forskellige krigere og tilhængere, hvilket hævdes ikke at være normalt på de mere kontrollerede og lukkede jihadi-fora.[160] Rapporten bidrager altså med en række indsigter i dynamikkerne og netværksstrukturerne i den sunni-ekstremistiske onlinekultur.

Ved at betragte og kvalitativt udvælge unikke fremmed-kriger-konti har forskergruppen været i stand til at erkende mønstre i informationsspredningen for særligt fremmed-krigere tilknyttet de to konkurrerende sunni-ekstremistiske terrorgrupper Jabhat al-Nusrah og Islamisk Stat.

Jytte Klausen fra Brandeis University i Massachusetts har sammen med et forskerhold fortaget et sammenligneligt studie.[161] Forskerholdet har taget udgangspunkt i 59 nøglekonti (seed accounts) af kendte vestlige fremmedkrigere i Syrien og Irak, som de har snowballet ud fra. Herefter har de kvantitativt kortlagt et netværk af fremmedkrigere. Indholdet har de dog efterfølgende kodet med kvalitativ metode udført af et hold af kodere.

Klausens resultater bekræfter nogle af konklusionerne i briternes rapport, men de stiller også spørgsmål ved andre. Klausen finder bl.a., at de såkaldte nye religiøse autoriteter har mindre indflydelse end briternes fund synes at antyde, og at de centrale og indflydelsesrige aktører i stedet skal findes omkring profiler og brugere, der er nært knyttet til al-Muhajiroun-miljøet omkring den radikale britiske salafist Anjem Choudary.[162] Forskellen i disse fund tilskriver Klausen bl.a. forskellen i metoder (omtales i næste afsnit).

158 Carter et al., 2014: 1.
159 Carter et al., 2014: 15-16.
160 Carter et al., 2014: 17.
161 Klausen, 2014.
162 Klausen, 2014.

Klausen finder også, at de forskellige jihadist-bevægelser slet ikke er så bottom up-baserede, som vi ellers forestiller os. Der er stramme tøjler i kontrollen med de sociale medier.[163] Endelig finder rapporten en klasse af kvindelige supportere – Klausen benævner dem 'Umm-faktoren', da mange profilnavne anvender denne præfiks (Umm er arabisk for mor). Således konstaterer rapporten en informationsstrøm, der starter med officielle profiler fra de forskellige terrorgrupper og undergrupper, som kæmper i Syrien og Irak. Disse informationer videredistribueres af fremmedkrigere i de respektive krigsområder, og herfra bliver informationerne delt af Umm'erne og andre følgere i Vesten.[164]

Carter et al. og Klausen havde i deres analyse fokus på noderne og nodernes betydning for informationsstrømmene. Denne tilgang kan siges at være individorienteret med fokus på en forståelse af sammenhængen mellem individ (mikroniveau) og miljø (mesoniveau). En anden tilgang kan være at supplere komparative analyser på makroniveau (fx staters politiske mulighedsstrukturer) med netværksanalysens blik på miljøet.

Et studie af Manuela Caiani og Claudius Wagemann anvender netop denne tilgang.[165] Caiani og Wagemann sammenligner via netværksanalysen Italiens ekstreme højrefløj med sin tyske ditto. Forfatterne anvender ekspertudvalgte nøgledata som afsæt for web crawling af statiske hjemmesidenetværk i de to lande. 'Partner sites', dvs. reciprokke eller gensidige netværksforbindelser, ses som udtryk for stærke forbindelser og som en indikator af tætheden mellem organisationerne. Disse links fortolkes også som spor efter kommunikation organisationerne imellem og som organisationernes redskab til gensidigt at hjælpe hinanden ud i offentligheden.[166] Forfatterne finder en række forskelle i de to landes højrenationale online-netværk, som de forsøgsvis tilskriver forskellene i landenes politiske mulighedsstrukturer og den politiske kulturs organisering i landet.[167] Forfatterne finder således, at Italiens netværk er polycentrisk opdelt, hvorimod det tyske netværk er stærkt centraliseret.[168]

Netværk illustreres ofte gennem komplekse modeller, der afbilleder et net af noder og forbindelser – somme tider med angivelser for reciprokke forbindelser. En anden måde at illustrere dette på, og samtidig hente flere informationer ud af de givne

163 Klausen, 2014.
164 Klausen, 2014.
165 Caiani & Wagemann, 2009.
166 Caiani & Wagemann, 2009: 68-71.
167 Caiani & Wagemann, 2009: 66.
168 Caiani & Wagemann, 2009: 92.

data, er at kombinere netværket med geografiske data, såfremt de er tilgængelige.[169] Et velkendt eksempel på et sådant socialgeografisk informationssystem er Google Earth; en søgemaskine, der forbinder geodata med andre søgeinformationer. Der er gjort enkelte forsøg på at kortlægge terrornetværk gennem anvendelsen af geodata for derved at undersøge vigtigheden af geografisk nærhed ved dannelsen af terrornetværk.

Richard M. Medina og George F. Hepner har udført et makrostudie af islamistiske terrornetværk, hvor de analyserer netværkene som sociogeografiske systemer ved brug af netværksanalyse.[170] Forfatterne operationaliserer det geografiske rum i intervaller af tusinde kilometer og viser derved, hvorledes langt de fleste direkte links fra de islamistiske netværk går til noder inden for den første rumlige afgrænsning – dvs. Inden for de første tusinde kilometer. Dette får forfatterne til at konkludere, at den globaliserede terrorisme i virkeligheden er knap så global, som den er forankret lokalt i klan-netværk, kulturelle identiteter og ideologiske anskuelser. Moderne terrornetværk er derfor ifølge forskerne begrænsede af sociale, virtuelle og geografiske rum, og de er først og fremmest afhængige af en kort afstand mellem noderne.[171] Netværkenes koncentration får Medina og Hepner til at konkludere, at islamistiske terrorister enten samler sig i bestemte områder, eller at det først og fremmest er folk fra regionen, som danner de forskellige terrornetværk.[172] Social interaktion på internettet er således, ifølge deres studie, mere sandsynlig, hvis den geografiske afstand er relativt kort.[173] Med andre ord fremhæver deres studie (af online-netværk) betydningen af en offline-virkelighed. Men hvad der er årsagen hertil (kulturelle, sproglige, mediemæssige kontekster?) finder rapporten ikke noget svar på. Fokus for de to forfattere er da også primært at videreudvikle en metode, der sammenholder geospatiale og sociale analyser.

Et af de studier, der i højere grad forsøger at nærme sig policyambitioner om at forbedre forebyggelsesindsatsen gennem netværksanalysen, er J.M. Berger og Bill Strathearns studie af højrenationale twitterkonti i USA.[174] Ifølge forfatterne er det nemt at identificere tusindvis at profiler på de sociale medier, som har et radikalt indhold. Men det er straks vanskeligere at afgøre, hvem der er værd at holde øje

169 Cioffi-Revilla, 2010: 262.

170 Medina & Hepner, 2011: 577.

171 Medina & Hepner, 2011: 578.

172 Medina & Hepner, 2011: 591-593.

173 Medina & Hepner, 2011: 593.

174 Berger & Strathearn, 2013.

med.[175] Et af forfatternes fokusområder er således forsøget på at udvikle en teknik til mere præcis udgrænsning af svage og påvirkningstruede unge mennesker, der eventuelt kan blive genstand for myndighedssponseret holdningspåvirkning og målrettede modnarrativer.[176] Til det formål forestiller de sig, at socialkonservative meningsdannere vil være gode alliancepartnere, da de vil have mulighed for ideologisk at nå ind til målgruppen.[177]

For at kunne optegne et fyldestgørende billede af den højrenationale online-ekstremisme har Berger og Strathearn taget afsæt i 12 nøglekonti, der er åbne profiler. Herudover medinddrager de informationer om de enkelte brugeres ideologiske selvidentifikation som udtryk for stort politiske engagement.[178] Herigennem udarbejder de et pointsystem, der gør det muligt at sortere i de mange tusinde aktive profiler med interesse for voldelig ekstremisme og afgøre, hvem der udgør den relevante målgruppe – hvem der er mest indflydelsesrig, og hvem der har størst risiko for at blive påvirket.[179]

Tanken har således været, at sociale medier og ekstremistiske fora kunne overvåges for at afdække soloaktører uden fysisk kontakt til ekstremistiske miljøer. Opsporingen er ifølge Neumann mulig, fordi disse aktører efterlader tilstrækkeligt med virtuelle spor, som efterforskere potentielt vil kunne benytte til at optegne deres interesser, lidenskaber og intentioner.

Berger og Strathearn finder, at indflydelse og eksponering er koncentreret omkring den øverste ene procent af twitterbrugerne, samt at der synes at være en høj korrelation mellem indflydelse/eksponering og engagement med nøglekontoens ideologi.[180] Efter deres vurdering er de mest radikaliseringssårbare twitterbrugere dem, som ligger mellem nummer 200 og 500 på den udarbejdede rangliste, da deres interaktioner indikerer en interesse i ekstremistisk ideologi, som endnu ikke er blevet til en ensidig besættelse. Berger og Strathearn fastslår dog, at flere undersøgelser kræves, som evaluerer deres fund, og som forsøger at indfange

175 Berger & Strathearn, 2013: 3.
176 Berger & Strathearn, 2013: 16.
177 Berger & Strathearn, 2013: 8.
178 Berger & Strathearn, 2013: 12.
179 Berger & Strathearn, 2013: 3.
180 Berger & Strathearn, 2013: 4.

endnu flere karakteristika for twitterbrugere i risikogruppen. Samtidig må mulige interventionspraksisser undersøges. Her fremsætter forfatterne dog et inspirationskatalog af policy-løsninger til forbedring af ekstremismeforebyggelse.[181]

Ovenstående eksempler belyser netværksanalysens metodiske og analysestrategiske alsidighed. Men en af de helt store drivkræfter bag indførelsen af netværksanalyser i terror- og forebyggelsessammenhæng har naturligvis været håbet om at kunne detektere de sårbare unges begyndende radikalisering og de ensomme ulves kampforberedelser. Tanken har således været, at sociale medier og ekstremistiske fora kunne overvåges for at afdække soloaktører uden fysisk kontakt til ekstremistiske miljøer. Opsporingen er ifølge Neumann mulig, fordi disse aktører efterlader tilstrækkeligt med virtuelle spor, som efterforskere potentielt vil kunne benytte til at optegne deres interesser, lidenskaber og intentioner. Endnu vigtigere kan deres online-aktivitet, såfremt myndighederne følger dem meget nøje, afsløre pludselige forandringer i adfærden: tiltagende trusler, forespørgsler om bombemanualer, kontakter til udenlandske grupperinger eller en direkte proklamation om en nært forestående aktion. Neumann fremhæver, at der er mange eksempler på soloaktører, som netop deler deres intentioner med andre via nettet.[182] Denne del af analysearbejdet bevæger sig dog et stykke ind på indholdsanalysens banehalvdel og vil derfor blive omtalt yderligere i afsnittet om indholdsanalyse.

Metodiske problemstillinger

Som ovenstående gennemgang tydeliggør, kan netværksanalysen kobles til en mængde teorier og tilgange, og den tilbyder en række brugbare indsigter i de sociale mediers funktion på radikaliseringsforskningens meso-niveau. Dette er bl.a. muligt gennem netværksanalysens særlige kompleksitetsreducerende epistemologi. Men et generelt og overordnet problem ved at anvende netværksanalyse er samtidig, at metoden netop har kompleksitetsreduktion som formål. Herved må en mængde faktorer udgrænses, som ellers også spiller en stor rolle for radikaliseringsproblemstillingen – det drejer sig om alt fra individuelle/biografiske faktorer til strukturelle og politiske problemstillinger på makro-planet.[183] Og heri består netop en af farerne ved at anvende netværksanalyse på så komplekse fænomener som radikalisering: den stærke reduktion risikerer at føre til overfortolkning af de inkluderede effekter og indikere kausalitet, hvor der reelt set kan være tale om en mængde spuriøse sammenhænge eller tilfældigheder, hvilket vil sige, at det, som ligner sammenhænge

181 Berger & Strathearn, 2013: 43.

182 Neumann, 2013: 451.

183 Lamberty, 2013: 132; Mejias, 2006.

mellem to variabler, i virkeligheden blot er et sammenfald, der kan skyldes tilfældigheder, eller at begge variabler påvirkes af den samme mellemliggende variabel.[184] Det er således ikke muligt i et radikaliseringsforskningsperspektiv at kontrollere for alle baggrundsvariabler (holde deres indflydelse konstant), hvilket en kvantitativ multivariat analyse som netværksanalysen ellers fordrer.[185]

Et centralt problem er, at datagrundlaget begrænser sig til ukomplette og somme tider ukorrekte offentligt tilgængelige oplysninger – det såkaldte open source intelligence (OSINT) – hvorfor en stor del af online-virkeligheden formodentlig stadig ligger skjult et sted i internettets mørke.

Herudover er der en række teknisk-metodiske problemstillinger forbundet med anvendelse af social netværksanalyse. Den første problemstilling handler om, hvordan store men ukomplette datasæt håndteres og fortolkes. Analyserne er ofte kun halvautomatiske, hvilket kan medføre en del manuelt arbejde for alene at frasortere irrelevant information. Hertil kommer, at indholdet – specielt med udviklingen af web 2.0 – er stadig mere flygtigt og under konstant forandring, hvilket bevirker, at visse analyser af dataudtræk allerede er forældede, inden de er afsluttede. Sker der forandringer i systemdynamikkerne påvirker det analysens grundlæggende algoritmer, hvorfor netværksanalysen står over for nogle svære udfordringer på så omskifteligt et område som terror og radikalisering. Det er med andre ord i udgangspunktet kun muligt at sige noget om fortiden og lidt om nutiden, hvorimod det fortsat vil være svært at komme med forudsigelser og prognoser for udviklingen, hvilket ellers er en forudsætning for en vellykket forebyggelsesindsats.[186]

Dette giver en række problemer og begrænsninger for indsamling og fortolkning af data. Medina og Hepner lokaliserer nogle hovedproblemer vedrørende dataindsamlingen.[187] Et centralt problem er, at datagrundlaget begrænser sig til ukomplette og somme tider ukorrekte offentligt tilgængelige oplysninger – det såkaldte open source intelligence (OSINT) – hvorfor en stor del af online-virkeligheden formodentlig stadig ligger skjult et sted i internettets mørke.[188] For netværksanalysen medfører

184 Agresti & Finlay, 1997: 362.

185 Agresti & Finlay, 1997: 359; Ressler, 2006: 6.

186 Correa & Sureka, 2013: 24.

187 Medina & Hepner, 2011: 582-583.

188 Carter et al., 2014: 12.

det altså et 'ude af øje, ude af sind'-problem. Hvis der ikke foreligger nogen online-informationer om ekstremister eller terrorister, 'findes de ikke'. Men reelt er problemet, at de blot ikke optræder inden for den virkelighedshorisont, som et socialt onlinenetværk af noder og forbindelser lader fremtræde.[189] Og vi ved ikke, hvor meget vi ikke ved. På grund af problematikkens højspændte karakter er informationsmaterialet dog fuldt af huller og fejl og i visse tilfælde bevidst manipulation. Derfor bør informationer som minimum søges bekræftet fra mange forskellige kilder samtidig.

Den anden problemstilling handler om repræsentationen af nodedynamikken. Som forklaret tidligere er sociale online-fællesskaber nogle meget foranderlige størrelser. Men de fleste netværksanalyser tager i realiteten et stillbillede af noget, som er i bevægelse, og det kan følgelig være svært at komme med præcise udsagn om billedets betydninger. Derfor er analyserne stærkest, når de fortæller noget om bevægelserne i sig selv. Men dette kræver realtids-analyser på et meget komplekst og højt niveau, og såvel regnekraften som de komplicerede computer-algoritmer, der skal styre slagets gang, er endnu i den spæde begyndelse for så vidt angår terrorisme- og radikaliseringsforskning.

Problemet er, at jo mere komplekse de analyserede processer er, jo flere perspektiver falder uden for den epistemologiske ramme af noder og forbindelser. Og som rapportens sidste radikalise-ringsteoretiske afsnit vil blotlægge, er den ekskluderede mængde stor, når radikalisering er undersøgelsesspørgsmålet.

Metodisk står analyserne altså stadig på et begynderstadie, hvor mere dynamiske algoritmer til realtids-analyser samt data mining-værktøjer til de hurtigt forandrende sociale medier er efterspurgt. Mange modeller skabes uden komplette datasæt, og selv de bedste analyseredskaber indfanger en mængde 'hvid støj' i form af aktiviteten fra journalister, universitetsstuderende eller almindelige videbegærlige mennesker, som ellers intet har med radikalisering og terror at gøre. Analyser af trafikken på de forskellige ekstremistiske hjemmesider og internetfora har således i nogle tilfælde været konfronteret med den problemstilling, at visse værdier eller målinger er blevet forstærket alene grundet 'forskerinteresse' og 'efterretningsklik'.[190]

189 Ressler, 2006: 4; Mejias, 2006.

190 Zelin, 2013: 7.

Det betyder, at analyseresultaterne kan være misvisende, da de ikke medregner adfærdsmæssige og kontekstuelle elementer, der potentielt kan påvirke netværkets udseende og aktiviteter, men som også kan optræde uden sammenhæng hermed.[191] Problemet er, at jo mere komplekse de analyserede processer er, jo flere perspektiver falder uden for den epistemologiske ramme af noder og forbindelser. Og som rapportens sidste radikaliseringsteoretiske afsnit vil blotlægge, er den ekskluderede mængde stor, når radikalisering er undersøgelsesspørgsmålet.

Det er således ikke muligt helt at adskille analysen af fænomenet fra forskningens og mediernes effekt herpå. Men netop heri ligger også, potentielt set, en af netværksanalysens styrker. Den tvinger os til at redefinere, hvad vi opfatter som analysens studieobjekt. Ved at betragte de sociale fænomener gennem de dynamiske sociale medier tvinges forskningen til at betragte strukturer og "det sociale" som foranderlige og midlertidige størrelser.[192]

Den tredje problemstilling handler om at aftegne grænserne til gruppen af sårbare, ekstremistiske og såkaldt radikaliserede unge. Her falder analysen tilbage til de ontologiske antagelser om individet, ideologien osv., som må tilskrives feltet, inden det kan analyseres. Mange års diskussioner i terror- og radikaliseringsforskningen er ikke kommet frem til nogen entydig definition af hverken terrorisme, ekstremisme eller radikalisering. Men en del af netværks- og indholdsanalyserne mangler endnu helt at omfavne konsekvensen af de mange uafklarede begrebsmæssige, ontologiske og radikaliseringsteoretiske spørgsmål. Det er særligt problematisk på et område som ekstremisme- og radikaliseringsforskning, hvor informationsstrømmens flydende og dynamiske karakter fordrer stor sikkerhed i teori og metode.[193]

Herudover repræsenterer den halvautomatiske metodes valg af nøgledata et videnskabsteoretisk problem. Hvem er de 'autoritative kilder', og hvad bestemmer relevansen af én kilde frem for en anden? Denne overvejelse finder sjældent plads i akademiske artikler, og netop udvælgelsen vidner om metodens dybest set politiske karakter, da udvælgelsen ikke springer ud af objektive forhold, men begrænser sig til nogle valgte (politisk givne) parametre. Som bekendt indeholder ethvert valg også et fravalg. Heller ikke inden for terror-litteraturen er der konsensus om, hvilke organisationer og hvilke personer, som er de mest centrale, mest ekstreme eller mest

191 Ressler, 2006: 6.

192 Markham, 2012: 52.

193 Correa & Sureka, 2013: 24.

indflydelsesrige. I eksemplerne på analysen af fremmedkriger-profiler vil en forsker, der borer sig ind i netværket fra en anden samling nøglekonti – fx konti af folk baseret i de omkringliggende arabisktalende lande – formodentlig finde frem til helt andre netværksledere.[194] Men hvis netværket afgiver et andet billede ved, at man starter et andet sted, er det samtidig et væsentligt problem for analysernes validitet. Er der overhovedet tale om det samme netværk?

En del af forskellen mellem konklusionerne fra henholdsvis Klausens forskningsgruppe[195] og forskerne på Kings College[196] tillægger Klausen således netop forskellen i metoden og angrebsvinklen på dette punkt. De starter med hver deres lille bid af Twitter-netværket, som de efterfølgende arbejder ud fra. Herudover er observationsperioden for de to studier overlappende, men ikke den samme. Dette understreger forskningsresultaternes midlertidige karakter.[197]

Som bekendt indeholder ethvert valg også et fravalg. Heller ikke inden for terror-litteraturen er der konsensus om, hvilke organisationer og hvilke personer, som er de mest centrale, mest ekstreme eller mest indflydelsesrige.

De metodiske begrænsninger peger også på et grundlæggende problem ved Caiani og Wagemanns komparative netværksanalyse. Det er naturligvis i sig selv interessant at kunne se korrelation mellem politiske mulighedsstrukturer og højrefløjens organisering, men analysen ser også bort fra en lang række forhold, der evt. kan være spuriøse variabler i den opstillede kausalforklaring. Hvad med politisk kultur, politisk historie osv.? Problemet handler dog primært om faktorer, som det er muligt at finde data på, eller som kan analyseres i andre komplementære analyser. På individniveau, hvor det særligt handler om den systematiske selvangivelse af biografiske data, er spørgsmålet endnu mere komplekst. Det er de færreste Facebook- og Twitterkonti, som ligefrem beretter ærligt om alt fra barndommens marginalisering til hverdagens anerkendelseskamp.

194 Klausen, 2014.
195 Klausen, 2014.
196 Carter et al., 2014.
197 Klausen, 2014.

Det er også et problem for fortolkningen af data, at de fleste forskere med teknisk ekspertise i netværksanalyse ikke har baggrund i terror- og radikaliseringsforskning.[198] De sætter ofte deres lid til meget simple radikaliseringsmodeller, som de har kunnet læse sig til i den rigt citerede policy- og tænketankslitteratur, uden at reflektere nærmere over radikaliseringsmodellernes forklaringskraft og videnskabelighed. Modellerne, som eksempelvis Wiktorowicz' model, har mødt stor kritik i akademiske kredse (psykologi, socialpsykologi, sociologi og politologi) og regnes blandt mange for at være uvidenskabelige. Rapportens del 3 dykker dybere ned i dette spørgsmål.

De metodiske problemstillinger understreger også en anden pointe ved netværksanalysen. Analysen er relativt nem at udarbejde, da der efterhånden findes et stort udvalgt af tilgængelige værktøjer. Til gengæld er det en kunst at kunne fortolke analysens resultater. Fortolkningen kræver både stor metodisk, teoretisk og empirisk indsigt.

De metodiske begrænsninger samt ekstremismens og radikaliseringens individuelle og kontekstuelle påvirkningsfaktorer gør det herudover svært at generalisere mediebrugen til andre grupper og netværk eller andre kontekster. De indsamlede data som Carter et al. møjsommeligt analyserer, kan derfor ikke uden videre siges at være repræsentative for vestlige fremmedkrigere eller for britiske fremmedkrigere, der ikke anvender de sociale medier på samme vis eller i samme udstrækning. Det er svært at generalisere ud over den efterforskede gruppe.[199] Hertil kommer problemet med de selvangivne biografiske data. Selvom forskerne har forsøgt kvalitativt at vurdere og dobbelttjekke informationerne, ved de kun, hvad de enkelte krigere selv har valgt (strategisk eller ej) at dele om sig selv og om den gruppe, de kæmper for – enten gennem offentlige statusopdateringer, offentlige diskussioner eller private online-interview.[200]

Problemet med 'selvangivelse' betyder også, at analysen har måttet udelade brugere med restriktive privatlivsindstillinger eller manglende villighed til at deltage i forbindelse med kortlægning af netværk. Forfatterne reflekterer desværre ikke over, hvorledes dette kan tænkes at påvirke resultaterne, og hvad det betyder for den efterfølgende fortolkning og anvendelse. Den samme problemstilling gør sig gældende for Berger og Strathearn.[201]

198 Ressler, 2006: 6.

199 Carter et al., 2014: 11.

200 Carter et al., 2014: 10.

201 Carter et al., 2014: 12; Berger & Strathearn, 2013: 13.

Som Klausen også fastslår, kan det være svært, hvis ikke umuligt, at fastslå identiteten af visse brugere, hvilket er endnu et problem for validiteten af undersøgelsen.[202] Somme tider skifter konti oven i købet ejer på tværs af køn. Herudover spekulerer Klausen over, hvorfor der med flere tusinde vestlige fremmedkrigere i Syrien og Irak kun er en lille gruppe, som er ekstremt aktive online? Det er Klausens egen fortolkning, at dette skyldes en høj grad af intern mediekontrol og censur.[203]

De metodiske problemstillinger understreger også en anden pointe ved netværksanalysen. Analysen er relativt nem at udarbejde, da der efterhånden findes et stort udvalgt af tilgængelige værktøjer. Til gengæld er det en kunst at kunne fortolke analysens resultater. Fortolkningen kræver både stor metodisk, teoretisk og empirisk indsigt.

Datafortolkningen løber således ind i en række hermeneutiske og dobbelthermeneutiske problemstillinger, og den stærkt sikkerhedsliggjorte adfærd på sociale medier får somme tider mere karakter af en agentthriller, hvor fjenden kender og forstår sin rolle i fortolkningsspillet. Forskeren betragter ikke blot en intetanende flok løveunger på savannen. Internetekstremismen er både refleksiv og performativ. Samtidig fortolker forskeren et virkelighedsbillede, som i forvejen er en fortolkning (den dobbelte hermeneutik), og ved at videregive den fortolkning til politiksmedene i det politiske system, konstruerer han den virkelighed, som efterfølgende underlægges 'objektive' kategoriseringer etc. af nye forskere.

Opsummerende kan det altså siges, at netværksanalysen får svært ved at forholde sig til det, som falder uden for analysens epistemologiske skema af noder og forbindelser. Og netop den manglende information stiller en lang række forhindringer for analysens udsigelse, som risikerer at blive indfanget i et net af fortolkningslag.

INDHOLDSANALYSER

Nodeindholdet kan analyseres på mange forskellige måder. Den mere strategiske og efterretningsorienterede terrorforskning har længe haft en forkærlighed for indholdsanalyse via kvalitative og kvantitative metoder. I den ene ende af spektret

202 Klausen, 2014.

203 Klausen, 2014.

anvendes kvalitative ekspertanalyser og -vurderinger af specifikt indhold (individuelle online-opslag). I den anden ende af spektret anvendes automatiseret kvantitativ indholdsanalyse i søgen efter generelle tendenser og dynamikker omkring holdninger, stemninger og dispositioner inden for forskellige grupper.[204]

I forhold til netværksanalysen bevæger den kvantitative indholdsanalyse sig selvsagt en smule tættere på substansen. Den er derfor også et hyppigt supplement til netværksanalysen. Indholdsanalyserne kan eksempelvis undersøge mønstre og tendenser i indhold opslået på ekstremistiske hjemmesider.[205] Som med netværksanalyse forudsætter indholdsanalyse i første omgang, at informationerne bliver ekstraheret via tekst mining-programmer, dvs. programmer, der høster specifikke informationer fra store mængder online-tekst, hvilket kan foregå på halv- eller helautomatisk vis.[206]

I nedenstående gennemgang vil 'indholdsanalyse' ofte blive anvendt synonymt med 'kvantitativ indholdsanalyse', da fokus er rettet mod den kvantitative metode som forebyggelsesbranchens nye vidundermiddel. I praksis vil dog langt de fleste indsatser supplere denne tilgang med en form for ekspert-drevet kvalitativ analyse, som ikke er i fokus i denne gennemgang. Nedenstående gennemgang går derfor ikke i dybden med konkrete (kvalitative) eksempler på indholdskodning.

Indeværende afsnit om indholdsanalyser er opdelt i to underafsnit. Første underafsnit redegør for indholdsanalysens metoder og centrale principper fulgt op af nogle eksempler på metodens anvendelsesmuligheder. Andet underafsnit udfolder diskussionen af de metodiske og analysemæssige problemstillinger, som medfølger, når indholdsanalysen appliceres på terror- og radikaliseringsforskning.

Metoder og eksempler

Tekstanalyseteknikker (også kaldet korpuslingvistik) benævnes også holdnings- eller meningsanalyse (sentiment analysis / opinion mining methods).[207] Teknikkerne kan også rette sig mod indholdets følelsesmæssige og affektive karakter (affect analysis).[208] Det er muligt via den kvantitative tekstanalyse at analysere udviklingen af og dynamikkerne omkring holdnings- eller meningsdannelse. Det enkelte korpus

204 Neumann, 2013: 450; Kaschesky et al., 2011: 317.

205 Correa & Sureka, 2013: 22.

206 Cioffi-Revilla, 2010: 261.

207 Cohen et al., 2014: 251; Gloor et al., 2009: 220; Bermingham et al, 2009: 2.

208 Correa & Sureka, 2013: 13; Brynielsson et al., 2012: 200.

analyseres således ved brug af en automatiseret metode, hvor computeralgoritmer identificerer sproglige mønstre og tendenser (fx hyppigheden af bestemte vendinger og udtryk). Det giver mulighed for i realtid at forarbejde store mængder data indhentet fra eksempelvis sociale medier.[209] Analyserne kan både udføres som monitorering retrospektivt eller i realtid, og de kan gennemføres med fokus på en diskursanalyse, der placerer bestemte udtalelser inden for deres respektive samfundskontekst.

Gennem monitorering af den diskursive holdningsdannelse er det eksempelvis muligt at udpege (og overvåge) de isolerede holdningsbobler (hjørner af internettet, hvor en ekstremistisk monokultur har slået rod) og sætte ind med målrettede politikker, der kan løse op for de sociale spændinger og modgå polarisering.

Den diskursanalytiske tilgang har i radikaliserings- og terrorforskning typisk fokus på, hvordan budskaber, der florerer i ekstremistiske online-miljøer, udvikler sig over tid, samt hvordan de kan tænkes at påvirke den enkelte modtager (de sårbare unge). Gennem monitorering af den diskursive holdningsdannelse er det eksempelvis muligt at udpege (og overvåge) de isolerede holdningsbobler (hjørner af internettet, hvor en ekstremistisk monokultur har slået rod) og sætte ind med målrettede politikker, der kan løse op for de sociale spændinger og modgå polarisering.[210] Et tænkt eksempel på sådanne politikker kunne være konkrete socialpolitisk tiltag eller modnarrativer i form af positive alternativer.

De kvantitative tekstanalysetilgange anvender ofte selvlærende computer-algoritmer til at skelne mellem radikalt og ikke-radikalt indhold på hjemmesider og i individuelle statusopdateringer på sociale medier. Herved kan myndighederne hurtigere identificere trusler rettet mod grupper eller individer. Forskningen inden for feltet er dog endnu i sin vorden, og de fleste videnskabelige tekster om emnet omhandler derfor potentialerne i de fremtidige tekstanalyseredskaber fremfor egentlige analyseeksempler, der påviser anvendeligheden.[210] Herudover er det endnu omdiskuteret, hvordan disse teknikker kan implementeres til analyse af dynamisk indhold på de sociale medier, hvor sprog og ramme ofte er mere fri og uformel.[212]

209 Lucas, 2014: 2.

210 Kaschesky et al., 2011: 320-325.

211 Cohen et al., 2014: 251.

212 Bermingham et al, 2009: 2.

En del af tanken er altså at lade computeralgoritmer foretage forarbejdet og indsnævre mængden af materiale, som kræver en efterfølgende ekspertvurdering, og som kalder på yderligere undersøgelser.[213] Førstesorteringen kan eksempelvis foregå ved at anvende emne-filtreret netværksanalyse efterfulgt at de kvantitative tekstanalyser, hvor indholdet klassificeres efter, om det forholder sig positivt, negativt eller neutralt til en bestemt problemstilling.[214] Med denne førstesortering kan hjemmesider og brugerkonti ifølge et forskerhold fra det svenske Totalförsvarets forskninginstitut (FOI) klassificere indholdets 'interestingness' ud fra indholdets ord- og sætningskonstruktioner.[215] Derved laves ud fra foruddefinerede kriterier en liste over de mest interessante hjemmesider eller brugerprofiler på et givent tidspunkt, hvilket kan anvendes til yderligere analyse af motiver og intentioner, der ifølge forfatterne peger på individernes 'radikaliseringsniveau'.[216] At vurdere et 'radikaliseringsniveau' ud fra rent sproglige markeringer er naturligvis ikke helt uproblematisk, hvilket rapportens del 3 vil dykke ned i.

Præcis som med netværksanalysens afsæt i 'nøgledata' (udpeget af eksperter) må indholdsanalysen således udvikles i tæt samarbejde med de relevante fagpersoner, som har et indgående kulturelt og sprogligt kendskab til de efterforskede miljøer. Tilgangen læner sig altså op ad tanken om eksperter som dem, der skal levere en objektiv tjekliste for analyserelevant ekstremistisk indhold.

Affektanalysen arbejder ud fra samme principper som de andre tilgange til indholdsanalyse. Den bruges til at analysere (mængden af) følelser i forhold til et bestemt emne. Analysen kan derfor anvendes til at udkrystallisere intensiteten af vold, racisme eller had i ekstremistisk online-indhold.[217] Herudover kan affektanalysen anvendes til at analysere og forstå adfærdsmønstre blandt de ekstremistiske online-brugere.

Uanset hvilke sproglige markører, som analysen tager afsæt i, anvendes en såkaldt 'bag of words' eller et 'discriminant word lexicon', hvor computerprogrammerne automatisk identificerer de mest anvendte ord eller ordpar i store mængder online-tekst og klassificerer tekststykker efter analyserelevant indhold.[218] For at kunne identificere de relevante nøgleord, som indikerer online-ekstremisme eller radikalisme, må de

213 Cohen et al., 2014: 251.

214 Brynielsson et al., 2012: 200; Cohen et al., 2014: 251.

215 Brynielsson et al., 2012.

216 Brynielsson et al., 2012: 201.

217 Correa & Sureka, 2013: 14.

218 Gloor et al., 2009: 220; Brynielsson et al., 2012: 201.

anvendte ordlister sammensættes af eksperter med et dybdekendskab til ekstremistiske miljøer.[219] Præcis som med netværksanalysens afsæt i 'nøgledata' (udpeget af eksperter) må indholdsanalysen således udvikles i tæt samarbejde med de relevante fagpersoner, som har et indgående kulturelt og sprogligt kendskab til de efterforskede miljøer. Tilgangen læner sig altså op ad tanken om eksperter som dem, der skal levere en objektiv tjekliste for analyserelevant ekstremistisk indhold. Denne tanke indeholder som allerede nævnt i foregående afsnit en række hermeneutiske problemstillinger.

Præcis som med netværksanalysens afsæt i 'nøgledata' (udpeget af eksperter) må indholdsanalysen således udvikles i tæt samarbejde med de relevante fagpersoner, som har et indgående kulturelt og sprogligt kendskab til de efterforskede miljøer. Tilgangen læner sig altså op ad tanken om eksperter som dem, der skal levere en objektiv tjekliste for analyserelevant ekstremistisk indhold.

Bag of words-tilgangen konstruerer en positiv og en negativ liste, som sættes i forbindelse med bestemte udtryk. Tilgangen tæller således antallet af samtidige ord for at finde et udtryk for, hvor stærk for eller imod formuleringerne synes at være.[220] I en videnskabelig artikel fra 2009, der undersøger mulighederne for at anvende netværks- og indholdsanalyse i jagten efter online-radikalisering, anvender Bermingham et al. den nævnte bag of words-tilgang til at tildele YouTube-profiler og -kommentarer positive og negative værdier. Herved kan de karakterisere brugere og grupper af brugere alt efter deres mening om et emne.[221] Teknikken kan ifølge Bermingham et al. bruges til at finde frem til indhold, der er konstrueret med det formål at radikalisere dem med forudgående lille eller ingen interesse i voldelig jihad.[222] Artiklen forbliver således på holdningsplanet i sine analyser og arbejder ud fra en forudsætning om kausalitet mellem radikale holdninger og voldelige handlinger. Dette kommer blandt andet til udtryk i artiklens forståelse af online-radikalisering, der beskrives som "en proces, hvori individer gennem deres

219 Cohen et al., 2014: 251; Brynielsson et al., 2012: 201.

220 Gloor et al., 2009: 220.

221 Bermingham et al, 2009: 2.

222 Bermingham et al, 2009: 1.

onlineinteraktion og eksponering for forskellige typer online-indhold i stigende grad accepterer anvendelsen af vold som en legitim metode til at løse sociale og politiske konflikter".[223] Forfatterne bemærker selv, at der ikke foreligger empirisk bevis for denne påstand, men at der – ifølge forfatterne – er bred enighed blandt forskere og policy-skribenter om internettets radikaliseringseffekt. Påstanden om bred enighed kan dog også diskuteres, hvilket denne review-series tidligere publikationer kommer omkring.[224]

De kvantitative tekstanalyseværktøjer giver med andre ord forskeren mulighed for at betragte de forskellige indholdsproducenters sprogbrug mere indgående. Det er muligt i større skala at opfange de mest overbevisende budskaber og sproglige vendinger, som de forskellige narrativer sammensættes af. Analysen vil derfor (under de rette forudsætninger) kunne påvise visse ekstremistiske trends på de sociale medier samt lokalisere ekstremismens trendsættere.[225]

I et studie af internetkommunikationen under Gaza-konflikten i 2008/2009 når Sheryl Prentice et al. frem til nogle karakteristika for udviklingen af sproget og argumenterne i terroristmedier via en kombination af manuelle og halvautomatiske kodningssystemer, de selv kalder for "Content and Composition Analysis (CCA)".[226] CCA består overordnet af to tekstanalysemetoder. Den første metode er en indholdskodning (bag of words), der fokuserer på beskeders overtalelsesevner, hvilket defineres som budskaber, rettet mod fx sårbare unge, der tilsigter at ændre modtagerens attitude og/eller adfærd i forhold til et spørgsmål.[227] Den anden metode er en korpuslingvistisk begrebsanalyse, der fokuserer på at udkrystallisere de mest gængse narrativer og tematikker (trends), som fremtræder i ekstremistiske medier.[228] Det handler altså om de ord eller koncepter, som optræder signifikant oftere i ét korpus frem for andre korpus.

Den første metode afslører et overtal af moralske argumenter på de ekstremistiske medier, og den sandsynliggør, hvordan aktører med forskellige gruppetilhørsforhold anvender distinkte argumentkonstruktioner. Den anden metode bekræfter en overvægt i brugen af moralske argumenter til at skabe en in group/out group-skillelinje. Analysen viser, hvorledes argumenterne ændrer sig fra at udtrykke generel

223 Bermingham et al., 2009: 1 – egen oversættelse.

224 Gemmerli, 2014a; Gemmerli, 2014b.

225 Prentice et al., 2010: 63.

226 Prentice et al., 2010: 62.

227 Prentice et al., 2010: 62.

228 Prentice et al., 2010: 62.

utilfredshed til mere specifikt og modtagerrettet at anvende voldelige udtryk efterhånden som konflikten tager fart.[229] Analysen påviser med andre ord en radikalisering eller skærpelse af retorikken. Forfatterne finder bl.a. en udbredt betoning af den negative eller manglende moral blandt ekstremisternes out group. Herudover bemærker de over tid et fald i anvendelsen af 'bevis'-baserede argumenter samt en stigende anvendelse af strategier og koncepter, der skal engagere den enkelte.[230]

Forfatterne sammensætter ud fra deres første analyse et 'topologisk' kort, som illustrerer hvilke aktører, der anvender hvilken overtalelsesadfærd (hvordan argumentet er konstrueret).[231] Det giver mulighed for en mere indgående forståelse af forskellige aktørers argumentationsmåder. Argumenterne bruges eksempelvis til at retfærdiggøre vold mod en amoralsk fjende. Herved kan forfatterne tegne kort over argumentationen før og efter konflikten og på et aggregeret niveau påvise forandringer, der måske er indtruffet som konsekvens af konflikten.[232] Korpuslingvistikken både understøtter og uddyber den første analyses fund.[233] Prentice et al. fremhæver derfor, at de to overlappende analyseformer giver analysens resultater validitet.[234] Men tilgangen efterlader stadig et stort spørgsmålstegn der, hvor argumentet slutter, og modtageren starter. Hvordan skal vi forstå individet, som modtager argumentet? Det synes at være en generel antagelse, at ekstremister drives frem af holdningsdannelsen. Men holder den antagelse? Det føres der ikke bevis for, og antagelsen er endnu ret omdiskuteret og derfor ikke uproblematisk.[235]

Tekstanalyseværktøjerne får også flere forskere til at forestille sig en anvendelse i den konkrete gerningsforhindrende og forbyggende indsats. Således spekulerer eksempelvis Neumann i, at tekstanalyse kan give forskere og myndigheder en forvarsling om et nyt 'modus operandi', og han giver som eksempel ændringerne i jihadistbevægelsens taktiske disposition efter, at Awlaki via webmagasinet Inspire fremførte ideerne om lone wolf-angreb i USA og Vesten.[236]

Spekulationerne går dog også et lag dybere hvad angår de automatiserede og halvautomatiserede teknikkers fortræffeligheder. Ansporet af frygten for de ensomme ulve a la Breivik spekulerer Cohen et al. fra det svenske FOI således i

229 Prentice et al., 2010: 61.
230 Prentice et al., 2010: 71.
231 Prentice et al., 2010: 67.
232 Prentice et al., 2010: 68.
233 Prentice et al., 2010: 69.
234 Prentice et al., 2010: 71.
235 Gemmerli, 2014a.
236 Neumann, 2013: 451.

mulighederne for en fremtidig sporing af individer, som planlægger at udføre voldelige handlinger.[237] I deres teoriudviklende artikel Detecting Linguistic Markers for Radical Violence in Social Media forestiller forfatterne sig således, at tekstanalyseredskaber kan opspore tre forskellige typer advarselssignaler eller bekymringsadfærd (warning behaviours): (adfærds)markører for radikal vold, som kan aflæses i den enkeltes brug af sociale medier. Ved at sammenligne med internetadfærden og den ekstremistiske indstilling fra andre tilfælde at voldelig ekstremisme (og skoleskydere), skal det på den måde blive muligt at opfange meninger, værdier og, i sjældnere tilfælde, egentlige voldelige intentioner i online-indhold, som så kan anvendes i den forebyggende indsats. Det er denne automatiserede og algoritmebaserede computergenkendelse, som forfatterne benævner "linguistic markers for radical violence".[238] Forfatterne baserer tankerne på en retspsykiatrisk adfærdsprofilering, der kan udkrystalliseres i tre typer online-adfærd. Disse tegn på online-radikalisering vil blive uddybet yderligere i rapportens tredje del.

En lignende tilgang fremføres også af blandt andre Bermingham et al. samt Brynielsson et al., der som Cohen et al. også kommer fra det svenske FOI og har enkelte gengangere i forfatterkredsen. Påskuddet er endnu en gang frygten for de ensomme ulves uforudsigelige hærgen – med specifik reference til Breivik. I Brynielsson et al. bliver ovennævnte tekstmarkør-tilgang formuleret på næsten tilsvarende vis. Forfatterne sammenligner selv deres tilgang med den metode, som anvendes til at identificere netværk, der deler børneporno,[239] og formålet er at udarbejde en analysemetode, som kan anvendes til at analysere ekstremistiske fora i jagten på ensomme ulve in spe.[240] Dette gør forfatterne ved at måle på tre trusselsparametre: Motiver/hensigt, kapabiliteter og muligheder.[241]

Metodiske problemstillinger

De metodiske indsigelser mod indholdsanalysernes potentialer til forebyggelse af radikalisering er mange og mangeartede. For overskuelighedens skyld er nedenstående gennemgang holdt relativt kort med fokus på sprog, fortolkningsproblemer, selvbiografiske data, visuelt indhold, dataoverload mm.

237 Cohen et al., 2014: 247.

238 Cohen et al., 2014: 253.

239 Brynielsson et al., 2012: 200.

240 Brynielsson et al., 2012: 197.

241 Brynielsson et al., 2012: 198.

Alene tekstniveauet stiller den automatiserede teknik over for en række vanskeligheder. Sproget kan således være en udfordring for analysen, da flere sprog ofte anvendes simultant og ofte også har forskellige læseretninger.[242] I en artikel om online-rekruttering af Jacob Scanlon og Matthew Gerbers fremhæver de også som forudsætning for deres metode, at det indsamlede data er på engelsk eller er oversat til engelsk med eksempelvis google translate.[243] Her støder indholdsanalysen med andre ord ind i problemer med oversættelse. Forfatterne vurderer selv, at den overordnede intention er mulig, men at det vil kræve inklusion af andre sprog på en mere fleksibel måde.[244]

Sproglige online-fænomener, som bærer præg af en ikke-regulær stavemåde eller grammatik, sløret og kodet sprog, sprogbilleder med overførte betydninger, hentydninger, metaforer, humor, sarkasme og slang på mange forskellige sprog stiller store (og måske for store) krav til såvel analysealgoritmer som eksperter. Fortolkningskunsten er her en vigtig mellemstation, som gør brugen af sandsynligheder og automatiserede pointsystemer yderst tvivlsom.[245] Herudover har eksperimenter vist, at algoritmer til brug for automatiseret holdningsanalyse indtil videre er for upålidelige, hvis det ikke foregår på engelsk.[246]

Alle komplikationerne taget i betragtning, hvordan skal voldelige inklinationer kunne analyseres ud fra online-adfærd? Her kommer ingen af de nævnte artikler med overbevisende svar.

Netop her undervurderer Brynielsson et al. sprogets kompleksitet og funktionalitet. Som Bermingham et al. også selv understreger i deres konklusion, er det problematisk at bruge ordbøger (bag of words), da der er stor risiko for polysemi (at et ord kan have mange betydninger) og synonymi (at der findes mange ord for det samme fænomen).[247] Tilgangen er for upræcis, og selv forskere, som skriver disse algoritmer, påpeger umuligheden i at kunne indrette indholdsanalysealgoritmer, som kan udpege de reelt farlige aktører.[248] Brian Lucas giver en række eksempler på analyser

242 Correa & Sureka, 2013: 15.
243 Scanlon & Gerber, 2014: 3.
244 Scanlon & Gerber, 2014: 9.
245 Lucas, 2014: 2; Glor et al., 2009: 220.
246 Falkenberg, 2012: 15.
247 Bermingham et al, 2009: 6.
248 Bartlett, 2015.

af hate speech online.[249] Selv denne opgave er ikke let til trods for, at den ikke forsøger at koble sproget til sandsynligheden for voldelig adfærd i den fysiske virkelighed. Alle komplikationerne taget i betragtning, hvordan skal voldelige inklinationer kunne analyseres ud fra online-adfærd? Her kommer ingen af de nævnte artikler med overbevisende svar.

Videoer er følgelig den kvantitative indholdsanalyses blinde plet til trods for, at de indtager en stadig større rolle i den jihadistiske propagandamaskine – i såvel radikaliserings- som rekrutteringsspørgsmål.

Herudover bygger mange algoritmer på de biografiske oplysninger om eksempelvis køn, alder, beliggenhed eller politiske overbevisning, som de enkelte brugere selv angiver.[250] Men muligheden for at tjekke korrektheden af disse selvangivelser på kvantitativt niveau er ikke til stede, hvorfor det kræver en intensiv kvalitativ vurdering udført af eksperter på området. Præcis denne kvalitative vurdering er tids- og ressourcekrævende, og den lægger en klar begrænsning på, hvor generelle udsigelser og konklusioner et givent arbejde kan komme med, hvilket eksempelvis rapporten fra ICSR også tydeliggør. Dette problem bemærker Bermingham et al. også, da de konstaterer, at aldersspredningen i deres testcase går fra 14 til 107 år.[251] Den 107-årige betragter forfatterne som en outlier, og vedkommende bliver derfor ekskluderet fra datamaterialet. Problemet er dog, at de reelt set ikke kan vide, hvor mange af de inkluderede data, som er korrekte. Metoden er altså blind over for forskellige identitetspolitiske og mikrosociologiske problemstillinger, som netop ligger i forlængelse af disse selvangivelser, ligesom den ikke har øje for internettets rolle i skabelsen af de mange forskellige online-identiteter og persona.

Automatiserede indholdsanalyser på tekstniveau er, set i forhold til analyser af visuelt indhold, relativt simple. Men det mest effektive ekstremistiske internet-propaganda – videoer og billeder – kræver stadig en manuel bearbejdning, hvorfor videoer ofte bevidst vælges fra i sådanne undersøgelser.[252] Videoer er følgelig den kvantitative indholdsanalyses blinde plet til trods for, at de indtager en stadig større rolle i den

249 Lucas, 2014.

250 Bermingham et al, 2009: 2.

251 Bermingham et al, 2009: 3.

252 Difraoui, 2012: 76.

jihadistiske propagandamaskine – i såvel radikaliserings- som rekrutteringsspørgsmål.[253] Dette ses ikke mindst i de meget avancerede videoproduktioner fra terrororganisationer som Islamisk Stat (IS) i Irak og Syrien. Udfordringen vil således være, hvordan eksempelvis kropslige og æstetiske elementer kvantificeres som genstand for analyser? Hvordan ekstraheres effekten af emotionelle billeder, når kontekst, modtager osv. kun meget svært kan tages med i betragtning?

Cohen et al. er dog også selv klar over en række af de automatiserede teknikkers begrænsninger. Forfatterne fremhæver således, at dataoverload, ikke-indekseret data i dark web samt behovet for en dybdegående forståelse for de mange forskellige aspekter af såvel skriftlig som visuel kommunikation gør det umuligt at finde frem til de ensomme ulve ved brug af helautomatiserede metoder alene. Derfor foreslår de redskaberne som supplement i en semi-automatiseret indsats.[254] Problemet er således ikke blot dataens ukomplette karakter, men også det faktum, at der samtidig er for meget af den, og at analysekapaciteten altid vil være begrænset. Herudover mangler de automatiserede redskaber til lokalisering af visuelt indhold endnu at blive udviklet.[255] Den nye computerteknologi til billedgenkendelse, som automatisk kan sætte ord på billeder og dermed lettere gøre visuelt indhold til genstand for kvantitative analyser, er således endnu i de allertidligste udviklingsfaser. Foreløbig kan denne teknik anvendes til den mest simple form for kategorisering eller indeksering, men teknologien tilskrives store potentialer.[256]

Et andet problem, som den individorienterede indholdsanalyse står overfor, er, at det kan være vanskeligt helt at fastslå, hvem der egentlig gemmer sig bag en given brugerprofil. Det er ikke ualmindeligt, at flere personer eksempelvis anvender samme profil, eller at en person har flere profiler. Derfor skal programmerne foretage 'alias matching' eller 'author recognition' for at kunne verificere forfatterne bag. Men der er aldrig nogen garanti.[257]

Anvendelsen af indholdsanalyse på ekstremisme- og terrorismeområdet må også reflektere emnets performative karakter samt den indflydelse dette måtte have på både indhold og netværk. En ofte grundlæggende forudsætning for indholdsanalysen er således, at folk gør, hvad de siger, de vil gøre, hvorfor tendenser på sociale medier kan anvendes som forvarsling for handlinger i den virkelige verden.[258] Den forud-

253 Steinberg, 2012: 14.

254 Cohen et al., 2014: 247; Neumann, 2013: 452-453.

255 Brynielsson et al., 2012: 203.

256 Karpathy & Fei-Fei, 2014; Frome et al., 2013.

257 Brynielsson et al., 2012: 202.

258 Gloor et al., 2009: 215.

sætning giver intuitivt god mening ved eksempelvis marketingsundersøgelser, og netværks- og indholdsanalyserne er derfor brugbare til undersøgelser af trend-fænomener i en majoritetskultur. Men jo stærkere tendensen mod sikkerhedsliggjorte minoritets-spørgsmål eller voldsforherligelse er, jo sværere er det at lægge sig op ad kvantit-eternes (popularitetens) visdom. Trends på sociale medier arbejder som regel ud fra nogle positive dynamikker, hvor det er godt at blive set. Radikalisering, rekruttering og ekstremisme fungerer i modsætning hertil på grænsen af normalitet, kriminalitet og sikkerhed, hvilket medfører nogle helt andre mekanismer omkring, hvad der bliver meldt ud, og hvad hensigten med udmeldingerne er. Trends og popularitetsmål er derfor problematiske begreber, når forskningen beskæftiger sig med et så sikker-hedsliggjort, overvåget og censureret fænomen som internet-ekstremismen. Her må der tages en række forbehold for datagrundlagets anderledes performative og dark web-orienterede karakter, hvilket også metodediskussionen i afsnittet om netværks-analyse kort var omkring.

Trends på sociale medier arbejder som regel ud fra nogle positive dynamikker, hvor det er godt at blive set. Radikalisering, rekruttering og ekstremisme fungerer i modsætning hertil på grænsen af normalitet, kriminalitet og sikkerhed, hvilket medfører nogle helt andre mekanismer omkring, hvad der bliver meldt ud, og hvad hensigten med udmeldingerne er.

På grund af den mulige online-radikaliserings mange fortolkningslag er spillet desto mere komplekst, overlejret af diverse identitetsmæssige og sociale processer, der skaber mulighed for en masse falske positiver. Det mørke internet har en pluralitet af identiteter, og hver identifikationsproces har sin helt unikke karakter. Som Randy Borum også bemærker, er radikaliseringsfænomenet karakteriseret ved ækvifinalitet og multifinalitet, dvs. at mange forskellige veje fører til radikalisering, og at personer, der følger den samme vej, alligevel kan ende forskellige steder.[259] Der er en stor grad af vilkårlighed og uforudsigelighed i individers vej ind i den voldelige ekstremisme.

Netop de sociale mediers omskiftelige og dynamiske karakter bevirker også, at analyserne hurtigt bliver forældede. Realtidsanalyser er derfor efterspurgte, da de fokuserer på at give en tidlig advarsel om nye tendenser på internettet.[260] Dette giver da også umiddelbart god mening, hvis man betragter simple sociale fænomener på

259 Borum, 2011b: 57.

260 Lucas, 2014: 3.

aggregeret niveau. Det kan fx, som Lucas fremhæver, anvendes til at demonstrere den geografiske fordeling af forskellige former for hadtale på Twitter over en bestemt periode.[261] Men hvordan kan dette oversættes til individuel netadfærd? Springet fra det aggregerede makro- eller mesoniveau til forudsigelser om adfærd på individniveau medfører en risiko for økologiske fejlslutninger.

Det fortaber sig således ofte i det uvisse, hvilken mere præcis sammenhæng forskellige forfattere forestiller sig, at der er mellem terrororganisationer, ekstremistisk online-indhold og radikalisering af sårbare unge. En registreret forbindelse mellem to noder betyder jo ikke nødvendigvis, at der har fundet en påvirkning sted, ligesom påvirkningens karakter og resonans ikke lader sig statistisk deducere. Dette hidrører imidlertid en radikaliseringsteoretisk diskussion, som er omdrejningspunktet for rapportens sidste del.

261 Lucas, 2014: 5.

Del 3:

ONLINE-LITTERATURENS RADIKALISERINGSMODELLER OG LØSNINGSBESKRIVELSER

De forudgående to rapportdele har beskrevet spektret af online-forebyggelse, som det ser ud på nuværende tidspunkt, og som særligt de kvantitativt drevne videnskabelige discipliner forestiller sig, at det måtte se ud i fremtiden, når vi har lært at udnytte de nye teknologiers potentiale til fulde.

Men for at forstå, hvad der genererer hele videnskaben inden for online-forebyggelse, er det væsentligt indledningsvist at dvæle lidt ved den frygt og det trusselsbillede, der mere end noget andet er med til at sætte den videnskabelige og policy-orienterede søgen i gang: forestillingerne om terrorismens ensomme ulve. Netop her adskiller den nye terrorfrygt sig fra terrorismebeskrivelsen, som den umiddelbart så ud efter Londonbomberne i 2005. Dengang fokuserede beskrivelsen af radikalisering i særdeleshed på den hjemmegroede terrorismes netværk, kontakter og gruppetilhørsforhold. Man frygtede de store (hjemme)koordinerede anslag, hvor selve udførelsen kræver en del planlægning og er relativt kompleks.

Truslen fra den hjemmegroede terrorisme har især i den danske kontekst foranlediget en socialpolitisk og kriminalpræventiv tilgang. Men problemstillingen er lidt anderledes hvad angår frygten for radikaliseringens og terrorismens enspændere: De socialt marginaliserede og isolerede unge, der antageligvis via internettet får kontakt til ekstremistiske grupper og ideer, og som via online-indhold og virtuelle netværk opbygger en militant modstandsidentitet og -kapacitet, der potentielt kan foranledige voldelige handlinger. Det tydeligste eksempel på denne type terrorisme er naturligvis

den nationalkonservative og selverklærede norske korsfarer Anders Behring Breivik. Problemet er, at gruppen af de potentielt radikaliserede på sin vis er et led længere nede i den voldelige ekstremismes fødekæde og dermed også sværere at få øje på.

Teknologi- og medieforskerne Salem, Reid og Chen beskriver de sociale medier som kanal til at sprede ekstremistisk ideologi og radikalisere sympatisører.[262] Og dette radikaliseringspotentiale har for alvor sat spekulationer i gang vedrørende de ensomme ulves selvradikalisering via internettet.[263] Professor i kommunikation ved universitetet i Haifa, Gabriel Weimann, indrammer trusselsbilledet med en kort og sigende beskrivelse: "The real threat now comes from the single individual, the 'lone wolf', living next door, radicalized on the internet, and plotting strikes in the dark".[264]

Et andet godt eksempel på opfattelsen af den nye trussel kan læses i en rapport af Kamaldeep Bhui og Yasmin Ibrahim, der forsker i transkulturel psykiatri hos Queen Mary University:

> "Within the realm of radicalization there has been increasing focus on the notion of "lone wolf terrorism" as a variant form of self-radicalization [...] Lone wolves lack the support and resources and may not commit themselves to continuous membership or group involvement. Self-radicalization is through exposure to secondary sources such as books, writings, and manifestos.[265] "

I Bhui og Ibrahims beskrivelse tillægges ideologien altså den væsentligste betydning for fænomenets udbredelse, hvilket fører til spekulationer om online-indholdets effekt og farlighed. De mange forestillinger om truslen fra ensomme ulve har derfor fået en række forskere og policy-skribenter til at spekulere i mulighederne for at opspore de ensomme ulve med computeren som den omnipotente sporhund.

Hertil kommer, at kravet og forventningen om forebyggelse presser på for at gøre brug af de nye teknologiske vidundermidler. Således opstår en litteratur om forebyggelse af online-radikalisering, der, som eksempelvis Brynielssen et al., baserer sine analyseværktøjer til opsporing af de potentielle ensomme ulves 'weak signals'

262 Salem et al., 2008: 620.

263 Dienstbühl & Weber, 2014: 41.

264 Weimann, 2012: 75.

265 Bhui & Ibrahim, 2013: 220-221.

på ideen om at kunne tilnærme sig en 'profil' for de sårbare unge.[266] Også Cohen et al., den anden forskergruppe fra FOI, har været hurtige til at se de nye teknologiers store potentialer. Jagten efter radikaliseringens 'svage signaler' sættes ind:

> "Lone wolf terrorism is a threat to the security of modern society, [and since] lone wolves are acting on their own, information about them cannot be collected using traditional police methods such as infiltration or wiretapping. One way to attempt to discover them before it is too late is to search for various "weak signals" on the Internet, such as digital traces left in extremist web forums. With the right tools and techniques, such traces can be collected and analyzed. In this work, we focus on tools and techniques that can be used to detect weak signals in the form of linguistic markers for potential lone wolf terrorism.[267]"

Problemet ved denne tilgang er, at den ekskluderer eller reducerer de mange sociale processer, som går forud for et engagement med ideologien – og som potentielt gør den enkelte 'terrorist' anderledes end alle andre, der beskæftiger sig med den samme ideologi uden at ende i et voldeligt engagement.

Et ofte anvendt eksempel på den såkaldte online-radikalisering er historien om den terrordømte amerikaner, Colleen LaRose (alias Jihad Jane), der i 2009 var med til bl.a. at planlægge et attentat på den svenske tegner, Lars Vilks. LaRose gjorde sig bemærket ved at have levet et dobbeltliv, hvor den islamistiske identitet nærmest udelukkende blev anvendt i online-kontakten med andre jihadister. Men som islamforsker og religionshistoriker Jeffry Halverson og Amy Way understreger, kan tilfældet LaRose ikke blot reduceres til et spørgsmål om farlig ideologi eller online-liv. Gennem socialteori og psykologiske tilgange når forfatterne frem til, at online-radikalisering af marginaliserede personer som LaRose bør forstås gennem den personlige historie og eksisterende sociale og kulturelle brydninger.[268]

Overordnet konkluderer flere forskere derfor, at forestillingerne om online-selvradikalisering og ensomme ulve ikke er særlig brugbare til beskrivelsen af radikalisering set i forhold til brugen af internettet.[269] Stevens og Neumann går

266 Brynielsson et al., 2012: 197.

267 Cohen et al., 2014: 246.

268 Halverson & Way, 2012: 140.

269 Sunde, 2013: 52.

endog skridtet videre og erklærer, at selvradikalisering eller selvrekruttering via internettet, og med lille eller ingen kontakt til den ikke-virtuelle ekstremisme, nærmest aldrig finder sted.[270] Carter et al.[271] understreger, at der findes en 'klasse' af online jihadi-supportere, der, som Irhabi 007, bliver populære og effektive informationsspredere, men som aldrig deltager i 'den virkelige verdens ekstremisme'. Et andet og nyere eksempel herpå er den populære pro ISIS-twitterkonto Shami Witness, der indtil december 2014 blev anset for at være en nøglekonto for den sunniekstremistiske terrorgruppe. Med over 129.000 tweets på kontoen (primært skrevet på engelsk), mere end 17.000 faste følgere og millioner af månedlige besøgende var han en nøglefigur i den jihadistiske online-bevægelse. Manden bag Shami Witness, Mehdi Masroor Biswas, viste sig at være et familiemenneske, der spiste pizza med vennerne, gik til Hawaii-fest på sit arbejde og til dejligt arbejdede som leder hos en stor virksomhed i Bangalore – Indiens svar på Silicon Valley.[272],[273] Der kan med andre ord være en stor diskrepans mellem online og offline, som bør inddrages i radikaliseringsforståelsen.

Overordnet konkluderer flere forskere derfor, at forestillingerne om online-selvradikalisering og ensomme ulve ikke er særlig brugbare til beskrivelsen af radikalisering set i forhold til brugen af internettet.

Rapportens tredje og sidste del vil i sin første halvdel udkrystallisere den gennemgåede online-litteraturs radikaliseringsmodel. Anden halvdel tager fat i litteraturens forestillinger om online-radikaliseringens kendetegn og mulige digitale løsninger. Undervejs diskuterer del 3 de overordnede radikaliseringsteoretiske problemer i de fremførte netværksanalyser og i forestillingen om forebyggelse af online-radikalisering.

270 Stevens & Neumann, 2009: 13.

271 Carter et al., 2014.

272 Læs mere om Shami Witness: http://english.alarabiya.net/en/perspective/features/2014/12/14/Shami-Witness-arrest-rattles-ISIS-cages-on-Twitter.html, http://www.channel4.com/news/unmasked-the-man-behind-top-islamic-state-twitter-account-shami-witness-mehdi

273 Se Shami Witness' twitterprofil: https://twitter.com/shamiwitness

ONLINE-LITTERATURENS RADIKALISERINGSMODEL (PROBLEMFORSTÅELSE)

Radikaliseringsbegrebet, som det fremføres både eksplicit og implicit mange steder i litteraturen om forebyggelse af online-radikalisering, kan kort beskrives som kombinationen af to elementer: ideologi og sårbarhed. Forholdene omkring samt opfattelsen af ideologi og sårbarhed varierer alt efter de forskellige tilgange og videnskabelige grundantagelser, men i store træk reducerer særligt den policy-rettede litteratur problemstillingen til disse to størrelser. Saltman og Russell fra Quilliam Foundation beskriver således radikalisering som følger: "It remains the case that radicalisation processes start with the introduction to extremist ideologies that then lead to violent extremism and potential terrorist acts".[274] Samme opfattelse ligger til grund for Anne Aly og hendes arbejde med det australske PaVE:

> "This paper proposes that radicalization is best approached as a combination of vulnerability (defined as the propensity for individuals and groups to come into contact with and be influenced by terroristic narratives) and exposure to terrorist supportive environments.[275] "

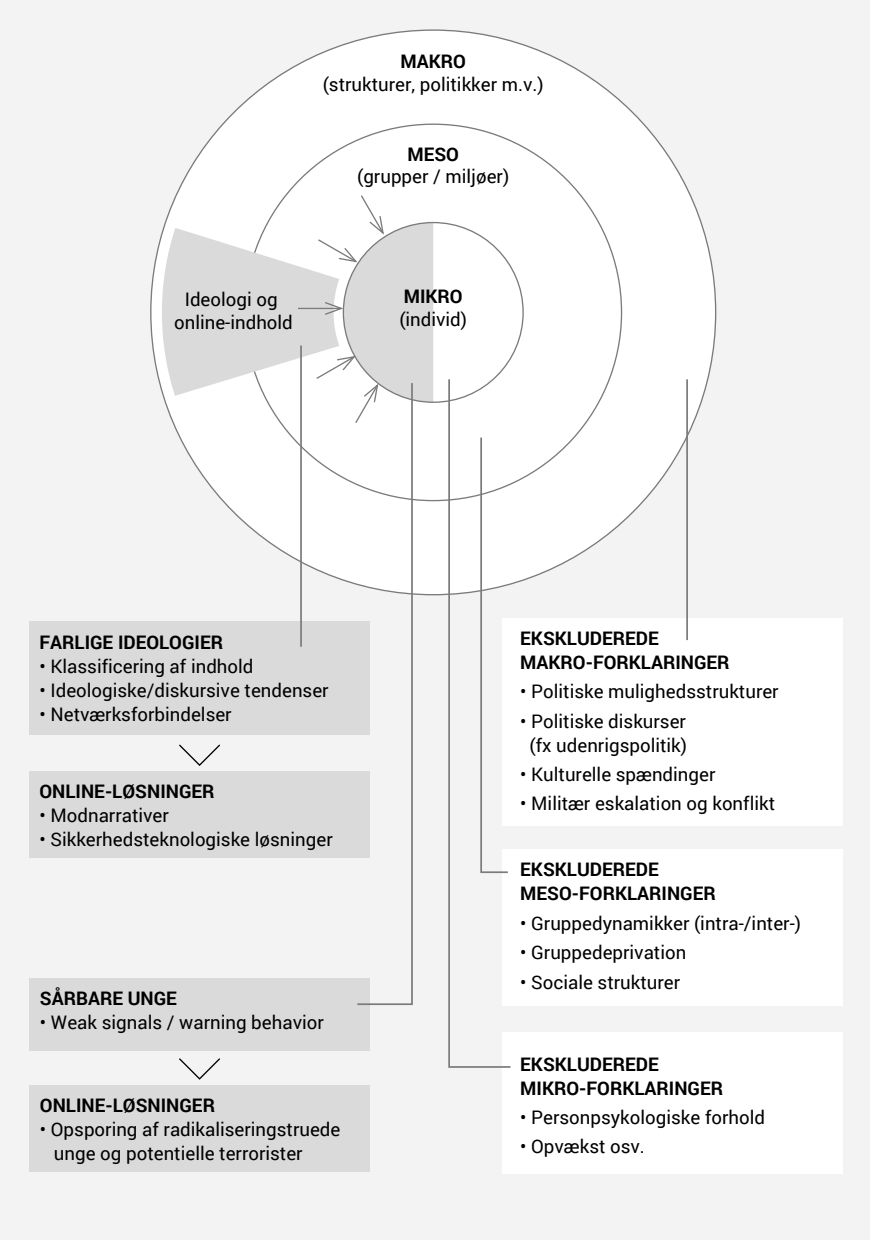
Dette efterlader en todelt radikaliseringsmodel, hvor en lang række sociale, psykologiske og politiske forhold reduceres til spørgsmål om enten en farlig og ekstrem udefrakommende ideologi eller individuel sårbarhed. Herved ekskluderer modellen (og dermed også de af modellen fremkomne løsningsforslag) en lang række videnskabelige perspektiver, hvilket fig. 5 anskueliggør. De mørkegrå kasser og modelindhold angiver online-litteraturens forklaringsmodel og løsninger, mens de lysegrå kasser og modelindhold anskueliggør den ekskluderede mængde af alternative forklaringer.

Modellen præsenterer naturligvis ikke en udtømmende beskrivelse af discipliner og forklaringsmodeller. Den er blot en abstraktion med eksemplificerende modelindhold. Det virkelige billede, såfremt man overhovedet kan tale om noget sådan inden for de mangefacetterede radikaliseringsteorier, er en langt mere kompleks og heterogen størrelse. Alene forsøget i at opsplitte radikaliseringsperspektivet i tre niveauer (mikro/meso/makro) ekskluderer en lang række elementer, der både i epistemologi og ontologi går på tværs af denne abstraktion.

274 Saltman & Russell, 2014: 8.

275 Aly, 2014: 70.

Fig. 5: Online-litteraturens radikaliseringsmodel samt udeladte perspektiver



Dette afsnit om online-litteraturens radikaliseringsmodel gennemgår, med et kritisk blik fra andre radikaliseringsperspektiver, modellens to hovedbestanddele. Første underafsnit diskuterer ideen om sårbarhed i lyset af Wiktorowicz' brug af begrebet 'kognitiv åbning,' og den indflydelse begrebet har haft på store dele af radikaliseringslitteraturen og radikaliseringspolitikken. Underafsnittet fremhæver, at den kognitive åbning har haft store implikationer for den efterfølgende tænkning (eller mangel på samme) om individets rolle i radikalisering. Andet underafsnit slår ned på beskrivelserne af ideologiens og/eller moralens rolle. I mange forklaringsmodeller, der ofte tenderer til cirkelslutninger, fremhæves ideologien som en faktor, der både skaber sårbarhed og er en effekt af sårbarheden. Samtidig hæftes forklaringerne om ideologiens farlighed op på en tænkning om ideologien som noget socialt fremmed, hvor radikal tænkning og voldelig handling sammenkobles i modsætningen til ideen om samfundets ikke-ideologiske og fredelige normalitet. Dette leder afslutningsvist videre til en kritisk diskussion af grundantagelsen om volden.

Sårbare unge og kognitive åbninger

Der er allerede forsket meget i og skrevet en del om radikaliseringsteoriernes antagelser og fund vedrørende individet før og under radikalisering (radikaliseringens subjektforståelse).[276] Men selv inden for denne litteratur er en række punkter endnu ubeskrevne, mens andre forbliver stærkt omdiskuterede – herunder antagelsen om, at radikalisering, som fænomen, kobler sig til de sårbare unge. Ifølge fx Bhui og Ibrahim er der størst risiko for radikalisering hos dem, der er sårbare. Og de er sårbare pga. egenskaber som isolation, generthed og potentiel aggressivitet, der bliver aktiveret i en kontekst af opfattet diskrimination, uretfærdighed eller trussel mod egen gruppe.[277] Forfatterne peger altså i retning af en særlig (men også ret almindelig) psykologisk profil. Men det springende punkt, hvor radikaliseringen antændes, bliver ifølge deres teori den enkeltes 'opfattelse'. Individets opfattelse af virkeligheden bliver derfor et kardinalpunkt for såvel problemforståelse som for løsninger.

Inden for radikaliseringspolitikkens virkelighed synes der efterhånden at være etableret konsensus om denne grundantagelse – særligt i Danmark. Ideen om sårbarhed peger på en værktøjskasse af allerede veletablerede kriminalpræventive og socialpolitiske indsatser. Og det skaber et lettere genkendeligt trusselsbillede, som derved reducerer en ubekendt og latent usikkerhed til en håndterbar størrelse.

276 Schmid, 2013; Schmid & Price, 2011; Silke, 2008; Borum 2011a; Borum 2011b; Lamberty, 2013; Pisoiu, 2013; Cole et al., 2012.

277 Bhui & Ibrahim, 2013: 230.

Endelig motiverer ideen til at tænke i individorienterede og socialpolitiske løsninger frem for at diskutere problematikkens samfundspolitiske konsekvenser. I stedet for at spørge til, om der er noget, vi som demokratisk samfund kan gøre bedre i mødet med ekstremismen – på politisk niveau – bliver spørgsmålet, hvordan vi kan genoprette og normalisere de socialt og ideologisk afvigende individer og generelt immunisere samfundets individer mod ekstremistiske kræfter.

Ideen om sårbarhed kan bl.a. spores tilbage til de første egentlige modelbeskrivelser af radikaliseringsbegrebet, og den kan især sættes i forbindelse med Quintan Wiktorowicz' teoretisering af det socialpsykologiske begreb 'den kognitive åbning'. Det er den samme Wiktorowicz, som gennem en årrække var toprådgiver vedrørende sikkerhedsspørgsmål for Det Hvide Hus i Washington, hvor han bl.a. var leder af den arbejdsgruppe, der skulle udvikle initiativer til bekæmpelse af online-radikalisering.

Wiktorowicz anvender den kognitive åbning til at forklare, hvorledes unge mennesker, der er vokset op i vestlige samfund og har været præget af vestlige værdier, kan ende med at vende disse værdier ryggen. Den kognitive åbning bliver således det forklarende mellemled, omvendelsen, i radikaliseringsfænomenets kognitive proces. Samtidig reducerer begrebet miljøfaktorer m.m. til at være effekter på individniveau. Wiktorowicz redegør selv for begrebet som følger:

> "This book argues that individuals are initially inspired by a cognitive opening that shakes certitude in previously accepted beliefs. Individuals must be willing to expose themselves to new ways of thinking and worldviews, and a cognitive opening helps facilitate possible receptivity. Any number of things can prompt a cognitive opening (experiences with discrimination, socioeconomic crisis, political repression, etc.), which means that there is no single catalyst for initial interest. In addition, movements can foster cognitive openings through activism and outreach by raising consciousness, challenging and debating alternative ideas, and persuading audiences that old ways of thinking are inadequate for addressing pressing economic, political and social concerns. [278] "

Men hvis den kognitive åbning blot medfører en reduktion af alle mulige sociale og politiske faktorer til individniveau, hvad er da pointen med at anvende begrebet? Den kognitive åbnings indtræden kan ikke påvises empirisk. Så hvordan kan Wiktorowicz

278 Wiktorowicz, 2005: 5.

fastslå kausalitet ved først at konstruere det sårbare individ, som forud for åbningen er gjort sårbar af en ukendt mængde af faktorer, men som efterfølgende – under påvirkning af fremmed ideologi – bevæger sig ind på radikaliseringens glidebane? Kan den kognitive åbning ikke anvendes til at forklare enhver ændring i overbevisning – uanset retningen? Og bliver ideologien så den eneste sikre indikation på, at en radikalisering finder sted? Hvad forklarer begrebet så egentlig?

Sårbarheden forklarer med andre ord, hvorledes individet bliver ideologisk og religiøst søgende – på jagt efter svar og eksistentiel mening. Problemet bliver derfor at forklare, hvornår og hvordan denne søgen ender i et engagement med voldelig ekstremisme og ikke blot i et intensivt filosofistudium?

Ydermere medfører denne nedskrivning til individniveauet, at der ikke findes nogen særegen sårbarhedsprofil for radikaliseringen, hvilket også Anne Aly fremhæver. Vejene ind i voldelig ekstremisme er lige så forskellige som voldelige ekstremistister i almindelighed.[279] Alligevel sniger behovet for at anvende den kognitive åbning og ideen om sårbarhed sig ind ad bagvejen, når de ekstremistiske ideers betydning for individet slås fast. Sårbarhed ender således ofte med at være den bagvedliggende årsag, som forklarer individets interesse for de farlige ideologier. Den optræder retrospektivt som indikation på, at radikaliseringen har slået rod, uden at den i sig selv har nogen specifikke kendetegn. Sårbarheden forklarer med andre ord, hvorledes individet bliver ideologisk og religiøst søgende – på jagt efter svar og eksistentiel mening. Problemet bliver derfor at forklare, hvornår og hvordan denne søgen ender i et engagement med voldelig ekstremisme og ikke blot i et intensivt filosofistudium?

Som blandt andre Schmid og Price anholder, er sårbarhed dog langt fra den eneste gangbare individantagelse i radikaliserings- og terrorforskning. Og det kan være endog meget svært at identificere denne særlige radikaliseringssårbarhed. Ganske vist kan 'svage individer' socialiseres og rekrutteres til terrororganisationer, men der er også eksempler på, at unge mennesker selv er opsøgende og/eller på udkig efter en god sag. Somme tider er de drevet af spænding og handling frem for ideologiske brandtaler, hvilket også kan betyde, at de socialiseres ind i en gruppes adfærd frem for tænkning, eller at tænkningen retrospektivt kobles til adfærden. Person-beskrivelserne er mange og radikaliseringslitteraturen hjemsøges derfor af uhåndterbart

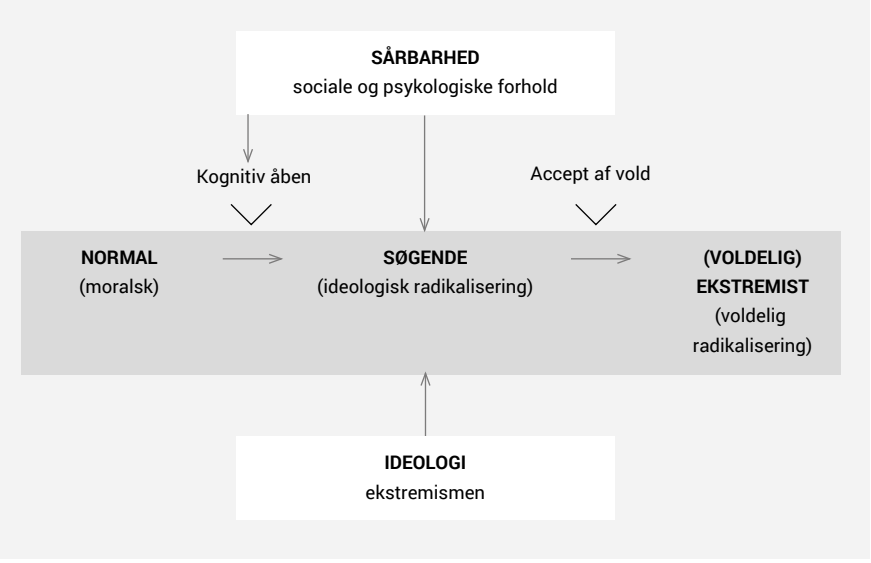
279 Aly, 2014: 69.

mange faktorer på mikroniveau.[280] Som Bhui og Ibrahim selv indrømmer, står teorierne om voldelig radikalisering (inden for forfatternes videnskabelige perspektiv) over for det samme dilemma som alle behavioristiske teorier – nemlig individuel variation.[281]

Problemet er, at ideen om sårbarhed vægter det kognitive/ideologiske element i radikaliseringen meget højt, hvilket peger på tænkningen som bagvedliggende årsag. Heraf følger, at tænkningen må være angrebspunktet for en effektiv radikaliseringsforebyggelse, hvilket igen leder til den konklusion, at internettet både har en meget stor betydning for radikalisering, samt er det sted, hvor forebyggelsesindsatsen må kæmpe med alle tænkelige midler.

Herudover peger sårbarhedstanken, og den Wiktorowicz-afledte overfokusering på de individuelle kognitive aspekter, på 'accept af vold' – den ofte anvendte formulering i radikaliseringsdefinitioner – som et relevant kriterium for radikaliseringsforståelsen. Men som andet underafsnit vil fremhæve er også denne forståelse blind over for samfundets egne normer og derfor alt for reduceret i sin (afkontekstualiserede) individforståelse. Som med den kognitive åbning synes ingen rigtigt at vide, hvad denne 'accept' egentlig indbefatter.

Fig. 6: Forebyggelseslitteraturens konstruktion af radikaliseringsprocessen



280 Schmid & Price, 2011: 338-339; Schmid, 2013: iv; Schmid, 2013: 33.

281 Bhui & Ibrahim, 2013: 229.

Radikaliseringsprocessen ender altså med at involvere to uforklarlige springende punkter. Det første punkt er den kognitive åbning, der indtræffer i individets overgang fra at være et normalt (moralsk) individ til at blive søgende. Denne første fase er kendetegnet ved ideologisk indflydelse, og her spiller sociale forhold og 'opfattede' konflikter med samfundsnormen såvel som personpsykologiske prædispositioner en central rolle. Efter tilstrækkelig ideologisk påvirkning og uhindret radikalisering indtræffer det andet punkt: accepten af vold. Det er her, hvor den sårbare unge går over til at blive en radikaliseret voldelig ekstremist. Radikaliseringsprocessen kan opsummeres som i ovenstående fig. 6, hvor den mørkegrå boks markerer individets radikaliseringsproces fra normal til voldelig ekstremist. Ideologien i den ovenstående model erstattes af radikalt online-indhold og ekstremistiske fællesskaber på sociale medier, når online-radikaliseringen af ensomme ulve skal forklares.

Radikaliseringsmodellens kobling af sårbarhed og ideologi har også en tendens til at ende i cirkelslutninger, hvilket bliver tydeligt i Quilliam Foundations forståelse af sårbare unge. Forskerne præsenterer således fire faktorer, der ifølge dem er med til at skabe sårbarhed over for ekstremistiske ideologier. En af disse faktorer er netop eksponering for ideologi, der legitimerer eller fordrer vold.[282] Herved fremstår ideologien som både årsagen til sårbarheden og effekten heraf.

Når modellen overføres til adfærd og holdninger på de sociale medier, støder tilgangen ofte på endnu en barriere i radikaliseringsforståelsen. Det ofte 'rationelle' fokus på, hvad de forskellige forskere og policy-skribenter opfatter som farlige ekstremistiske tanker fører til en til en-fortolkninger af forskellige udmeldingers betydning. Tilgangen tager med andre ord ikke forbehold for online-identiteternes performative karakter[283] til trods for, at den lægger vægt på forandring og proces. Den kan, som Jonathan Githens-Mazer og Robert Lambert formulerer det, ikke skelne mellem 'doers' og 'sayers'. Ved at koble fra holdninger til handlinger (gennem ideen om 'accept') forbliver tilgangen uvidende omkring de forskellige roller, som unge mennesker antager i deres omgang med identiteter på de sociale medier. Tilgangen mangler således ofte en konkret viden om den identitetsmæssigt komplekse sociale virkelighed, som den enkelte bruger bevæger sig i.

Herved risikerer radikaliseringsforståelsen (ubevidst) at sætte lighedstegn mellem affektive, følelsesladte udtryk og politikkens eller ekstremismens farlighed. Bag ved tilgangen gemmer sig normer om følelsesmæssigt afmålte individer, som er modtagelige for rationelle argumenter og ikke foretager uberegnelige valg. Modellen

282 Saltman & Russell, 2014: 2.

283 Papacharissi, 2012: 2000.

har således en normativ forkærlighed for det følelsesmæssigt afdæmpede rationelle individ og ser affektiv online-kommunikation som udtryk for farlighed. Netop forkærligheden for 'rationelle individer', der kan gøres til genstand for cost/benefit-analyser og rational choice-forklaringer er en ofte forekommende vinkel.

Arun Kundnani fremhæver hertil, at det valgte individfokus og de (ofte fortrængte) blinde vinkler i radikaliseringsforståelsen på belejlig vis fraskriver vestlige regeringers handlinger og deres alliancer forskellige steder i verden at have underliggende virkning på radikaliseringen. I stedet tillægges den psykologiske og ideologiske udvikling hovedårsagen for radikaliseringsprocessen – afkoblet fra større sociale og politiske omstændigheder. Samfundet og normaliteten opfattes kun som en positiv faktor. Det eneste sted, konstaterer Kundnani, hvor de sociale og politiske elementer anerkendes, er i eufemistiske vendinger som 'individets følelse af reelle eller opfattede uretfærdigheder'.[284] Og netop denne formulering, "a range of perceived sociopolitical grievances, to which there may seem to be no credible and effective non-violent response", er endnu en af Quilliam-forfatternes fire sårbarhedsfaktorer.[285]

Forsøget på at holde samfundspolitikken og samfundsdebatten skadesfri i diskussionen om radikalisering og derved ensidigt placere ansvaret og forklaringen ved de sårbare unge, der skal hjælpes tilbage til normaliteten, og den farlige ideologi, der skal holdes uden for indflydelse, risikerer at være blind over for både brugbare alternative problemforståelser og løsninger.

Opsummerende og med den britiske terror- og radikaliseringsforsker Charlotte Heath-Kellys ord kan det siges, at den radikaliseringsproces, som Wiktorowicz og andre har bekrevet, efterfølgende har fundet anvendelse som forklaringsmodel i en række forskellige kontekster: hvor politisk vold skulle tilskrives en kausalitet, hvor opmærksomheden skulle afledes fra ubelejlige politiske radikaliseringsfaktorer såsom fattigdom, eksklusion eller den førte udenrigspolitik og hvor der var behov for at indgyde et håb om, at fremtidige voldelige handlinger kan forhindres med den rette kombination af bløde og hårde forebyggelsestiltag.[286]

284 Kundnani, 2015: 16.

285 Saltman & Russell, 2014: 2.

286 Heath-Kelly et al., 2015: 7.

I denne radikaliseringspolitiske kabale passer truslen fra de ensomme ulve perfekt til en forestilling om online-radikaliseringens kausalitet. Her synes den sociale og politiske kontekst at være fraværende, og hårde såvel som bløde løsninger er allerede afprøvet. Der er både et klart problem og en række klare løsninger. Spørgsmålet bliver dog, om forebyggelseslitteraturens ensidige fokus risikerer at blive kontraproduktiv? Forsøget på at holde samfundspolitikken og samfundsdebatten skadesfri i diskussionen om radikalisering og derved ensidigt placere ansvaret og forklaringen ved de sårbare unge, der skal hjælpes tilbage til normaliteten, og den farlige ideologi, der skal holdes uden for indflydelse, risikerer at være blind over for både brugbare alternative problemforståelser og løsninger. Ifølge Schmid har der længe været for stort fokus på sårbare unge, der skal frelses fra rekruttering til terrorisme. Der er i stedet behov for at betragte og analysere radikali-seringens andre niveauer.[287] Og der er behov for at anerkende, at radikalisering er en dialektisk proces, som kræver to parter. Radikalisering sker både for 'dem' og for 'os'.[288]

Den farlige ideologi og ideen om 'viljen til vold'

Hussain og Saltman fra Quilliam Foundation opsummerer i deres rapport Jihad trending: A Comprehensive Analysis of Online Extremism and How to Counter it, hvorledes ekstremismen ikke kan modgås, såvel offline som online, uden en dybdegående forståelse for ekstremismens ideologi og strategi.[289] Saltman omtaler, i en Quilliam-publikation om online-ekstremisme forfattet sammen med Jonathan Russell, konsekvent ideologier som 'ekstremistiske ideologier' eller 'potentielt farlige ideologier', hvilket får forfatterne til at argumentere stærkt for også at modarbejde den ikkevoldelige ekstremisme.[290]

Således behandler Quilliam-forfatterne terrorisme og ekstremisme som problemstillinger, der netop skal løses gennem ideologiske mod- og dekonstruktioner. Problemet er dog for det første, at ideologien netop synes at virke særligt dragende der, hvor den ikke afslører sig selv som ideologi men tværtimod har fat i fantasier og følelser. Modnarrativerne tager med andre ord ofte afsæt i en alt for simpel opfattelse af individet – en individforståelse, som formentlig selv Islamisk Stat har forstået begrænsningerne i. Betragter man således terrororganisationens spillefilmsprojekter Flames of War eller The Clanging of the Swords fra 2014 – og ikke mindst trailerne til disse – er de ofte som propaganda sammensat således, at det ideologiske

287 Schmid, 2013: 54.

288 Schmid, 2013: 37.

289 Hussain & Saltman, 2014: 108.

290 Saltman & Russell, 2014: 11.

narrativ tydeligvis sidestilles, hvis ikke underordnes, den visuelle krigs- og voldsæstetik. Her forbindes både æstetik, politik og følelse til et bredt modkultursfænomen, der tilbyder en følelsesmæssig dyrkelse af forskellige former for overskridelse (transgression) af vestlige normer og tabuer: sammenblanding af politik og religion; affektiv og militant politik, der dyrker hævnen; kommunitære fællesskaber/broderskaber, hvor mænd og kvinder er adskilte osv.

Det er klart, at denne politisk afkoblede individforståelse – hvor det sårbare individ fremstilles, som var det en laboratorieklar petriskål, der blot venter på en radikalisators udstrygning af fremmed ideologi, som derved gennem teoretisk og tankemæssig forprogrammering lægger grunden til de voldelige handlinger – virker fristende på en forklaringshungrende handlingspolitik.

Modkulturen er i flere henseender præcis en spejling og overskridelse af den vestlige normalitet, og som sådan hænger de to fænomener uløseligt og dialektisk sammen. Når online-tilgangene derfor frafalder det dialektiske perspektiv (modkultursforståelsen) ved at reducere den sociale kompleksitet til effekter på individniveau under indflydelse af 'ekstremistiske ideologier', bliver det også muligt for forskerne at tro på modnarrativernes virkning (at aflive myter og misinformation) og samtidig reducere radikaliseringsproblemet til en kausalrelation mellem ideologisk radikalisering og voldelig ekstremisme. Som Salem et al. formulerer det: "the myths and disinformation propagated in the groups' videos can be countered by designing and disseminating credible messages from authentic and trusted sources at the grassroots level".[291]

I stedet for den dialektiske forståelse fæstner tilgangene hele radikaliseringsproblemet ved Wiktorowicz' svage individ, der gradvist accepterer 'high risk activism' og de radikale bevægelsers ideologi gennem religiøs uddannelse og 'kultivering'.[292] Det er klart, at denne politisk afkoblede individforståelse – hvor det sårbare individ fremstilles, som var det en laboratorieklar petriskål, der blot venter på en radikalisators udstrygning af fremmed ideologi, som derved gennem teoretisk og tankemæssig forprogrammering lægger grunden til de voldelige handlinger – virker fristende på en forklaringshungrende handlingspolitik.

291 Salem et al., 2008: 620.

292 Wiktorowicz, 2005: 6.

I Wiktorowicz tilfælde bruges David Snow og Robert Benfords teorier om 'frame alignment'[293] til at forklare denne kognitive forandringsproces på individniveau.[294] Men hver radikaliseringsteoretiker har næsten udviklet sin egen forklaring på ideologiernes kognitive smitteevne og voldens ideologiske udspring. Anne Aly anvender teorien om 'moral disengagement' som forklaringen på, hvad der sker ved det punkt, hvor individet mister sin normalitet og det 'naturlige' moralske ubehag ved volden som metode. For at udvikle en 'terrorismepropensitet', dvs. en naturlig inklination i retning af terrorisme, må mennesker ifølge teorien blive udsat for terrorismefordrende moralsk kontekst (eksponering). Og for at kunne blive påvirket som konsekvens af eksponeringen, må individet være "sårbart over for moralsk forandring".[295] Det er denne moralske forandring som ifølge Aly medfører, at individerne bliver koblet fra deres egen naturlige moralske forbehold for vold og derved bliver i stand til at engagere sig i vold og aggressiv adfærd – i modsætning til deres oprindelige moralske standarder.[296] Moralen bliver i Alys teori et begreb, der forbinder ideologi og handling:

> "Moral disengagement is a psychological process through which self-regulatory mechanisms of internal control are disengaged or dismissed. Self-sanctions are disengaged through the mechanisms of moral disengagement […] Collectively, the mechanisms of disengagement allow individuals to cognitively reconstruct the moral value of violence, putting aside self-sanctions, so that acts of violence can be committed.[297] "

Samme tanker kan findes hos en anden af online-radikaliseringens teoretikere, Scott Helfstein, der hæfter sig ved, at radikalisering i sin kerne er en proces, hvor folk ender med at tro på, at voldsanvendelse i bestræbelsen efter visse politiske eller religiøse mål ikke er umoralsk.[298] Der er altså en moralsk fredelig kerne i mennesker, som på en eller anden måde først kognitivt skal omprogrammeres eller tilsidesættes, før individet er i stand til at handle voldeligt.

293 Se mere: Snow & Benford, 1998.
294 Wiktorowicz, 2005: 16.
295 Aly, 2014: 70.
296 Aly, 2014: 74.
297 Aly, 2014: 74.
298 Helfstein, 2012: 15.

På linje med andre af online-radikaliseringens ringbærere såsom Gabriel Weimann og Scott Helfstein, forstår Aly radikaliseringen som inddelt i forskellige faser. Aly ser det således som modnarrativernes opgave at fange unge mennesker, der endnu er i 'søgefasen' ved at tilbyde dem alternative fortællinger, som leder individerne væk fra voldelig ekstremisme.[299] For Helfstein er det strategiske angrebspunkt i stedet 'acceptstadiet' (der kommer efter søgefasen). På acceptstadiet søger individet sociale forbindelser til at overvinde egne normative forbehold over for voldelig adfærd.[300] Nogenlunde samme beskrivelse kan findes ved det hollandske radikaliseringsforebyggelsesprojekt, Wij Amsterdammers, der selv har Wiktorowicz som inspirationskilde.[301] Det hollandske projekt har samtidig fungeret som hovedinspirationskilde for Embedsmandsrapporten[302], der i 2008 foretog alt forarbejdet til den første danske handlingsplan til forebyggelse af radikalisering og ekstremisme fra 2009.[303] Der ligger altså en klar opfattelse af radikalisering som en kognitiv/moralsk udviklingsproces, der udvikler sig i faser og ender i et voldeligt engagement. Denne tænkning kan delvist spores tilbage til Wiktorowicz, og den har haft stor indflydelse på såvel den danske forebyggelsespolitik som på meget af litteraturen om online-radikalisering. Netop denne radikaliseringslogik har dog også mødt stor modstand og kritik andre steder i litteraturen.[304]

Ikke desto mindre er den fremherskende blandt mange af online-radikaliseringens trusselsforfægtere – forskere og policy-skribenter, som tillægger radikalt online-indhold stor farlighed.[305] Bermingham et al. fremhæver eksempelvis troen på, at noget netindhold og interaktion er konstrueret med det formål at radikalisere dem med lille eller ingen interesse i voldelig jihadisme, hvilket får forfatterne til at konkludere relevansen af de kvantitative metoders optrevling af ekstremistisk online-indhold.[306] Dette afspejler sig også i forfatternes definition af online-radikalisering, der beskrives som "en proces, hvorved individer, gennem deres online-interaktion og eksponering for forskellige typer internetindhold, accepterer [come to view] volden som en legitim metode til at løse sociale og politiske konflikter"[307].

299 Aly, 2014: 77.

300 Helfstein, 2012: 3-4.

301 Mellis, 2007.

302 Embedsmandsrapporten, 2008.

303 Regeringen, 2009.

304 Schmid, 2013; Bigo et al., 2014; Kundnani, 2015.

305 Gemmerli, 2014b.

306 Bermingham et al, 2009: 1.

307 Bermingham et al, 2009: 1 – egen oversættelse. Den originale formulering lyder: "Online radicalization is here conceived as a process whereby individuals, through their online interactions and exposure to various types of Internet content, come to view violence as a legitimate method of solving social and political conflict".

Samme forståelse lægger Brynielsson et al. til grund for deres analyser: "Online extremist forums and web sites allow for aberrant beliefs or attitudes to be exchanged and reinforced, and creates environments in which otherwise unacceptable views become normalized".[308] I stedet for argumenter om moral bygger de altså deres radikaliseringsforståelse på en 'normalisering', som er med til at forbinde ideologi og handling.

Selve ideen om en radikaliseringsproces, der består i koblingen mellem de sårbare unge og den farlige ideologi, er, ifølge Heath-Kelly, skabt som politisk værktøj til at tilskrive visse radikale elementer en farlig andethed, til trods for, at de som regel er både født og opvokset i samfundet og om noget er produkter af velfærdsstatens socialisering. Men det er denne andethed, der gør det muligt at se bort fra de større samfundspolitiske spørgsmål. Det er denne andethed, som stabiliserer normaliteten.

Bermingham et al. er blandt de få artikler, der både har ambitioner om at udvikle et værktøj til radikaliseringsforebyggelse, og som tør definere online-radikalisering. Som allerede diskuteret i Gemmerli (2014a) medfører denne definition en del problemer – ikke mindst betydningen af 'accept af vold' som legitim metode til at løse sociale og politiske konflikter. Præcis hvad denne accept indbefatter, uddyber forfatterne ikke, men det er tydeligvis en videreførelse af den mest populære policy-definition, som også PET og flere danske kommuner har taget i anvendelse. Problemet er naturligvis, at definitionens tilstræbt objektive formulering kører frontalt sammen med en subjektiv og politisk virkelighed, hvor parlamentariske politiske konflikter løses inden for en ramme, der er sanktioneret af voldsmonopolet, som alle parlamentariske partier forventeligt respekterer. Der ligger med andre ord en fundamental accept af vold til grund for alt politik – ikke kun den ekstremistiske del af slagsen. Vores politiske normalitet hviler på et fundament af (legitimeret) vold, men den er samtidig demokratisk sanktioneret for derved at kunne forandre sig via fredelige midler, og uden at monopolet destabiliseres.

Arun Kundnani drager her en parallel til Den Kolde Krig, hvor Vesten ligeledes opfattede ideologi som noget, der udelukkende kendetegnede fjenden. Og det er ifølge Kundnani denne tendens til at opfatte os selv som ideologiløse, der medvirker,

308 Brynielsson et al., 2012: 197.

at samfundet inden for radikaliseringsperspektivet kun er i stand til at acceptere en afpolitiseret Anden.[309] Vesten ser således sunniekstremismen som indbegrebet af en farlig ideologi og kan kun acceptere en afpolitiseret og verdslig Islam, der underlægger sig det politiske systems normalitetsforståelse og voldsmonopol. For Heath-Kelly er dette et symptom på en politik, der udpeger den skyldige (voldens årsag) og finder på modforanstaltninger, uden først at indregne sin egen rolle i problematikken. Selve ideen om en radikaliseringsproces, der består i koblingen mellem de sårbare unge og den farlige ideologi, er, ifølge Heath-Kelly, skabt som politisk værktøj til at tilskrive visse radikale elementer en farlig andethed, til trods for, at de som regel er både født og opvokset i samfundet og om noget er produkter af velfærdsstatens socialisering. Men det er denne andethed, der gør det muligt at se bort fra de større samfundspolitiske spørgsmål.[310] Det er denne andethed, som stabiliserer normaliteten.

Frygten for de ideologiske udfordrere af voldsmonopolet ville være mere reel, hvis der var en kausalsammenhæng mellem radikale tanker og viljen til at følge op på denne udfordring med voldelige midler. Men årtiers forskning i terror og radikalisering har for længst afskrevet dette perspektiv. Det er kun en forsvindende lille minoritet af de radikalt tænkende, som rent faktisk ender i et voldeligt engagement. Til gengæld er litteraturen om politisk vold og sociale bevægelser rig på teorier og modeller for, hvordan forskellige strukturer m.v. kan påvirke udfaldet i såvel voldelig som ikkevoldelig retning. Men en inddragelse af den litteratur og de perspektiver fordrer, at vi tør stille spørgsmålet om, hvad der får minoriteter, grupper, miljøer eller individer til at reagere voldeligt, mens andre ikke gør? Og svaret (hvis der er et svar,) skal findes ved kritisk at eksaminere hele problemstillingen – ikke ved blot at konstruere en virkelighed, hvor politik ikke findes.

Den teoretiske båndsløjfe mellem sårbarhed og ideologi fungerer således som generator for løsninger, der ligger uden for radikaliseringsproblemets samfundsskabte politiske og sociale kontekst, og som samtidig (bort)forklarer paradokserne i demokratiets kerneland.[311] Som Heath-Kelly formulerer det:

309 Kundnani, 2014: 16.

310 Heath-Kelly et al., 2015: 7.

311 Heath-Kelly et al., 2015: 2.

> "'Radicalisation', or 'violent radicalisation', is taken to refer to a socialization process through which people become involved in terrorism [...]. This motif forms the centerpiece of the feedback loop constructed to explain terrorist events through combinations of vulnerability and ideology. However, such renderings of socialization are misleading in the sense that these processes do not have to be 'violent' or involve violence. Moreover, there is an inherent difficulty that exists in differentiating between people who adopt or support political positions or beliefs that might be interpreted as 'radical' and identifying those who would actually engage in acts of political violence as a direct result of those same political positions or beliefs.[312]"

En udfordring for hele online-litteraturens radikaliseringsmodel, som også Aaron Zelin påpeger, er naturligvis, at det endnu er uafklaret, hvorvidt og hvordan den nemme adgang til 'jihadi social media platforms' vil føre til, at flere individer tilslutter sig den globale terrorbevægelse, eller om den sociale bevægelse forvitres og modereres ved at legitimere ideen om, at man kan 'heppe' på sikker afstand i stedet for at deltage i ekstremismens voldelige kamp.[313] Betyder et øget online-engagement også en øget voldspropensitet? Eller betyder en mere udadvendt internetadfærd, at flere får afløb for indestængte aggressioner, og som Irhabi 007 eller Shami Witness forbliver rene online-jihadister.[314] Og såfremt muligheden for at bruge sproget og online-identiteten som en slags frustrationsventil virker afværgende på den ekstremistiske vold, risikerer en øget overvågning af sproget da ikke blot at lægge en dæmper på frustrationsventilen og presse voldsfantasierne tilbage i mørket, hvor de kan vokse sig større i en kontekst af offeridentitetens frygt, miskendelse og marginalisering?

Som flere forskere påpeger, mangler der ganske enkelt forskning og analyser, som undersøger og påviser online-indholdets effekt – den reelle online-radikalisering – frem for blot at antage indholdets virkning og deraf slutte til nødvendigheden af at bekæmpe indholdets farlighed.[316] Der har ifølge Edwards og Gribbon således været et alt for stort fokus på udbuddet (online-indholdet) frem for egentlige undersøgelse af udbuddets effekter (ibid.). Og som Schmid fremhæver i sin ekstensive litteraturgennemgang: "It is important to understand the way extremist ideas and beliefs translate into terrorist actions. We still lack good answers to this question".[316]

312 Heath-Kelly et al., 2015: 5.

313 Zelin, 2013: 6.

314 For en diskussion heraf se Gemmerli (2014a).

315 Edwards & Gribbon, 2013: 41.

316 Schmid, 2013: 28.

Selv hvis man går ind på præmissen om, at ideologien kan påvirke mennesker til voldelig adfærd, så synes dette netop kun at gøre sig gældende for et lille mindretal af de ideologisk radikaliserede. Andre voldelige ekstremister er, med Schmids ord, ideologisk usofistikerede eller næsten indifferente over for store forkromede tanker.[317] I mange tilfælde har det politiske ikke nødvendigvis den største betydning, og somme tider tilkobles ideologien retrospektivt som argument for individets voldelige inklinationer.[318]

Når det alene er online-adfærd, der ligger til grund for analyserne, bliver jagten efter de radikaliseringstruede sårbare unge internetbrugere derfor til en jagt efter de voldsfascinerede og ekstremismenysgerrige unge, som meget vel kan være 'store i munden', men som ikke nødvendigvis evner eller ønsker at bringe deres voldsomme retorik til handling. Og, som også tidligere nævnt, går radikaliseringsjagten derved fejl af sondringen mellem 'doers' og 'sayers', hvilket gør, at mulighederne for at lokalisere terrorister in spe forbliver små.[319]

Som flere forskere påpeger, mangler der ganske enkelt forskning og analyser, som undersøger og påviser online-indholdets effekt – den reelle online-radikalisering – frem for blot at antage indholdets virkning og deraf slutte til nødvendigheden af at bekæmpe indholdets farlighed.

Når dette ubesvarede spørgsmål så desperat søger solide videnskabelige udredninger, skyldes det ikke mindst, som Schmid også bemærker, at spørgsmålet stiller forebyggelsespolitikken over for store valg.[320] Er det således nødvendigt med en tilgang, der aktivt forebygger hele feltet af ideologiske modstandsformer, eller er det bedre at holde fokus på udelukkende at bekæmpe den voldelige ekstremisme? Eller er hele forestillingen om overhovedet at kunne bekæmpe ekstremismen dybest set kontraproduktiv?

317 Schmid, 2013: 28.

318 Githens-Mazer & Lambert, 2010: 891; Merkl, 1986: 39; Crone, 2009: 73; Lamberty, 2013: 139.

319 Githens-Mazer & Lambert, 2010: 896.

320 Schmid, 2013: 53.

Radikalisering er som fænomen desværre endnu for flygtigt og upræcist beskrevet og defineret til, at det er muligt at operationalisere begrebet gennem kvantitative analyser uden derved at negligere eller fortrænge en lang række uafklarede spørgsmål – som afsnittets indledende model også antyder. Samtidig risikerer de kvantitative metoders empiri-rigdom at føre til et informationsoverload, hvor potentielt vigtige informationer overskygges af et hav af ligegyldige 'falske positiver'. Det betyder ikke, at fænomener som ekstremisme eller voldelig ekstremisme ikke kan eller bør studeres gennem kvantitative metoder og data mining-teknikker. Tværtimod. Men det betyder, at koblingen til radikaliseringsbegrebet risikerer at føre til forsimplede og misvisende konklusioner, der kan afstedkomme nogle kontra-produktive politikker.

FOREBYGGELSESTANKENS TEKNOLOGIFASCINATION

Som denne rapport har forsøgt at klarlægge, kobler litteraturen om forebyggelse af online-radikalisering allerede kendte radikaliseringsforståelser og forebyggelses-metoder til den forhåndenværende empiri for (retrospektivt) at skabe en radikaliseringsmodel, der også kan begribes kvantitativt. Dette skaber en forståelse af den radikale Anden, som i højere grad er styret af epistemologiens blinde vinkler (jf. diskussionen om forbindelser og noder), kulturelle fordomme og teknologi-fascination end kritisk videnskabelig praksis. Men forestillingen om at kunne anvende internettet og den nyeste computersoftware til at løse den virkelige verdens ekstremismeproblemer er blot et aspekt af en tendens til teknologifetichisme eller tekno-utopisme, der fungerer som et forlokkende multiværktøj på mange policy-områder.[321] Ifølge Morozov er det således dybt problematisk, at den sociale kontekst ofte ignoreres, når politiksmedene forledes til at tro, at de har et uovertruffet kraft-fuldt værktøj på deres side, som de formår at beherske.[322]

Med denne kritik kaster Morozov lys på et fænomen, som breder sig over en lang række policy- og forskningsområder. Fantasierne står i kø, når fremtiden beskrives i lyset af teknologiens nye landvindinger. Ny teknologi har en tendens til at skænke forskere og policy-skribenter en værkstøjskasse med besnærende potentialer og ultimative løsninger. Det gør sig også gældende på terror- og radikaliseringsområdet. Ofte sættes så stor lid til vores beherskelse af teknologiens løfte om informations-behandling og -kontrol, at det sociale underordnes teknologiens orden.[323] Dette betyder, at både metodiske og videnskabsteoretiske spørgsmål fortrænges til fordel for det teknologiske fix.

321 Bartlett, 2015.

322 Morozov, 2012: xvi; Morozov, 2014b: 5.

323 Mejias, 2006; Bartlett, 2015.

Problemet er dog, at teknologiske eksperter, hvor tekniksmarte de end måtte være i forhold til teknologiens muligheder, sjældent er bekendt med de komplekse sociale og politiske kontekster, som de teknologiske løsninger skal operere i.[324] Sociale problemer kan, med Morozovs egne ord, ikke reduceres til tekniske problemer, og vi skal derfor passe på ikke at falde ukritisk for denne 'cyber-centrisme' eller 'technological solutionism'.[325] Noget af det mest problematiske ved de teknologiske løsninger bliver derfor, at reduktionen til tekniske problemer risikerer at aflede politiksmedene fra at håndtere de udfordringer, som netop ikke kan reduceres.[326] Som medieforsker Christina Archetti pointerer: "The not unjustified, but certainly disproportionate, focus on the Internet prevents us from seeing the wider social – and never online-only – space in which extremism is rooted".[327]

Dette sidste afsnit vil gå dybere ned i forestillingen om online-radikaliseringens kendetegn og løsningsmodeller, som de fremkommer i en litteratur, der har sat indholds- og netværksanalyse i førersædet. Dette gøres ved i første underafsnit at gennemgå et par eksempler på forestillingen om online-radikaliseringens kendetegn. Her vil de etiske konsekvenser af den masseovervågning, som litteraturen synes at argumentere for, kort blive diskuteret. Andet underafsnit vil redegøre for forebyggelseslitteraturens ide om teknologiske løsninger samt konsekvenserne af de fantombilleder som løsningerne synes at frembringe.

Forestillingen om online-radikaliseringens kendetegn

Store dele af online-radikaliseringens forebyggelseslitteratur udtrykker ideer og intentioner om en form for profilering – ønsket om at kunne tegne et fantombillede af den potentielle ensomme ulv, der radikaliseres og (selv)rekrutteres via internettet og de sociale medier. Denne profil omtales blandt andet som individer med bestemte 'personlighedsstrukturer'.[328] Men profileringstanken bliver mest konkret udfoldet i den del af litteraturen, hvor ideen oprindelig hører hjemme. De artikler om online-radikaliseringens kendetegn, der således i mest konkrete vendinger beskæftiger sig med muligheden for at lokalisere de prospektive ensomme ulve gennem en profilering af internetadfærd og internetkommunikation, er ofte den del af litteraturen, der henter sin inspiration fra den behavioristiske, psykiatriske terrorforskning (kriminologien).

324 Morozov, 2012: 311.

325 Morozov, 2014b.

326 Morozov, 2012: 305.

327 Archetti, 2015: 51.

328 Dienstbühl & Weber, 2014: 41-42.

Cohen et al. oplister i artiklen "Detecting Linguistic Markers for Radical Violence in Social Media" tre typer advarselssignaler/bekymringsadfærd, som de mener at kunne identificere ved at skanne de sociale medier.[329] I artiklen, der som mange andre artikler på området er af teoriudviklende art, tager forskerholdet afsæt i retspsykiateren, Reid Meloy[330], som har udviklet et batteri af otte generelle 'advarselssignaler' til brug ved trusselsvurderinger. De tre udvalgte advarselssignaler, som forfatterne mener, kan appliceres på online-adfærd, er lækage (leakage), fiksering (fixation) og identifikation (identification).[331]

Her gælder altså samme kritik som ved de indholdsanalyser, der skal finde affekt og følelser. Risikerer analyserne ikke blot at finde de 'unormale', som ikke overholder vores forventninger om rationel argumentation og dialog?

Lækagen indbefatter, at en tredjeperson bliver informeret om intentionerne om at gøre skade på et mål, hvilket ifølge teorien ofte afspejler sig i en intensiv optagethed af målet.[332] Helt konkret beskriver forfatterne de lingvistiske lækagemarkører således: "Leaked information of intent is likely to contain auxiliary verbs signaling intent (i.e., "I will…," "…am going to…," "someone should") together with words expressing violent action, either overtly or, perhaps more likely, through euphemisms".[333] Tanken er, at de lækkede ord skal matches med en foruddefineret liste over ord (indholdsanalyse ud fra 'bag of words'), der indikerer voldelige intentioner.[334] Forfatterne indrømmer dog, at denne metode vil få vanskeligt ved at vurdere ironi, tomme trusler, trolling mv., hvorfor en systematisk skanning risikerer at finde en del falske positiver. Som algoritme- og teknologiforskeren Jamie Bartlett også påpeger, har denne tekno-utopisme en tendens til groft at overvurdere algoritmernes muligheder og egenskaber.[335]

Fiksering som advarselsadfærd defineres som en patologisk optagethed af en person eller en sag (fx tiltagende perseverationstendenser over for fikserings-objekter), stigning i voldsomme og gennemskærende meninger samt stigning i

329 Cohen et al., 2014.
330 Meloy et al., 2011.
331 Cohen et al., 2014: 248.
332 Cohen et al., 2014: 248.
333 Cohen et al., 2014: 253.
334 Cohen et al., 2014: 253.
335 Bartlett, 2015.

negative beskrivelser af fikseringsobjekter.[336] Dette giver sig ifølge forfatterne til kende som en person eller sag, der for visse personer nævnes med højere frekvens end andre steder på nettet.[337] Her gælder altså samme kritik som ved de indholdsanalyser, der skal finde affekt og følelser. Risikerer analyserne ikke blot at finde de 'unormale', som ikke overholder vores forventninger om rationel argumentation og dialog?

Endelig defineres identifikation som en advarselsadfærd, der indikerer ønsker om at blive en kommandosoldat, at have krigermentalitet, fascination af våben og militært udstyr, identifikation med visse gerningsmænd eller begivenheder m.fl.[338] Denne identifikation kan rette sig mod radikale handlinger (krigermentalitet), rollemodeller og idoler samt radikale grupper. Det er klart at denne online-adfærd i en eller anden udstrækning kobler sig til forventningen om voldelig adfærd. Men også her må antallet af falske positiver være uforholdsmæssigt højt, da denne form for volds- og våbenfascination er relativt udbredt blandt drenge og unge mænd.

Ud over alle de metodiske problemer, som blev omtalt under indholdsanalysen i rapportens del 2, er det uklart, hvordan programmerne skal kunne skelne mellem den store mængde af løsslupne online-fantasier og de konkrete intentioner om at udleve fantasien i en voldelig form. Hvorvidt Meloy et al. rent faktisk har udviklet et anvendeligt profileringsværktøj til brug ved trusselsvurderinger vil ikke blive vurderet i denne rapport. Men det er i sig selv tankevækkende, at Cohen et al. uden videre vil kopiere 3 af Meloys 8 koncepter til online-adfærd uden først at gøre sig klart, hvordan online-virkeligheden kan tænkes at adskille sig fra den fysiske virkelighed, Meloys kategorier er udviklet til. Med kun tre løst definerede kendetegn er risikoen for falske positiver under alle omstændigheder høj, og chancen for rent faktisk at kunne lokalisere de ensomme ulve er svær at vurdere.

Det andet forskerhold fra FOI, Brynielsson et al., udvikler med afsæt i de samme metoder ligeledes et tekstsporingsværktøj, der på sin vis skal kunne profilere de potentielle terrorister. Forfatterne nedbryder således 'ulvespørgsmålet' til tre mulige underkategorier, der skal anvendes til at udregne trusselsniveauet: Motiver/hensigter, kapabiliteter og muligheder.[339] Som motiv eller hensigt indregner forfatterne, om den enkelte er aktiv på radikale internetfora og skriver radikale opslag. Tanken er altså, at jo mere den enkelte er aktiv på internettets mange

336 Cohen et al., 2014: 249.

337 Cohen et al., 2014: 253.

338 Cohen et al., 2014: 249.

339 Brynielsson et al., 2012: 198.

ekstremistiske fora, jo større er risikoen for, at engagementet udvikler sig voldeligt. Denne implicitte påstand er dog stærkt omdiskuteret, ligesom det er tvivlsomt, om online-aktiviteten reelt kan tilskrives samme bruger jf. diskussionen om brugerprofiler.

Kapabilititeten måles ved, at den enkelte er aktiv på kapabilitetsfora (dvs. taktiske fora om voldeligt ekstremistisk/terroristisk engagement) og skriver opslag om sine indkøb. Interessen for 'how to jihad' samt besiddelse af farligt udstyr indikerer med andre ord et større trusselsniveau. Endelig opererer de med muligheder eller potentialer for et angreb. Derved tages bestik af konteksten. Er der med andre ord noget i tiden, som bør øge opmærksomheden om problemet? Analysemetoden kombinerer dernæst resultaterne fra de forskellige mål til en samlet vurdering:

> "The results from the various sub-processes are then fused and used to come up with an estimate of how likely it is that someone is or is starting to become a potential lone wolf terrorist, resulting in a list of potentially dangerous actors to keep and extra eye on.[340]"

Forskerholdet baserer overordnet set deres antagelse om online-radikalisering på en udtalelse fra historiker og forsvarsanalytiker ved Stockholm Universitet, Michael Fredholm, der ifølge forfatterne til et seminar i Stockholm skulle have udtalt, at nærmest al radikalisering af ensomme ulve foregår over internettet. Som et eksempel på denne radikalisering nævner forfatterne AQAP's Inspire Magazine:

> "This kind of Internet-based radicalization processes often result in various digital traces, created when visiting extremist forums, making postings with offensive content etc. In fact, a notable characteristics of lone wolf terrorists is that they often announce their views and intentions in advance.[341]"

I ovenstående citat slutter forfatterne baglæns uden at have belæg for det. Selv hvis den antagelse, at de fleste efterlader spor om deres intentioner, skulle være sand – hvilket de ikke fremkommer mod nogen dokumentation for – så ved vi ikke, hvor

340 Brynielsson et al., 2012: 199.

341 Brynielsson et al., 2012: 198.

mange online-trusler, insinuationer og antydninger, som ikke er blevet ført ud i livet. Hvor mange falske positiver giver denne tilgang? Hvor mange internettrolde og selvophøjede online-ekstremistister kommer unødvendigt i myndighedernes søgelys?

Endnu en gang er risikoen ikke nødvendigvis, at de rigtige informationer med denne tilgang vil glide forebyggelsesindsatsen eller terrorbekæmpelsen af hænde. Tværtimod risikerer denne tilgang blot at føre til en informationsforstoppelse, hvor det bliver umuligt at finde nålen i høstakken, og hvor vi derfor først retrospektivt kan konstatere, at vi hele tiden har ligget inde med informationer om dette og hint. Som Archetti også påpeger, er radikalisering et momentant og kontekstafhængigt fænomen, som ikke kan forudsiges eller beregnes.[342]

Selv tilfældet Breivik, der i Brynielsson et al. nævnes som hovedargument, er kendetegnet ved hverken at være specielt ideologisk ekstrem eller at have afsløret detaljer om sine intentioner. Breivik var nationalkonservativ og holdt sine intentioner for sig selv indtil dagen for sine brutale gerninger.[343]

Fremfor at gå fuldautomatisk til værks fremfører Berger og Strathearn det synspunkt, at de kvantitative tilgange kan anvendes til at analysere og rangordne de potentielle radikaliseringskandidater og dernæst kvalitativt vurdere dem, der falder i risikogruppen:

> "We believe manually examining users whose interactivity rank falls between 200 and 500 might be fruitful in identifying people vulnerable to radicalization or in its early stages, whose interactions indicate an interest in an extremist ideology but not a single-minded obsession with it.[344] "

Forfatterne giver derved udtryk for en radikaliseringsforståelse, der er faseopdelt og tager udgangspunkt i ideologien. Sårbarheden ses i deres model som en form for ideologisk svaghed. Og radikale tanker opfattes som en kognitiv virus, som samfundet bør immunisere unge radikaliseringstruede mennesker imod.[345]

342 Archetti, 2015: 54.

343 Ravndal, 2013: 173.

344 Berger & Strathearn, 2013: 43.

345 Archetti, 2015: 49.

Ønsket om at indsnævre målgruppen for nærmere efterforskning begrunder Berger og Strathearn i, at størstedelen af folk, som deltager i ekstremistiske samtaler på internettet, er uinteressante for radikaliseringsforebyggelsen (jf. ovenstående diskussion om problemet ved for mange falske positiver). Disse personer deltager blot lejlighedsvist eller periodevist i debatten, og deres retorik er, ifølge forfatterne, kun minimalt involveret i ideologiens transformation til voldelig ekstremisme.[346] Hvor effektiv denne semi-kvalitative eller halvautomatiske tilgang egentlig er, må tiden vise. Om den uden videre kan overføres fra studiet af amerikanske supremacister på Twitter til andre grupper, tendenser og medieflader, er dog tvivlsomt.

Den gennemskærende profileringslogik og forestillingen om i online-adfærden at kunne skelne tydelige tegn på radikalisering udtrykkes sjældent lige så gennemsigtigt som i de ovennævnte litteratureksempler. Men antagelserne og forestillingerne går alligevel igen, så snart mulige løsninger skal udpeges, og radikaliseringsprocessen skal begrebsliggøres. Bag den besnærende logik gemmer sig dog netop en form for teknologioptimisme, som overlader tvivlsspørgsmål og metodeproblemer til de alvidende algoritmer og den kyndige programmør, samt en radikaliseringsforståelse, som reducerer processen til individplanet og derved konstruerer et afkontekstualiseret fantombillede af den potentielle terrorist.

Simple modeller og teknologiske løsninger?

Cyber-centrismens teknologioptimisme og fantasierne om algoritmernes omnipotente sporingsegenskaber har skabt forventninger om at kunne udpege de radikaliseringssårbare potentielle terrorister, inden de ender i den voldelige ekstremismes løbebane.[347] Håbet er, at de automatiserede eller halv-automatiserede teknikker med afsæt i de forestillede lingvistiske kendetegn vil gøre det muligt at afsløre individer (særligt ensomme ulve), inden de begår voldelige eller kriminelle gerninger.[348]

Problemet har dog indtil nu været, at der ikke findes en konsistent profil af en ensom ulv, hvilket Brynielsson et al. også indrømmer.[349] Alligevel gøres forsøget på, i det mindste hvad angår sprog og online-adfærd, at tegne et konsistent, men bredt

346 Berger & Strathearn, 2013: 36.

347 Cohen et al., 2014: 253.

348 Cohen et al., 2014: 247.

349 Brynielsson et al., 2012: 204.

favnende fantombillede. Men spørgsmålet er, hvorvidt det overhovedet giver mening at arbejde med forestillingen om ensomme ulve, hvis der ikke er tale om ét fænomen? Som Schmid understreger, har vi tidligere forsøgt uden held at profilere 'terroristen', der viste sig at være 'normal' i både klinisk og sociologisk forstand.[350] Og der er i dag bred enighed om, at forestillingen om en terroristprofil er ufrugtbar.[351]

Det til trods forsøger forskningen og policy-litteraturen i stedet at profilere 'ekstremisten', hvilket der ifølge Schmid også er mere mening med, da denne øvelse fokuserer på ekstremisternes sprogbrug.[352] Andre vurderer dog modsat Schmid, at forsøget på at tegne online-radikaliseringens fantombillede er lige så frugtesløst.[353] Men for at få netværks- og indholdsanalyserne til at give mening i radikaliseringssammenhæng må radikaliseringsbegrebet nødvendigvis reduceres til et spørgsmål om enkle og målbare faktorer, som kan understøttes af empiri fra internettet. Og ekstremismens kognitive smittefare må derfor antages på forhånd for at kunne sige noget om radikaliseringsfaktoren af bestemte netværk. Analyserne tillader derfor kun ganske bestemte radikaliseringsforståelser at finde anvendelse og operationalisering inden for de nye forebyggelseslogikker.

At betragte radikalisering ud fra en topologi af noder og forbindelser reducerer 'virkeligheden' til et spørgsmål om ganske få elementer i det sociale, og tilgangen overser den sociale kompleksitet, som ligger mellem noderne. Jo mere individer ligner noder, jo lettere er de at forstå og håndtere inden for analysemetodens erkendelseshorisont.

Men de samme radikaliseringsmodeller (der kobler sårbarhed og ideologi) er blinde over for en af kausalmodellernes største metodiske udfordringer: samtidighed af ækvifinalitet (radikalisering til vold kan foregå ad mange forskellige spor) og multifinalitet (to individer, der følger samme spor, ender ikke nødvendigvis med begge at udøve vold).[354] Herudover har modellerne, grundet det ekstensive fokus på sårbarhedsprofilering og ideologi, svært ved at dechifrere ideologiens betydning.

350 Schmid, 2013: 54.

351 Lamberty, 2013: 159; Borum, 2011a: 14; Gartenstein-Ross, 2013; Köhler, 2012: 10.

352 Schmid, 2013: 54.

353 Gartenstein-Ross, 2013.

354 Borum, 2011b: 57.

Ideologiens rolle kan således let blive misforstået og overfortolket. Der er mange veje til radikalisering, som ikke involverer ideologi, og ideologien anvendes ofte som en legitimering af vold frem for at være årsag til vold.[355]

Den manglende konsensus om, og videnskabelige indsigt i, radikaliseringsbegrebets mangefacetterede problemforståelse får således dyb indvirkning på resultaterne af de forskellige data mining-øvelser, da videnskabeligheden og anvendeligheden af de Wiktorowicz-inspirerede radikaliseringsmodeller antages forud for overhovedet at kunne sige noget meningsfuldt om radikalisering via internettet. Oftest bliver disse antagelser kun implicit angivet, og man kan være i tvivl om, hvorvidt forfatterne selv er sig disse antagelser bevidste.

De beregningsmæssige og kvantitative metoder er også blinde over for den magt, som ligger indlejret i kontrollen med netværket. Såvel en række tilfældigheder som bevidste webmasterbeslutninger kan afgøre hvorledes et netværk fremstår i en analyse. Netværksanalysens epistemologi, der erkender virkeligheden som opbygget af noder og forbindelser, muliggør betragtninger af visse sammenhænge – ovenikøbet inden for et kvantificerbart og hyperkomplekst system. Men den samme nodocentristiske epistemologi har også en række blinde vinkler, som den, specielt hvad angår nogle af radikaliseringens kernespørgsmål, ikke har mulighed for at beskrive. Videnskabelige forklaringer baseret på ideen om sociale netværk har således en tendens til at erstatte symbolsk og sproglig rigdom med kausalitet og økonomisk udveksling baseret på interesser.[356] At betragte radikalisering ud fra en topologi af noder og forbindelser reducerer 'virkeligheden' til et spørgsmål om ganske få elementer i det sociale, og tilgangen overser den sociale kompleksitet, som ligger mellem noderne. Jo mere individer ligner noder, jo lettere er de at forstå og håndtere inden for analysemetodens erkendelseshorisont.[357]

Men horisonten begrænses netop af teoriens antagelser. Derfor byder det massive fokus på de sårbare, men rationelle aktører på endnu en metodisk og teoretisk udfordring, når det kommer til studiet af brugerprofiler på sociale medier. Det er meget muligt, at man – til trods for store tekniske vanskeligheder – kan koble flere brugerkonti til unikke personer,[358] men hvordan vurderer man de forskellige personaer (online-identiteter), som et individ leger med?

355 Schmid, 2013: 22.

356 Mejias, 2006.

357 Mejias, 2006.

358 Brynielsson et al., 2012: 202-203.

Netværksanalyserne postulerer at kunne identificere 'individer'. De agentfokuserede analyser antager, at brugerne bag profilerne er rationelle aktører, der handler, som de siger, og siger, som de tænker. Men vejen mellem disse positioner er langt mere kompleks, end analyserne tillader. Identitet og identifikationsprocesser har mange lag.[359] For det første er der alle de politiske såvel som private kontekstuelle faktorer, som ikke kommer med i fortolkningen af ytringer og adfærd på nettet. For det andet lægger analyserne sig op ad illusionen om et 'helt' individ med en klar intention og vilje. Men netop med de radikale identiteter er der et stort element af eksperimenterende og grænsesøgende adfærd involveret. Følelser og fantasier lader sig ikke omsætte til rationelle kalkuler og sammenhængende forklaringer. Brugerprofilernes performative karakter kan ikke uden videre skrives ind i analyseprogrammernes algoritmer. Som Bartlett også påpeger: "In the end, automated systems and online monitoring can only go so far".[360]

Kortlægger netværksanalyserne med andre ord ikke blot forbindelser mellem identiteter, fantasier og normoverskridelser? Og ville de ikke netop her være et meget brugbart værktøj, hvis de kunne løsrive sig fra deres agentsensitivitet?

Det er meget muligt, at netværks- og indholdsanalyser er et godt supplement til mange studier af sociale online-fænomener, også hvad angår studiet af radikalisering og ekstremistiske grupperinger. Men metodernes duperende effekt – med komplekse algoritmer og smarte visualiseringer – må ikke fortrænge en kritisk distance til alle analyser, der mener at kunne reducere følende, sansende og komplekse mennesker til et kommunikativt spil mellem noder og forbindelser. Specielt så uafklaret et fænomen som radikaliseringens individ (subjekt) tåler ikke den slags reduktion, uden at meningen med øvelsen går tabt.

De kvantitative analyser af online-radikalisering illustrerer således faren ved de multidisciplinære og eklektiske tilgange, hvis disciplinernes interne kompleksitet og sammenhæng ikke medinddrages. Det er med andre ord umuligt alene på baggrund af netværket at sige noget om radikaliseringstruslen, og det kræver under alle omstændigheder en grundig kvalitativ vurdering af de mange forskellige informationer. Metoderne kan formodentlig i et begrænset omfang bruges til at identificere visse fremmedkrigere og fremskaffe enkelte beviser for kriminelle gerninger eller kontakter. Men som forebyggelsesværktøj synes meget at tale imod.

359 Papacharissi, 2012.

360 Bartlett, 2015.

Men hvad er egentlig bivirkningerne af en forebyggelsespolitik som denne? Cohen et al. medgiver, at metoderne nok primært er effektive værktøjer i hænderne på efterretningsanalytikere, når de jager terrorister, men at det ellers kan være problematisk i forhold til vore demokratiske frihedsrettigheder at gribe for hårdt ind – man vil komme til at overvåge en masse harmløse civilister.[361] Netop dette bemærker også Inger Marie Sunde fra Politihøgskolen i Oslo. Hun udtaler bekymring over, at mange af de hjemmesider, som bliver kvantificeret, ikke indeholder hadesytringer eller opfordringer til vold og terror, men alene indeholder ideologiske ytringer. Det kan være et problem for ytringsfriheden.[362]

Ligesom hjemmesider og sociale grupper af mere harmløs ideologisk karakter risikerer at blive udsat for forskellige grader af (unødvendig) overvågning og censur, er enkelte forfattere også bekymrede for individernes retsstilling. Scanlon og Gerber fremhæver således en bekymring for, at de omfattende og bredspektrede kvantitative tilgange kan anvendes til at overvåge og klassificere ikkevoldelige individer. I deres perspektiv skal der rettes op på dette gennem klassifikationsmetoder, som udelukkende er målrettede voldelige grupperinger, der sættes i forbindelse med terrorhandlinger.[363]

Sociale problemer kan ikke uden videre reduceres til tekniske problemer. Og, som Morozov også tilføjer, politiksmedene bør undgå alle forsøg på at tage det politiske ud af teknologien. Sociale og politiske problemstillinger kræver sociale og politiske løsninger.

Problemet med denne, som med så mange andre teknologiske løsninger er, at selv dens varmeste tilhængere ikke kender omkostningerne.[364] Når de teknologiske løsninger slår fejl eller synes utilstrækkelige, er tilhængerne hurtige til at foreslå endnu en effektiv teknologisk udbedring. Eksperterne står, med Morozovs ord, klar til at bekæmpe ild med ild.[365] Morozov kommer derfor med denne generelle advarsel:

361 Cohen et al., 2014: 254.
362 Sunde, 2013: 29.
363 Scanlon & Gerber, 2014: 9.
364 Morozov, 2012: 303.
365 Morozov, 2012: 306.

> "Many calls to apply technological fixes to complex social problems smack of the promotion of technology for technology's own sake—a technological fetishism of an extreme variety—which policymakers should resist. Otherwise, they run the risk of prescribing their favorite medicine based only on a few common symptoms, without even bothering to offer a diagnosis. But as it is irresponsible to prescribe cough medicine for someone who has cancer, so it is to apply more technology to social and political problems that are not technological in nature.[366]"

Morozovs kommentar gælder den generelle anvendelse af ny informationsteknologi og internetbaserede løsninger – og i særdeleshed inden for overvågning og registrering. Men netop den afsluttende kommentar synes næsten som skrevet til diskussionen om online-radikalisering. Sociale problemer kan ikke uden videre reduceres til tekniske problemer. Og, som Morozov også tilføjer, politiksmedene bør undgå alle forsøg på at tage det politiske ud af teknologien.[367] Sociale og politiske problemstillinger kræver sociale og politiske løsninger.

Problemet ligger derfor ikke i de enkelte analysemetoder som sådan. Det ligger i de spekulationer, som forskere og policy-skribenter ofte gør sig om radikalisering. Problemets kerne er den til enhver tid nødvendige operationalisering af radikaliseringsmodeller, som ikke har nogen egentlig forklaringskraft eller noget tydeligt og veldokumenteret videnskabeligt fundament. Som internetforskeren Vidar Falkenberg også metaforisk påpeger i en kritisk tekst om netværksanalysens metodiske udfordringer: "A hammer is a great tool when building a house, but is equally suitable for smashing a window or beating someone".[368]

366 Morozov, 2012: 308.

367 Morozov, 2012: 314.

368 Falkenberg, 2012: 20.

Konklusion

RADIKALISERING I EN TID MED 'CYBER HYPE'

Indeværende rapport er den tredje og sidste rapport i en serie om online-radikalisering. Formålet med denne rapport har været at skabe overblik over den spirende forebyggelseslitteratur inden for feltet. Rapporten har søgt at skabe dette overblik ved at undersøge og redegøre for de grundlæggende rationaler bag forestillingerne om forebyggelse af online-radikalisering, samt ved at diskutere disse rationaler op imod den øvrige radikaliseringslitteratur. Rapporten har således været eksplorativ og redegørende med et kritisk teoretisk afsæt.

Det overordnede formål er blevet undersøgt i tre dele. Første del redegjorde for de forskellige eksisterende tilgange til ekstremismen på internettet – fra de 'hårde' sikkerhedsteknologiske løsninger til de 'bløde' modnarrativer. Anden del redegjorde for de beregningsmæssige og kvantitative analyse- og forebyggelsesmetoder ved at fokusere på henholdsvis netværks- og indholdsanalyse. Tredje del diskuterede en række grundantagelser i den gennemgåede litteratur ud fra radikaliseringsteoriernes videnskabsteoretiske kritik af samme.

Rapporten konkluderer, at såvel nye som eksisterende tilgange til forebyggelse af online-radikalisering og lokalisering af de potentielle terrorister via internettet bygger på simple (men uholdbare) radikaliseringsmodeller. For at kunne foretage komplekse beregninger af de massive mængder online-indhold må særligt de kvantitative tilgange derfor ofte tage afsæt i radikaliseringsmodeller, som i store træk allerede er skudt ned af andre grene af radikaliseringslitteraturen.[369]

369 Borum, 2011b: 40; McFarlane, 2010: 4; Köhler, 2012: 11.

I den gennemgåede forebyggelseslitteratur fremstilles ideologien således ofte som en virus, der gennem en kognitiv åbning gør de sårbare unge modtagelige over for accepten af brugen af vold. Desværre definerer metodeudviklere og teoretikere udi online-radikalisering sjældent egne normative, teoretiske og metodiske standpunkter, inden analyserne rulles ud. Herved fortrænges den manglende videnskabelige konsensus om online-litteraturens radikaliseringsforståelse til gengæld for en implicit postuleret videnskabelig objektivitet. Og netop heri ligger en fare for, at litteraturen ender i en alt for kompleksitetsreducerende profileringslogik (forstået som en profilering af den radikaliseringssårbare internetadfærd), der kan virke forlokkende enkel på de politiksmede, som er blevet bedt om at finde på løsninger til forebyggelse af online-radikalisering.

Anvendelsen af simple radikaliseringsforståelser skyldes ikke mindst radikaliseringsbegrebets performative karakter. Begrebet har fra starten været konstrueret og anvendt med det formål at gøre det muligt for embedsværk og forskerkredse at lette problemforståelsen gennem lineære kausalmodeller, der foreskriver og muliggør forskellige løsningsmodeller.[370] De kvantitative tilgange til radikaliseringsproblematikken kan dog sagtens gøre samfundet klogere på karakteren af ekstremistisk online-indhold og forbindelserne mellem bestemte grupper. Men de kan overordnet betragtet ikke anvendes til mere præcist at afgøre, hvem af netværkets individer, der er i risiko for at tage ekstremismen til sit ultimo ratio.

Rapporten kan afslutningsvist kondenseres til tre overordnede hovedpointer eller anbefalinger. For det første synes kortlægningstilgangene i udgangspunktet styret af idéen om, at et overblik over ideologien og dennes organisatoriske eller netværksmæssige forankring vil kunne sige noget om, hvor risikoen for radikalisering og fortætningen af radikaliserende kræfter er størst. Men som denne rapport slår fast, er informationerne for upræcise. Online-radikalisering er et mere alsidigt fænomen, der ikke kan kvantificeres og sættes op i algoritmer, som meget af den gennemgåede forebyggelseslitteratur ellers synes at foreslå.

Specielt i konfrontationen med truslen fra ensomme ulve som Anders Behring Breivik kan det være skæbnesvangert at sætte sin lid til netværksanalyse. Selvom Breivik flere steder bliver fremhævet som den trussel, som en ny og mere intensiv netværksovervågning skal gøre op med, er Breivik måske netop et eksempel på en person, der sandsynligvis ville være gået under algoritmeradaren eller i det mindste ikke ville blive erkendt som nogen alvorlig trussel. Breivik var således ikke atypisk

370 Nouri & Whiting, 2015: 179.

ekstrem i sine holdninger (han var nationalkonservativ), og han diskuterede ikke direkte sine terrorplaner med andre på nettet.[371] Men er Breivik blot en klassisk outlier – en undtagelse der bekræfter reglen. Eller er han et klassisk eksempel på, hvordan vi forblændes, hvis vi blot forledes til at sætte den mest ekstreme handling i forbindelse med den mest ekstreme tænkning? Det finder vi muligvis aldrig noget entydigt svar på. Men så længe tvivlen er så stor, skal vi passe på ikke at forsimple og overfortolke ideologiens betydning.

Netop derfor er der, for det andet, behov for at bryde med de seneste års cyber hype på forebyggelsesområdet. Hussain og Saltman konkluderer selv, at langt størstedelen af individerne introduceres til den ekstremistiske ideologi gennem offline-socialisering.[372] Det er med andre ord uklart, hvilken betydning internettet har for radikalisering som sådan, og der mangler endnu videnskabelig empirisk belæg til at understøtte en påstand om internettets radikaliseringseffekt.[373] Internettet bør følgelig i stedet medregnes som en af mange understøttende faktorer (i den ideologiske radikalisering), der muligvis kan forstærke de processer, som allerede finder sted i den fysiske virkelighed.[374] Og netop derfor bør online-radikalisering ikke betragtes som et særskilt fænomen, der skal løses gennem særskilte indsatser. Alt andet lige skal online-radikalisering behandles og forebygges på samme vis som voldelig ekstremisme og radikalisering i almindelighed.

Det er, for det tredje, et problem, at meget af litteraturen og politikken på området reproducerer stereotype forestillinger om radikaliserede unge normalitetsafvigere og samtidig undlader at forholde sig til de mange videnskabelige og etiske spørgsmål, som problemet tager afsæt i. Rapporten opfordrer derfor til mere forskning på området samt en mådeholden forebyggelsespolitik, der ikke lader sig besnære af det hurtige teknologiske fix. Den videnskabelige litteratur om forebyggelsesmetodernes effekt og brug er endnu aldeles underudforsket.[375] Vi ved, med andre ord, ingenting om, hvad der virker.[376] Og uden de rette forbehold kan 'automatisk sporing' af radikaliseringstruede sårbare unge blive et politisk vildspor, der ikke alene risikerer at indsnævre ytringsfriheden og det demokratiske rum, men som også i illusorisk forvildelse mener at kunne spotte en alarmerende og spirende terrorisme, hvor der i grunden ikke er andet end en ideologisk inspireret sub- og modkultur.

371 Ravndal, 2013: 173.
372 Hussain & Saltman, 2014: 7.
373 Lennings et al., 2010: 435; Difraoui, 2012: 72.
374 Pisoiu, 2013: 75.
375 Aly, 2014: 64.
376 Schmid, 2013: 50.

Diskussionen om online-radikalisering kan således, som rapportens tredje del understreger, ikke føres uafhængigt af en diskussion om en dybere forståelse af radikaliseringsbegrebet. Som Pia Lamberty også påpeger, afspejler problemet med at definere radikaliseringsbegrebet sig direkte i operationaliseringen.[377] Således også for online-radikalisering og den hastigt voksende forebyggelseslitteratur.

Samtidig er diskussionen, om radikalisering overhovedet findes dog også et overstået kapitel. Som Heath-Kelly påpeger, har forskning, medier og stat for længst diskursivt slået fast, at radikalisering altid går forud for vold.[378] Tilbage står altså at forankre begrebet og fænomenet i de forskellige videnskabelige traditioner ud fra en kritisk gennemgang af den eksisterende forskningslitteratur og politik. Og ud fra nye empirisk baserede studier. Men den manglende klarhed og konsensus om problematikkens hovedbegreber – radikalisering, ekstremisme, terrorisme, foreign fighter, etc. – er stadig en stor hindring for en mere præcis og nuanceret problemforståelse, der kan føre til bedre forskning og forbedrede politikker på området.[379]

377 Lamberty, 2013: 142.

378 Heath-Kelly et al., 2015: 1.

379 Schmid, 2013: iv.

Litteraturliste

Alan & Barbara Finlay (1997): **Statistical Methods for the Social Sciences**, New Jersey: Prentice-Hall, Inc.

Aly, Anne (2014): "Walk Away from Violent Extremism: a campaign to address violent extremism online", **Journal EXIT-Deutschland**, Zeitschrift für Deradikalisierung und demokratische Kultur, 4, s. 64-77

Archetti, Christina (2015): "Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age", **Perspectives on Terrorism**, 9:1, s. 49-59

Awan, Akil N. (2007): "Virtual jihadist media: Function, legitimacy and radicalizing efficacy", **European Journal of Cultural Studies**, 10:3, s. 389-408.

Bartlett, Jamie (2015): "Algorithms and computers won't stop terrorism", **The Telegraph**, 24. Februar 2015, (http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11431757/Algorithms-and-computers-wont-stop-terrorism.html) [13. marts 2015]

Behr, Ines von, Anaïs Reding, Charlie Edwards, Luke Gribbon (2013): **Radicalisation in the digital era – The use of the internet in 15 cases of terrorism and extremism**, RAND Europe, http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf [13. marts 2015]

Berger, J.M. & Bill Strathearn (2013): **Who Matters Online: Measuring influence, evaluating content and countering violent extremism in online social networks**, the International Centre for the Study of Radicalisation and Political Violence (ICSR). (http://icsr.info/wp-content/uploads/2013/03/ICSR_Berger-and-Strathearn.pdf) [13. marts 2015]

Bermingham, Adam, Maura Conway, Lisa McInerney, Neil O'Hare, Alan F. Smeaton (2009): **Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation**, Conference paper, In ASONAM 2009 – Advances in Social Networks Analysis and Mining, 20-22 July, 2009, Athens, Greece, (http://doras.dcu.ie/4554/3/DCU_asonam09.pdf) [13. marts 2015]

Bhui, Kamaldeep & Yasmin Ibrahim (2013): "Marketing the 'radical': Symbolic communication and persuasive technologies in jihadist websites", **Transcultural Psychiatry**, 50:2, s. 216-234.

Bitso, Contance, Ina Fourie and Theo J. D. Bothma (2013): "Trends in transition from classical censorship to Internet censorship: selected country overview", **Innovation**, 48, s. 166-191

Borum, Randy (2011a): "Radicalization into Violent Extremism I: A Review of Social Science Theories", **Journal of Strategic Security**, 4:4, Henley-Putnam University Press, s. 7-36.

Borum, Randy (2011b): "Radicalization into Violent Extremism II: A Review of Conceptual Models and Empirical Research", **Journal of Strategic Security**, 4:4, Henley-Putnam University Press, s. 36-62.

Briggs, Rachel & Sebatien Feve (2014): **Inspire, Radicalise, Recruit: Countering the Appeal of Extremism Online**, Institute for Strategic Dialogue, Policy Briefing, (http://www.strategicdialogue.org/Inspire_Radicalize_Recruit.pdf) [13. marts 2015]

Brynielsson, Joel, Andreas Horndahl, Frederik Johansson, Lisa Kaati, Christian Mårtenson and Pontus Svenson (2012): "Analysis of Weak Signals for Detecting Lone Wolf Terrorists", **European Intelligence and Security** Informatics Conference, s. 197-204

Busch, Christoph (2008): "Rechtsradikale im Web 2.0 – "…take up positions on 'Mainstream' groups"", (https://www.lmz-bw.de/fileadmin/user_upload/Medienbildung_MCO/fileadmin/bibliothek/busch_rechtsradikale/busch_rechtsradikale.pdf) [13. marts 2015]

Caiani, Manuela & Claudius Wagemann (2009): "Online networks of the Italian and German extreme right", **Information, Communication & Society**, 12:1, s. 66-109.

Carter, Joseph A., Shiraz Maher, Peter R. Neumann (2014): **#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighters Networks**, The International Center for the Study of Radicalisation and Political Violence, (http://icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Infleunce-in-Syrian-Foreign-Fighter-Networks.pdf) [13. marts 2015]

Cioffi-Revilla, Claudio (2010): "Computational Social Science", **WIREs Computational Statistics**, 2, s. 259-271

Cohen, Katie, Frederik Johansson, Lisa Kaati & Jonas Clausen Mork (2014): "Detecting Linguistic Markers for Radical Violence in Social Media", **Terrorism and Political Violence**, 26:1, s. 246-256.

Cole, Jon, Emily Alison, Ben Cole & Laurance Alison (2012): **Guidance for Identifying People Vulnerable to Recruitment into Violent Extremism**, Institute for Strategic Dialogue, (https://www.counterextremism.org/resources/details/goto_url/224/3343) [13. marts 2015]

Correa, Denzil & Ashish Sureka (2013): **Solutions to Detect and Analyze Online Radicalization**: A Survey. (http://arxiv.org/pdf/1301.4916) [13. marts 2015]

COWI (2014): **Evaluering af indsatsen for at forebygge ekstremisme og radikalisering**, COWI-rapport på vegne af Social-, Børne- og Integrationsministeriet, (http://sm.dk/filer/arbejdsomrader/forebyggelse-af-radikalisering-og-ekstremisme/evaluering-af-indsatsen-for-at-forebygge-ekstremisme-og-radikalisering.pdf) [13. marts 2015]

Crone, Manni (2010): **Dynamikker i ekstremistiske miljøer**, DIIS Working Paper, 2010:24

Deibert, Ronald, John Palfrey, Rafal Rohozinski & Jonathan Zittrain (2010): **Access Controlled – The Shaping of Power, Rights, and Rule in Cyberspace**, London: The MIT Press

Dienstbühl, Dorothee & Meike Weber (2014): „Rekrutierung im Cyberspace – wie Extremisten das Internet nutzen", **Journal EXIT-Deutschland. Zeitschrift für Deradikalisierung und demokratische Kultur**, 2:2014, s. 35-45

Difraoui, Asiem El (2012): "Web 2.0 – mit einem Klick im Medienjihad", i Guido Steinberg (red.): **Jihadismus und Internet: Eine deutsche Perspektive**, Berlin: Stiftung Wissenschaft und Politik, s. 67-75.

Edwards, Charlie & Luke Gribbon (2013): "Pathways to Violent Extremism in the Digital Era", The RUSI Journal, 158:5, London: Routledge, s. 40-47.

Embedsmandsrapporten (2008): **En fælles og tryg fremtid – forslag til en handlingsplan om forebyggelse af ekstremistiske holdninger og radikalisering blandt unge**, embedsmandsudvalg under Ministeriet for Flygtninge, Indvandrere og Integration

Falkenberg, Vidar (2012): "We have the data – what do you want to know?", s. 9-23, i Stine Lomborg (red.) **Network Analysis**: Methodological Challenges. Aarhus: The Centre for Internet Research

Frome, Andrea, Greg S. Corrado, Jonathon Shlens, Samy Bengio, Jeffrey Dean, Marc' Aurelio Ranzato, Thomas Mikolov (2013): **DeViSE: A Deep Visual-Semantic Embedding Model**, (http://machinelearning.wustl.edu/mlpapers/paper_files/NIPS2013_5204.pdf) [13. marts 2015]

Gartenstein-Ross, Daveed (2013): "Online Radicalization to Violence", Interview with Daveed Gartenstein-Ross by Maria Prosviryakova, (http://russiancouncil.ru/en/inner/?id_4=1967#top) [13. marts 2015]¨

Gemmerli, Tobias (2014a): "Onlineradikalisering: et uafklaret begreb – litteraturreview af definitioner og tilgange inden for onlineradikalisering (del 1 af 3)", **DIIS Report 2014:07.**

Gemmerli, Tobias (2014b): "Onlineradikalisering: en rundrejse i forskningslitteraturen – litteraturreview af definitioner og tilgange inden for onlineradikalisering (del 2 af 3)", **DIIS Report 2014:08.**

Githens-Mazer, Jonathan & Robert Lambert (2010): "Why conventional wisdom on radicalization fails: the persistence of a failed discourse", **International Affairs**, 86:4, s. 889-901

Gjerding, Sebatian, Henrik Moltke, Anton Geist & Laura Poitras (2014, 17. juni): "Snowden-dokumenter afslører dansk partnerskab med NSA", **Information**, (http://www.information.dk/501256) [13. marts 2015]

Gloor, Peter A., Jonas Krauss, Stefan Nann, Kai Fischbach, Detlef Schoder (2009): "Web Science 2.0: Identifying Trends through Semantic Social Network Analysis", **Computational Science and Engineering,** 2009, MIT: Institute of Electrical and Electronics Engineers, s. 215-222

Halverson, Jeffry R. & Amy K. Way (2012): "The curious case of Colleen LaRose: Social margins, new media, and online radicalization", **Media, War & Conflict**, 5:2, s. 139-153.

Heath-Kelly, Charlotte, Christopher Baker-Beall & Lee Jarvis (2015): "Introduction", pp. 1-13 **in Counter-Radicalisation – Critical perspectives**, Christopher Baker-Beall, Charlotte Heath-Kelly and Lee Jarvis (eds.), London: Routledge

Helfstein, Scott (2012): **Edges of Radicalization: Individuals, Networks and Ideas in Violent Extremism**, Westpoint: Combating Terrorism Center. (http://www.ctc.usma.edu/wp-content/uploads/2012/06/CTC_EdgesofRadicalization.pdf) [13. marts 2015]

Holbrook, Donald, Gilbert Ramsay & Max Taylor (2013): "'Terroristic Content': Towards a Grading Scale", **Terrorism and Political Violence**, 25:2, s. 202-223.

Hussain, Ghaffar & Erin Marie Saltman (2014): **Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it,** Quilliam Foundation, (http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/jihad-trending-quilliam-report.pdf) [13. marts 2015]

IHS (2013): **Analysis: Internet forums, social media and militant Islamism**, (https://justplainbill.wordpress.com/2014/01/22/janes-intel-internet-forums-jihadi-22-jan-14/) [13. marts 2015]

Jacobsen, Jeppe Teglskov (2014): "Kampen for en klar sondring i cyberspace", **DIIS Report 2014:09**.

Kapathy, Andrej, Li Fei-Fei (2014): **Deep Visual-Semantic Alignment for Generating Image Descriptions**, (http://cs.stanford.edu/people/karpathy/deepimagesent/devisagen.pdf) [13. marts 2015]

Kaschesky, Michael, Pawel Sobkowicz & Guillaume Bouchard (2012): "Opinion Mining in Social Media: Modeling, Simulating, and Visualizing Political Opinion Formation in the Web", **Government Information Quarterly**, 29:7, s. 470-479.

Katz, Rita (2014): "The State Department's Twitter War With ISIS is Embarrassing", **Time**, (http://time.com/3387065/isis-twitter-war-state-department/) [13. marts 2015]

Kenney, Michael (2010): "Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists", **Terrorism and Political Violence**, 22:2, s. 177-197.

Klausen, Jytte (2014): "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq", **Studies in Conflict & Terrorism**, DOI: (http://dx.doi.org/10.1080/1057610X.2014.974948) [13. marts 2015]

Köhler, Daniel (2012): "Internet and Radicalization – Connecting the Dots – the Role of the Internet in the Individual Radicalization Processes of Right-Wing Extremists", **ISRM Working Paper**, 01:12, Institute for the Study of Radical Movements.

Kundnani, Arun (2014): **The Muslims are Coming**, London: Verso

Kundnani, Arun (2015): "Radicalisation – The journey of a concept", pp. 14-35 **in Counter-Radicalisation – Critical perspectives**, Christopher Baker-Beall, Charlotte Heath-Kelly and Lee Jarvis (eds.), London: Routledge

Laclau, Ernesto & Chantal Mouffe (2001 [1985]): **Hegemony and Socialist Strategy – Towards a Radical Democratic Politics**, London: Verso

Lamberty, Pia (2013): "Methodologische Schwierigkeiten und Herausforderungen einer quantitativen Radikalisierungsforschung am Beispiel des Rechtextremismus. Ein Über- und Ausblick", **Journal EXIT-Deutschland**, Zeitschrift für Deradikalisierung und demokratische Kultur, 3, s. 115-181

Lennings, Christopher J., Krestina L. Amon, Heidi Brummert & Nicholas J. Lennings (2010): "Grooming for Terror: The Internet and Young People", **Psychiatry, Psychology and Law**, 17:3, s. 424-437.

Lomborg, Stine (2012): "Preface: Network analysis – methodological challenges", pp. 6-8, in Stine Lomborg (ed.) **Network Analysis: Methodological Challenges**. Aarhus: The Centre for Internet Research

Lucas, Brian (2014): "Methods for monitoring and mapping online hate speech", (http://www.gsdrc.org/docs/open/HDQ1121.pdf) [13. marts 2015]

Markham, Annette N. (2012): "Moving into the flow: Using a network perspective to explore complexity in the internet contexts", pp. 47-58, in Stine Lomborg (ed.) **Network Analysis: Methodological Challenges**. Aarhus: The Centre for Internet Research

McFarlane, Bruce (2010): **Online Violent Radicalisation (OVeR): Challenges facing Law Enforcement Agencies and Policy Stakeholders**. (http://artsonline.monash.edu.au/radicalisation/files/2013/03/conference-2010-online-violent-radicalisation-bm.pdf) [13. marts 2015]

Medina, Richard M. & George F. Hepner (2011): "Advancing the Understanding of Sociospatial Dependencies in Terrorist Networks", **Transactions in GIS**, 15:5, s. 577-597

Mejias, Ulises A. (2006): "The tyranny of nodes: Towards a critique of social network theories", (http://blog.ulisesmejias.com/2006/10/09/the-tyranny-of-nodes-towards-a-critique-of-social-network-theories/) [13. marts 2015]

Mellis, Colin (2007): "Amsterdam and Radicalisation: The Municipal Approach", pp. 40-48, in **Radicalisation in broader perspective**, http://www.google.dk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CE0QFjAA&url=http%3A%2F%2Fenglish.nctb.nl%2FImages%2FCongresbundel%2520UK%2520compleet_tcm92-132318.pdf&ei=sIn9T4znG8TT4QSmqODFBg&usg=AFQjCNEx8cTPGLDpRXhGSZzqJFGiL8c2DQ [13. marts 2015]

Meloy, Reid, Jens Hoffmann, Angela Guldimann & David James (2011): "The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology", **Behavioral Science and the Law,** (http://onlinelibrary.wiley.com/doi/10.1002/bsl.999/epdf) [13. marts 2015]

Merkl, Peter H (1986). "Approaches to the Study of Political Violence", pp. 19-58, in Peter H. Merkl (ed.) **Political Violence and Terror**. Motifs and Motivations, Berkley: University of California Press

Morozov, Evgeny (2012): **The Net Delusion – How not to liberate the world**, London: Penguin Books

Morozov, Evgeny (2014a): "The rise of data and the death of politics", The Observer, (http://www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics-evgeny-morozov-algorithmic-regulation) [13. marts 2015]

Morozov, Evgeny (2014b): **Technology, solutionism and the urge to fix problems that don't exist**, London: Penguin Books

Neumann, Peter (2013): "Options and Strategies for Countering Online Radicalization in the United States", **Studies in Conflict & Terrorism**, 36:6, s. 431-459.

Nouri, Lella & Andrew Whiting (2015): "Prevent and the internet", pp. 175-189 **in Counter-Radicalisation – Critical perspectives**, Christopher Baker-Beall, Charlotte Heath-Kelly and Lee Jarvis (eds.), London: Routledge

Papacharissi, Zizi (2012): "Without You, I'm Nothing: Performance of the Self on Twitter", **International Journal of Communication**, 6, s. 1989-2006

Pariser, Eli (2011): **The Filter Bubble – What the Internet Is Hiding from You**, New York: The Penguin Press

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

Poell, Thomas (2014): "Social Media Activism and State Censorship", **Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in an Age of Facebook, Twitter and YouTube**, by D. Trottier & C. Fuchs (eds.). s. 189-206. London: Routledge

PPN – Policy Planners' Network / Institute for Strategic Dialogue (2011): **Radicalization: The Role of the Internet**, A Working Paper of the PPN. (https://www.counterextremism.org/download_file/11/134/11/) [13. marts 2015]

Prentice, Sheryl, Paul J. Taylor, Paul Rayson, Andrew Hoskins & Ben O'Loughlin (2010): "Analyzing the semantic content and persuasive composition of extremist media: A case study of texts produced during the Gaza conflict", **Information Systems Frontiers**, 13:1, s. 61-73.

Quiggin, Tom (2009): "Understanding al-Qaeda's Ideology for Counter-Narrative Work", **Perspectives on Terrorism**, 3:2, s. 18-24

Ramalingam, Vidhya (2014): **Responding to Hate Speech and Incitement**. Insitute for Strategic Dialogue. (http://www.strategicdialogue.org/2_Responding_to_hate_speech.pdf) [13. marts 2015]

Ravndal, Jacob Aasland (2013): "Anders Behring Breivik's use of the Internet and social media", **Journal EXIT-Deutschland, Zeitschrift für Deradikalisierung und demokratische Kultur** 2, s. 172-185.

Regeringen (2009): **En fælles og tryg fremtid – Handlingsplan om forebyggelse af ekstremistiske holdninger og radikalisering blandt unge**, Købehavn: Socialministeriet

Regeringen (2014): **Forebyggelse af radikalisering og ekstremisme – Regeringens hanglinsplan**. (http://sm.dk/filer/nyheder/handlingsplan-om-forebyggelse-af-radikalisering-og-ekstremisme-tilgaengelig.pdf) [13. marts 2015]

Ressler, Steve (2006): "Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research", **Homeland Security Affairs**, (file:///C:/Users/toge/Downloads/2.2.8.pdf) [13. marts 2015]

Rieger, Diana, Lena Frischlich & Gary Bente (2013): **Propaganda 2.0 – Psychological Effects of Right-Wing and Islamic Extremist Internet Videos**, Köln: Luchterhand Verlag.

Royal Canadian Mounted Police (2011): **Youth Online and at Risk: Radicalization Facilitated by the Internet**. (http://www.rcmp-grc.gc.ca/nsci-ecsn/rad/youth-jeune-eng.pdf) [13. marts 2015]

Ryan, Johnny (2007): "The Internet, the Perpetual Beta, and the State: The Long View of the New Medium", **Studies in Conflict & Terrorism**, 33:8, s. 673-681

Salem, Arab, Edna Reid & Hsinchun Chen (2008): "Multimedia Content Coding and Analysis: Unraveling the Content of Jihadi Extremist Groups' Videos", **Studies in Conflict and Terrorism**, 31:7, s. 605-626

Saltman, Erin Marie & Jonathan Russell (2014): "White Paper – The Role of Prevent in Countering Online Extremism", Quilliam Foundation, (http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/white-paper-the-role-of-prevent-in-countering-online-extremism.pdf) [13. marts 2015]

Scanlon, Jacob R & Matthew S Gerber (2014): "Automatic detection of cyber-recruitment by violent extremists", **Security Informatics**, 3:5 (http://link.springer.com/article/10.1186%2Fs13388-014-0005-5#page-1) [13. marts 2015]

Schmid, Alex P. (2013): **Radicalisation, De-Radicalisation, Counter-Radicalisation**: A Conceptual Discussion and Litterature Review, ICCT Research Paper, Haag: International Centre for Counter-Terrorism. (http://www.icct.nl/download/file/ICCT-Schmid-Radicalisation-De-Radicalisation-Counter-Radicalisation-March-2013.pdf) [13. marts 2015]

Schmid, Alex P. & Eric Price (2011): "Selected literature on radicalization and de-radicalization of terrorists: Monographs, Edited Volumes, Grey Literature and Prime Articles published since the 1960s", **Crime, Law and Social Change**, 55, s. 337-348

Silke, Andrew (2008): "Holy Warriors: Exploring the Psychological Processes of Jihadi Radicalization", **European Journal of Criminology**, 5:1

Sivek, Susan Currie (2013): "Packaging Inspiration: Al Qaeda's Digital Magazine Inspire in the Self-Radicalization Process", International Journal of Communication 7, s. 584-606.

Snow, David A. & Robert D. Benford (1988): "Ideology, Frame Resonance, and Participant Mobilization", **International Social Movement Research**, 1, s. 197-217

Steinberg, Guido (2012): "Jihadismus und Internet. Eine Einführung", i Guido Steinberg (red.), **Jihadismus und Internet – Eine deutsche Perspektive**, Berlin: Stiftung Wissenschaft und Politik, s. 7-22.

Stenersen, Anne (2008): "The Internet: A Virtual Training Camp?", **Terrorism and Political Violence**, 20:2, s. 215-233.

Stevens, Tim & Peter R. Neumann (2009): **Countering Online Radicalisation – A Strategy for Action, A policy report published by the International Centre for the Study of Radicalisation and Political Violence** (ICSR). (http://icsr.info/wp-content/uploads/2012/10/1236768491ICSROnlineRadicalisationReport.pdf) [13. marts 2015]

Stormhøj, Christel (2010): Poststrukturalismer – **Videnskabsteori, Analysestrategi, Kritik**, Frederiksberg: Forlaget Samfundslitteratur

Sunde, Inger Marie (2013): "Del II – Forebygging av nettekstremisme i et politiperspektiv", i Inger Marie Sunde (red.): **Forebygging av radikalisering og voldelig ekstremisme på internett**, Oslo: Politihøgskolen.

Torok, Robyn (2013): "Developing an explanatory model for the process of online radicalisation and terrorism", **Security Informatics**, 2:6. (http://www.security-informatics.com/content/2/1/6) [13. marts 2015]

Torres-Soriano, Manuel R. (2014): "The Hidden Face of Jihadist Internet Forum Management: The Case of Ansar Al Mujahideen", **Terrorism and Political Violence**, http://www.tandfonline.com/doi/pdf/10.1080/09546553.2014.950419 [13. marts 2015]

Venhaus, John M. (2010): **Why Youth Join al-Qaeda**, United States Institute of Peace – Special Report, http://www.usip.org/sites/default/files/SR236Venhaus.pdf [13. marts 2015]

Weimann, Gabriel (2004): **www.terror.net: How Modern Terrorism Uses the Internet, United States Institute of Peace**. (http://www.usip.org/sites/default/files/sr116.pdf) [13. marts 2015]

Weimann, Gabriel (2008): "The Psychology of Mass-Mediated Terrorism", **American Behavioral Scientist** 52, s. 69-86.

Weimann, Gabriel (2011): "Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking", paper submitted to the Israeli Communication Association. (http://cleanitproject.eu/files/95.211.138.23/wp-content/uploads/2012/08/2012-Terrorists-using-online-social-nerworking.pdf) [13. marts 2015]

Weimann, Gabriel (2012): "Lone Wolves in Cyberspace", **Journal of Terrorism Research**, 3:2, s. 75-90.

Wiktorowicz, Quintan (2005): **Radical Islam Rising – Muslim Extremism in the West**, Oxford: Rowman & Littlefield Publishers

Zelin, Aaron Y. (2013): **The State of Global Jihad Online – A Qualitative, Quantitative, and Cross-Lingual Analysis**, New America Foundation. (http://www.washingtoninstitute.org/uploads/Documents/opeds/Zelin20130201-NewAmericaFoundation.pdf) [13. marts 2015]

LITTERATUR-REVIEW AF DEFINITIONER OG TILGANGE INDEN FOR ONLINE-RADIKALISERING (DEL 3 AF 3):

Denne rapport er tredje rapport i et litteraturstudie af definitioner og tilgange inden for online-radikalisering. De to forudgående rapporter beskæftiger sig med begrebs- og fænomenforståelsen mere generelt.

Den første rapport, **Online-radikalisering: et uafklaret begreb (DIIS Report 2014:07)**, peger bl.a. på, at radikaliseringsbegrebet i litteraturen om online-radikalisering ofte beskrives implicit og med afsæt i en række forsimplede modelantagelser, som mange radikaliseringsforskere allerede har bevæget sig væk fra. Litteraturen om online-radikalisering ender derfor ofte i tendentiøse trusselsbeskrivelser og uvidenskabelige cirkelslutninger.

Den anden rapport, **Online-radikalisering: en rundrejse i forskningslitteraturen (DIIS Report 2014:08)**, finder bl.a. et sammenfald mellem trusselsbeskrivelsen og de anvendte radikaliseringsmodellers syn på individet. Jo mere radikaliseringsmodellerne således vægter kognitive og ideologiske aspekter i radikaliseringen, jo større bliver interessen for det ekstremistiske online-indhold, og jo højere ender trusselsniveauet også med at være.

Rapporterne er tilgængelige på DIIS' hjemmeside.

DIIS · DANSK INSTITUT FOR INTERNATIONALE STUDIER
Østbanegade 117 | 2100 København Ø | www.diis.dk