Countering violent extremism on social media

An overview of recent literature and Government of Canada projects with guidance for practitioners, policy-makers, and researchers

Suzanne Waldman
Simona Verga
DRDC – Centre for Security Science

Defence Research and Development Canada

Scientific Report
DRDC-RDDC-2016-R229
November 2016

Abstract

Increasingly, social media is playing a role in recruitment to violent extremism, and governments are designing interventions to detect, understand, and counteract the impact of violent extremist recruitment materials on social media and other internet channels. In addition to more traditional surveillance and law enforcement interventions, authorities are increasingly focusing on policies and programs to enable preventive activities such as employing on-line counter-messaging to counteract susceptibility to violent extremist ideologies, or engaging and supporting communities in "real life" efforts to build resilience to these ideologies at the grassroots level. However, sparse metrics and a shortfall of detailed and contextualized understandings of the processes by which radicalization occur make it difficult for governments to assess the success of these policies and programs. Specifically, more evidence is needed to support direct interventions for countering violent extremism on social media and the internet with assurance. This report sums up research that has been funded by various agencies and departments of the Government of Canada into the effectiveness of different countering violent extremism activities on social media and the internet, with the intent of helping to guide further actions. After reviewing the literature on what types of interventions into violent extremism on the internet appear to work, it concludes with a set of recommendations for policy-makers, messagers, and researchers to help develop and refine counter violent extremism activities.

Significance to defence and security

The internet and social media are increasingly understood to be fields where violent extremist ideas proliferate and where violent extremist agents are able to exert a radicalizing influence and develop recruiting relationships that expand the reach and scope of their activities. Interventions to counteract these efforts are essential for national defence and national security, but better understanding of processes of radicalization, and better ability to measure the success of different types of interventions, is required to inform their development.

Résumé

De plus en plus, les médias sociaux jouent un rôle dans le recrutement des adeptes de l'extrémisme violent. C'est pourquoi les gouvernements conçoivent des procédés pour dépister les méthodes de recrutement dont se servent les extrémistes violents, dans les médias sociaux et sur Internet, pour comprendre ce phénomène et contrer son incidence. En plus d'employer les procédures traditionnelles de surveillance et d'application de la loi, les autorités s'en remettent de plus en plus à des politiques et des programmes de prévention comme l'utilisation du contre-discours en ligne afin de neutraliser l'attrait de l'idéologie des extrémistes violents, ou encore à la mobilisation et au soutien des collectivités par des mesures réelles pour opposer une résistance à cette idéologie au niveau de la base. Toutefois, en raison de la rareté des mesures et d'une compréhension insuffisamment détaillée et contextualisée des processus à l'origine de la radicalisation, les gouvernements ont du mal à juger du succès de ces politiques et programmes. En particulier, il faudrait davantage d'éléments probants pour appuyer des interventions directes permettant de combattre avec assurance l'extrémisme violent dans les médias sociaux et sur Internet. Dans le présent rapport, on résume les travaux de recherche financés par divers organismes et ministères du gouvernement canadien pour trouver des méthodes efficaces de lutte contre l'extrémisme violent dans les médias sociaux et sur Internet, méthodes qui serviront à orienter d'autres actions. Après avoir passé en revue ce qui a été écrit sur les types d'interventions qui semblent fonctionner contre les manifestations de l'extrémisme violent sur Internet, les auteurs du rapport concluent en donnant un ensemble de recommandations aux décideurs, aux messagers, et aux chercheurs pour les aider à créer et à perfectionner des activités permettant de contrer l'extrémisme violent.

Importance pour la défense et la sécurité

Il est de plus en plus évident qu'Internet et les médias sociaux constituent un terreau où prolifèrent les idées de l'extrémisme violent et où les agents de cet extrémisme peuvent radicaliser des gens et établir des relations propices au recrutement, ce qui leur permet d'accroître la portée de leurs activités. Pour la défense et la sécurité nationales, il est essentiel d'intervenir pour contrer ces efforts. Néanmoins, il faut mieux comprendre le processus de radicalisation et être mieux à même de juger de la réussite des différents types d'interventions afin de contribuer à leur élaboration.

Table of contents

1 Introduction

1.1 Overview

Internationally, social media (SM) has become a significant battlefield upon which violent extremism (VE) is being organized and on which states are continuously struggling to find strategies to counter VE.

"Violent extremism" is currently a preferred term for describing destructive actions or support for such actions undertaken by groups or individuals formally or informally affiliated with them, in the name of "extreme" political or religious ideals—that is, ideas that cannot coexist with the policies of democratic countries such as Canada. The term indicates an important distinction between the perpetration of violence in the pursuit of political ideals, and the holding and communicating of such ideals which are protected by the individual rights to "freedom of thought" and "freedom of expression" [1].[1] VE thus reflects the accompaniment of political or religious ideals with the belief that the pursuit of these ideals warrants violence as well as the intention of undertaking or supporting such violence. Radicalization is a related term that emphasizes the process that an individual must go through to adopt extreme political views as well as a willingness to use violence to advance them [2]. Radicalization appears to require a combination of four factors to occur: 1) grievances or root causes; 2) social networks that facilitate recruitment; 3) Ideological narratives that bind individuals to causes; and 4) enabling and supportive environments, which may or may not include the internet [3].

It is important to point out that despite some of the current headlines; evidence does not suggest VE is growing in Canada. The recent uptick in Islamicist incidents on domestic soil have not reversed gradual overall declines of racially and politically motivated violence [4]. However, the recent rise in VE internationally, the relatively novel phenomenon of Canadians perpetrating terrorist acts abroad (since 2013) [4], and the availability of social media as a ripe potential site for VE recruitment and activation, are more than sufficient reasons to investigate strategies to sustain active engagement in countering violent extremism (CVE) on SM and elsewhere. In particular, Public Safety Canada has a policy mandate to develop means of "protect[ing] Canada and the safety and security of Canadians at home and abroad" by countering domestic terrorism as well as international terrorism through means including detection and prevention, both of which inevitably involve activity on social media channels [5]. As evidence to be covered in this report indicates, however, social media-oriented activities need to be carefully coordinated with engagement in communities at the offline level, a requirement signaled by the new Office of Community Outreach and Counter-Radicalization being created at Public Safety Canada [6].

CVE is defined as activities designed to reduce the phenomenon of VE, as well as policies designed to enable them. Some researchers and institutions are limiting the definition of CVE more narrowly to "positive", "non-coercive" or "soft power" activities that are separate from more "negative", intelligence and law enforcement approaches focusing on removing content, suspending accounts, or even seeking prosecutions [7], [1]. Meanwhile, others expand the definition into "CVE-relevant" forms of community development that can facilitate individuals streaming in other,

[1] With the exception of some forms of persecutory communication that have been criminalized in the concept of "hate speech".

more positive directions [1]. Yet others categorize CVE in terms of the level at which it is aimed: the micro, individual-oriented level of individualized interventions; the meso (i.e., middle), community-based level of community relationships and development; and the macro, society-wide level of social media as well other sites of monitoring, analysis, reaction, and counter-narrative dissemination [1].

Our report is focused on all types of what we call "CVE on SM", that is, efforts to counter violent extremism that make use of social media channels and/or are oriented towards obstructing the nurturing of VE on social media. Promoters of radicalization have turned to the internet as governments have attempted to curtail their recruiting activity in "real-world" sites, focusing their efforts towards developing online magazines, video clips and montages, and even video games that could be distributed through online networks [3]. Social media adds the possibility of forging personalized and relational connections that give potential recruits—who might be experiencing social alienation—a "sense of communal belonging" [3]. Observing the potential to access recruits in this domain, VE groups have become "active and savvy users of social media spaces" [8]. They use SM channels for broadcasting and sharing sophisticated propagandist materials, such as videos, that offer narratives warranting and justifying VE, and also for creating enclaved social forums in which such narratives can become reinforced (Ducol, B. et al, 2016). At the same time, VE groups have learned to use online and offline realms of networks and activity in increasingly interconnected ways [2]. SM sites offer open channels for recruiters and individuals across the globe to become acquainted, possibly intimately and personally or with the illusion of intimacy (Ducol, B. et al, 2016). While it is clearly impossible and undesirable to either eliminate or survey the entire internet and social media landscape for VE recruitment activity, a potentially more productive approach is to seek to use SM and the internet to support pro-social, anti-VE ends, which can be supported, in turn, through offline, community-based activities [9].

For all of these reasons, SM is an increasingly important locus for identifying VE networks and activity and for countering them through both online and offline means [2]. This report accordingly sums up current understandings of best practices in countering VE on social media, as indicated through government-funded research in Canada and abroad, with a target audience of Canadian policy-makers, program-developers, and researchers who are developing and honing the types of interventions as well as understandings of the contexts in which they operate.

1.2 Subcategories of CVE on SM

There are two significant ways in which VE groups use SM that invoke different types of CVE reactions on the part of states. The first is the use of SM channels to stimulate, organize and activate violent actions. The second is using SM to publicize activities and views to potential supporters, and also to dialogue with potential new recruits. While promotional and recruitment activity constitutes the typical target for CVE intervention, detecting VE organization and activation on SM can require similar analytical tools as detecting VE promotion and recruitment, and we have addressed both of these types of activities in this report.

1.2.1 VE promotional and recruitment activities on SM

A first aim for CVE efforts—generally considered CVE proper—is to counteract the use of SM by groups to recruit individuals and to engender a wide and supportive environment for their activities. Although there seems to be consensus in the literature that social media recruitment does not usually happen in a vacuum, and that real world contexts are often the starting point for CVE recruitment, SM activity by VE groups does appear to provide a high degree of support.

VE groups recruit on social media through the broadcast of various types of propagandist materials and also through initiating or participating in ideologically-based dialogues with susceptible individuals. The premise of monitoring for VE stimulation and recruitment on SM is that individuals undergo radicalization processes that involve exposure to, and internalization of, extremist ideology as well as socialization into violence [8]. Individuals may be vulnerable to recruitment in part because SM and the internet as a whole constitute a venue which allows them to undertake philosophical, political, and religious lines of inquiry and meaning [7]. For instance, a small-n study funded by the Kanishka Project observed that recruits to Islamicist VE began as inquisitive seekers of knowledge about religion [10]. Further, the collective social structures of the internet can provide an enclaved social forum in which VE can be promoted by individuals who may seem to share a seeker's identity, values and concerns [7]. As well, large volumes of SM content are constantly being produced by VE groups to feed individuals' quests for ideologically oriented solutions to their concerns [11]. SM specifically avails recruitment to VE by immersing participants amidst graphic and violent imagery that desensitizes them to violence, and also amidst social networks that provide individuals with social connections and identity support while simultaneously working as echo chambers where extremist views are reinforced [9], [11]. "Lone wolf" VE actors are thought to be the most impacted by internet materials, with offline relationships playing a greater role in other types of VE recruits [7].

One way to combat these activities is through the exercising of "soft power" influence over individuals and communities who might not be members of VE organizations but who might be susceptible to their influence [1]. Such means may include:

1. Undertaking strategic communications and public awareness activities that broadcast positive actions in which the government is engaged as well as positive "alternative narratives" that portray what the government stands for, including values as such tolerance, openness, freedom and democracy [12].
2. Participating in—or, more likely, sponsoring others to participate in—dialogues with those propagating VE information in order to interfere with their spread of influence and programming of new recruits.
3. Monitoring SM for the purpose of understanding, and potentially disrupting, VE networks and tactics. Law enforcement, security, and defence organizations may conduct Open Source Intelligence operations (OSINT), which involve monitoring and applying analytic techniques to extract useful and actionable information. For example, network analysis may be performed to identify power and affiliation structures, and semantic analysis to identify hallmark VE discursive content. Such techniques applied to data in the public SM domain are collectively known as Open Source Social Media analytics (OSSM) [8]. When it comes to scanning large social media flows for signs of VE content, however, questions of how to preserve social expectations of privacy around social media activity are paramount and to some degree unanswered.

4. Monitoring SM to identify individuals who are indicating susceptibility to recruitment strategies and, where suitable, arranging offline interventions, such as counseling and mentorship [1].
5. Removing internet content [1]. Because the use of these tactics to counter the reach of VE overlap with law enforcement and intelligence activities for combatting VE described below, it is arguable impossible to completely enclave CVE as a "non-coercive" activity. Although some definers consider CVE to be only the exertion of "soft power" influence and to exclude law enforcement and intelligence interventions, we have included SM monitoring, intelligence collection and content removal in this report because they constitute important elements in the suite of tools and approaches to countering VE on the internet.

1.2.2 VE stimulation, organization and activation of violent actions

To varying degrees, VE groups conduct the organization and activation of their activities on social media, since it is an easy and free way of reaching memberships at large and over large areas. It is believed that 90% of terrorist activity on the internet is conducted on SM [11]. VE may be explicitly organized and then activated through SM channels in a centralized fashion, or VE may alternatively be stimulated amongst distributed or even lone wolf, unaffiliated operatives. For VE organizations to achieve these ends, SM is also used as a channel for circulating information, resources, and best practices for VE activities [11], [5]. Different VE groups use a wide and constantly evolving range of SM platforms and other open or closed channels to conduct their activities, a good number of which CVE practitioners should ideally be aware and competent in using as well [11]. Often these platforms are used in combination, with recruits identified on public social media platforms and invited to join private forums for instructions [11].

A first challenge with countering VE organization, activation, and stimulation on SM is the "big data problem" of observing them amidst the large social media flows. Presumably, with the help of specialized analytical tools and techniques (collectively known as "big data analytics"), this type of VE activity is monitored, collected, and analyzed for its potential to generate intelligence. Such processes are known as Open Source Intelligence (OSINT) or more specifically Social Media Intelligence (SOCMINT) [11].

OSINT and SOCMINT can produce subtle dividends in CVE. Being able to enumerate and monitor VE network dynamics can potentially yield insights and intervention points for CVE practitioners. Data feeds can reveal the key influencers and gatekeepers of networks; the core, trending, and "hallmark" (that is, specifically identifiable and resonant) content that members of the networks use and respond to; how information is flowing within the network; changes that may be occurring in the network; and how members are clustered in offline communities [8]. Privacy concerns around observing data flows remain, however.

Law enforcement operations may follow, such as removing content, suspending accounts, or prosecuting individuals engaged in VE activities [1]. Yet in the last number of years the use of encryption services, self-made encryption tools, as well as anonymous, privacy-enhanced, and decentralized distributed social networks have made monitoring efforts more difficult, and these difficulties are likely to continue to grow [11].

1.3 Research questions

This report accordingly pursues three research questions:

1. What federally funded research projects (e.g., with funding from the Canadian Safety Security Program (CSSP) and/or from Public Safety Canada's Kanishka project) have investigated approaches to CVE on SM in the Canadian context, and what are some of the key findings?
2. What is the evidence produced by other important international research projects about the effectiveness of CVE interventions on SM, including both "soft power" influence and law enforcement and intelligence approaches? Which of these interventions seem to work best, and in what specific way ought they to be undertaken?
3. Based on the results of the first and second question, what types of CVE SM interventions should be considered within Canada, and what further types of research into CVE on SM ought to be pursued?

1.4 Methodology and key resources

In developing this report we consulted general literature reviews on the subject of CVE efficacy on SM as well as investigations into federally funded research projects investigating CVE and SM. A list of publicly available reports and other publications based on research funded by CSSP and the Kanishka Project can be found in Annex A; see the bibliography for other works consulted.

1.5 Limitations of the report

To develop this report, we compiled literature reviews and research reports on CVE that were funded by the Government of Canada as well as some of their key references, using a snowball approach to accumulating references. We also scanned mass media for recent developments in the CVE field, in particular those emphasizing effectiveness. We did not, however, undertake a sweeping international scan literature on online VE and CVE, for instance of reports developed under the auspices of international entities such as the United States State Department or the Organization for Security and Cooperation in Europe, or of the wide range of articles and books presenting situated, conceptual, as well as critical dives into radicalization phenomena and counter-radicalization activities As such, the report draws on a selective and partial sample of the field as a whole, but in the understanding that the reports and articles referred to typically reach further and deeper into their respective subject domains.

2 Results: Evidence of effective and ineffective CVE

In general, research findings emphasize that the field of CVE on SM is still experimental, providing "no proof positive that current efforts are effective" [1] and indicating a lack of "operational indicators and early detection approaches" for discovering and countering VE [8]. Nonetheless, most research reviewed herein indicates that continuing to seek ways of intervening in the SM space to counter VE are essential. Evidence of what does and does not work has typically been derived from results of "first wave" CVE programming initiated in the 2000s, though input is constantly incoming.

2.1 What appears not to work in CVE

2.1.1 Takedowns and account suspensions

Taking down VE content and suspending accounts may initially tie up VE organizations and lead to diminished effectiveness in the short term [11]. However, this tactic is considered generally inadequate for handling VE on SM, given how much content there is to sift, the difficulty and expense of doing so, and the difficulties of distinguishing between extremist content and VE content [5], [9]. As well, accounts are a moving target, as VE organizations may be well poised to create new SM accounts virtually at the same time as suspensions occur and to use "swarmcast"[2] tactics across multiple platforms to alert followers of relocated content [11]. The growth of encrypted social media services, anonymous social networks, "dark nets", decentralized distributed social networks, and the use of encryption applications by SM users make it even more unlikely that censorship of VE content will be substantially useful for CVE [11]. Displacing their content may in fact motivate VE groups to make their materials harder to detect, undermining the ability to monitor them [8].

Content takedowns can also lead to unintended consequences where those actions are seen to fulfill extremist narratives about bias, discrimination, and censorship, potentially leading indirectly to more radicalization. As such, it is important not to over-rely on negative efforts such as take-downs and other security and law enforcement measures to combat VE, but to couple these with strategic efforts such as community engagement and dialogue that may disrupt VE group structures and behaviours at the grassroots level [1].

2.1.2 SM monitoring for indicators of radicalization

Effective use of SM data continues to be "awash in methodological and ethical challenges" [13]. Searches on Facebook pages and profiles for indications of VE propensity or activity did not yield useful results, failing to discover solid indications of either extremist or violent extremist content or to establish a workable distinction between offensive and inciting language [8]. Social media monitoring across the domestic population also raises privacy and ethical concerns, particularly if surveillance targets are derived from the expression of ideological views [2]. Most extremist

[2] Swarmcast is a term used in the security community to describe communications through a dispersed network of accounts that reconfigures itself continuously, like a swarm of bees; see http://terrorismanalysts.com/pt/index.php/pot/article/view/426/html.

material is not strictly speaking illegal and it is extremely difficult to draw a line between critical and inciting language [10], [8]. It also seems impossible to derive adequate generalizations about individualistic, social or behavioural processes of radicalization to develop algorithms guiding the discovery of individuals at risk of VE recruitment. Social media monitoring for specific personal grievances (vs. collective; see Section 2.2.1) is unlikely to be effective [2] as narratives of grievance are shared by broad populations, many of whom are not susceptible to VE [8]. Broad monitoring of SM flows for the presence of extreme ideology is similarly difficult and impractical. It may be possible to develop more specific algorithms that reflect radicalization patterns of recruits to specific groups; however this research is in its infancy [8].

2.1.3 Geospatial data for pinning down VE member locations

At this point, geospatial data embedded in SM is typically too sparse and of too low quality for practical applications such as connecting it with offline activity, but the potentialities for verifying geographic content of SM material, or alternatively the locations of key individuals generating that material, may evolve [8]. As well, metadata analysis shows promise for surfacing more latent aspects of social media networks, such as the age, gender, location and other demographics of its participants [11]. These prospects raise, however, privacy concerns around intensive surveillance of social media users. See Section 2.2.2 for a discussion on the use of Social Network Analysis for analyzing VE networks and network power structures and for potentially targeting specific nodes for maximum VE network disruption.

2.1.4 Government-based CVE counter-messaging

It has become widely believed that a significant way to counteract VE narratives is to create counter-narratives that offer credible alternative interpretations of the world and directions for agency and action to those being circulated by VE groups [12]. Yet indications from programs in the United Kingdom (UK) and the United States (U.S.) suggest that government efforts to circulate counter-messaging can produce backlash and unintended consequences. The U.S. Department of State's *Think Again Turn Away* campaign, which publishes counter-extremist material and argues with high profile jihadist accounts, appears to have significantly backfired [11]. The program's honing in on the violence of IS groups as an argument against recruitment is thought to have been ineffective, given that the violence is typically understood as a basis for enthusiasm amongst recruits [9]. Programs such as these can also trigger counter-productive debates about whether government actions match their expressed values, giving jihadists a platform for their views [1]. Likewise, in Denmark, dogmatic emphases on specific state values (freedom, equality, etc.) are observed to have heightened alienation and indignation [1].

See Section 2.2.4 for a discussion of how governments can alternatively foster the development of CVE counter-messages by community groups.

2.1.5 CVE programs that stigmatize communities

Critics have noted a detrimental overemphasis in government CVE activity on Muslim radicalization, leading to stronger feelings of alienation amongst Muslim youth [9]. Stigmatization has occurred most notoriously in the UK's "Prevent" strategy which continues to attract "criticism for targeting… the whole Muslim community as potential terrorists" [1].

Singling out Muslims is further an inaccurate emphasis in many contexts, including North American ones, where white supremacist VE remains more significant [9].

2.2 What holds promise in CVE

2.2.1 Social media monitoring

Social media analysis can potentially be useful for identifying individuals, groups, subcultures, networks, online communities, tactics, and specific types of content and language that encourage and inspire violence on behalf of a cause [2]. Analysis can look for indications of political, economic, social or cultural factors regarded as root causes of VE that cumulate in a social environment in which violent extremism can grow, and which may include social alienation, collective narratives of grievance, de-legitimizations of the state and radicalizing ideologies that revere, glamorize, or offer of rewards for violence [2].

Closely analyzing the discourse of radical groups can provide further information about the relationship between the circulation of VE ideologies and the undertaking of violent behaviour. CVE subcultures on SM typically have specific language known as "hallmark content" through which they signal intentions and utter calls to action or violence [8]. This language can be discovered through "netnography"[3] or qualitative analysis of the pages of known VE group members [8], [11]. If specific forms of "hallmark language" are identified, social media flows can be monitored for indications of content featuring this language [2]. Eventually, Natural Language Processing (NLP) algorithms may also be developed that can analyze SM language and make judgements about what types of content and vocabulary are relevant amongst VE groups [11].

SM monitoring can also be used to ensure CVE content is directed towards individuals who are especially susceptible to violent narratives. The Extreme Dialogue project targeted advertisements towards specific individuals they identified through browser cookie data [9].

Additionally, advanced SM monitoring techniques such as NLP are being developed to monitor Open Source Intelligence (OSINT) to facilitate prediction or detection of terrorist events, which can be signalled by rapid or anomalous changes in sentiment or geo-located occurrences of certain semantics [11]. Even now, OSINT is being used to obtain situational awareness when an event is underway through the location of key information posted by VE members or citizen journalists [11].

2.2.2 Social Network Analysis

Social Network Analysis can help to identify and understand online social networks that support the organized coordination of violence [2]. Social Network Analysis (SNA) predates the internet and aims to measure, map, model, and/or describe the nature, intensity, and frequency of networks of social ties in the hopes of better understanding and even predicting their relationship to individual actions [11]. SNA can be conducted on data sets of online activities including readership or participation in blogs, news stories, discussion boards or social media sites. Data on

[3] A netnography is an interpretive research method that studies interactions and experiences occurring through digital communications.

site content, links, or usage can be used to reveal the numbers of people in an online social network, how and what information flows amongst them, and structures through which influence is exerted [2]. It can thereby help to explain how ideologies, motivations and messages spread amongst networks and provide warnings of when online VE networks are expanding recruitment activities [11]. "Centrality analysis", which characterizes the position of any given node in a network to other nodes, can model features of the network such as "degree" or the density of interconnections, typically highest amongst leaders and influencers; "betweenness", or the proximity of a node to others, highlighting gate-keepers who connect clusters of a diffuse network; and "closeness", or the summed proximity of individuals to each other in a network, which describes the ease of communication amidst it [11].

Reconstruction of the specific membership and hierarchy of a VE organization on SM may also be possible through SNA of network interactions [11]. A community analysis applied to data from websites, blogs, chatrooms, forums, communities of interests, Facebook pages, Twitter accounts and YouTube channels can potentially identify members of a given network based on their density of links with each other [11]. This information can be used to provide further information about key communicators, influencers, and recruiters [11], [2].

Finally, SNA can also be used to understand or leverage language being shared within a group or network. When "hallmark content" of VE groups is discovered, it can be used to surface channels in a VE network through the use of web scrapers and Application Programming Interfaces (APIs) [11]. Machines can potentially also be trained to use metadata to probabilistically profile features VE content authors, such as their age, gender and geo-location [13].

2.2.3 Sponsoring community-based, evidence-based counter-narratives

Online CVE counter-messaging that disseminates alternative messages to those being circulated by VE groups can leverage the internet as a powerful and flexible medium to reach and engage with young populations who are looking for information and meaning [9]. Narratives are simple, culturally rooted stories that provide a framework that "ring[s] true" for organizing experiences and understanding events [9]. VE narratives portray the world in a unifying way that is emotionally and intellectually satisfying and provides target audiences with a sense of direction and purpose [9]. Counter-narratives can especially help to reach individuals who end up finding VE after a quest for identity affirmation and recognition [9]. A small-n study funded by the Kanishka Project observed recruits to Islamicist VE causes began as seekers of information about religion, and only in time became recruited to VE views, leaving an opportunity for counter-radicalization during the preliminary phase of these quests [10].

Because these populations are unlikely to trust messaging coming directly from the government, however, communities can play a significant and useful role in developing alternative narratives to VE narratives. Yet in comparison with VE groups, non-radical groups typically suffer from a deficit of passion, confidence, and resources for circulating their narratives [12]. Governments can support training, development programs, and other resources for civil society groups that can enable them to construct messages and develop high production-value products [12]. Capacity building programmes can be rolled out in a cascade to seed training among those who can train others [12].

Once target communities for VE activities are identified, governments are recommended to develop a theoretically and empirically informed understanding of radicalization processes in the identified contexts, including: 1) general root causes and psychology of radicalization; 2) specific cultural and political root causes in the given community, including political and economic grievances; 3) pertinent VE organizations and ideologies targeting community members; 4) the types of individuals being targeted by VE groups and are being drawn in and why; and 5) processes, strategies, and networks through which individuals are being recruited; and how these various factors are working in combination [9]. It has been suggested that successful CVE programs are conceptualized in relation to a clear sense of "the perceived 'benefits' of radicalization to be replaced" [9]. Content that is discovered through SNA to be particularly effective in recruiting activity can also be used to develop effective counter-narratives [2].

After background information is gathered, a CVE approach can be designed that: 1) specifies who should develop and deliver the approach; 2) where and how it should be implemented (e.g., online, offline); and 3) through what types of measures [9]. Awareness raising, engagement, and collaborative experimentation are first steps in building community capacity for CVE activities that can open the door to successful collaborations and delegations of CVE practice [8].

2.2.4 Coupling or sequencing CVE with community and relationship building

It has been proposed that CVE should be regarded as a policy theme encompassing community relationship-building activities across a wide range of government domains [14]. In this vein, the 2016 Government of Canada created an Office of the Community Outreach and Counter-radicalization Coordinator, to coordinate "leadership on Canada's response to radicalization to violence, coordinate federal/provincial/territorial and international [counter-radicalization] initiatives, and support community outreach and research" [15].[4]

Community-building programs can strengthen communities' resilience, capacity, and leaderships. An example is Muslim Youth Canada, developed by the Canadian Council of Muslim Women and funded by Citizen and Immigration Canada, which sought to enable leadership as well as effective communication and web skills among young Muslims [10]. Relationship-building programs can help to bring out community's perspectives of what might be causing alienation in some of its members and leading to VE, such as discrimination or lack of economic opportunities [1].

2.2.5 Pairing CVE on SM with micro-level, face-to-face interventions

When it comes to CVE on SM, online communication campaigns should cohere with and be supported by offline, face-to-face engagement, which is far more effective than online interventions at dissuading vulnerable individuals from VE [1]. Referral programs can identify vulnerable individuals and groups and intensively discuss and deconstruct extremist arguments [12]. Identifying vulnerable individuals and addressing behavioural radicalization through counselling and mentorship has been found to be effective in the UK "Channel" program [1]. Off-line or online referral programs involving community members such as social workers and teachers, or alternatively members of society, can

[4] http://www.budget.gc.ca/2016/docs/plan/budget2016-en.pdf , p. 188.

identify susceptible individuals at large via hotlines [1]. These individuals can in turn be placed in mentoring relationships with former extremists, religious scholars, and other credible messengers who can build trusted relationships with them and dissuade them from extremist views, in an approach the Institute for Strategic Dialogue (ISD) has pioneered around the world [12], [11]. Leaders of the Exit White Power program in Australia found that counter-messaging programs that combat or ridicule the narratives and ideologies of white supremacists "can help to dissuade young people from becoming involved" in those groups, but only when opportunities are also available for them to have two-way conversation with frontline workers such as teachers, counsellors, or youth workers [9].

In the creation of referral programs, training for social service providers, school counsellors, law enforcement providers, and clergy on how to identify individuals susceptible to CVE seems to contribute to the effectiveness of these programs [1]. Exit White Power provided a guidebook and other resources for youth workers, social workers, councillors, psychologists, teachers, and police on how to identify at-risk or recruited youth and talk about white VE with them [9]. In turn, programs soliciting community-based referrals may require ongoing monitoring to ensure that stereotyped suspicion is not being directed towards certain ethnic groups, as has been observed to occur in the UK's "Prevent" strategy [15].

2.2.6 Developing and/or translating alternative resources

Other useful actions for governments in combatting the monopoly of VE narratives are collaborative efforts at translating key texts or developing media products that widen the range of alternative resources for people in quest of meaning and understanding [12]. Enabling the development of alternative, non-violent but relevant online or offline religious, political, and ideological resources can help stream individuals away from more toxic options [7]. A 2014 project jointly created by the Royal Canadian Mounted Police (RCMP) and the British Columbia (BC) Muslim Association aimed to increase knowledge of mainstream Islam and its interpretations of Muslim texts to counter radical interpretations through community educational experiences [9]. Another acclaimed example of such a project is Muflehun, an independent think tank initiated by the Muslim American community that promotes community integration and social responsibility based on faith-based values [9].

2.2.7 Enhancing internet literacy and civility

Media literacy programs can raise students' critical thinking and awareness of the tactics of online ideological propagation and recruitment [7]. Users' panels could raise awareness of reporting mechanisms for unacceptable content, monitor companies' complaint procedures, develop partnerships between Internet companies and non-governmental organizations (NGOs), and generally serve as ombudsmen [16]. A 2011 RCMP project "Youth Online and at Risk" was a four-step program that targeted parents, caregivers, and teachers to engage in conversations with youth about online content appropriateness and the importance of offline connections, leverage tools and strategies for monitoring youth online behaviour, and report material of concern [9]. The Federal Bureau of Investigation's (FBI's) (2016) "Don't Be a Puppet" campaign runs a

website that uses quizzes and videos to help alert youth to VE strategies and assigns them a certificate for successful completion [9].[5]

2.2.8 Strategic government messaging

While it is increasingly believed that governments should steer clear of the production of CVE counter narratives (see Section 2.1.4), there remains a role for government in the production of strategic communication that clarifies government principles and policies and "sets the record straight" on controversial subjects [12]. For strategic government communications to be effective at countering VE discourse, it may need to be centralized through a cross-departmental entity that is capable of flexible and responsive dialogue in real-time to match the pace of 24-hour news and social media cycles [12]. Ensuring that government policies are genuinely consistent with declared principles and values can prevent strategic government communications from giving a platform for those with VE agendas [12].

[5] Neither of these programs appear to have been evaluated for their effectiveness.

3 Recommendations for CVE policy and program developers, messagers, and researchers

As we have seen, the domains of VE and CVE on SM are continuously and quickly evolving. In some cases "backfire mechanisms" have been observed in response to early CVE efforts, including self-silencing, hushing, and the exacerbation of distrust in governments and investment in the initial narratives [17]. As well, policy-makers and researchers have demonstrated difficulty in building on past experience from CVE programs, due to a shortfall of evaluations which is in turn attributed to a lack of meaningful metrics by which to measure their effectiveness. A scan of available reviews and evaluations of CVE programs, policies, and research helped to articulate the following guidelines for ensuring ongoing CVE efforts are acceptable, effective, and measurable.

3.1 Recommendations for CVE policy and program developers

3.1.1 Convene multi-disciplinary panels to inform CVE activities

Government is in a unique position to convene actors from civil society, academics, the private sector and international organizations to inform CVE activities [12]. Public-private-partnerships and funding programs can help facilitate multi-disciplinary advisory networks that can determine ways to overcome social and technological challenges in CVE action [12]. Community leaders can help policy-makers and program designers understand what types of CVE monitoring practices community-based practitioners can endorse and what types of information they need to develop CVE activities [8].

3.1.2 Develop broad society-wide—as well as place-based and culturally contextualized—CVE policies and programs

Broad-based society-wide CVE programs addressing all types of VE founded in intolerance and extremism can ensure that communities are not stigmatized [1]. If more targeted and community-specific measures are necessary, risk-based and evidence-based metrics for assessing which communities to address can help to prevent backlash, in contrast with targeting communities based on generalized assumptions or demographic measures such as ethnic density, which is likely to arouse resentment [1]. Contextualized, place-based assessments can also help to highlight potential community-specific bases of resilience to radicalization, which can in turn be drawn upon in designing CVE strategies.

3.1.3 Sponsor non-governmental community-based actors to develop CVE programs

The risks posed by misdirected CVE engagement to community cohesion and government reputations has led to the conclusion that community-based NGOs are the most appropriate agents of CVE messaging and other activities [1]. Working with communities to develop any types of

monitoring programs that are deemed necessary helps to avoid the implication that specific communities are being unfairly targeted [8]. Communities who are themselves concerned that their youth may be at risk of VE may be highly interested in participating in CVE strategies and may welcome CVE data and techniques that can help them hone counter-narratives and other CVE strategies [8]. Such communities can also potentially help to legitimize some forms of SM monitoring activities [8].

On a tactical level, community organizations are well positioned to know their audiences' communicative and organizational nuances, to identify hallmark content pointing to VE to help shape data requirements for VE monitoring [8]. Community-based NGOs are well placed to understand and define root causes of CVE in their community, possibly including discrimination or lack of economic opportunities, which if not addressed may exacerbate disenchantment with governments [1]. They are more likely to understand what types of interventions and remedies are likely to be effective or potentially counterproductive. Community organizations are also better equipped as well to identify vulnerable individuals and are more likely to be trusted and invested with moral authority by community members, making them better able to take conversations with individuals offline where they are more likely to be effective [1]. Communities may also be better able to cultivate nuanced relationships with non-violent extremists whom governments might not want to be seen as endorsing [1].

3.1.4 Involve the private sector

Some highly promising CVE approaches are resource-intensive as well as skills-intensive. Private sector stakeholders have the potential to provide civil society with technical guidance on search-engine optimisation techniques, marketing and crowdsourcing strategies, and digital media-making talents as well as access to tools such as graphic design programs and visual editing equipment [12]. Involving the private sector may be the key, to ensuring that NGOs are operating on a similar playing field of production values and messaging effectiveness as VE groups.

3.1.5 Layer—but also distinguish—multiple CVE approaches

On one end of the intervention spectrum, engagement programs at the level of the community appear to enable CVE programming oriented towards individual members; while on the other end, the effectiveness of CVE programs is enhanced when susceptible individuals can be micro-targeted and directed to offline resources in the community grassroots; see Sections 2.2.5 and 2.2.6 [12].

Nonetheless, it is important to distinguish certain programs from each other in communications with stakeholders and the public. Introducing community-building and relationship-building programs separately from CVE programs can help to ensure that engagement and development activities are not viewed as singularly aimed at reducing CVE, which may exacerbate distrust amongst communities [1]. As well, introducing CVE programs separately from intelligence gathering or law enforcement activities can prevent the exacerbation of distrust and dispel the perception that communities are being targeted and spied upon [1].

3.1.6 Work with a CVE "theory of change" and within a CVE policy cycle

Conceptualizing a "theory of change" that describes how a CVE intervention is hoped to cause a desired outcome helps to ensure that CVE programs can be meaningfully analyzed, evaluated, and compared [1]. A theory of change for a specific intervention specifies "hypothesized causal links among program inputs, activities, outputs, outcomes, and impacts" that could achieve one or more specific outcomes in a specific target population—for instance, changes to ideology, cognition, or behaviour [1]. Simplistic, untheorized, or unmeasurable approaches to CVE can produce poor policy results and may in turn lead to disenchantment with the CVE process as a whole [1]. In turn, a CVE policy cycle that moves through tangible stages of policy development, implementation, evaluation, and assessment can ensure that lessons about VE and CVE are learned and incorporated in an ongoing way [1].

3.1.7 Retain continuity in CVE policy and program staffing

Continuity in CVE policies and programs is especially important, as starting and stopping CVE programs can elicit disillusionment and distrust amongst communities [1]. As well, continuity in staffing the programs will help to ensure that known figures can develop networks in communities and sufficiently deep relationships to breed trust [1].

3.1.8 Be alert to evolving norms and attitudes concerning privacy

The public tends to be suspicious of state activities that involve surveillance, even of open source materials, and thus online CVE programmers as well as law enforcement agencies undertaking OSINT activities must proceed with care [11]. Stakeholder engagement on privacy subjects may engage key government agencies as well as researchers, community-based CVE practitioners, and privacy and human rights officers, advocates, and lawyers [8]. As expectations are likely to vary from platform to platform and to evolve over time, ongoing assessment can ensure that measures are broadly acceptable and do not undermine the free and open internet, which is important for social and economic well-being [11]. Questions to be probed in an ongoing way may include "what constitutes truly 'open' data"; "who should be responsible and accountable for early detection"; and "when does support for enhancing the resilience of 'at-risk communities' cross the line into profiling and targeting" [13]. Additionally, public engagement, such as is being undertaken through Public Safety Canada's recently launched consultation on National Security [18], helps to ensure that policy-making is respectful of the landscape of privacy norms. As information about people's reasonable expectations of privacy is obtained, careful guidelines may be developed and followed to ensure people's reasonable expectations of privacy are met. Citizens are typically comfortable with proportionate network monitoring for specific urgent applications such as child protection, so it is possible that societal attitudes may increasingly break in this direction for CVE applications as well [8].

3.2 Recommendations for CVE messagers

3.2.1 Use positive messages oriented against behaviour, not ideas

In general, it is believed effective CVE counter-narratives are positive, inclusive, and focussed on bringing people together and on "what we are for" as opposed to the "what we are against", "us vs. them" narratives of VE groups [19]. Effective counter-narratives are simple, clear, consistent, and realistic, and offer compelling, long-term goals related to people's cultural norms, values, and interests that hold potential for progress and success [19]. Counter-messaging efforts that target extremist violence rather than extremist ideas are less likely to produce defensiveness and backlash amongst those most susceptible to VE ideologies [1].

Some especially innovative campaigns have encouraged communities or even individuals of concern to be a part of the communication strategies [12]. The European Commission-funded Radicalisation Awareness Network (RAN) working group on the Internet and Social Media (RAN @), co-chaired by the Institute for Strategic Dialogue, connects credible messengers to private sector resources; one of their sponsored products has been a graphic novel and set of online videos called "Abdullah X", developed by a former Muslim extremist [12].The Digital Disruption project led groups of young people who were considered at risk of radicalization to co-produce films that launched their own "conspiracy campaign[s]", thereby internalizing as well as disseminating independent and critical thought about the Internet amongst their peers [12].

3.2.2 Target audiences surgically

In a well-conceived CVE campaign, there are likely to be numerous distinct target audiences for CVE messaging, and it is more valuable to try to reach these audiences on their own specific terms than to create messages that "go viral" [12]. Audience profiling and marketing research may be tapped into on how to reach audiences [12]. "Trojan" advertising that concealed CVE messaging amidst material that looks like VE content, paired with Search Engine Optimization to give this material prominence in internet searches, has been used to target the most susceptible individuals [9].

3.2.3 Involve credible messengers

Counter-narratives appear to be most credible when they originate from messengers that will have authority amongst targeted groups, such as religious scholars, former VE members, and VE survivors [12], [20]. An example of a CVE projects that leverage survivors are the Extreme Dialogue project, overseen by the Institute for Strategic Dialogue (ISD) and funded by the Kanishka Project, which produced a series of short documentaries for the mass market featuring Canadians with firsthand experience of VE [11]. Others are the 2015 "Open Letter to our Sons and Daughters in Syria and Iraq" campaign by Mothers for Life that spread a counter narrative through Facebook as well as the 2011 Against Violent Extremism project, a global network of former extremists and survivors of VE groups who disseminated their information and perspectives [9]. Individuals involved should, however, have renounced violence and their VE connections and be cognizant of risks of repercussions against them [12].

3.2.4 Produce high quality and engaging messages and platforms

High production values and savvy branding in CVE are essential for combatting the often intensively produced materials of VE groups [12]. As there are no straightforward or consistently effective ways of reaching target audiences, new approaches to communication—possibly including games, cartoons, and interactive content—need to be encouraged, trialled and tested in an ongoing way [12]. Involving the private sector might be a way to expand the range of resources, tools, and skills available to non-governmental groups in their production of materials; see Section 3.1.9.

3.2.5 Use existing platforms and social networks as far as possible

Governments should be cautious about funding new websites and ideally disseminate, or help others disseminate good content into existing social networks. Setting up new websites can have the effect of dividing up the audience or not reaching an audience at all [12].

3.3 Recommendations for CVE researchers

The success of CVE programs reflected by a reduction in recruitment and incidents remains difficult to measure, as the ultimate goal of CVE initiatives is a "non-event", or the lack of VE activity [1]. Significant research is required to establish and validate proxy measures of success, including indicators of changes in attitude, behaviour, and discourse amongst susceptible individuals and groups, and building resistance to radicalizing influences amidst communities [20]. At the same time, researchers on CVE must tread carefully around sensitive issues of privacy.

3.3.1 Develop large-scale quantitative research projects

Research using databases or undertaking further data collection and analysis could help to provide sound evidence for program development and evaluation. Social network analyses that systematically gather information on online as well as offline social interactions could give context to the interaction of offline and online variables [7]. More exhaustive research on the nature and extent of extremist messaging and its impacts on target audiences could also help to inform CVE programs [12]. Large-scale research is also required for understanding what makes an effective counter-narrative campaign and to disseminate the results to civil society messengers in an operationally useful way [12].

3.3.2 Develop intensive qualitative research projects

Formats such as interviews, surveys, focus groups, research panels, and stakeholder consultations are required to provide deeper insight into appropriate CVE strategies and potential sources of backlash [1]. Longer studies that systematically code and analyze the characteristics and trajectories of people in VE networks could in turn produce more statistically significant causal information on paths leading individuals to undertake VE activity [7].

3.3.3 Undertake contextualized assessments of VE processes

Better understanding of the radicalization processes that unfold in distinct social and community contexts are required to design "theories of change", specifying what particular counter-radicalization programs are aiming to achieve [1]. Comparative analyses of radicalization in different communities may help to describe how multiple, variable causes can lead to similar outcomes in different contexts [7].

3.3.4 Transparently manage privacy concerns

Research can in itself raise concerns about privacy. Even where data is anonymized in results, there is increasing concern about "pseudo" anonymous data, where individuals could potentially be identified through cross-referencing data sets [11]. To avoid privacy concerns in social network analysis, general forms of research that seek to understand patterns can be emphasized over and above the surfacing of specific SM networks [8].

References

[1] Romaniuk, P. *Does CVE Work? Lessons Learned from the Global Effort to Counter Violent Extremism*. Global Center on Cooperative Security. Goshen, IN. (September 2015).

[2] Abdo, R. *The causes of radicalization: A review of social science literature to assess its operational utility for opens source social media research.* The SecDev Group. Ottawa, ON, (May 2014).

[3] Hafez, M. and Mullins, C. (2015). The radicalization puzzle: A theoretical synthesis of empirical approaches to homegrown extremism. *Studies in Conflict and Terrorism*, (38)1a, pp. 958–975 (2015).

[4] Hiebert, D. *Pattern analysis of events of terrorism and violent extremism in the Canadian Incident Database for use in the 2016 public report on the terrorist threat to Canada.* Canadian Network for Research on Terrorism, Security and Safety (TSAS). Vancouver, BC, (March 2016).

[5] Public Safety Canada. Building Resilience against Terrorism: Canada's Counter-terrorism Strategy. 2011. (Online) https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-eng.aspx. (Access date: 25 Oct 2016).

[6] Public Safety Canada. 2016 Public Report On The Terrorist Threat To Canada. 2016. (Online) https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-pblc-rpr-trrrst-thrt/index-en.aspx. (Access date: 25 Oct 2016).

[7] Ducol, B., et al. (2016*). Assessment of the state of knowledge: Connections between research on the social psychology of the Internet and violent extremism*. Canadian Centre for the Study of Terrorism, Security, and Society (TSAS). Working Paper No 16.05 (2016).

[8] SecDev. (2014). *Social media, online networks, and the prevention of violent extremism*. The SecDev Group. Ottawa, ON, (2014).

[9] Davies, G., et al. (2016). Toward a framework understanding of online programs for countering violent extremism. *Journal for Deradicalization*. (6), pp. 51–86 (2016).

[10] Vidino, L., et al. *Terrorist chatter: Understanding what terrorists talk about – A Working Paper*. Canadian Centre of Intelligence and Security Studies. Carleton University. Ottawa, ON, (2015).

[11] Bartlett, J. and Reynolds, L. (2015). *State of the Art 2015*. Demos. London, UK, (September 2015).

[12] Briggs, R. and Feve, S. (2013). *Review of programs to counter narratives of violent extremism: What works and what are the implications for government?* Institute for Strategic Dialogue. London, UK, (2013).

[13] SecDev. Research Portal (Online) http://preventviolentextremism.info/. (Access date: 30 Apr 2016).

[14] Government of Canada. Growing the Middle Class (Budget 2016). 22 March 2016. (Online). http://www.budget.gc.ca/2016/docs/plan/budget2016-en.pdf. (Access date: 25 Oct 2016).

[15] Adams, R. Teachers back motion calling for Prevent strategy to be scrapped. 28 March 2016. (Online) http://www.theguardian.com/politics/2016/mar/28/teachers-nut-back-motion-calling-prevent-strategy-radicalisation-scrapped. (Access date: 25 Oct 2016).

[16] Stevens, T. and Neumann, P. *Countering online radicalisation: A strategy for action*. International Centre for the Study of Radicalisation (ICSR). London, UK, (January 2009).

[17] Lindekilde, L. *A typology of backfire mechanisms, in Dynamics of Political Violence: A Process Oriented Perspective on Radicalization and the Escalation of Political Conflict*. Burlington. VT: Ashgate, (2014).

[18] Public Safety Canada. Consultation on National Security, 8 September 2016. (Online) https://www.canada.ca/en/services/defence/nationalsecurity/consultation-national-security.html?_ga=1.32379959.867201753.1462455657. (Access date: 25 Oct 2016).

[19] Schmid, A. *Al-Qaeda's "Single Narrative" and attempts to develop counter-narratives: The state of knowledge*. International Centre for Counter-Terrorism. The Hague. SW, (2014).

[20] Neumann, P. R. *Victims, perpetrators, assets: The narratives of Islamic State defectors*. International Centre for the Study of Radicalization of Political Violence. London, UK, (2015).

Annex A Federally-funded research on CVE and SM

Over the past five years, there have been two primary sources of funding for research on CVE on SM in Canada: Public Safety Canada's Kanishka Project and Defence Research and Development Canada's Canadian Safety and Security Program.

The Kanishka Project Contribution Program was founded in 2010 at Public Safety Canada by the Government of Canada as a multi-year investment in terrorism-focused research as well as in other activities necessary to build knowledge and scholarly networks. The intent of the project was to fund external research seeking to understand how terrorism is "changing over time, and how policies and programs can best counter terrorism and violent extremism in Canada".[6]

The Canadian Safety and Security Program (CSSP) at Defence Research and Development Canada, was launched jointly by Public Safety Canada and the Department of National Defence in 2012 to foster innovative science and technology advancements that contribute to the safety and security of Canadians through the anticipation, prevention, mitigation, preparation for, response to, and recovery from hazards including terrorism.[7] CSSP funds collaborative projects amongst national, provincial, municipal and international government agency partners in conjunction with partners in industry and/or academia.

We have listed these two entities' funded projects and their publications to provide a narrative of research funding of CVE on SM in Canada.[8]

A.1 Federally-funded research and associated/related publications

A.1.1 Public Safety / Kanishka Project-funded research

- **Demos Centre for Analysis of Social Media:**
  - State of the art: A review of social media research techniques that have emerged which can help to maintain public safety by preventing terrorism, preparing for it, protecting the public from it and pursuing its perpetrators (2013/2015).
- **Global Centre on Counterterrorism Cooperation:**
  - Romaniuk, P. and Chowdhury Fink, M. From input to impact: Evaluating terrorism prevention programs (2012).
  - Chowdhury Fink, M. et al. (2013) Evaluating countering violent extremism programming: Practice and progress.

[6] http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/r-nd-flght-182/knshk/frst-rnd-sccssfl-prjcts-eng.aspx.
[7] http://www.science.gc.ca/eic/site/063.nsf/eng/h_D6358D2D.html
[8] Project titles are cited in boldface and titles of publications in plain text.

- Romaniuk, P. Does CVE work? Lessons learned from the global effort to counter violent extremism (2015).

- **Institute for Strategic Dialogue:**
  - Review of programs to Counter narratives of violent extremism: What works and what are the implications for government? (2013).
- **Centre for the Prevention of Radicalization Leading to Violence:**
  - Assessment of the state of knowledge: Connections between research on the social psychology of the internet and violent extremism (PowerPoint).
  - Toward a framework understanding of online programs for countering violent extremism, Journal for Deradicalization (2016).
- **International Centre for the Study of Radicalization and Political Violence:**
  - Neumann, Peter R. Victims, perpetrators, assets: The narratives of Islamic State defectors (2015).
- **Donnybrook Research and Analysis (2011):**
  - Davies, G. et al., Terrorist and extremist organizations' use of the Internet for recruitment. (2015) Book chapter in Social Networks, Terrorism, and Counter-Terrorism. Routledge, New York, NY: Routledge. Pp. 105–127.
- **The SecDev Group:**
  - Spectral Sentinel: Advanced analytics for situational awareness and early warning of violent extremism (2013):
    - Abdo, R. The causes of radicalization: A review of social science literature to assess its operational utility for open source social media research (2014). Available on: www.preventviolentextremism.info.
    - SecDev. Social media, online networks, and the prevention of violent extremis (2014).
    - SecDev. Social Media Research—Prevent Violent Extremism: A Research Portal https://preventviolentextremism.info/.
  - Social media target audience analysis: Measuring the impact of counter narrative resources for education professionals in Canada (2015).
- **Royal United Services Institute:**
  - Performance measurement and evaluation of countering violent extremism interventions (2013):
    - Dawson L., Edwards C., and Jaffray C. et al. Learning and adapting: The use of monitoring and evaluation in countering violent extremism. RUSI Publications (2014).

- **Flashpoint Global Partners (2013):**
  - Vidino, L. et al. Terrorist chatter: Understanding what terrorists talk about. Canadian Centre of Intelligence and Security Studies Working Paper No. 03 (2015) http://carleton.ca/npsia/wp-content/uploads/Abstract-Terrorist-Chatter.pdf.
- **Trialogue Educational Trust:**
  - Briggs, Rachel and Sebastien Feve. Review of programs to counter narratives of violent extremism. London: Institute for Strategic Dialogue, July 2013.
  - Counter Narrative Resources for Education Professionals (2014).
- **The Canadian Network for Research on Terrorism, Security and Society (TSAS) (2015):**
  - Pattern analysis of terrorism and violent extremism in the Canadian Incident Database for use in the 2016 Public Report on the Terrorist Threat to Canada (2016); (funded in conjunction with Canadian Safety and Security Program).
- **Concordia University:**
  - Development of curricula to combat and prevent hate speech leading to violence and violent extremism: using social media to build resilience in Canadian youth (2015).
- **Dr. Susan Benesch:**
  - Evaluating methods to diminish expressions of hatred and extremism online (2015).
- **Fourth Freedom Forum:**
  - Evaluating countering violent extremism programming: A handbook for civil society organizations (2015).

A.1.2 Canadian Safety and Security Program-funded research

- **Canadian Network for Research on Terrorism, Security and Society:**
  - Collaborative research on countering extremist violence (2015).
  - Pattern Analysis of Terrorism and Violent Extremism in the Canadian Incident Database for Use in the 2016 Public Report on the Terrorist Threat to Canada (2016); (funded in conjunction with Public Safety Canada).
- **Defence Research and Development Canada's Centre for Security Science collaborations with federal, provincial, and municipal agencies and academic researchers:**
  - Shared resources for interventions to counter violent extremism (2015).
  - Open source intelligence: Exploiting social media and big data to fight crime and extremism in the 21st century (2015).

List of symbols/abbreviations/acronyms/initialisms

API	Application Programming Interface
BC	British Columbia
CVE	Countering Violent Extremism
FBI	Federal Bureau of Investigation
ISD	Institute for Strategic Dialogue
NGO	Non-governmental Organization
NLP	Natural Language Processing
OSINT	Open Source Intelligence
OSSM	Open Source Social Media Analytics
RAN	Radicalization Awareness Network
RCMP	Royal Canadian Mounted Police
SM	Social Media
SNA	Social Network Analysis
SOCMINT	Social Media Intelligence
UK	United Kingdom
U.S.	United States
VE	Violent Extremism

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean St., 11th Floor
Ottawa, Ontario K1A 0K2
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC DECEMBER 2013

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Countering violent extremism on social media: An overview of recent literature and Government of Canada projects with guidance for practitioners, policy-makers, and researchers

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

Waldman, S.; Verga, S.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
November 2016	28	20

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Scientific Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean St., 11th Floor
Ottawa, Ontario K1A 0K2
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2016-R229	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

Increasingly, social media is playing a role in recruitment to violent extremism, and governments are designing interventions to detect, understand, and counteract the impact of violent extremist recruitment materials on social media and other internet channels. In addition to more traditional surveillance and law enforcement interventions, authorities are increasingly focusing on policies and programs to enable preventive activities such as employing on-line counter-messaging to counteract susceptibility to violent extremist ideologies, or engaging and supporting communities in "real life" efforts to build resilience to these ideologies at the grassroots level. However, sparse metrics and a shortfall of detailed and contextualized understandings of the processes by which radicalization occur make it difficult for governments to assess the success of these policies and programs. Specifically, more evidence is needed to support direct interventions for countering violent extremism on social media and the internet with assurance. This report sums up research that has been funded by various agencies and departments of the Government of Canada into the effectiveness of different countering violent extremism activities on social media and the internet, with the intent of helping to guide further actions. After reviewing the literature on what types of interventions into violent extremism on the internet appear to work, it concludes with a set of recommendations for policy-makers, messagers, and researchers to help develop and refine counter violent extremism activities.

De plus en plus, les médias sociaux jouent un rôle dans le recrutement des adeptes de l'extrémisme violent. C'est pourquoi les gouvernements conçoivent des procédés pour dépister les méthodes de recrutement dont se servent les extrémistes violents, dans les médias sociaux et sur Internet, pour comprendre ce phénomène et contrer son incidence. En plus d'employer les procédures traditionnelles de surveillance et d'application de la loi, les autorités s'en remettent de plus en plus à des politiques et des programmes de prévention comme l'utilisation du contre-discours en ligne afin de neutraliser l'attrait de l'idéologie des extrémistes violents, ou encore à la mobilisation et au soutien des collectivités par des mesures réelles pour opposer une résistance à cette idéologie au niveau de la base. Toutefois, en raison de la rareté des mesures et d'une compréhension insuffisamment détaillée et contextualisée des processus à l'origine de la radicalisation, les gouvernements ont du mal à juger du succès de ces politiques et programmes. En particulier, il faudrait davantage d'éléments probants pour appuyer des interventions directes permettant de combattre avec assurance l'extrémisme violent dans les médias sociaux et sur Internet. Dans le présent rapport, on résume les travaux de recherche financés par divers organismes et ministères du gouvernement canadien pour trouver des méthodes efficaces de lutte contre l'extrémisme violent dans les médias sociaux et sur Internet, méthodes qui serviront à orienter d'autres actions. Après avoir passé en revue ce qui a été écrit sur les types d'interventions qui semblent fonctionner contre les manifestations de l'extrémisme violent sur Internet, les auteurs du rapport concluent en donnant un ensemble de recommandations aux décideurs, aux messagers, et aux chercheurs pour les aider à créer et à perfectionner des activités permettant de contrer l'extrémisme violent.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Violent extremism; CVE (countering violent extremism); radicalization; counter-radicalization; community engagement; social media; SOCMINT (social media intelligence); OSINT (open source intelligence).