JOURNAL FOR DERADICALIZATION

Spring 2016
Nr. 6
ISSN: 2363-9849

Toward a Framework Understanding of Online Programs for Countering Violent Extremism

By: Garth Davies[1]

Christine Neudecker[2]

Marie Ouellet[3]

Martin Bouchard[4]

Benjamin Ducol[5]

Abstract

There is an emerging consensus that ideologically-based narratives play a central role in encouraging and sustaining radicalization to violence, and that preventing, arresting, or reversing radicalization requires some means by which to address the effects of these narratives. *Countering violent extremism* (CVE) is a broad umbrella phrase that covers a wide array of approaches that have been advanced to reduce the radicalizing effects of extremist narratives. There is considerably less agreement, however, regarding the most appropriate means by which the mitigation of extremist narratives might best be accomplished. An important emerging area of interest is the role of the Internet, both as a forum through which narratives are transmitted and as an avenue for delivering CVE programs. At present, very little is known about which principles and practices should inform online CVE initiatives. This study attempts to establish a foundation and framework for these programs: first, by identifying the concepts and constructs which may be most relevant to countering violent extremism online, and second, by examining the available material from six online CVE programs in relation to these concepts. This examination suggests that these programs are lacking strong theoretical foundations and do not address important elements of radicalization, such as contextual factors or identity issues. It is important that future iterations of CVE programs consider not just the specific content of the narratives, but also take into account why these narratives have resonance for particular individuals.

Author's Note: The authors wish to thank Public Safety Canada for their generous support of the research on which this article is based. The article has been adapted from material found in, Her Majesty the Queen in Right of Canada, "Assessment of the State of Knowledge:

[1] Simon Fraser University

[2] Simon Fraser University

[3] Simon Fraser University

[4] Simon Fraser University

[5] Research affiliate, International Centre for Comparative Criminology, Université de Montréal.

Connections between Research on the Social Psychology of the Internet and Violent Extremism." The views expressed in the current article only engage the authors.

Introduction

Recently, the appearance of countering violent extremism (CVE) programs has garnered the attention of both researchers and policy makers alike. These programs are perceived by many as to central to the process of addressing the pressing need to combat radicalization to violence. At the same time, the relatively recent influx of these programs has raised a variety of questions. In particular, policy makers and practitioners are being asked to account for the effectiveness of these programs. Simply put, CVE programs have been around long enough for people to begin to inquire as to whether or not they work. Although CVE programs in the online milieu are comparatively new, they are facing similar questions. But while there is burgeoning interest in the evaluation of CVE programs, it is possible to argue that the foundations of these initiatives are not sufficiently understood, and that a better foundation is required before such assessment are undertaken.

This study aims to better understand online CVE programs in two ways. First, by reviewing the literature on radicalization with an eye to identifying the concepts and constructs which may be most relevant to countering violent extremism online. This literature is then used to create a 'good practices' model for developing online CVE programs, based on recommendations across CVE scholars. Second, this model is applied to eight online CVE programs to examine to what extent, if any, they incorporate these practices. This study concludes by discussing possible implications of the findings.

Radicalization and the Internet

Broadly speaking, radicalization is the process by which individuals come to adopt radical or extremist views and ideas (Jensen, 2006). Radicalization might be best understood as the mental component of the process that leads to extremism. It has been described as the process by which individuals "are introduced to an overtly ideological message and belief system that encourages movement from moderate, mainstream beliefs toward extreme views" (Smith, 2009, p. 1). In and of itself, radicalism is not necessarily problematic (Kühle &

Lindekilde, 2010, p. 23). Radicalization is an issue, however, when it involves individuals gradually adopting views that favour, condone, or legitimize political violence as a legitimate avenue for action. Put another way, the concern here is with violent radicalization, whereby radical ideas develop into “a willingness to directly support or engage in violent acts” (Dalgaard-Nielsen, 2010, p. 798). It is important to note that violent radicalization is not limited to the perpetration of violence. Terrorist and extremist groups rely on a base of radicalized supporters, many of whom may never actually commit acts of violence, but who are nonetheless willing to support the use of violence for advancing their agenda.

Despite several areas of disagreement regarding what exactly is covered by the concept of radicalization (Sedgwick, 2010), there is an emerging consensus on what factors converge to produce violent radicalization. Hafez and Mullins (2015), for example, identify four such factors: grievances, or “root causes” that set the stage for radicalization; social networks, which facilitate recruitment to the movement; ideology, the discursive narratives the bind individuals to the cause, and enabling environments and support structures, including the internet. The first three of these factors are very common to the radicalization literature and have been discussed at length by numerous authors. The fourth factor, enabling factors, have also been considered previously. However, the specific role of the internet in radicalization remains contentious.

There seems to be little doubt that the Internet is increasingly implicated in the radicalization process. With regard to the West, it has been argued that radicalization is predominantly taking place online. There are many examples of individuals who have radicalized with the help of the Internet (Neumann, 2013). Jenkins (2010) remarks that many of the terrorists studied since 9/11 began their journeys on the Internet. This is hardly surprising, given the ubiquitous nature of the Internet in relation to Western lives, particularly the lives of young people who are the primary targets of radicalization efforts.

There are a wide variety of perspectives on how online radicalization works. At the most basic level, the issue concerns the effects of exposure to particular forms of content. The Internet is a vast repository of information. In relation to radicalization, the Internet allows extremist groups to disseminate their messages and ideologies, as well as videos (Davies et al., 2015). These ideologies and videos have the potential to inspire radicalization. Pauwels and Schils (2016) clearly demonstrate that active extremist content and exposure to extremism through new social media are strongly associated with self-reported political violence. On one hand, video images may produce a sort of "awakening" within individuals who are becoming aware of issues for the first time. Muslims in the West may be introduced to events in areas such as Iraq, Syria, Chechnya, and Palestine. On extremist sites, these events will be framed as atrocities to be avenged. On the other hand, for those who are already leaning toward extremist viewpoints, such content may serve to harden opinions. The power of these messages may be amplified by graphic video images. Sageman (2008a), for example, maintains that shocking videos may trigger a "sense of moral outrage" (Jasper, 1997) that could mobilize people to violence. More generally, research has confirmed that the Internet both creates a greater number of opportunities to be radicalized and accelerates the process of radicalization (von Behr, Reding, Edwards, and Gribbon, 2013).

From a social psychological perspective, it is important to consider the context of exposure to and the context of reception of extremist contents and discourses. It is highly unlikely that mere exposure, in and of itself, is enough to promote radicalization and set individuals down the path to violence. Instead, responses to extremist content are conditioned by the environment within which they are received. Neumann (2013:435) contends that "no single item of extremist propaganda is guaranteed to transform people into terrorists. Rather, in most cases, online radicalization results from individuals being immersed in extremist content for extended periods of time, the amplified effects of graphic images and video, and the resulting emotional desensitization." The themes of immersion and amplification are reflected in the characterization of online forums as "echo chambers", places largely devoid of dissent, where moderating influences are drowned out by more extreme voices (Gerraerts, 2012). Out of these insular environments emerges a powerful "groupthink" marked by violence. Attitudes supportive of violence may also be fostered by the form of the Internet, particularly what has been referred to as Web 2.0, with its emphasis on interactivity, graphic images, and video content. It has been suggested that extended exposure to and immersion in extremist content amplifies their effects (Neumann, 2013). The resulting desensitization to violence, or "online disinhibition" (Suler, 2004), further polarizes groups and may increase the likelihood of violent actions.

More generally, the primary role for the Internet in the radicalization process is the extent to which it facilitates social networks, ultimately culminating in virtual communities (Ducol, 2012). Bowman-Grieve (2009) argues that these communities are real social spaces that are important because "they encourage the construction of political and ideological discourses supporting and justifying the use of terrorism and political violence" (p. 990). Utilizing the example of Stormfront, a radical right-wing forum, Bowman-Grieve (2009) demonstrates how forums can provide validation for personal grievances, which in turn may result in individuals deepening their involvement with the extremist cause. Virtual communities such as Stormfront are key social arenas for the formation of the types of interpersonal bonds that are central to the radicalization process. Recent research indicates that the Internet is a signficant driving factor in the development of "radical contrast societies" (Koehler, 2014), which foster the transmission of violent radical ideologies and aids in translating these ideologies into political activism.

Owing at least in part to social media, the Internet has fundamentally altered the manner in which individuals participate in social movements. Halverson and Way (2012) maintains that the Internet functions as a "contact point", a "social nexus that facilitates the formation of relationships among previously unrelated entities" (p. 140). Drawing on the case of Colleen LaRose (a.k.a. JihadJane), Halverson and Way (2012) illustrate how social media enables isolated and marginalized individuals to experiment with and construct new identities as member of a community that values the individual. These new identities, and the concomitant acceptance, become a source of self-respect, dignity, and personal meaning. Extremist movements function online by offering individuals a connection and an opportunity to espouse their ideas in a supportive environment. In fact, one of the greatest challenges of the Internet is the manner in which it brings together people with anti-social interests and provides "easy access to ideological structures that provide some semblance of order, a renewed sense of self, and greater meaning to troubled realities" (Halverson & Way, 2012, p. 148). In this way, the Internet has become the locus for gathering and coordinating marginalized individuals.

In its most extreme form, this socializing aspect of the Internet can even be extended to include so-called "lone wolves". Weimann (2012) maintains that lone-wolf terrorists are not really alone. Few lone wolf attackers are really alone; despite the appearance of solitude, there is usually evidence of social ties linking them to others. Many of these lone-wolves have been radicalized via online platforms. Pantucci (2011) comments that "many of the [lone-wolves] demonstrate some level of social alienation – within this context, the community provided by the Internet can act as a replacement social environment that they are unable to locate in the real world around them" (p. 34). Simply put, radicalization is a social phenomena, and lone-wolves are not exempted.

There is, moreover, a potentially darker aspect to social networks and virtual communities. In contrast to the implied vision of individuals connecting with a like-minded community, it is also possible that there is a level of coercion involved. It is worth remembering that many of those individuals that extremist groups would like to radicalize and recruit are highly vulnerable. Extremist groups are primarily targeting individuals who are young, disillusioned, alienated, isolated and marginalized (Seib & Janbek, 2011; Decker & Pyrooz, 2015). These groups can use the Internet to manipulate grievances and lure individuals with promises of friendship, acceptance, and a sense of purpose. "Users may one day find themselves down the proverbial radical rabbit hole" (Thompson, 2011, p. 168). Sageman (2008a) holds that one of the most problematic aspects of the Internet is the degree to which individuals can be influenced by other participants on extremist forums. These milieus can do more than merely reinforce and solidify perspectives. Sageman indicates that individuals can have their minds changed through their participation in these forums.

Not often recognized in the extant research on the role of the Internet in radicalization are the opportunities to use it to reverse the process of radicalization, and potentially counter violent extremist narratives. If the Internet is a powerful medium to first expose, and then facilitate the radicalization process of many individuals, such power to reach young populations can be used for pro-social purposes (Neumann, 2013; Bouchard & Thomas, 2015). While many counter-narrative programs exist, their effectiveness as a dissuasive or preventative tool has yet to be assessed. The existing work on countering violent extremism online is reviewed below to frame the analysis of how they align with current online CVE programs.

Countering Violent Extremism Online

Countering violent extremism is a broad umbrella phrase that covers a wide array of possible approaches to dealing with radicalization to extremist violence. To keep this literature review on point, several key distinctions must be made. First, the demarcation line between countering violent radicalization and deradicalization is often unclear. The concepts are related, connected by their focus on the cognitive (as opposed to behavioral) aspect of radicalization (Horgan, 2008). They are also linked by their mutual recognition of the importance of the importance of both narratives and credible messengers (Ashour, 2010). But there are also subtle differences between CVE and deradicalization, particularly the extent to which associated campaigns are designed as tools for prevention or intervention. Although most programs do not explicitly differentiate, they appear to predominantly preventive in nature.

Second, CVE efforts may take place offline, online, or involve some combination of the two. In keeping with the focus of this paper, this review is primarily aimed at CVE initiatives that include at least some online component. Finally, online CVE programs are routinely divided into positive and negative measures. In general terms, positive CVE strategies are those that "seek to challenge extremist narratives and propaganda by producing counter-content," while negative strategies are designed to "block, filter, take-down or censor extremist content" (Hussain & Saltman, 2014, p. 10). Western governments have tended to be more concerned with negative measures, technological "solutions" aimed at restricting the supply of extremist content on the Internet (for discussion of the full range of negative measures, see Stevens and Neumann, 2009). However, the potential effectiveness of such measures is subject to a number of practical (Briggs & Feve, 2013) and political (Hussain & Saltman, 2014) limitations. There is simply too much content on the Internet to try to sift through it all; it is too difficult and expensive to block, filter, or censor content; and even if it were possible, there are issues surrounding what properly constitutes "extremist content" that have thus far remained resistant to resolution. As Briggs and Feve (2013) note, "only a tiny fraction of extremist content is actually illegal" (p. 5).

While governments continue to mine for efficacious negative measures, attention has increasingly turned to trying more positive CVE means. For example, Stevens and Neumann (2009) have proposed a number of alternatives. They recommend empowering online communities by creating Internet user's panels that would be charged with "raising awareness of reporting mechanisms for unacceptable content; monitoring companies' complaints procedures; highlighting best and worst practices; facilitating partnerships between Internet companies and non-governmental organizations; and serving as an ombudsman of last resort" (p. 31). They further suggest reducing the appeal of extremist content by increasing media literacy through schools and other stakeholders. Finally, Stevens and Neumann (2009) support the establishment of a funding agency, independent of the government that could support the promotion of positive messages. Projects would be funded through small grants, and projects evaluated as having positive effects would be eligible to apply for more funding.

Related to this last point, attention has increasingly turned to counter-messaging as a central response to violent extremism. In contrast to more negative and reactive orientations, counter-messaging is a more proactive approach, one that "focuses on reducing the demand for such content by undermining its appeal through offering credible alternatives" (Briggs & Feve, 2013, p. 5). Counter-messaging activities exist along a spectrum (Briggs & Feve, 2013). One type of counter-messaging involves government strategic communications, which essentially involve "getting the message out." The goal of strategic communications is for the government to raise awareness of what it is doing and to forge positive relationships with key constituencies. Counter-messaging may also take the form of alternative narratives, positive stories about "social values, tolerance, openness, freedom and democracy (Briggs & Feve, 2013, p. 5). Schmid (2014) maintains that alternative narratives should be able to bridge the "us" versus "them" divide that is fostered by extremists and bring together people from all sides. They should focus more on "what we are for" and less on "what we are against". Whereas strategic communication is the purview of government, alternative narratives may be issued both government and civil society activists and groups. Finally, counter-messaging may be realized through counter-narratives. This approach has become central to CVE, and is the focus of the remainder of this literature review.

A narrative has been described as a “simple unifying, easily-expressed story or explanation that organises people’s experience and provides a framework for understanding events” (Kilcullen, as cited by Schmid, 2014, p. 3). These interpretations, deeply rooted in culture, can in turn encourage specific types of personal action (Corman, 2011). Narratives are powerful because they hold the pieces of the story and “ring true” for members of the target audience (Goodall, 2010). Schmid maintains that one of the keys to understanding the ascendance of al-Qaeda’s ideology is understanding the extent to which it functions as a single narrative. “[It is] a unifying framework of explanations that provides its followers with an emotionally satisfying portrayal of the world in which they live and their role in it, offering them a sense of identity and giving meaning to their lives” (2014, p. 5). Extremist violence, then, is supported by convincing narratives that justify violence.

To the extent that narratives form the foundation of the appeal of extremism, and if counter-narratives are to serve as a vital element in CVE strategies, it is important to understand what constitutes a strong narrative. Schmid (2014, p. 29) has identified the following as the ingredients of an effective narrative: 1. It has to articulate a clear, realistic and compelling mission purpose without getting entangled in sub-goals and details, but keeping the focus on long-term, overarching goals that have to be related to cultural norms and values as well as interests; 2. It has to have legitimacy in that it matches cultural and public norms and values and is seen by relevant publics as justified; 3. It has to hold the prospect of success and provide a feeling of progress towards its goals; 4. The narrative has to be presented in a consistent manner in order to be effective and withstand the attacks of counter-narratives that might cost it public support; and 5. The narrative must fit within an overall communication plan that reflects major themes of our own identity.

Counter-narratives represent attempts to directly or indirectly challenge violent extremist messages (Briggs & Feve, 2013). These programs can function both online and offline, and many initiatives utilize both platforms. This approach is premised on trying to win the ‘battle of ideas.’ Counter-narratives highlight what is wrong with extremist ideologies, challenge assumptions, expose fallacies, and dismantle associated conspiracy theories (Schmid, 2014). It involves creating and promoting narratives that stand in opposition to those presented by extremists and is intended to undermine extremist ideologies and compete for the 'hearts and minds' of potential recruits (Aldrich, 2014; Berger & Strathearn, 2013). The idea behind counter-narratives is relatively straightforward, but its application in practice is much more complicated. Much of the literature on counter-narratives is currently centered on understanding how best to construct effective counter-narrative programs.

Current Study

The current study looks at whether current CVE programs are designed according to the 'good practices' put forward by CVE scholars. To do this, it first merges the work of three CVE scholars, who have outlined good practices for designing counter-narrative programs. Next, the grid is applied to six online CVE programs to examine the extent to which they incorporate or neglect these practices. Rather than representing an evaluation of CVE programs, which would require presently unavailable measure of effectiveness, this study instead take a first step towards assessing whether these programs are created on firm theoretical foundations based on the recommendations of CVE scholars.

Designing Online CVE Programs

The 'good practices' model utilized here draws on the efforts of previous CVE scholars who have identified what works, and what doesn't, in the context of CVE programs. Specifically, the model is premised on work conducted by USAID (2009), the International Centre for the Study of Radicalisation and Political Violence (Stevens & Neumann, 2009), the Institute for Strategic Dialogue (Briggs & Feve, 2013), and Braddock and Horgan (2015). These reports and articles were selected based on their focus on outlining the most effective measures for countering online violent extremist narratives.

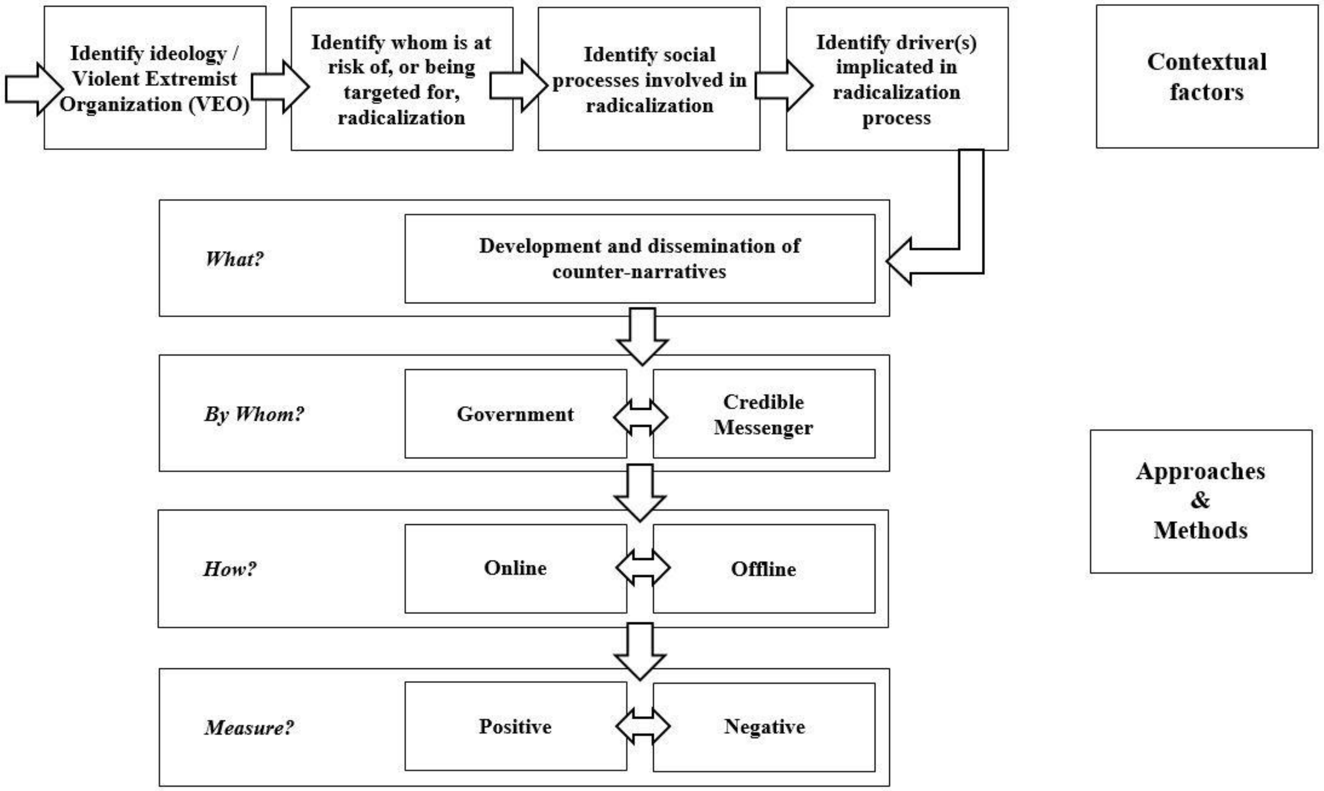
Identify ideology / Violent Extremist Organization (VEO)
Identify whom is at risk of, or being targeted for, radicalization
Identify social processes involved in radicalization
Identify driver(s) implicated in radicalization process
Contextual factors
What?
Development and dissemination of counter-narratives
By Whom?
Government
Credible Messenger
How?
Online
Offline
Measure?
Positive
Negative
Approaches & Methods

Figure 1. CVE Program Structure

Figure 1 combines the work of USAID (2009), Briggs and Feve (2013), Stevens and Neumann (2009), and Braddock and Horgan (2015) to outline the process required for building counter-narrative programs. Each set of CVE scholars focused on different aspects of building effective CVE programs. USAID (2009) primarily addressed contextual factors, to understand the specific mechanics of the radicalization process. Braddock and Horgan (2015) provided a detailed description of how to develop counter-narratives. Briggs and Feve (2013) concentrated on the medium through which CVE programs are delivered, distinguishing between government and non-government actors in providing counter-narratives. Stevens and Neumann (2009) primarily looked at the different types of approaches that may be used in an online context, distinguishing between positive and negative approaches, that is, the difference between removing and blocking online content versus providing content that counters radical perspectives, respectively. Together, these four approaches complement one another, providing a set of guidelines to consider when developing a CVE program.

As illustrated in Figure 1, the process of CVE development begins generally with the specification of a variety of contextual factors. First, identify the violent extremist organization or ideology that is to be the target of the intervention. Second, identify the individuals who are being targeted, or who are most likely to be targeted. This involves determining which individuals are most vulnerable to being influenced by the extremist narrative and are thereby more at risk of recruitment and/or radicalization. Third, determine the social processes used for radicalization. Social processes refer to the nature and mechanics of the radicalization process, and addresses questions such as: “Are individuals being recruited?” “At what venues is recruitment occurring?” and “What is the role of peer groups and social networks?” Finally, establish which types of drivers – political, socioeconomic, cultural, or a combination thereof – are pushing and/or pulling individuals toward violent extremist radicalization. Of note, the contextual approach presented by USAID (2009) assumes that the radicalization process rests largely on the active efforts of extremist groups and ideologues. This perspective is not without critics, as other researchers have argued for a more “bottom up” approach that emphasizes individual initiative (Sageman, 2008b; Hoffman, 2008). Nonetheless, this framework is broadly useful for identifying and understanding those factors that provide context and 'set the stage' for the acceptance of extremist narratives and radicalization to extremist violence.

After the contextual factors have been assessed, the next step in the process is to determine what approach will be used. As noted earlier, there are a wide variety of possible CVE approaches from which to choose. The focus here is on counter-narratives. Braddock and Horgan (2015) maintain that effective counter-narratives must identify key themes in the extremist narrative and then develop responses that reveal incongruities and contradictions in those narratives. Other aspects of the counter-narrative would include contesting often misleading or invalid analogies that support extremist narratives and disrupting the binary nature of these narratives (Braddock and Horgan, 2015). Counter-narratives should not merely attempt to tear down the extremist narrative, but rather, rebut it and provide and alternative interpretation of reality.

Regardless of the specific approach, all CVE initiatives must determine who will develop and deliver the program. This issue is particularly notable for counter-narrative programs. More precisely, the question is "what should be the role of government" in relation to counter-narratives? Briggs and Feve suggest that "governments must tread with caution in the area of counter-messaging … their efforts can be ineffective or even counter-productive when they act as the messenger, due to their credibility gap with target audiences, which often gets in the way of what they have to say" (2013, p. ii). This is not to say that there is no role for government. As noted above, governments can fruitfully engage in both strategic communications and alternative narratives. But much of the counter-narrative work increasingly relies on the identification of credible messengers, especially former violent extremists and survivors of extremist violence (Braddock and Horgan, 2015). These messengers have unique insights, and their experiences carry weight (e.g. Helmus et al., 2013). Their messages are perceived as having greater authenticity. Credible messengers would also include scholars or persons that hold expertise in the information that is being countered. Using the Islamic State (IS) as an example, a credible messenger could be a religious scholar who can relay the proper interpretations of Islamic religious texts.

The final considerations in Figure 1 are the "how" of the program (that is, how is the program to be delivered), and the nature of the measures employed. As noted earlier, CVE efforts, including counter-narratives, can be delivered online, offline, or via a hybrid approach, and can consist of positive or negative measures (or some combination of the two). Together, all of these considerations provide a method to systematically outline key elements of CVE efforts across initiatives.

Programs for Countering Violent Extremism Online

The current section applies these best practices identified across CVE scholars to assess whether they are being implemented in current online CVE programs. Six online CVE programs were selected for review, based on four main criteria. The first consideration was practical, requiring programs that have detailed information on their objectives, their target population, and how their objectives are implemented. Second, consistent with the research objectives, all programs had to have an online component. Third, programs were favoured, to the extent that they appeared to contain many of the elements associated with "good practices" for countering violent extremism, based on consistencies with the radicalization literature. Lastly, we attempted to capture a range of programs to reflect the diversity of approaches currently being implemented to counter violent extremism.

While all programs have an online component they vary in the extent to whether they are delivered in online or offline contexts. Across the six programs, the majority targeted jihadist-motivated extremists (n=3), while two targeted all types of violent extremism, and one focused only on white supremacist motivated extremists. The programs also differed in terms of how they attempted to counter violent extremism. Most programs aimed to provide counter-narratives, offering evidence-based arguments to counter extremist voices (n=4), while others focused on educating youth on appropriate Internet behaviour (n=1), or educating and providing recommendations to policymakers on violent extremism (n=1). All programs were implemented in Western contexts, including Australia, Canada, and the United States. This section first provides a description of each program and then examines the extent to which they align with guidelines outlined by CVE scholars.

1. Youth online and at risk: Radicalization facilitated by the Internet

Youth online and at risk: Radicalization facilitated by the Internet is a program delivered as a report produced by the RCMP (http://www.rcmp-grc.gc.ca/nsci-ecsn/rad/rad-eng.htm). It is a four-step program targeting parents, caregivers, and teachers of youth who are active online (RCMP-GRC, 2011). This first step encourages two-way conversation between an adult and youth concerning online content appropriateness and expectations of behavior when content is found to be inappropriate. The second step is to leverage existing programs. This step involves developing ways to keep youth safe from Internet threats. Some examples that are stated in the report are software controls, monitoring download activity, keeping the computer in an open space/community area, developing "what if" scenarios, and consulting website reviews. The third step is to reach out to their space, emphasizing the importance of genuine connections. The fourth step is reporting material of concern. This highlights the importance of avoiding inappropriate content as well as reporting this content when it is found.

2. Campaign Against Violent Extremism

The Campaign Against Violent Extremism (CAVE) is a project jointly created by the BC Muslim Association and the RCMP (The BC Muslim Association, 2015). The program is premised on notion that the misunderstanding of Islam and improper interpretation of religious Islamic texts are key drivers in today's conflicts. In response, the principal goal of this program is to increase the awareness and knowledge of 'mainstream' Islam, offer correct interpretations of Islamic texts, and counter those voices that are offering radical interpretations of Islamic religious doctrine. CAVE delivered three community forums in Surrey and Burnaby, BC, in 2014. Advertised with the tagline "Dare to be Informed," these forums are designed as community educational experiences, as opportunities for members of the public to ask questions and raise their concerns. (The BC Muslim Association, 2015). According to Mufti Assim Rashid, the objectives of CAVE are to deal with the radicalization of youth, to create a preventive campaign to educate Muslims and non-Muslims, and to tackle how non-Muslims feel about Muslims.

3. Against Violent Extremism

Against Violent Extremism (AVE) was originally launched at the 2011 Summit Against Violent Extremism in Dublin. It is a unique private sector partnership between the Institute for Strategic Dialogue (ISD), Google Ideas, the Gen Next Foundation and rehabstudio and is currently being managed by ISD in London. AVE is a global network of former extremists and survivors of extremism that leverages the lessons, experiences and networks of individuals who have dealt first-hand with extremism. Its official aims are "to prevent the recruitment of 'at risk' youth and encouraging the disengagement of those already involved." AVE uses technology to connect, exchange, and disseminate information and perspectives on violent extremism. The network does not focus on any particular extremist narrative or ideology; instead, it is dedicated to countering all types of violent extremism (from far right and far left to AQ-linked and inspired and gangs).

AVE is a private sector venture with no government assistance. Members – subject to approval from management – join this network from all over the globe to interact and converse with former extremists and each other to combat extremist narratives. AVE is designed to be inclusive. Members have the option of adding their own counter-narrative project to the wide array already available. Through its various media platforms, members can stay in touch, share ideas, collaborate, find investment and partners, and project their messages to wider audiences.

4. EXIT White Power

EXIT White Power is one of several initiatives offered by All Together Now, a national, independent, not-for-profit organization dedicated to erasing racism in Australia. All Together Now seeks to achieve its vision of an Australia that embraces cultural diversity and is free from racism by promoting the prevention of racism using creating innovative, evidence-based and effective social marketing that is positive, provocative and courageous. Its work targets the behaviour of the 40 percent of adult Australians who are ambivalent about cultural diversity by engaging the 50 percent of adult Australians who are already positive about diversity and encourage them to speak to their ambivalent friends, colleagues and family members. All Together Now's strategic plan is to facilitate a national conversation about racism that will lead to: improved racial literacy among Australians; increased confidence among Australians to speak up when they witness racism; change in behaviour of the 40 percent of Australians who are ambivalent about cultural diversity; and a greater understanding of the types of activities that effectively reduce racism in the Australian context (http://alltogethernow.org.au).

As part of All Together Now's overall program, EXIT White Power (EWP) was launched in October 2012. Utilizing a website (http://exitwhitepower.com), Facebook discussion page (https://www.facebook.com/wptalksau) and Twitter (https://twitter.com/exitwhitepower), the goal of EWP is to challenge recruitment efforts of white extremist organizations to prevent more young people from becoming involved in white nationalism and white supremacy. By monitoring the content of white supremacist discussions online and responding by writing and publishing evidence-based counter-arguments that debunk myths and conspiracy theories, EWP seeks to build resilience to white nationalism by planting a seed of doubt among young men at risk of being involved. EWP has found that writing counter-arguments and ridiculing the narratives, ideology and conspiracy theories of white supremacists can help to dissuade young people from becoming involved. It also concludes that Trojan advertising coupled with Search Engine Optimisation (SEO) and discussion on white supremacy forums have thus far been the most successful tactics for attracting attention to evidence-based counter-arguments.

EWP notes that individuals who are at risk of radicalisation may become more entrenched if counter-narrative activities are not combined with an opportunity for young people to have two-way conversation with the experts. To this end, EWP has focused on creating a resource for front-line workers so that they are better equipped to have this conversation with at risk young people. The publication, *Responding to White Supremacy: A Guide for Frontline Workers*, is available for download on the EWP website. It is intended for use by all frontline workers, including youth workers, social workers, counsellors, psychologists, teachers and police, and includes information on: the white supremacist movement in Australia; why people get involved in white supremacy and who is most at risk; how white supremacy groups operate; the radicalisation process and how to recognise it; and assisting someone involved/at risk of involvement in white supremacy group.

The website has several other notable features. There is an Information for Community Workers section that, in addition to the frontline workers' guide, includes additional sources of information on how "you and your community can respond to individuals at risk of involvement in white supremacy." There is also a section on How to Spot a White Nationalist that highlights the symbols, words and numbers associated with white nationalism. EWP notes that "by being confident that you have identified their association with white nationalism, you will be able to confront the person directly about their involvement." A section titled I Need Help offers directions on how one can leave, or help a friend escape from, a white power group. This section also encourages people that have information about a threat of violence from a white nationalist to report it to the local police station or to the National Security Hotline. Finally, the website has archived entries related to Conspiracy Theories, Identity, and Problems in Society, as well as a forum.

5. Think Again, Turn Away

The Think Again, Turn Away campaign was developed and launched by the USA State Department in December 2013 (Katz, 2014). According to its Facebook page, Think Again, Turn Away's "… mission is to expose the facts about terrorists and their propaganda. Don't be misled by those who break up families and destroy their true heritage." This program utilizes a broad spectrum of social media platforms in attempts to dispute and undermine extremist information in various ways. One way in which they do this is by engaging extremists in debates (Katz, 2014). More controversially, extremist narratives are also challenged through the posting of satirical mock recruitment videos. One video featured the phrases such as, "Travel is inexpensive because you won't need a return ticket", "useful new skills such as blowing up mosques and crucifying and executing Muslims" (Hansen, 2014).

The debut video released by the campaign featured graphic images of the Islamic State (IS) committing atrocities, including beheadings. By highlighting the brutality of IS, the videos were intended to dissuade potential jihadists from joining IS.

6. Muflehun

Muflehun is an independent think tank that specializes in preventing radicalization and countering violent extremism. Its initial focus is to first, understand the nature of the threat of violent extremism, and second, develop effective, innovative, and research-driven preventative programs within a religious paradigm. Initiated by the Muslim American community, Mulfehun believes that preventing radicalization, violent extremism and other threats from taking root is the first step for ensuring a safe civic society. The word muflehun is based in Quranic verse (Q3:104) and means "those who will be successful."

> Let there be a group (community) from amongst you that invites towards good, enjoins what is right (reasonable & just), and forbids what is wrong; and they will be the successful ones (muflehun).

Muflehun's stated vision is to help establish a community that promotes good work and justice, while peacefully working against wrongs and injustice. Its mission is to conduct independent research and provide recommendations to policymakers and the American Muslim community, as well as develop programs that directly and indirectly use faith-based values to: Promote the continued integration of the community within the larger society; enable civic engagement through awareness and promotion of available resources; and facilitate the fulfillment of social responsibilities by utilization and expansion of service channels.

Muflehun is a non-profit organization. Financed by contributions from individuals, foundations, and corporations, it is an independent and strictly non-partisan organization. It does not have any government funding; rather, it relies entirely on support from private sources. Muflehun purports to offer programs in several countries covering the Countering Violent Extremism landscape (although there are no specific programs listed on its website). Muflehun's CVE Programming Landscape is presented in Figure 4. Muflehun primarily engages through its website, http://muflehun.org/, which includes information on CVE News, CVE-related events, and a blog.

7. Don't be a Puppet

Don't be a puppet is an initiative developed and launched by the Federal Bureau of Investigation (FBI) in consultation with community leaders and other partners in February of 2016. Utilizing a website (https://cve.fbi.gov/info-discussion-leaders.html), the aim of the program is to engage and educate youth on the often deceptive realities of violent extremism. The site has five main sections that utilize quizzes and videos amongst other interactive materials: 1. What is Violent Extremism 2. Why do people become violent extremists? 3. What are known violent extremist groups? 4. How do violent extremists make contact? 5. Who do violent extremists affect? Once youths have worked through these sections they are prompted to a final section – Where to get help – where upon completion they receive an FBI certificate that they can sign and keep. These certificates are then used as a metric to determine how many people the program has reached.

8. Open Letter to our Sons and Daughters in Syria and Iraq

The 'Open Letter to our Sons and Daughters in Syria and Iraq' campaign was launched in June of 2015 by Mothers for Life. Essentially, it is an open letter that utilizes counter-narratives. The original letter's structure was designed by the German Institute on Radicalization and De-radicalization Studies (GIRDS) in conjunction with mothers from seven different countries. The letter was distributed across many different media platforms, including the social media giant, Facebook and a PDF version of it is available on the GIRDS website (http://girds.org/mothersforlife/open-letter-to-our-sons-and-daughters). A gripping passage from the letter reads,

> Allah has enjoined on man kindness to his parents; in pain did his mother bear him, and in pain, did she give him birth" (Quran:46:15). We, your mothers, taught you many things but most importantly justice, freedom, honour and compassion for all of God's creation and for every human being. Every human being belongs to the wonder of life. That wonder of life in all its essence, that we were part of together and were meant to be together, was taken from us. Why?
>
> Someone, told you that another life, beyond this one that we share together is more important, more valuable than the life with your mother. They told you to leave us and fight for justice and honour and eventually give up your life in order to find "that other life.

The power and far reach of this letter can be inferred from the statistics from the GIRDS website which state that the letter was: reported on by news outlets 1,785 times; shared 7000 time on Facebook; translated into eight languages – Turkish, German, Arabic, French, Italian, Dutch, Belgian, and Spanish; responded to by ISIS within three and a half hours after publishing it and; mothers from many more countries have since reached out for help.

Application of Good Practices

The list of CVE programs reviewed here is not intended to be representative or exhaustive. Rather, the aim is to offer a scan of the breadth of available online programs. But even this modest sampling provides some important insights into how we should be thinking about these programs. Specifically, applying the 'good practices' grid to existing programs demonstrates the variation across programs, and the extent to which they are currently following approaches identified by CVE scholars.

Table 1. Summary of Online CVE Programs

	Contextual Factors				By Whom?		How?		Measures?	
	Identify ideology/ VEO	*Identify at risk / targeted*	*Identify social processes*	*Identify driver(s)*	*Govt.*	*Credible Mssngr.*	*Online*	*Offline*	*Positive*	*Negative*
Youth Online and at Risk		✓			✓	✓	✓	✓	✓	✓
Campaign Against Violent Extremism (CAVE)	✓				✓	✓	✓	✓	✓	
Against Violent Extremism (AVE)	✓	✓				✓	✓		✓	
EXIT White Power (EWP)	✓					✓	✓		✓	
Think Again, Turn Away	✓				✓		✓		✓	
Muflehun	✓					✓	✓		✓	
Don’t be a Puppet		✓	✓	✓	✓		✓		✓	
Open Letter to our Sons and Daughters in Syria and Iraq	✓	✓				✓	✓		✓	

Contextual factors

First, CVE interventions pay scant attention to contextual factors. The programs were usually specific about the target ideology or violent extremist group of interest (see Table 1), but showed little interest in the types of social processes and push/pull factors that often contribute to the process of radicalization. This narrowness of approach has potentially negative implications for the effectiveness of CVE efforts. However, this also represents one of the most challenging factors for assessing the following programs, as our assessments are based on open source materials and we do not have access to the decision-making process, or specific details of designing the programs. For instance, Muflehun is premised on research-driven preventative programs; however, they do not provide a demonstration of explicitly adhering to these principles. Similarly, Youth Online and at Risk, lists as part of their strategy to develop contacts and genuine relationships with youth who are potentially at risk. While this may represent an effort to counter exposure and influence of extremist perspectives, the link between this approach and the outcome is broad and not clearly defined as part of the aim.

By whom?

Another important variation in programs relates to those charged with delivering the messages. Credible messengers are critical to several of the programs, present in six of the eight CVE programs discussed. The BC Muslim Association, particularly Mufti Aasim Rashid, is essential to the CAVE program. Muflehun similarly is rooted in the American Muslim community. AVE is an example of the need to incorporate the voices and experiences of survivors of extremist violence and former violent extremists. Other programs, such as Youth Online and as Risk and EWP, are closely tied to important stakeholders such as teachers and social workers. Open Letter to our Sons and Daughters in Syria and Iraq is created by and backed by mothers around the world. Two programs, Think Again, Turn Away and Don't be a Puppet, are run solely by the government. It appears that many programs are cognizant of, and have taken steps to address, the ‘credibility gap’ that is perceived to hamper government efforts.

Perhaps not coincidentally, the Think Again, Turn Away initiative has been the most controversial of the programs, and has been the most negatively received. This campaign is widely criticized by experts and the media as legitimizing terrorists, giving them a platform to further spread their propaganda (Katz, 2014; Edelman, 2014). In response to the video showing IS barbarism referenced earlier, Kohlmann (cited by Gearan, 2014) argues that “The problem with this video is the same problem that seems to happen over and over again with these type of initiatives. They don’t seem to have a clear picture of what audience they are trying to reach, or how to influence them.” Kohlmann further adds that “most of the Westerners trying to join ISIS are actually enthused by videos of executions and suicide bombings, not deterred by them”.

Measures?

In keeping with the philosophical priorities that underlie CVE, the programs here are predominantly centered around the presentation of information. This is consistent with what Stevens and Neumann (2009) have identified as ‘positive’ approaches, using education and alternate information to counter radical messages. Positive approaches were observed among five of the six programs. For instance, CAVE provided a venue with which to counter radical interpretations, providing alternate perspectives. Open Letter to our Sons and Daughters in Syria and Iraq also chose to counter interpretations by highlighting specific passages from the Quran in specific relation to mothers. This is also consistent with AVE and EXIT White Power which both have as a primary aim to challenge extremist beliefs. However, at least one of the approaches incorporated more ‘negative’ tactics. While the Youth Online and at Risk program delivered by the RCMP makes no mention of removing extremist material from websites, this program does encourage the monitoring of download activity and minimizing any contact with radical content.

At the same time, there are notable differences in the manner in which the information is conveyed. These distinctions can be considered along two close related dimensions: one regarding the level of “activity”, the other reflected in the degree of “online-ness.” For example, both of the Canadian initiatives, Youth Online and at Risk and Campaign Against Violent Extremism (CAVE), might be characterized as being relatively passive in their online approaches. The former purely involves the provision of information, while that latter really takes place offline. In both cases, the Internet is more peripheral to radicalization efforts. In contrast, AVE, Think Again, Turn Away, and Don’t be a Puppet are much more actively engaged in online milieus. The first two being examples of the trend of initiatives utilizing the widest possible range of social media platforms.

Discussion

The eight CVE programs presented in this paper provided a range of venues through which organizations have attempted to counter radicalization processes. The programs reviewed tended to focus on providing counter-narratives, that is, alternative sources of knowledge regarding political, ideological, and religious material found online.

Although CVE efforts in relation to radicalization constitute a relatively new field of study, attention has increasingly turned to the question of evaluation: what works? And how do we know? Assessing the utility and effectiveness of CVE programs is inherently difficult (Vidino, 2010). First, the lack of a clear definition of CVE makes it hard to evaluate the CVE agenda as whole (McCants & Watts, 2012). Second, the “success” of any program is most likely to be a matter of degree. To put it in more concrete terms, Vidino (2010, p. 10) poses the following question: “If, for example, one hundred individuals go through a deradicalization program and only a handful of them revert to terrorism, how is the program to be assessed?” Third, appraising the outcome of CVE programs is particularly challenging because it involves trying to measure a non-outcome; that is, one has to demonstrate that (some proportion) of subjects did not engage in violent extremism because of exposure to, or participation in, a specific program or intervention (Aldrich, 2014). While it may not be impossible to prove a negative, it is nonetheless very problematic.

In addition to the problems highlighted above, it is reasonable to ask whether there is any utility in evaluating CVE initiates as they are currently being conceptualized. Before we try to determine if programs are effective, however that may be defined, it is important to ascertain whether these programs have been built on solid theoretical foundations. Any policy prescription should, at a minimum, explicitly take into account the putative causes of the phenomenon of interest: CVE programs should be firmly grounded in the "causes" of radicalization to violent extremism. Based on the programs reviewed above, there would appear to be a substantial gap between what is known about the factors that are purported to animate the radicalization process and the factors that CVE interventions attempt to address.

Understanding the radicalization process is greatly complicated by a lack of consensus with regard to the causes of radicalization. In the absence of solid empirical evidence, pet theories and speculation abound. However, there seems to be an emerging consensus that a wide range of interrelated factors are implicated. "It seems that radicalization is a complex and highly individualized process, often shaped by a poorly understood interaction of structural and personal factors" (Vidino, 2010, p. 3). This characterization, emphasizing complexity and interaction, is at odds with the comparatively narrow focus of online CVE strategies. While almost all of the programs targeted a group or an ideology, none made any mention of social processes or socioeconomic, political, or cultural drivers. Given their incomplete theoretical underpinnings, it would be difficult for these programs to meet their desired aims.

Individuals are drawn into violent extremism for a host of reasons, many of which are unrelated to ideology. For example, Venhaus (2010) offers a typology of potential extremists comprised of four categories of 'seekers," individuals with unfulfilled needs that may turn to violent extremism as a means of defining themselves: "Revenge seekers need an outlet for their frustration, status seekers need recognition, identity seekers need a group to join, and thrill seekers need adventure" (p. 1). Two of these groups, status and identity seekers, are especially relevant in light of the perspectives advanced in this paper. CVE programs are not geared toward these individuals. More broadly, it is concerning that none of the programs reviewed here attempted to incorporate elements of social psychology. If individuals are motivated not by ideology but by needs rooted in identity, belonging, recognition and respect, refuting erroneous ideological interpretations, correcting historical inaccuracies, and unravelling conspiracy theories would be insufficient to divert them from the path of violent radicalization. Problematic ideologies provide a convenient focal point for intervention, but ameliorating them cannot offset or replace the social bonds that are being forged, both offline and online. Generally speaking, voluntarily abandoning one's perceived social support network would be perceived as being irrational. This calculus is not necessarily altered by the fact that the context is violent extremism. This realization presents a thorny but nonetheless crucial dilemma: CVE programs cannot merely be oriented toward preventing, arresting or reversing the process of radicalization to extremist violence. They must also with grapple with an equally compelling consideration: with what are the perceived 'benefits' of radicalization to be replaced?

Policy Implications

Currently CVE approaches have been classified based on their target audience and approaches used. While these centre on recruitment methods by groups, we would also encourage tailoring programs according to the specific methods through which violent extremists, or individuals 'at-risk' of violent extremism used the Internet – differentiating between those who use it as a key resource to develop and shape radical beliefs, from those for which the Internet is a trigger or reinforcer of radical beliefs. Targeting these individuals in particular, who are using it to reinforce, from those who use it as solely an initial trigger of radical beliefs – may require an entirely different approach.

Further, most of the programs presented are implicitly or explicitly directed toward jihadist violence. One endeavour, EXIT White Power (EWP), focuses on white nationalist and white supremacist extremism, while Against Violent Extremism (AVE) takes a much more expansive view and attempts to address violent extremism in all of its various guises. The (over)emphasis on Muslim radicalization has been noted by CVE critics. For example, Berger (2011) has commented that "(i)f the first step in making Muslims feel less alienated is to single them out for remedial social engineering, then we have a problem before we even start". This singling out seems especially misguided in light of the fact that, in the US, violent right-wing extremists have proved to a much more lethal threat. “Since Sept. 11, 2001, nearly twice as many people have been killed by white supremacists, anti-government fanatics and other non-Muslim extremists than by radical Muslims…” (Shane, 2015). Against this backdrop, Western governments would be well served to adopt a broader stance on radicalization programs.

Previous studies have also emphasized the role of the Internet in serving as a cognitive resource, to learn about religion (Helmus et al., 2013). This information seeking may lead individuals to come across extremist perspectives that shaped their radical beliefs. Providing alternative resources, specifically developing online resources for individuals who may be looking for – religious, political and ideological – resources. While the programs mentioned in the report aimed to provide counter-narratives and messaging, we would recommend furthering these efforts by providing credible information resources online for individuals to access. This may assist in them falling upon more nuanced and less Manichean discourses. However, recognizing that alternative cognitive resources, while valuable, will likely never completely overshadow radical perspectives, we would also recommend developing school programs that address digital literacy. These programs could foster critical thinking regarding ideological content available online.

Lastly, findings from the CVE programs also emphasize the need for 1. counter-narrative programs to be guided by theory; and 2. development of systematic evaluations of these programs. The first point extends from the above discussion that CVE programs should be built on strong theoretical foundations. This is particularly important for a phenomenon in which there is relatively few empirical studies on either radicalization or counter-radicalization processes, and where this process has been described as a “poorly understood interaction of structural and personal factors” (Vidino, 2010, p. 3). Theory can guide towards the most effective measures, rather than using measures that are argued to be intuitive, which is particularly important in a mis-understood process. This leads to the second point, evaluation of programs. Given the poorly understood nature of counter-violent extremism programs, we encourage systematic evaluation of the effectiveness of these programs. This is particularly important in light of allegations that these programs may even be counter-productive. For instance, this has been illustrated in the case of the US’ Governments effort to counter ISIS messages through their Twitter Account, Think Again, Turn Away, which has been publicly critiqued for not only being effective, but also providing a platform for terrorist groups to legitimize their organization, with individual members engaging in direct, open debates with government actors.

Our analysis aimed to provide a review of the literature on ‘good practices’ for designing programs that aim to counter violent extremism online, and an examination of whether current CVE programs adopt these principles. Our findings suggest that online CVE programs are lacking strong theoretical foundations and do not address important elements of radicalization, such as contextual factors or identity issues. Pathways towards radicalization appear as much the result of several identified pre-conditions as the product of relational and developmental configurations that may occur online and/or offline. This illustrates the need to pay close attention to the multiplicity of causal factors involved in such processes as well as the ways they interact together (Ducol 2015), as not doing so may hinder efforts aiming to prevent radicalization processes.Given increases in online CVE programs, this paper hopes to have served as a further step towards understanding this evolving landscape, and how online programs may be designed in order to effectively prevent and, even counter radicalization processes.

References

Aldrich, D. P. (2014). First steps towards hearts and minds? USAID's countering violent extremism policies in Africa. *Terrorism and Political Violence* (Online first), 1-24.

Ashour, O. (2011). Online de-radicalization? Countering violent extremist narratives: Message, messenger and media Strategy. *Perspectives on Terrorism*, 4(6), 15-19.

Berger, J. M. (2011, July 8). Terrorist acts, terrorist thoughts. *Intelwire*. Retrieved from http://news.intelwire.com/2011/07/policing-terrorist-acts-policing.html

Berger, J. M., & Strathearn, B. (2013). *Who Matters Online: Measuring Influence, Evaluating Content and Countering Violent Exremism in Online Social Networks*.

Bouchard, M., & Thomas, E. (2015). Radical and Connected: Concluding thoughts and future research. In M. Bouchard (Ed.). *Social network, terrorism and counter-terrorism: Radical and connected*. New York: Routledge.

Bowman-Grieve, L. (2009). Exploring "Stormfront" A virtual community of the radical right. *Studies in Conflict & Terrorism, 32*(11), 989-1007.

Braddock, K., & Horgan, J. (2015). Towards a guide for constructing and disseminating counter-narratives to reduce support for terrorism. *Studies in Conflict & Terrorism,* 00-00. doi:10.1080/1057610X.2015.1116277

Briggs, R. & Feve, S. (2013). Report on *Review of programs to counter narratives of violent extremism: What works and what are the implications for government*. Institute for Strategic Dialogue. Retrieved from http://www.strategicdialogue.org/ISD_Kanishka_Report.pdf (Accessed April 10, 2015).

Corman, S. (2011). Understanding the Role of Narrative in Extremist Strategic Communication. In L. Fenstermacher and T. Leventhal (Eds.). *Countering Violent Extremism: Scientific Methods and Strategies.* Washington, DC: NSI, Inc., pp. 36-43.

Dalgaard-Nielsen, A. (2010). Violent radicalization in Europe: What we know and what we do not know. *Studies in Conflict & Terrorism, 33*(9), 797-814.

Davies, G., Bouchard, M., Wu, E. Frank, R., & Joffres, K. (2015). Terrorist and extremist organizations' use of the Internet for recruitment. In M. Bouchard (Ed.), *Social* *network, terrorism and counter-terrorism: Radical and connected*. New York: Routledge.

Ducol, B. (2012). Uncovering the French speaking Jihadisphere: An exploratory analysis. *Media, War & Conflict, 5*(1), 51-70.

Ducol, B. (2015). A radical sociability: In defense of an online/offline multidimensional approach to radicalization. In M. Bouchard (Ed.) *Social networks, terrorism and counter-terrorism: Radical and connected* (pp. 82-104). London: Routledge.

Edelman, A. (2014). State Department's 'embarrassing' 'Think Again Turn Away' Twitter campaign could actually legitimize terrorists: expert. *New York Daily News,* September 16, 2014.

Gearan, A. (2014). U.S. attempts to combat Islamic State propaganda. *The Washington Post*, September 7, 2014.

Gerraerts, S. (2012). Digital radicalisation of youth. *Social Cosmos*, *3*(1), 25-32.

Goodall, H. L. (2010). From tales of the field to tales of the future. *Organizational Research Methods*, *13*(2), 256-267.

Hafez. M.,and Mullins, C. (2015) The radicalization puzzle: A theoretical synthesis of empirical approaches to homegrown extremism. Studies in Conflict & Terrorism, 38:11, 958-975.

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

Hansen, M. (2014). State Department combats Islamic State recruitment via social media. *Los Angeles Times, September 6, 2014.*

Helmus, T. C., York, E., & Chalk, P. (2013). *Promoting online voices for countering violent extremism.* RAND Corporation.

Hoffman, B. (2008). The myth of grass-roots terrorism: Why Osama bin Laden still matters. *Foreign Affairs.* Retrieved from http://www.foreignaffairs.com/articles/63408/bruce-hoffman/the-myth-of-grass-roots-terrorism (Accessed April 18, 2015).

Horgan, J. (2008). Deradicalization or disengagement? A process in need of clarity and a counterterrorism initiative in need of evaluation. *Perspectives on Terrorism*, 2(4), 3-8.

Hussain, G. & Saltman, E. M. (2014). Report on *Jihad trending: A comprehensive analysis of online extremism and how to counter it.* Quilliam. Retrieved from http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/jihad-trending-quilliam-report.pdf

Jenkins, B. (2011). Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001. Santa Monica, CA: RAND.

Katz, R. (2014, September 16). The State Department's Twitter war with ISIS is embarrassing. *Time*. Retrieved from http://time.com/3387065/isis-twitter-war-state-department/ (Accessed June 15, 2015).

Koehler, D. (2014). The radical online: Individual radicalization processes and the role of the Internet. *Journal for Deradicalization*, Winter (2014/15), 116-134.

Kühle, L., & Lindekilde, L. (2010). *Radicalization among young Muslims in Aarhus*. The Centre for Studies in Islamism and Radicalisation & Department of Political Science, Aarhus University.

McCants, W., & Watts, C. (2012). *US Strategy for Countering Violent Extremism: An Assessment*. Foreign Policy Research Institute, Philadelphia, PA.

Neumann, P. R. (2013). Options and strategies for countering online radicalization in the United States. *Studies in Conflict and Terrorism*, *36*(6), 431-459.

Pantucci, R. (2011). *A typology of lone wolves: Preliminary analysis of lone Islamist terrorists*. International Centre for the Study of Radicalisation and Political Violence. Retrieved from http://icsr.info/wp-content/uploads/2012/10/1302002992ICSRPaper_ATypologyofLoneWolves_Pantucci.pdf (Accessed June 1, 2015).

Pauwels, L., & Schils, N. (2016). Differential online exposure to extremist content and political violence: Testing the relative strength of social learning and competing perspectives. *Terrorism and Political Violence*, 28(1), 1-29.

RCMP-GRC. (2011). *A national security criminal investigations program on youth online and at risk: radicalization facilitated by the internet*. Retrieved from http://www.rcmp-grc.gc.ca/nsci-ecsn/rad/rad-eng.htm (Accessed November 14, 2014).

Sageman, M. (2008a). A strategy for fighting international Islamist terrorists. *The Annals of the American Academy of Political and Social Science*, 618, 223-231.

Sageman, M. (2008b). *Leaderless jihad: Terror networks in the twenty-first century*. Philadelphia: University of Pennsylvania Press.

Schmid, A. P. (2013). *Radicalisation, de-radicalisation, counter-radicalisation: A conceptual discussion and literature review*. The Hague: International Centre for Counter-Terrorism. Retrieved from http://www.icct.nl/download/file/ICCT-Schmid-Radicalisation-De-Radicalisation-Counter-Radicalisation-March-2013.pdf (Accessed November 14, 2014).

Schmid, A. P. (2014). Al-Qaeda's "Single Narrative" and Attempts to Develop Counter-Narratives: The State of Knowledge.

Sedgwick, M. (2010). The concept of radicalization as a source of confusion. *Terrorism and Political Violence*, *22*(4), 479-494.

Seib, P., & Janbek, D.M. (2011). *Global terrorism and new media: The post al-Qaeda generation*. London & New York: Routledge.

Shane, S. (2015, June 24). Homegrown extremists tied to deadlier toll than Jihadists in U.S. since 9/11. *New York Times.* Retrieved from http://www.nytimes.com/2015/06/25/us/tally-of-attacks-in-us-challenges-perceptions-of-top-terror-threat.html?_r=0 (Accessed June 25, 2015).

Stevens, T. & Neumann, P.R. (2009). *Report on countering online radicalization: A strategy for action by the international centre for the study of radicalization and political violence*. The International Centre for the Study of radicalization and political violence. Retrieved from http://icsr.info/wp-content/uploads/2012/10/1236768491ICSROnlineRadicalisationReport.pdf (Accessed November 14, 2014).

Suler, J. (2004). The online disinhibition effect. *Cyber Psychology and Behavior*, 7(3), 321-326.

Thompson, R. L. (2011). Radicalization and the use of social media. *Journal of Strategic Security*, 4(4), 167-190.

Venhaus, J. M. (2010). *Looking for a Fight: Why Youth Join al-Qaeda and How to Prevent It*. U.S. Army War College, Carlisle Barracks, PA.

Vidino, L. (2010). *Countering radicalization in America*. Washington, DC: United States Institute of Peace, Special Report 262, November, 2010.

Von Behr, I., Reding, A., Edwards, C., & Gribbon, L. (2013). *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*. Brussels: RAND Europe.

Weimann, G. (2012). Lone wolves in cyberspace. *Journal of Terrorism Research, 3*(2) doi:10.15664/jtr.405