JOURNAL FOR DERADICALIZATION

Spring 2018
Nr. 14
ISSN: 2363-9849

‘Sometimes you just have to try something’ - A critical analysis of Danish state-led initiatives countering online radicalisation

Anna Warrington[a1]
[a]Academic Coordination Officer, University of Copenhagen

Abstract
This research paper argues that Danish online radicalisation policies are driven by logics of urgency (the threat is imminent) within a limited realm of discursive possibilities (the threat is securitised) which blur the lines between state and civil society as well as state and private sector interactions. Potential political implications bring into play questions about the democratic values that are perceived as safeguarded by these policies. The Danish case shows that we (as citizens, policy makers and researchers) must engage in further discussions on dynamics between the current threat perception of online radicalisation and policies addressing such a threat. My argument is constructed from a discourse analysis of official documents as of 2016-2017 on countering and preventing violent extremism and an analysis of the political logics driving a state-level conceptualisation of online radicalisation through interviews with government officials. The two-part analysis is theoretically based on Securitisation from the Copenhagen School in combination with Critical Terrorism Studies to create a critically inspired approach that remains within existing structures of Danish politics. This is done to engage with the current political landscape characterised by a securitisation of specific forms of online content associated with the Islamic State as an Other. Online radicalisation is herein constructed as a multidimensional threat towards a societal Self referring to the physical safety of citizens and a value based ‘way of life’. The decentralised structure of the internet allows communication flows that enable radicalisation to be understood as an inter-sectoral threat where multiple elements of the referent object are threatened simultaneously. This threat perception challenges government officials in developing and implementing policies to address the threat of the Other while safeguarding the democratic values of the Danish Self.

Article History
Received Oct 13, 2017
Accepted Feb 28, 2018
Published Mar 30, 2018

Keywords: Online Radicalisation, Countering Violent Extremism, CVE, Terrorism, Critical Terrorism Studies

Introduction: The new battlefield is online

The internet is increasingly becoming a part of terrorism studies and of counter-terrorism policies. Researchers from the International Centre for the study of Violent Extremism argue

[1] Corresponding Author Contact: Anna Warrington, Email: anna-warrington@hotmail.com University of Copenhagen Faculty of Social Sciences, Øster Farimagsgade 5, 1353 Copenhagen K. LinkedIn: https://www.linkedin.com/in/anna-warrington/

that the future 'war on terror' will be situated less in the physical realm and increasingly become a battle in the digital sphere (Lorrand Bodo and Speckhart 2017: 1). The Islamic State (IS) has firmly placed online counter-terrorism on the political agenda in Denmark. Yearly action plans have been launched since the emergence of the self-proclaimed caliphate in June 2014. The most recent National Action Plan (NAP) was launched in October 2016 (Byman 2016; Ministry of Justice 2016).

I argue that studies of radicalisation-drivers and how IS uses digital technologies are covered relatively well in academia as shown in the literature review below. Yet not much research has been done on potential political implications of state-led initiatives online– at least not in Denmark. This has led to my research on how online radicalisation is conceptualised and what political logics drive state-led initiates aimed at countering a threat from IS online as well as which political implications can arise from these dynamics.

My focus is limited to Denmark where the state, I argue, is the most significant actor in discursively constructing a threat towards the Danish society by having the legitimate authority to formulate and enact policies (Buzan et al. 1998: 123). Therefore, the Danish state is the main actor of my analysis. To conduct the analysis on a more specific level, I examine state-led initiatives aimed at online radicalisation from the 2016 NAP on countering and preventing violent extremism. I explore the conceptualisation of online radicalisation as a threat to society understood as the physical safety of citizens and a value based 'way of life' in the context of IS. The analysis is based on official documents and qualitative interviews with governmental officials to discuss potential political implications of logics driving these policies. I do not conclude whether policies 'work' as an objective truth nor do I define concrete impact as this is not within the ontological or epistemological realm of my research. Instead, I analyse a state-level understanding of online radicalisation and the political realm of possibilities enabled through discursive logics of this threat perception. I argue, securitisation has left little room for debate as a threat from online radicalisation is constructed as part of a broader discourse on terrorism.

All interviews were conducted as part of my thesis in the summer of 2017. While conducting my research, I met highly professional government officials and civil service actors who navigate in a challenging political landscape (read more in the section on 'ethical considerations'). Thus, my analysis does not imply critical aspects at an individual level. My objective is to analyse a discursive state-level understanding of online radicalisation and the policies developed to address this threat. My findings aim at being a conversation starter on why and how online policies are developed to address this threat perception.

Literature review and (Western) policy responses to online radicalisation

The field of counter-terrorism research entails, among others, studies on Countering Violent Extremism (CVE) and radicalisation as a political and social concept (Richards 2015; Eroukhmanoff 2015; Dalgaard-Nielsen 2013). While Dutch scholar Schmid (2013) focuses on a conceptual analysis of meanings assigned to radicalisation and de-radicalisation, other recent academic studies analyse the efficiency of CVE policies such as U.S based researcher Romaniuk (2015). By analysing lessons learned from the implementation of CVE policies, he argues that practitioners from governments and NGOs 'should integrate past lessons into current and future programming' for these policies to be effective. His study constructs a typology of CVE policies differentiating target audiences, implementing agents and activities (Romaniuk 2015: 10f). To ensure cohesion and clarity in CVE research, he recommends focusing on evaluations (Ibid. 39).

Other studies focus on the Islamic State (IS) and their strategic use of digital media. Lakomy (2017) explores the coverage, quality and effectiveness of 'cyber jihad' through qualitative and quantitative analyses. While Lakomy discusses broad digital strategies, Klausen (2015) analyses the spread of IS content on Twitter. His study argues that social media increases the reach IS communication and is an effective recruitment tool (Klausen 2015: 19). Some researchers mainly analyse how IS utilises online communication (Friis 2015) and others focus on those engaging with such content (Koehler 2014).

Research on governmental campaigns aimed at countering a threat from violent extremism online include, amongst others, Ashour (2011: 17f) who argues that constructing counter-narratives are a global task where lessons from other countries should be the basis for developing online narratives. Greenberg (2016: 170f) underscores the importance of state-led online policies to note how the internet is used by those whose messages they are trying to counter. She also outlines the necessity for further considerations into how internet companies can work with governments using the U.S government as an example (ibid.).

Defining radicalisation remains a contested concept in academia (Dalgaard-Nielsen 2010; Eroukhmanoff 2015; Meleagrou-Hitchens and Kaderbhai 2017: 14). Nevertheless, there appears to be a common notion of radicalisation as a process towards views perceived as extreme by an established society, which can legitimise violence (Davies et al. 2016: 52; Dalgaard-Nielsen 2010: 798; Muro 2016: 3; Horgan and Braddock 2010: 279). Studies on drivers of (offline and online) radicalisation explore political, societal, psychological and historical aspects and include Sheik (2016) who notes socio-economic push factors while highlighting the meaning assigned to pull factors in joining groups in Syria and Iraq. Crone (2016) argues that most studies overemphasise ideology and discusses radicalisation as constructed with not only ideological or religious but also political, societal and bodily aspects (Crone 2016: 588). Her research also explores dynamics of extremist milieus and gangs as preconditions for political violence (Crone 2016: 598). A recent U.S study compares gang members and domestic extremists finding the groups vastly different with commonalities such as seeking like-minded communities (Lafree 2017: 2). Other studies include Torok (2013: 2f) who develops an explanatory grounded theory model of cyclic development through networks of power and knowledge and Koehler (2014: 120ff) analysing individual radicalisation processes and the role of the internet in such processes.

I delimit my focus to a Western securitised discourse while I acknowledge that terrorism is not a Western phenomenon and that Western policies and academic research are not an objective 'truth' nor the only lenses for research. Western policies on CVE and Preventing Violent Extremism (PVE) increasingly include the internet. Online policies

include, amongst others, removal of online content (Meleagrou-Hitchens and Kaderbhai 2017: 54) and engagement with users on social media (Aistrope 2016a: 130).

Davies et al. (2016: 78f) argue that most counter-terrorism policies do not address key elements of radicalisation such as contextual factors or identity aspects. The study recommends that policy makers consider local contexts for how policies are perceived by target audiences. This argument is a common critique of such policies. Talbot (2015) argues that state-led initiatives lack dialogue with audiences. Others argue that state actors lack knowledge about radicalisation processes locally (Hemmingsen and Castro 2017: 31f; Gemmerli 2016: 2). A similar argument is presented Aistrope (2016b: 134f) noting a deficit of legitimacy in US counter-terrorism by discussing underlying ideologies driving online policies where he argues that a 'Muslim paranoia' has impacted policies and how they are (sceptically) received by audiences.

Countering and preventing radicalisation as an independent policy area is a field where Denmark has been proactive in coordinating social policies into counter-terrorism programs. The approach is based on close cooperation between state, regional and local levels and actors from the private sector, law enforcement, intelligence agencies and civil society (NAP 2016: 13). Denmark is mainly known for the 'Aarhus model' focusing on social inclusion and interdisciplinary collaborations with 'SSP' partnerships between schools, law enforcement and social authorities (Bertelsen 2015: 242f). Initiatives aimed specifically at a threat from extremism online have been launched since 2009 (Lindekilde 2015: 425). Among those are the most recent NAP from October 2016 on countering and preventing violent extremism.

Theory: Critical Terrorism Studies and the classic Copenhagen School

Analysing online policies through the lenses of security theory is relatively new within International Relations (IR) where Political Science meets Computer Science in conceptualising the internet as a theoretical and empirical realm (Nissenbaum 2005; Radu

2014; Jungherr 2014). I focus on logics driving online policies and political implications thereof and do not engage with technical specificities of cyber space.

My theoretical outlook is based in the diverse field of Critical Terrorism Studies (CTS) which tends to focus on deconstructing the meaning of concepts within the field of terrorism and questioning who, what, when and where concepts are developed and maintained (Jackson 2009: 3f). Drawing on this ontology means that I do not take for granted key concepts such as 'radicalisation' or 'terrorism' but explore how, why and by whom their meaning is constructed in official documents and by government officials. These lenses enable me to broaden an existing understanding of what it means to develop policies in the complex area of online radicalisation. Being 'critical' can refer to an array of approaches even within the relatively narrow CTS (Jackson et al. 2011: 13ff). CTS is characterised by being more an approach than a theory that is 'committed to disciplinary and intellectual pluralism and a willingness to engage with a range of perspectives and approaches' (Jackson 2009: 4). For me, CTS means that I question common understandings of concepts related to online radicalisation as an academic and political term and acknowledge that no production of knowledge is neutral (Jackson et al. 2011: 19). The aim of my research is not to denounce existing structures for Danish policies nor to normatively assess if policies are 'good'. Hence, I do not deconstruct current power structures for online radicalisation policies. Instead, I focus on current policies and the understandings which they rely on to enhance debates on potential political implications of logics driving said policies. My approach entails some classic CTS emancipatory elements but I rely on a relatively stable understanding of the current political landscape where I engage with policy makers and thereby remain in existing political structures. Using securitisation as part of my theoretical lenses allows me to analyse discursive possibilities in which policies are created (Buzan et al. 1998: 26; Hansen 2006: 21).

Securitisation is ontologically understood as an inter-subjective process, which relates to an epistemological notion of threats as linguistically constructed and accepted by a relevant audience as an existential threat needing extraordinary measures (Buzan et al. 1998: 30). Threats can thus not be defined objectively. There are however recognised elements of

objectivism in the Copenhagen School as some threats are (analytically) relatively stable and can be analysed through somewhat fixed discursive structures pertaining to analytical sectors characterised by specific logics (Buzan et al. 1998: 7f). Within a securitised discourse, the realm for action is limited as securitisation enables politicians to act with urgency and legitimately use the means deemed necessary towards a perceived threat (Ibid.: 26). This understanding of securitisation is important for my analysis as constructions of specific discourses enables certain policies within a realm of possibilities (Hansen 2006: 21).

While the Copenhagen School broadens the scope of what can be constructed as threat against whom and by who, I place my analysis in the common situation where the main actor is the state with the legitimacy to 'speak' security on behalf of a constructed national identity (Buzan et al. 1998: 40f). Nevertheless, I acknowledge that an official Danish discourse on terrorism is shaped by (and in interaction with) global discourses on terrorism shaped by (and within) history, events and actors (Ditrych 2014: 77f).

Radicalisation can be understood as a process where a person develops views towards what is defined as extremism - often referred to as Islamic terrorism (Gemmerli 2014: 9f). A 'radical' can be seen as; 'a person harbouring a deep-felt desire for fundamental socio-political changes and radicalisation is understood as a growing readiness to pursue and support far- reaching changes in society that conflict with, or pose a direct threat to, the existing order' (Dalgaard-Nielsen 2010: 798). I understand radicalisation as a construction contingent upon context drawing on CTS and the Copenhagen School. Hence, I explore how government officials understand it in the context of a perceived threat from IS online.

Terrorism is also seen as a concept that depends on who assigns meaning to an act with what purpose and in which context (Jackson et al. 2011: 119). Violence by none-state actors is typically seen as disruptive to an 'order' in the sense of a normatively desired system which often benefits those in power (Jackson 2009: 13). By using the word 'terrorism' or 'extremism' in relation to radicalisation, a power relation is (re)established as the state constructs and performs its own authority in discursively defining 'terrorism' and responding to such a threat (Collins and Glover 2002: 158; Thorup 2010: 43).

It can be argued that a state developing counter-terrorism policies is simply acting within its boundaries of legitimate power cf. a classic Weberian definition of monopoly on the use of force (Ramsay 2015: 219). However, those boundaries are not as clear online as in the physical realm. The online sphere is said to be a 'new domain of power' where such monopoly is not solely held by states (Radu 2014: 5). The internets interconnected structure enables new possibilities, constraints and risks for governance such as predicting citizens' behaviour to prevent them from being what is perceived as threatening towards the state (Aradau and Blanke 2016: 2). An anticipatory form of governance relies on the assumption of attacks as imminent which is often seen in terrorism discourses (Jackson 2015: 35).

What is political?

There are many definitions of politics so this outlines how I understand politics and securitisation.

'One of the central implications of this idea is that once established, securitisation enables policy makers to immediately adopt whatever means they deem appropriate to curb the threat' (Balzacq and Guzzini 2014: 4). This argument presents securitisation as a political concept. According to Hansen (2012: 528) politics in securitisation is simultaneously 'Schmittian, Habermasian, Derridarian, Arendtian and (latently) Foucaultian' (Hansen 2012: 528). How to grasp securitisation as political is not clearly stated by the Copenhagen School but it can be seen as a 'middle ground' definition (Buzan et al. 1998: 143) in line with a normative ideal of free and active engagement in a public sphere inspired by Arendt and Habermas as well as drawing on the classic 'friend vs enemy' distinction from Schmitt. An issue can be brought back to the realm of normal politics to be subject of debate in a reconstruction of the opposing relations constructed in securitisation (Hansen 2012: 530).

This friend-enemy distinction can be analysed through analytical constructions of, inspired by Derrida, 'Self' and 'Other' identities that are discursively performed as relations of opposition (Hansen 2006: 38f). These identities are suggested analysed through ethical, spatial and/or temporal dimensions in analyses of foreign policy (Hansen 2006: 46f). I mainly

draw on a spatial understanding of a Western Self constructed in a securitised discourse with a terrorist Other while noting how communication flows online blur spatial lines enabling a form of expanded, abstract spatial identity that is primarily value based (NAP 2016: 6).

Wæver (2014: 28) argues that an illocutionary approach, where securitisation is action and not just communication, entails transformative potential opposed to focusing on perlocutionary acts entailing more of a cause and effect relationship between speech acts and securitisation. Securitisation as illocutionary can be understood as 'an operational method that can be designed to protect politics in Arendt's sense' (Wæver 2014: 27). The theoretical critique of the Copenhagen School requests more analytical focus placed on the interaction between securitisation moves and audiences (Sjöstedt 2017: 6f; Balzacq and Guzzini 2014: 2). I align myself with Wæver (2014: 28) in understanding the politics of online radicalisation policies and use this to discuss potential implications of political logics driving such policies.

Methods: Discourse analysis and qualitative interviews

Analysing qualitative data is inherently 'messy' – notes Bryman and Burgess (2002: 2). Discussing my methodology and methods is relevant for the scope of the following analysis as reflections of my analytical process in a transparent manner is an attempt to limit this unavoidable 'messiness'.

My chosen ontology creates the lenses from where I enter and engage with the field of online radicalisation. The lenses of securitisation help me understand the context for analysis as a guiding tool for exploring what drives political logics on online radicalisation and what realm of possibilities is enabled. CTS helps me critically discuss potential implications from constructions of political logics. This is done to discuss what realm of possibilities the discourse on online radicalisation opens in a securitised context.

The construction of meaning can be analysed in different contexts through analytical lenses of discursive structures (Hansen 2006: 57) and a discourse on terrorism changes in interaction with actors in the discourse and other discourses (Ibid). My analysis is an

analytical 'snapshot' of an empirical time and place where theoretical lenses provide a framework for working with (and within) an understanding of a dynamic construction of Danish online radicalisation policies.

As noted by Buzan et al. (1998: 25) 'to study securitisation is to study discourse'. The ontological understanding of a threat from radicalisation as part of a broader securitised discourse on terrorism leads me to an epistemology of analysing an official Danish discourse (Buzan et al. 1998: 177). I thereby accept an argument of a political landscape understood as somewhat stable where discourses operate within a structure of meaning that is changeable but tends to be relatively stable (Ibid.: 35).

Choosing official documents for discourse analysis

The aim of a discourse analysis based on official documents is to understand how a threat from online radicalisation is officially conceptualised within recent policies. I argue that the chosen documents are 'central in the sense that if a security discourse is operative in this community, it should be expected to materialise in this text because this occasion is sufficiently important' as argued by Wæver (1989: 190 in Buzan et al. 1998: 178). As the state is the primary actor in my analysis, I focus on the 2016 NAP on countering and preventing violent extremism. Other documents include a local action plan from the municipality of Copenhagen, statements on online policies and ministerial websites. All documents are from 2016-2017. This (limited) timeframe is chosen to analyse logics of a current political landscape on online radicalisation and to discuss potential implications of maintaining these. Since the first NAP in 2009, two plans have been launched by respective governments. While former plans note the online sphere, in 2016 online radicalisation was placed more prominently as a policy area (Lindekilde 2015: 440; NAP 2016: 29).

Choosing to interview

The objective of my analysis is to explore dynamics of discursive structures constructing meaning assigned to policies. The discourse analysis shows an official notion of

online radicalisation as a threat. Yet, little can be said on considerations for developing corresponding policies. To explore logics driving the polices, I interviewed government officials working with NAP policies. This qualitative and interpretive approach can illustrate dynamics that are unique to a context (Schofield 2002: 174). My analysis provides an insight into the Danish political landscape of online radicalisation as of 2016 and 2017, which can indicate more general patterns (to a certain extent) on how 'we' as a society respond to this threat perception. See more in the section on 'limitations'.

My interviews can tell me how government officials attribute meaning to this field (Rubin and Rubin 2005: 28). I gain insights into how online radicalisation is perceived as a threat (and towards what). The interviewees are referred to by office and not by name due to my ethical considerations and as my level of analysis is the state - not individual. I view the interviewees as representatives of offices while being aware of diversity at an individual level. The Danish state thus becomes an analytical construction where each office represents a working area.

I chose to conduct all interviews in the working language of my interviewees (Danish) as a language barrier could hinder conversation flows. This was to create semi-structured interviews that allowed them to speak as freely as possible as I was interested in their conceptualisation of meaning on a sensitive and complex topic (Maxwell 2002: 48). All data was compiled in Danish and English interchangeably. All translations were done by me as a bi-lingual researcher.

Selecting and gaining access to interview people

Representatives from government offices involved with developing and implementing NAP policies were my primary interview persons. Interviewees were selected based on my assumption that they could construct insights into how online radicalisation policies are understood beyond official documents. I expected some contacts to be limited in what they could discuss given the sensitivity of such policies. Gaining access was not difficult and nearly all agreed to participate. However, the Central Intelligence Service (PET) did not wish

to participate. As the PET plays a role in implementing NAP policies, I chose to interview a researcher on the legal framework for PET to gain insight into their working methods online.

Three common barriers for obtaining information and conducting interviews emerged; confidentiality and sensitivity of the topic, lack of resources not allowing government employees to spend time at an interview and the complexity and overlapping nature of the issue. There also appeared to be a lack of consensus on who was responsible for what where no one wanted to speak on behalf of others and were mindful of their authority in their official capacity. I view these barriers as speaking to the complexity of online radicalisation as a field.

To the extent practically possible the interviews were conducted in the offices of the interviewees. Nevertheless, being primarily government officials it was not always possible. I acknowledge the potential lack of context associated with conducting interviews online as there is not the same interaction with eye contact and body language. Interviews were conducted via Skype, as I considered this to be the next best option (Mosley 2013: 7f)

The researcher in the interview process

The choice of an interpretive approach makes me an active part of the field that I analyse throughout planning, conducting, coding and analysing interviews (Maxwell 2002: 41f). I adhere to a concept of 'rigorous subjectivity' arguing that openly using rather than discarding an (inherent) element of subjectivity in my research creates a more reflexive approach to interviews (MacLean 2013: 68). This means that my theoretical reflections and pre-notions of the field helped construct themes for my semi-structured interviews and for the coding process. I also acknowledge that there is no objective interpretation of neither theory nor of official documents or interview transcripts. The validity of my analysis thus relies on the willingness of the reader to follow my argumentation, presented in the most transparent way possible, and to accept my analysis as a snapshot of the chosen empirical context based on a specific theoretical framework.

All interviews began with an introduction of my research followed by an opening question on the work of the interviewee. That way the interview started like a conversation

flowing relatively free and follow up questions and encouraging interjections moved it along (Rubin and Rubin 2005: 108ff). My interview guide was not static but a guiding tool with themes that were deliberately broad including online radicalisation definitions, political corporation, objectives of the policies and evaluation criteria. The themes are based on radicalisation studies (Dalgaard-Nielsen 2010; Crone 2016; Christmann 2012; Ashour 2011), literature on security studies (Buzan et al. 1998; Jackson et al. 2011) and official documents (NAP 2016; Foreign Ministry 2016; Justice Ministry 2016).

Semi structured interviews required flexibility and adaptability (Leech et al. 2013: 210f). An example hereof was in the initial communication with the Justice Ministry where the person solely mentioned aspects of implementing the 2016 NAP. In the interview, the person noted how they were part of developing policies which I then decided to use as a starting point for the interview.

Ethical considerations on data collection and data management

Prior to contacting interviewees, I considered presenting them with a confidentiality form, which would classify my research and hinder public publications. After discussing this option with an academic advisor, I decided not to present this option when initially contacting potential interviewees. Instead, all contacted persons were met with an open approach asking if they would like to take part in an interview on their role in the development and implementation of policies related to online radicalisation. This went alongside my choice of allowing interviewees to direct the interview in the direction they saw fit. I decided, prior to interviews, that while I would not myself present a confidentiality form, I would immediately grant this, if any of the interviewees requested such a form. None of them did at any point of communication. I chose to be as open as possible to wishes from the interviewees. One person requested to review the interview transcript prior to my analysis thereof. The transcript was sent in writing and the person accepted my use of the material for analysis. Another interviewee solely wished to participate with written answers to questions (based on themes from my interview-guide).

While only two the contacted persons requested anonymity, due to the sensitive nature of the topic, I decided not to disclose any names of interviewees or specific offices. This was done to ensure a degree of anonymity and for the interviews to represent an office, not a person, which was collectively interpreted as the 'state'. This brings limitations to the interpretation of my analysis as my findings become analytical representations of a discursive snapshot of selected representatives interpreted as an aggregated threat perception of online radicalisation and state-led policies responding hereto.

All interviewees were contacted after I concluded my analysis. I sent a summary of my conclusions and encouraged anyone to contact me with questions or requests for clarifications. They were also given the opportunity to read my entire analysis. This gave interviewees the chance to clarify their role, read their quotes or in other ways impact my use of their interview. None of the interviewees requested additional information or readings. All audio files were kept and stored on a computer which I had sole access to. The selected codes where reviewed and discussed with an academic advisor from the field of security studies but no original transcript was shared.

Analysis: processing data

The process of structuring transcripts as qualitative data was interactive using the presented theories and empirical data in an abductive manner (Blaikie 2000: 114). While the structuring of my data was heavily inspired by the practical approach to coding in grounded theory, the aim of creating new theory based on theoretical memos constructed in the coding process, tested in hypotheses, was not my aim (Urqhart 2013: 108; Bryman and Burgess 2002: 4). Analytically, I use generated codes to go beyond the level of conceptual descriptions and explore general patterns. My aim was not to create new theory per se although theoretical reflections were a part of processing, analysing and discussing the conducted interviews as qualitative data.

I chose an open coding method as I wanted to 'let the data speak' in exploring understandings of the threat itself and its policies. However, no coding process is without influences from prior understandings (Gibbs 2007: 47). What is important to note is the engagement with many of interviewees prior to recorded interviews via phone calls and emails confirming the scope of the interview. This gave me a pre-notion of understandings used by the actors in their everyday work with policies on online radicalisation.

When constructing open codes, I moved back and forth by revisiting the presented theoretical concepts, official documents and interview transcripts in an interpretive process (Gibbs: 2007: 47). An advantage is that new nuances from the interview data emerge as the knowledge increases (Blaikie 2000: 117). I was mindful of not searching for pre-notions from the literature as my approach required a degree of openness towards the data. I re-read texts and asked questions to each section of each interview making sure not to simply summarise what was already known. This was to explore layers of possible interpretations and thereby analyse general ideas rather than describing what the interviewees said (Gibbs 2007: 143).

After creating open codes, they were organised through selective coding placing all codes related to each other under narrower core-categories. At this stage, Urqhart (2013: 85) argues how research can change as the scope narrows. This was also the case for me as the interviews to a minor extent discussed concrete policies. Instead, a common sense of uncertainty, urgency and work in progress emerged as the interviewees seem to operate in a challenging political landscape of complexity where online threat perceptions change rapidly while bureaucratic structures do not enable policies to change at the same pace (NCP Interview).

I elevated the level of abstraction beyond descriptions to general patterns, oppositions, repetitions expressed in the interviews by generating six narratives, or logics, driving understandings on online radicalisation. This was done by working with the open codes and revising selective codes several times to explore possible underlying logics for the understandings expressed in the interviews. For instance, open codes on corporation between governmental and local entities were lifted from being descriptions of ways of working

together to being understood as a normative claim for civil society engagement as a positive contribution to CVE and PVE policies.

In these initial analytical steps, I paid attention to what was not explicitly said. 'Common truths' were noted when re-reading transcripts to explore if they were patterns. For instance, an assumption on how preventing radicalisation is about ensuring that views do not become extremist for those who feel marginalised and that such a process can be reversed by fostering democratic values (Foreign Ministry Interview; Justice Ministry Interview). This indicates an underlying logic that is (somewhat) taken for granted. Whether this assumption is 'true' is not relevant for my analysis as I operate with an ontology and epistemology that understands concepts as discursively constructed. I am however interested in how online radicalisation is conceptualised as a threat and how this understanding impacts policies. Therefore, I constructed what I subjectively analysed as general patterns from the transcripts and accumulated the meaning into six prominent narratives, or logics, that are based on the interview data and shown in figure 1.

Figure 1: Six prominent narratives from interviews in a wider discursive context

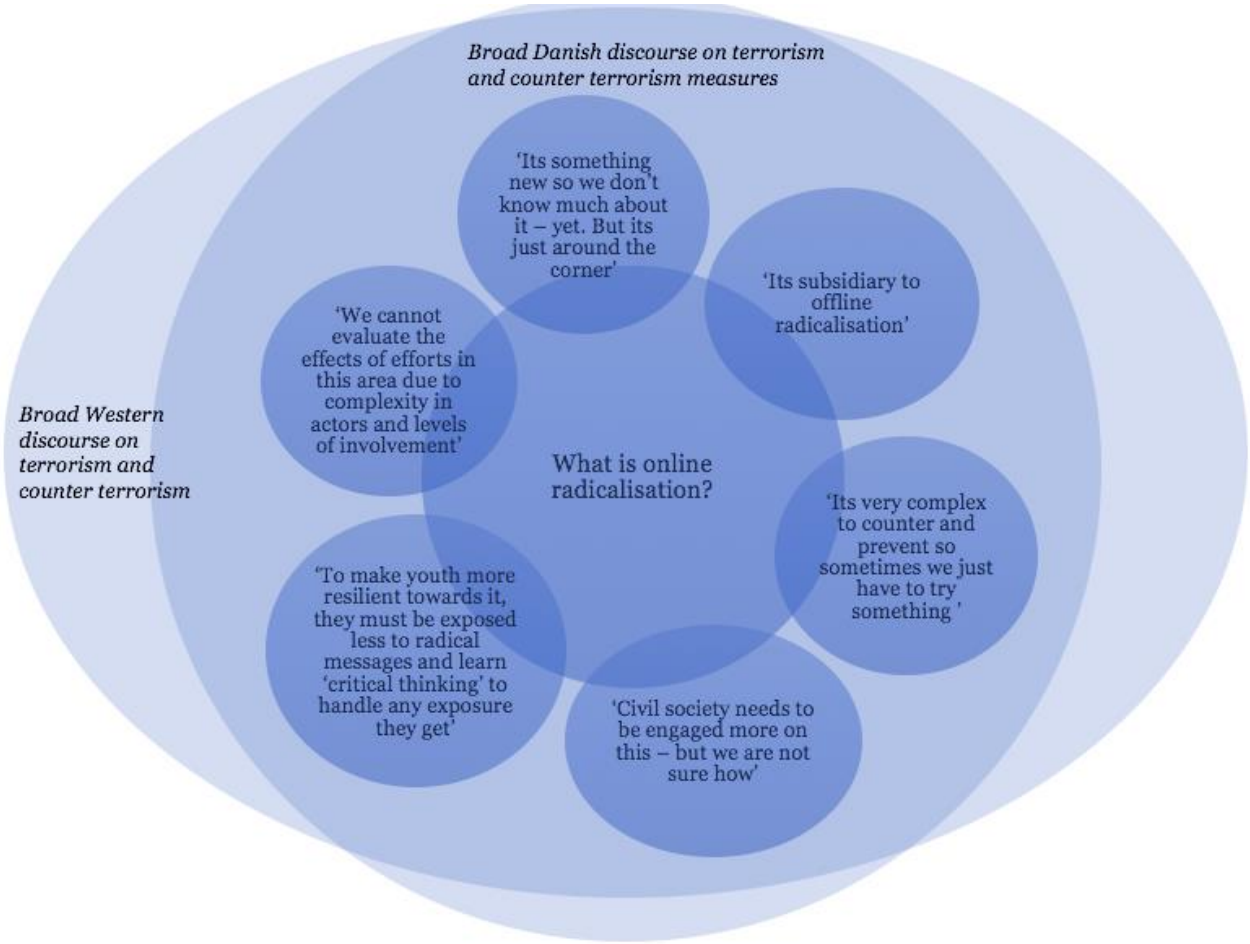

Figure 1 shows six prominent narratives, or logics, on how online radicalisation is understood based on the interviews. They are not direct quotes but accumulated meaning interpreted from my data.

The construction of narratives can legitimise specific actions and policies (Hansen 2011: 53). Figure 1 illustrates an ontological assumption that the meaning of online radicalisation is not constructed in a vacuum. Narratives operate within (and interact with) a broader Danish discourse on terrorism which also operates within (and interacts with) a broader Western discourse on terrorism (Hansen 2006: 60f). The overlapping and interactive

logics also rely on epistemologically understanding them as an analytical tool to structure the complexity of my empirical data.

The official understanding of online radicalisation

Obtaining an understanding of the political landscape with related actors and policies is like a jigsaw puzzle. Pieces of varying size relate to each other through different interfaces that link pieces into a complex image. The puzzle of relevant actors is part of a bigger image of CVE and PVE efforts of yet more actors linked by other pieces. The triangle of prevention focuses on implementation with exceptions as some actors also work with development. It is inspired by the criminal justice system (Muro 2016: 4) and is referenced throughout former and recent NAPs and in my interviews (Justice Ministry Interview; NCP Interview; Foreign Ministry Interview).

The NAP primarily involves the Justice Ministry, Ministry of Immigration and Integration and the Ministry for Higher Education. The Ministry of Immigration and Integration manages social policies and the National Prevention Centre (NCP) provides governmental support through analyses on violent extremism (NAP 2016: 27). The Foreign Ministry also works with online radicalisation albeit in a more indirect way through international collaborations. The online realm transcends and blurs already lose distinctions between actors, initiatives and audiences where many overlap. The figure below illustrates actors and initiatives from Danish CVE and PVE efforts that are characterised by an inter-disciplinary and inter-departmental approach with state, regional and local actors. It appears inevitable that policies interact on multiple levels (NAP 2016: 12f).

Figure 2: The Danish Triangle of Prevention including the online sphere

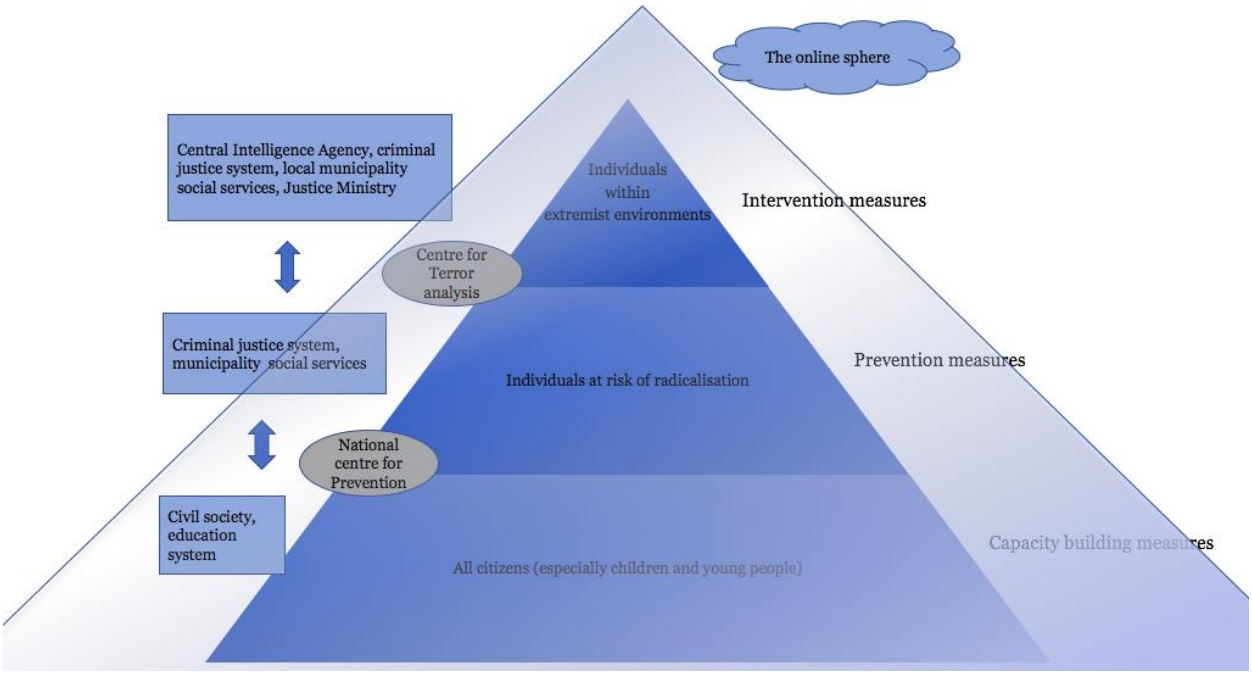

Figure 2 is made freely from the 2016 NAP (12f) of the triangle of prevention including actors and efforts.

Definitions of radicalisation in official documents include references like in Dalgaard-Nielsen's (2010: 800) research where 'radical' views are opposing an existing system of democracy. The ministry of Justice launched the 2016 NAP by noting 'the government is rearming in the struggle against parallel societies' (Justice Ministry 2016). The term 'rearm' is reminiscent to military rhetoric while 'parallel societies' invokes societal norms. An interplay between a military and societal sector sets the tone for understanding democracies as free and safe - threatened by not further defined 'forces' that encourage violence. They linguistically become the opposition to the Danish society. The Minister of Immigration and Integration underlines this opposition by referring to a Danish 'we' connected by values of freedom, safety and democracy opposed to violence, hatred and insecurity defining those of 'parallel societies' (Justice Ministry 2016). The 'we' goes beyond the state as a political

system and constructs a national identity through enacting this opposition (Buzan et al. 1998: 123f).

The table below shows official definitions on extremism and radicalisation where the normative power of the state is indicated as democracy becomes 'anti-extreme'. It is noteworthy how little is said. Firstly, nearly all actors use their own definitions and secondly none of the definitions clearly state how content or views are 'extreme' besides being anti-democratic. There appears to be a sense of taken for granted in what concepts refer to and who defines what is considered extreme.

Table 1: Definitions for extremism and radicalisation by governmental entities

Entity	Extremism definition	Radicalisation definition
National Action Plan (2016: 7)	Extremism characterises persons or groups who commit or seek to legitimise violence or other illegal acts by referring to the social conditions they are dissatisfied with. The term includes left-wing extremism, right-wing extremism and militant Islamism	Radicalisation refers to a shorter or longer process in which a person adheres to extremist views or legitimises their actions through extremist ideology
The municipality in Copenhagen unit for anti-radicalisation plan for action (Municipality of Copenhagen 2016: 6)	An animosity towards the established society and its order which is based on beliefs such as: rejection of basic democratic values and norms and of democratic decision making; Simplified world views and conspiracy theories; enemy images where groups or social conditions are labelled as threats that must be removed; Intolerance and lack of respect for other people's views, freedom and rights. These beliefs may	A process in which a group or an individual gets increasingly extreme viewpoints and / or support the use of illegal or violent acts to promote them. It is far from everyone who commits such actions, but the risk leads to the viewpoints to be problematic

	be accompanied by the support or use of extreme actions which are illegal and possibly violent means of achieving a political or religious ideological goal	
Centre for Terror Analysis. Department in the Danish Central Intelligence Service (2017: 10)	Extremism is a term of far reaching behaviour or beliefs, especially in relation to politics or religion	Radicalisation is a dynamic process in which an individual increasingly accepts the use of violence or other illegal means to achieve political, religious or ideological goals
National Prevention Centre is newly established as part of the Agency for International Recruitment and Integration under the Ministry of Immigration and Integration (2017b)	Extremism is a term of far reaching behaviour or beliefs, especially in relation to politics or religion	Radicalisation refers to a shorter or longer-term process in which a person adheres to extremist views or legitimises their actions with extremist ideology
Foreign Ministry (2016)	Refers to the 2016 government report on the Danish approach towards terrorism	Refers to the 2016 government report on the Danish approach towards terrorism

Resources are increasingly allocated to online initiatives aimed at extremism (NAP 2016: 29). New initiatives appear based on an assumption that countering and preventing online radicalisation requires a multi-sectoral approach and that radicalisation is understood as something directed at youth, which can be prevented if they are 'resilient' towards anti-democratic content (Hemmingsen and Castro 2017: 35). Labelling something 'extreme' makes democracy logically be the 'normal'. Constructions of a dichotomous relationship are common for securitisation. A referent object is often a national identity intertwined with a political system (Buzan et al. 1998: 124; Hansen 2006: 29). Sectoral discursive lenses of the Copenhagen School tend to overlap (Buzan et al. 1998: 166). A threat perceived as operating online can be understood as blurring overlaps further. I argue, based on Hansen and

Nissenbaum (2009: 1171) that a threat from online radicalisation blurs analytical sectors as multiple referent objects are threatened simultaneously. The NAP (2016: 3) notes radicalisation as a threat to 'our freedom and security' while not specifying 'our' that appears to be self-evident collective Self. This value based referent object of a 'way of life' touches upon the political system, ideological democratic values and physical safety of citizens as all impacted by an online threat perception.

There is a securitisation of specific forms of online communication from certain groups (extremists associated with IS) that threatens to radicalise Danish users, especially youth, if they are not countered and/or prevented by state-led initiatives including blocking content online, teaching youth critical online thinking and internationally cooperating with states and civil society to share 'moderate' messages (NAP 2016: 17; Foreign Ministry 2016: 16; Justice Ministry 2016).

The six core logics driving the current threat perception

Denmark's inter-agency strategy involves multiple actors. I understand this, undoubtedly recourse heavy, approach in combination with a political landscape of securitisation where the threat operates in a decentralised digital sphere. This appears to construct logics of CVE and PVE efforts enacted with an understanding of 'this is something new' and many initiatives are 'just around the corner'. These, and other logics, are presented below.

Online radicalisation is something new so we don't know much about it – yet

The PET is given increased powers to monitor and block content online in the NAP which can indicate a shift towards censorship online as the definitions of 'normal' and 'extreme' could blur rights of freedom of speech online when certain forms of communication (perceived as extremist) are securitised as it legitimises blocking and monitoring specific content (NAP 2016: 29).

So-called official IS sites are automatically blocked by a filter and data sent to PET. The legal basis is the Procedural Code (Justice Ministry Interview). Questions remain not only on what kind of content is 'extremist' but also who defines what content is threatening (the Other) and what is considered non-threatening (the Self). New sites emerge constantly and content can be shared on social media which a filter cannot pick up. Denmark mainly relies on civil society to flag content to be blocked (Justice Ministry Interview). Some studies argue that censorship on social media potentially complicates the work of law enforcement by enhancing marginalisation of those who feel on the verge of 'normality' and thereby strengthens a self-understanding of a legitimate battle towards an established society (Gemmerli and Jacobsen 2014: 2). By blocking content, the Otherness of the Other could be strengthened which would be counterproductive to the aim of policies to strengthen a democratic value-based Self and reduce the violent extremist Other.

There are several purposes of blocking and monitoring content. Besides removing IS sites to reduce exposure, monitoring data is also articulated by the Justice Ministry as 'building a knowledge base' to understand how to interact with social media users to potentially develop alternative narratives. The complexity of how not much is known about the dynamics of such a policy was noted when asked about the usage of narratives;

> 'It's hard to tell, right? Because the question is what does this entail, right? Well I think that they had a classic thought that said if let's say Al Qaeda or ISIS says you're going to do this and this, then you're creating a narrative saying, that you're not going to do this or this. But I do not think it will be like that as I do not think there are many who have insight into this kind of thing that will encourage doing so but it's all about knowing what's affected. What is affected when a young person sees this? Is it appealing to the rationality or your feelings or to create identification between your local community in Europe and a population down there. So, what is it? And then you have to try to see if you can do something that's equivalent to it' (Justice Ministry Interview).

This illustrates the aim of engaging with dynamics of radicalisation online but not much information on how. The threat remains understood as relatively new and so are policy responses. It is noted that recourses are to be allocated for experts to create narratives if they are put in place (Ibid.) Other initiatives being developed are teaching material for youth to become critical online users (NCP Interview) and hackathons where youth in schools develop and share 'positive' non-violent messages. This is to be implemented in the spring of 2018 (SUS 2017). The understanding in the interviews of online radicalisation as a new threat where not much is known appears to be re-enforced by a sense of urgency to 'do something' making the 'new' logic remain relatively stable. Combined with the securitisation of (some) online content there is little room for reflections on policies themselves or how they interact with the threat that they are addressing.

Online radicalisation is subsidiary to offline radicalisation

The digital realm can foster extremist views that originate offline as it is easy to find like-minded communities online (Koehler 2014: 123). There appears to be an assumption among government officials that online is primarily a realm of ideas and can be a gateway to offline engagement with extremism or reinforce a sense of belonging beyond the existing society in virtual communities. The interaction between offline and online policies engages with local and state levels according to the NCP, referring to the triangle of prevention, as online efforts mainly targets youth 'to build them up towards being democratic co-citizens' as a normative benchmark whereas offline efforts mostly target those already deemed at risk of radicalisation. This division (and overlap) of initiatives indicate that online measures are mainly seen as preventative. Interactions between offline and online in an international context indicate a similar notion of the threat as online policies are seen as more effective in interaction with (local) offline efforts:

> 'Well I think, or what I can hear from some of our (global) meetings and here I'm unfortunately no expert but that online efforts only work if they are followed by or what works is mainly if it is also followed with something locally (...) Just so you

know that there is this link between online and something physical is what works best' (Foreign Ministry Interview).

The discursive terrain appears to have changed from 'counter to 'alternative' narratives. This is supported by research noting radicalisation as largely about belonging to a community (Dalgaard-Nielsen 2010: 801). A study recommends not to engage with IS but provide alternatives based on contextual knowledge of an audience (Hemmingsen and Castro 2017: 6). Question emerge on what alternative community online efforts offer. There is an understanding of alternative narratives as more effective if they are based on local actors which opens a discussion on including civil society in CVE and PVE efforts (Foreign Ministry Interview; NCP Interview).

'Sometimes you just have to try something'

The interviews indicate that there is no need to talk about if but rather when a terrorist attack occurs. This logic is constructed as a characteristic of the discourse on terrorism post 9/11 (Jackson 2015: 35). A logic about what could happen illustrates how terrorism is securitised in a Western discursive terrain (Stephens and Vaughan-Williams 2009: 7). The interviews also indicate that a logic of urgency and uncertainty is driving Danish policies with a speed that challenges governmental actors as policies take time to develop, process and implement. The perception of how the threat and policies interact online is driven by this logic that appears to encourage an approach of 'let's just try something' (inspired by other countries facing similar political landscapes) where policies are developed with a limited concept of why and how they interact with other perceptions, policies or actors. The complexity of the decentralised internet combined with a threat perception that entails multiple aspects (ideology and physical attacks) within a discursive terrain on terrorism leaves governmental officials with a sense of acting urgently (as the threat is imminent) within a limited realm of possibilities (as the threat is securitised) and with uncertainty (as they have little knowledge about how the threat is addressed online).

The interviews appeared to have a taken for granted notion of the securitisation of terrorism and thereby of online radicalisation. The interviewees perhaps assumed I already knew what online radicalisation 'is' so there was no need to specify beyond official documents or perhaps they did not want to speak beyond their capacity (Ministry of Immigration and Integration Interview; Justice Ministry Interview; NCP Interview). This could have something to do with me as a researcher (MacLean 2013: 78f). I physically present as part of the 'Self' - probably adhering to the values of 'democracy' and 'freedom' as noted in the NAP (2016: 6). Internalised 'truths' of online radicalisation as part of a securitised discursive terrain on terrorism requiring urgent (and continuous) action seems to reduce debates on why policies are put in place and how they operate. It provides state-level policies with a relatively limited discursive realm of possibilities.

Civil society needs to be included in countering and preventing online radicalisation

The need for increased engagement by civil society actors appears to be driven by an assumption of the state as not trusted within some groups. The use of civil society 'voices of reason' is included in the NAP to 'seek out and critically engage in relevant forums, enter into dialogue and challenge extremist views' (NAP 2016: 29).

The Ministry of Immigration and Integration (Interview) refers to the upcoming hackathon project with the aim to 'involve youth in developing and implement dialogue-creating (online) activities that target youth who may be at risk of online radicalisation. Through equal level dialogue efforts will help youth gain knowledge of online radicalisation and propaganda. Also, efforts strengthen a constructive dialogue in positive communities based on democratic values'. To what extent a democratic state outweighs the importance of safeguarding not only physical lives of citizens but also democratic values while reducing the realm of acceptable expression, is a dilemma. What is noteworthy in an online context is that the state does not have all the information but relies on private, profit driven companies and civil society intelligence gathering related to content deemed 'extremist', which is a potential decline in transparency. This is discussed in the sections below.

Young people need to be educated in critical thinking

There is an assumption in the NAP that eliminating extremist content online is impossible. Therefore, youth must learn to be resilient when exposed to such content. This is done through not only blocking content but also through social initiatives that include law enforcement, municipalities and schools (NAP 2016: 22). The core of such projects is to teach youth critical thinking that does not legitimise violence (Justice Ministry Interview). There also seems to be a normative idea of the threat as more prevalent among youth who feel socially marginalised (Justice Ministry 2017c). Policies on 'critical thinking' appear to be driven by a logic where strengthening the Self (through resilience building) makes the Other less threatening as a form of predicting future behaviour. The distinction between Self and Other is thus not dissolved by online policies but initiatives are a way of preventing certain forms of online communication perceived as threatening towards the Danish Self.

The hackaton initiative can be seen as resembling a governance-network. Dalgaard-Nielsen (2016: 1) argues that networks have advantages in preventing violent extremism as a collaborative approach challenges hierarchal control in being decentralised and informal. Networks are mainly based on voluntary participation and 'a network is more likely to possess the necessary resources and expertise to tailor interventions to individual cases than any single agency of central government, no matter how competent the agency may be' (Ibid. 2f). Some studies recommend using 'alternative narratives' developed locally rather than engaging directly with messages seen as extremist online (Winter and Bach-Lombardo 2016). Developing 'voices of reason' could be a way of meeting the perceived grievances of those at risk argues Hemmingsen and Castro (2017:42). Nonetheless, initiatives may have negative consequences 'if they fall into the trap of attempting to expose, correct, or ridicule the ideology, or simply promote their own normality as superior' (Ibid). Similar points on potential unintended consequences are noted by Teglskov and Gemmerli (2014).

Evaluation of polices on online radicalisation

One can question how to ensure that what is put online is seen by those intended to be reached. Lorrand Bodo and Speckhart (2017: 2) argue that reaching an audience with an anti-extremist message is strengthened by using knowledge about how IS spread news. Thus, using the same hashtags as IS sites. So-called 'echo rooms' result in youth interacting in somewhat homogenous virtual communities where they are exposed to content that fit into their existing views (Von Behr et al. 2013: 18). It appears challenging for government officials to grasp how online policies 'work' to reach intended objectives. I argue that the securitisation of specific forms of communication enables logics driving a perception of the threat making evaluations nearly impossible due to the abstract and multi-layered nature of policies. The NCP (Interview) notes the challenge of evaluation as highly prevalent.

> 'It's also a question, as I said before, about measuring an effect. Right and how incredible difficult it is in this area. So, it is also sometimes about us having to just sometimes do what we think will work. And that is of course a weakness because here people can obviously turn it around and be critical as; you don't know if this works so why are you doing it?' (…) Well I know that if you compare the development of propaganda and something like that with how or with our initiatives then I see how it simply takes longer for us to develop things'.

The Foreign Ministry (Interview) notes a similar view of the challenge. The objective of the NAP is the overarching aim of safeguarding Danish democratic values. Online radicalisation threatens this aim through multiple referent objects indicating that evaluation is nearly impossible as views are ever-evolving, contingent on context and cannot be quantified (Ibid.).

The NCP is working on having an external actor evaluate NAP initiatives. However, this is still being developed (NCP Interview). The Justice Ministry referred me to their Research Centre when asked about evaluations. The Centre noted a new 'mapping project' aimed mainly at preventative offline initiatives between law enforcement and local actors. This is in the early phases of development and focusses on mapping local experience and not evaluation as; 'it is completely impossible to do something, i.e. to measure an effect of this. It

becomes very much with a focus on that something is working and something is not working' (Research Centre Justice Ministry Interview). They have not initiated mapping or evaluation for online policies (Ibid.).

Potential political implications of current online radicalisation policies

I argue that we need to discuss implications of current policies and engage in critical (public) debates to understand (and question) the logics that are somewhat taken for granted yet actively driving policies on online radicalisation. If not, there might be implications to the democratic values that are perceived as safeguarded by said policies. 'We' is used in this argument as I accept the formation of a Danish societal Self and IS Other (offline or online) in a securitised context. This opposition is linked to a Western discursive terrain on terrorism. I accept the political landscape and engage with this while maintaining a somewhat critical approach. This is my way of slowing down the pace in which 'we' counter and prevent an online threat while working on understanding how 'our perception of online radicalisation impacts our policies and potentially democracy.

Theoretically, the current political landscape could increase democratic engagement by using the decentralised structure of the internet to engage civil society actors in online policies. However, when we enable policies that appear to be based on assumptions from a broader discursive (securitised) terrain and that lack knowledge of dynamics between actors, policies and threat perceptions, we risk a decline in freedom rights if there is no debate on how and why we develop and implement policies aimed at countering radicalisation online.

New state-led initiatives increasingly rely on various civil society actors to implement online policies where virtual communities are influenced through 'critical voices of reason' spreading 'moderate messages' with the intention of changing views (NAP 2016: 29). Policies are driven by a logic of civil society being necessary in CVE and PVE efforts as local actors are preferred to ensure legitimacy in some communities (Hemmingsen and Castro 2017: 42).

Power relations can be argued as re-established within constructions of 'critical voices of reason'. when the state (the Self) defines what is 'extremism' (and thereby the Other). The state can hereby use civil society to indirectly perform its own authority through discursively constructing what is 'reason' within a specific online context that is often delaminated to targeting youth. While a critical perspective could argue that state power is (re)asserted through the policies, I could also argue that initiatives might foster democratic engagement as the internet enables more actors to be involved in the discursive construction of identity relations. A theoretical potential for enhancing democracy through extraordinary polices exists in securitisation (Williams 2014: 20). Audiences outside official structures can be mobilised as structures, no matter how stable they seem, are changeable. To argue that a change in identity relations happens in the first phase of communication is stretching this argument. If a civil society actor engages with the state in sharing 'moderate' message in their online circles then they are at first re-enacting state power. However, when other users view the message and potentially share a slightly different version, then one can (albeit theoretically) argue that new meaning is (re)constructed.

Currently, anyone can flag content online, which is sent to the private company that owns the site. Thereafter, data can be shared with intelligence services or other governmental actors. This means that civil society actors take part in assessing what is a threat as one cannot objectively flag content without assessing it. One can argue that this form of co-production of intelligence challenges bureaucratic control of the PET. One can however also argue that intelligence services have always used civil society, private companies and other actors in investigations and that this is too complex to govern or regulate (Greve 2014: 98).

On the one hand the responsibility for policy implementation are at risk of being shifted to a grey area where there is next to no democratic oversight or regulation as the PET is largely independent in their methods and the current legal basis says little about online measures (Greve 2014: 136). On the other hand, countering and preventing online radicalisation through pro-democratic messages should perhaps not be a state matter at all. To follow this line of argumentation is to understand civil society differently as the online realm of views

might be best left ungoverned. Current Danish policies are a form of middle ground as the state intervenes by blocking certain content and indirectly engages by spreading alternative views via local civil society actors (NAP 2016: 29).

Despite the relatively stable understanding of online radicalisation as a new threat, recent legislative changes have been made. A bill on how law enforcement gathers and stores data on citizens' online behaviour was adopted in June of 2017 so 'the police can collect and process information from publicly available sources when necessary for carrying out their responsibilities and assignments' (The Justice Ministry 2017; Parliament 2017). The bill shows concrete changes from what I understand as logics driving a state-level threat perception. The freedom to express thoughts privately or publically are democratic rights and it can be intrusive to citizens if they are monitored online. This is a political (and legal) balancing act of preventing crimes while safeguarding rights.

Currently, the PET uses open (public) and closed (private) sources. It is however a grey area what constitutes open source. For instance, public Facebook profiles are open source but imitating friend requests to gain access to profiles are not (Greve 2014: 126). To systematically gather open source data, Denmark purchased databases for the PET. The use data has been criticized as 'predictive policing' enabling surveillance of citizens without formal charges (Gjerding and Andersen 2016: 2). The concept of surveillance in detail goes beyond the scope of my research. Nevertheless, the purchases and recent legislative changes indicate political (and legal) implications of the political landscape surrounding online radicalisation policies where extraordinary measures such as data-monitoring is understood as necessary given the securitisation of the threat.

Limitations and potential bias of my analysis

The main source of potential bias is, in my view, the risk of over-emphasising my findings based on few statements by selected interviewees that are (unfairly) made to be representative of an entire political landscape. My analysis is meant to be an analytical snapshot of a

discourse within a specific context – given the limited interviews over a short timeframe. Moreover, my analysis is a result of subjective interpretation. The qualitative process of coding and analysing transcripts could have led to different conclusions if someone else had interpreted my data. A potential bias in this regard is the personal angle. As a researcher, my personal blind spots of looking for connections to a broader discourse on terrorism and being a long-time student within this field, could have made me pay more attention to remarks in this direction than others. I also appear to be part of a Western Self in speaking fluent Danish, which could make me prone to specific responses. My findings could also be different if I had differently framed questions. These hypothetical reflections are, to an extent, part of qualitative research and impossible to eradicate. They do however deserve consideration to underscore the importance of how findings are contingent on their gathering, processing and interpretation. My findings are meant to serve as a conversation starter on the dynamics of a state-level understanding of online radicalisation as a threat towards the Danish society and the political possibilities (and thereby implications) that are enabled in the discursive realm of logics driving this threat perception.

Conclusions

In this research paper, I explored how online radicalisation is conceptualised as a threat towards Denmark as of 2016-2017 and analysed the political logics driving state-led policies aimed at countering and preventing a threat from the Islamic State (IS) online. I furthermore discussed potential political implications arising from these political logics driving the current Countering Violent Extremism (CVE) and Preventing Violent Extremism (PVE) efforts with a focus on policies from the 2016 National Action Plan (NAP) on countering and preventing violent extremism.

I argue that there is a lack of debate on understanding how underlying logics actively drive the securitisation of a threat perception of online radicalisation and policies addressing this threat. This can have political implications by blurring lines between civil society and

state interactions where distinctions between what is private and public are shifted with little to no transparent oversight. If underlying logics are taken for granted, there might be implications to the democratic rights that are intended to be safeguarded by the policies. However, a transformative potential of securitisation could be enhanced within an online realm (Wæver 2014: 27f; Williams 2014: 20f) as interactions between how the threat and online policies are constructed at the state-level also bring into play theoretical dynamics of what is considered political where meaning can be reconstructed.

I conclude that Danish state-led initiatives operate in a political landscape where the threat from online radicalisation is constructed as part of a broader discursive terrain on terrorism that calls for urgent (and continuous) action. The threat is perceived within a decentralised digital sphere that enables a multidimensional (ideological and physical) and inter-sectoral threat towards multiple referent objects (Hansen and Nissenbaum 2009: 1157). I understand the referent object as a Danish value based Self entailing political, economic, military and societal aspects based on the NAP (2016: 6f) and my conducted interviews.

The securitisation of terrorism has enabled an understanding of online radicalisation as simultaneously threatening multiple referent objects within a Danish value based Self. This political landscape appears to construct a relatively limited discursive realm of possibilities for policies addressing the threat. Further studies are needed on how to include civil society into state-led initiatives aimed at countering and preventing online radicalisation and which underlying dynamics that are driving the development and implementation of said initiatives.

References

Aistrope, T. (2016b) *The Muslim paranoia narrative in counter-radicalisation policy*. Critical Studies on Terrorism, 9:2. p. 182-204

Aradau, C. and T. Blanke (2016) *Politics of prediction: Security and the time/space of governmentality in the age of big data.* European Journal of Social Theory. p. 1-19

Ashour, O. (2011). Online De-Radicalization? Countering Violent Extremist Narratives: Message, Messenger and Media Strategy. Perspectives on Terrorism, 4(6). p. 15-19

Balzacq T., Guzzini S., Williams M. C., Wæver, O., and Patomäki, H. *Forum: What kind of theory—if any—is securitization?* p. 26-32

Bertelsen, P. (2015) "Danish Preventive Measures and De-radicalisation Strategies: The Aarhus Model" in Hofmeister, W. and M. Sarmah (editors). *From the desert to world cities: The new terrorism.* Panorama: Insights into Asian and European Affairs. Konrad-Adenauer-Stiftung Ltd. p. 241- 252

Blaikie, N. (2000) "Strategies for answering research questions" in *Designing Social Research – The Logic for Anticipation*, Polity Press, Cambridge. p. 85-119

Blakeley R. (2010) 'State terrorism in the social sciences: theories, methods and concepts' in Jackson, R., E. Murphy and S. Poyting, *Contemporary State Terrorism - Theory and Practice.* Routledge. p. 12-28

Bryman, A. and G. Burgess (2002) "Developments in qualitative data analysis" in *Analyzing Qualitative Data*, Routledge. p. 1-18

Buzan, B., O. Wæver and J. de Wilde (1998) *Security: A New Framework for Analysis.* Boulder, CO: Lynne Rienner Publishers, p. 1-239

Byman, D. (2016) *Understanding the Islamic State - A review essay.* International Security, Volume 40, Number 4. p. 127-165

Christmann, K. (2012). Preventing Religious Radicalization and Violent Extremism. A Systematic Review of the Research Evidence. Youth Justice Board. p. 1-77

Collins, J. and R. Glover (2002) "Terrorism" in Collins, John and Ross Glover *Collateral Language: A User's Guide to America's New War*, New York University Press, p. 155-173

Crone, M. (2016). *Radicalization revisited: violence, politics and the skills of the body.* International Affairs, 92(3). p. 587–604

Dalgaard-Nielsen, A. (2010) *Violent Radicalization in Europe: What We Know and What We Do Not Know,* Studies in Conflict & Terrorism, 33:9, p. 797-814

Dalgaard-Nielsen, A. (2013) *Promoting Exit from Violent Extremism: Themes and Approaches,* Studies in Conflict & Terrorism, 36:2, p. 99-115

Dalgaard-Nielsen, A. (2016) *Countering Violent Extremism with Governance Networks.* Perspectives on Terrorism. Vol 10. Issue 6. p. 135-139

Davies, G., Neudecker, C., Ouellet, M., Bouchard, M., & Ducol, B. (2016). *Toward a Framework Understanding of Online Programs for Countering Violent Extremism.* JD Journal for De-radicalization, 6(Spring 2016). p. 51-86

Ditrych, O. (2014) "Concerning Method" and "Enclosure 2000s" In *Tracing the Discourses of Terrorism: Identity, Genealogy and State.* Springer. p. 76-94

Eroukhmanoff, C. (2015) "The remote securitization of Islam in the US post-9/11: euphemisation, metaphors and the "logic of expected consequences" in *counter-radicalization discourse.* Critical Studies on Terrorism, 8:2. p. 246-265

Friis, S. M. (2015) *Beyond anything we have ever: beheading videos and the visibility of violence in the war against ISIS.* International Affairs vol. 91, no. 4, p. 725-746

Geeraerts, S. B. (2012) Digital Radicalization of Youth, Social Cosmos 3(1) 2012, p: 25–32

Gibbs, Graham R. (2007) Analyzing Qualitative Data, Sage Research Methods. p. 38-49; 143-150

Greenberg, K.J. (2016) *Counter-radicalisation via the internet.* The ANNALS of the American Academy of Political and Social Science. Vol 668, Issue 1, p. 165 – 179

Greve, E. B. (2014) *Politiets Efterretningstjeneste – en retlig belysning af tjenesten virksomhed og det samlede kontrolsystem.* Jurist- og Økonomforbundet. p. 13-168

Hansen, L. (2006) *Security as practice,* The New International Relations Series, 1-255

Hansen, L. (2011) *Theorizing the image for Security Studies: Visual securitization and the Muhammad Cartoon Crisis.* European Journal of International Relations, vol. 17, no. 1, p. 51–74

Hansen, L. (2012) Reconstructing Desecuritization: The Normative-Political in the Copenhagen School and Directions for How to Apply It. Review of International Studies, vol. 38, no. 3, p. 525 –546

Hansen, L. and H. Nissenbaum (2009) *Digital Disaster, Cyber Security, and the Copenhagen School.* International Studies Quarterly, 53(4), p. 1155-1175

Hemmingsen, A.S and K. I. Castro (2017) *The trouble with counter narratives*. Danish Institute for International Studies, Report. February 2017. p. 1-48

Horgan, J. and Braddock, K. (2010). Rehabilitating the Terrorists? Challenges in Assessing the Effectiveness of De-radicalisation Programs. *Terrorism and Political Violence, 22*(2), p. 267-291

Jackson, R. (2009) *Critical Terrorism Studies: An Explanation, a Defence and a Way Forward* Paper prepared for the BISA Annual Conference, 14-16 December 2009, University of Leicester, UK. p. 1-25

Jackson, R., Murphy, E. and S. Poyting (2010) 'Introduction: terrorism, the state and the study of political terror' in *Contemporary State Terrorism - Theory and Practice.* Routledge. p. 1-12

Jackson, R. Smyth, M., Gunning J. and L. Jarvis (2011) 'Conceptualizing Terrorism *'in Terrorism: A Critical Introduction,* Palgrave Macmillan, p. 99-124

Jackson, R. (2015) *The Epistemological Crisis of Counterterrorism*. Critical Studies on Terrorism 8 (1). p. 33–54

Jungherr, A. (2014) *The Logic of Political Coverage on Twitter: Temporal Dynamics and Content.* Journal of Communication 64.2. p. 239-259

Klausen, J. (2015) *Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq*, Studies in Conflict and Terrorism 38(1), 2015, p: 1–22

Koehler, D. (2014). *The Radical Online: Individual Radicalization Processes and the Role of the Internet.* Journal for Deradicalization, Winter (2014/15), p. 116-134

Lakomy, M. (2017) *Cracks in the Online Caliphate: How the Islamic State is Losing Ground in the Battle for Cyberspace*. Perspectives on Terrorism. Vol 11, No 3. p. 40-54

Leech, B. L and F. R. Baumgartner, J. M. Berry, M. Hojnacki and D. C. Kimball (2013) "Putting it all together. Lessons from the 'Lobbying and Policy Change' Project in L. Mosley, Interview Research in Political Science. Cornell University Press. New York. p. 209-225

Lindekilde, L. (2015) *Danish prevention of extremism and radicalization 2009:2014: developing trends and future challenges*. Politica, 47. vol. nr. 3. p. 424-444

Lorrand Bodo, M.A. and Speckhart, A. (2017) *The Daily Harvester: How ISIS Disseminates Propaganda over the Internet Despite Counter-Measures and How to Fight Back.* The International Center for the Study of Violent Extremism. p. 1-5

MacLean, L. M. (2013) The Power of the Interviewer in L. Mosley, Interview Research in Political Science. Cornell University Press. p. 67-84

Mavelli, L. (2013) *Between Normalisation and Exception: The Securitisation of Islam and the Construction of the Secular Subject. Millennium.* Journal of International Studies 41(2) p. 159–181

Maxwell, J. (2002) 'Understanding and Validity in Qualitative Research' in Huberman, A. M. and M. B. Miles. *The Qualitative Researcher's Companion.* Sage Publications. p. 36-61

Mosley, L. (2013) Introduction. "Just talk to people"? Interviews in Contemporary Political Science" in L. Mosley, Interview Research in Political Science. Cornell University Press. New York. p. 1-31

Muro, D. (2016) *What does Radicalisation look like? Four visualizations of socialization into Violent Extremism.* Barcelone Centre for International Affairs, p. 1-5

Nissenbaum, H. (2005) *Where computer security meets national security*. Ethics and Information Technology 7. Springer. p. 61–73

Radu, R. (2014) "Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace" in J.F. Kremer and B. Müller, *Cyberspace and International Relations - Theory, Prospects and Challenges*. Springer Heidelberg New York Dordrecht London. p. 3-21

Ramsay, G. (2015) *Why terrorism can, but should not be defined*, Critical Studies on Terrorism, 8:2. p. 211-228

Richards, A. (2015*) From terrorism to 'radicalization' to 'extremism': counterterrorism imperative or loss of focus?* International Affairs 91: 2. p. 371–380

Romaniuk, P. (2015) *Does CVE Work? Lessons Learned From the Global Effort to Counter Violent Extremism.* Global Center on Cooperative Security, September issue. p. 1-50

Rubin, H. J. and I. S. Rubin (2005) *Qualitative Interviewing: The Art of Hearing Data.* Second Edition. Thousand Oaks: London: Sage Publications. 19- 38; 64-78; 108-128; 129-150; 151-172; 201-223

Schofield, J.W. (2002) 'Increasing the Generalizability of Qualitative Research' in Huberman, A. M. and M. B. Miles. The Qualitative Researcher's Companion. Sage Publications. p. 171-202

Sheikh, J. (2016) "*I Just Said It. The State": Examining the Motivations for Danish Foreign Fighting in Syria.* Perspectives on Terrorism. Vol 10, issue 6. p. 59-67

Sjöstedt, R. (2017) Securitization Theory and Foreign Policy Analysis, Politics. Oxford Research Encyclopedias, April 2017, p. 1-18

Stephens, A. C. and N. Vaughan-Williams (2010) *Terrorism and the Politics of Response.* Routledge. p. 1-17; 60-79

Thorup, M. (2010) *An Intellectual History of Terror - War, violence and the state.* Routledge. p. 1-58

Torok, R., 'Developing an Explanatory Model for the Process of Online Radicalisation and Terrorism', *Security Informatics* 2(6), 2013, p. 1–10

Urqhart, C. (2013) *Grounded Theory for Qualitative Research: A Practical Guide*, London. Sage Publications. p. 78-105; 106-126

Walker, C., and Conway, M. (2015) *Online Terrorism and Online Laws*, Dynamics of Asymmetric Conflict 8(2), p. 156–175

Williams, M.C. (2014) 'Securitization as politica theory: The politics of the extraordinary. in Balzacq T., Guzzini S., Williams M. C., Wæver, O., and Patomäki, H. *Forum: What kind of theory—if any—is securitization?* P 19- 25

Wæver, O. (2014). 'The Theory Act: Responsibility and Exactitude as seen from Securitization'. in

Interviews conducted in the spring and summer of 2017:

The Danish Foreign Ministry – April 28, 2017 (43 min)

The Danish Ministry of Justice – April 24, 2017 (48 min)

The Danish Ministry of Justice Research department – May 6, 2017 (Skype interview 24 min)

The National Centre for Prevention (NCP) – May 25, 2017 (Skype interview: 51 min)

The Ministry of Immigration and Integration – June 28, 2017 (Written interview)

The Municipality of Copenhagen – May 3, 2017 (Skype interview 28 min)

Researcher on Central Intelligence Services (CIS) – May 11, 2017 (Skype interview: 38 min)

Classified contact within the Danish Foreign Ministry – May 1, 2017 (55 min)

Websites:

Gemmerli, T. (2014) "Radicalisation: a battle between politics and science" in *Udenrigs. Tema: Radikalisering.* The Danish Foreign Policy Society. p. 4-15 (online). Available at: http://udenrigs.dk/wp-content/uploads/2015/03/Udenrigs_3_2014_Web.pdf
Published December 2014
Read on November 7, 2017

Gemmerli, T. (2016) *Avoid the pitfalls of counter-narratives.* Danish Institute for International Studies. Policy Brief. p. 1-4 (online). Available at: http://pure.diis.dk/ws/files/633658/Undg_modnarrativernes_faldgruber_til_webben.pdf
Published in September 2016
Read on November 1, 2017

Gemmerli, T. and J. Teglskov Jacobsen (2014) *Censorship on social media is not a good idea,* Danish Institute for International Studies, Policy Impact. p. 1-2 (online). Available at: http://pure.diis.dk/ws/files/79796/Censur_er_en_d_rlig_ide_IMPACT_forweb.pdf
Published in November 2014
Read on November 17, 2017

Gjerding, A. and L. Skou Andersen (2016) *Denmark purchase surveillance system from NSA supplier,* Information. p. 1-5 (online). Available at https://www.information.dk/indland/2016/10/danmark-koeber-overvaagningssystem-millioner-nsa-leverandoer
Published on October 28, 2016

Read on November 14, 2017

Lafree, G. (2017) *6 reasons why stopping worldwide terrorism is so challenging*. The Conversation – Academic rigour, journalistic flair p. 1-5 (online). Available at https://theconversation.com/6-reasons-why-stopping-worldwide-terrorism-is-so-challenging-70626
Published May 22, 2017
Read on November 13, 2017

Meleagrou-Hitchens, A and N. Kaderbhai (2017). *Research Perspectives on Online Radicalisation: A Literature Review 2006-2016*. Kings College London. p. 1-74 (online). Available at http://icsr.info/wp-content/uploads/2017/05/ResearchPerspectivesonOnlineRadicalisation.pdf
Published April 30, 2017
Read on November 15, 2017

Municipality of Copenhagen (2016) *Efforts by the municipality of Copenhagen to prevent radicalisation.* Municipality of Copenhagen. p. 1-47 (online). Available at: https://www.kk.dk/sites/default/files/edoc/e893f1d0-8b2d-4cc2-867d-5378ee177bd3/21df14fa-4608-4639-8b79-6aadd9e09525/Attachments/15361379- 18737342-1.PDF
Published May 2016
Read on November 2, 2017

Parliament (2017) *Referatet af Folketingets forhandlinger: 1. behandling af lovforslag nr. L 171: Forslag til lov om ændring af lov om politiets virksomhed og toldloven. (Politiets anvendelse af databaserede analyseredskaber og adgang til oplysninger om flypassagerer).* Meeting number 85. The first reading of the bill. p. 1-10 (online). Available at http://www.ft.dk/samling/20161/lovforslag/L171/BEH1-85/forhandling.htm#dok
Published on April 25, 2017
Read on November 14, 2017

SUS – Social Development Centre (2017) *Hackathons for young people* (online). Available at: https://www.sus.dk/cases/hackhadet-hackathons-for-unge/
Published in September 2017
Read on November 29, 2017

Talbot, D. (2015, September 30). Fighting ISIS Online. *MIT Technology Review*. p. 1-10 (online). Available at: https://www.technologyreview.com/s/541801/fighting-isis-online/
Published on September 30, 2017
Read on November 10, 2017

The Danish Foreign Ministry (2016) *Redegørelse af indsatsen imod terrorisme. Maj 2016.* p. 1-19 *(*online). Available at http://um.dk/~/media/UM/Danish-site/Documents/Udenrigspolitik/Nyheder_udenrigspolitik/2016/Redegrelse%20-%20Indsatsen%20mod%20terrorisme%202016.pdf?la=da
Published on May 2016
Read on November 21, 2017

The Danish Ministry of Justice (2016) *Regeringen opruster I kampen mod parallelsamfund* p. 1-3 (online). Available at http://justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2016/regeringen-opruster-i-kampen-mod-parallelsamfund
Published on October 11, 2016
Read on November 11, 2017

The Danish Ministry of Justice (2017) *Forslag til Lov om ændring af lov om politiets virksomhed og toldloven (Politiets anvendelse af databaserede analyseredskaber og adgang til oplysninger om flypassagerer)* (L171) p 1-8 (online) Available at https://www.retsinformation.dk/forms/R0710.aspx?id=188277
Published on March 29, 2017
Read on November 8, 2017

The Danish National Action Plan (2016) *Countering and Preventing Violent Extremism.* p. 1-36. (online). Available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/docs/preventing_countering_extremism_radicalisation_en.pdf
Published on October 2016
Read on November 12, 2017

Von Behr, I., Reding, A., Edwards, C., and Gribbon, L. (2013) *Radicalisation in the digital era. The use of the internet in 15 cases of terrorism and extremism*. Brussels: RAND Europe. p. 1-76 (online). Available at http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf
Published July 2013
Read on November 11, 2017

Winter, C. and J. Bach-Lombardo (2016) Why ISIS propaganda works and why stopping it requires that government get out of the way. The Atlantic. p. 1-8 (online). Available at https://www.theatlantic.com/international/archive/2016/02/isis-propagandawar/462702/
Published on February 13, 2016
Read on June 08, 2017

About the JD Journal for Deradicalization

The JD Journal for Deradicalization is the world's only peer reviewed periodical for the theory and practice of deradicalization with a wide international audience. Named an "essential journal of our times" (Cheryl LaGuardia, Harvard University) the JD's editorial board of expert advisors includes some of the most renowned scholars in the field of deradicalization studies, such as Prof. Dr. John G. Horgan (Georgia State University); Prof. Dr. Tore Bjørgo (Norwegian Police University College); Prof. Dr. Mark Dechesne (Leiden University); Prof. Dr. Cynthia Miller-Idriss (American University Washington); Prof. Dr. Marco Lombardi, (Università Cattolica del Sacro Cuore Milano); Dr. Paul Jackson (University of Northampton); Professor Michael Freeden, (University of Nottingham); Professor Hamed El-Sa'id (Manchester Metropolitan University); Prof. Sadeq Rahimi (University of Saskatchewan, Harvard Medical School), Dr. Omar Ashour (University of Exeter), Prof. Neil Ferguson (Liverpool Hope University), Prof. Sarah Marsden (Lancaster University), Dr. Kurt Braddock (Pennsylvania State University), Dr. Michael J. Williams (Georgia State University), and Aaron Y. Zelin (Washington Institute for Near East Policy).

For more information please see: www.journal-derad.com

Twitter: @JD_JournalDerad
Facebook: www.facebook.com/deradicalisation

The JD Journal for Deradicalization is a proud member of the Directory of Open Access Journals (DOAJ).

ISSN: 2363-9849

Editors in Chief: Daniel Koehler, Tine Hutzel