Partnerships for Preventing Online Radicalisaton

Susan Szmania and Matt Conway

1 June 2017

As a response to the attacks by violent extremists around the world, policymakers have invested considerable effort into comprehending terrorists' use of the Internet and initiating counter-measures.

Author's Note: *The opinions expressed by the writers are theirs alone and not necessarily those of the United States government or any of its departments.*

The internet is undeniably an important factor in understanding the radicalization trajectories of many violent extremists. A senior official at the U.S. Department of Homeland Security recently observed that extremists' "deft use of Internet propaganda, together with that content's wide availability, has broadened the population of potentially vulnerable individuals, and shortened the timespan of their recruitment." Supporting this statement, terrorism expert Magnus Ranstorp lists social media as one of nine factors that may exacerbate causes of an individual's radicalization, including individual and social factors as well as cultural and ideological motivators.

Research has also shown that the internet facilitates both early engagement with violent ideologies and opportunities for learning and sharing criminal information. For instance, a study by the University of Maryland's START terrorism consortium found that "the internet played a primary or contributing role in the radicalization of 86%" in the cases of over 200 U.S.-based foreign fighters. These individuals used the internet to "view extremist materials, research conflicts, groups and attack methods, and participated in online communities of like-minded individuals." Moreover, results from the same dataset show that the internet "may be speeding up the radicalization timeframe" as compared to radicalization before the advent of the internet.

Latest

An Update on the Security Policy Change Programme

Chances for Peace in the Third Decade

A Story of ORG: Oliver Ramsbotham

A Story of ORG: Gabrielle Rifkind

Most read

The Role of Youth in Peacebuilding: Challenges and Opportunities

Making Bad Economies: The Poverty of Mexican Drug

Similar findings from a study of over 200 terrorist offenders in the United Kingdom found that 54% of the perpetrators used the internet to learn about their intended criminal activities and, in 44% of the cases, extremist media (e.g., videos, audio lectures and photographs) were found, viewed, or downloaded by the perpetrators.

The authors of the UK study, however, recognize that terrorists' use of the internet "is perhaps unsurprising given the ubiquity of Internet usage in the most benevolent activities across wider society." Indeed, a good deal of research has examined terrorists' expansive use of the internet, such as the terrorist organization known as the Islamic State of Iraq and Syria (ISIS) to build a network of ideological conformity through social media platforms like Twitter. A report from the Institute for Strategic Dialogue has shown not only how life under the Islamic State is romanticized through social media postings, but also how important digital connectivity can be to those in the field, describing young women in ISIS controlled territory who resort to "climbing pine trees to gain Internet reception."

Countering extremism online

These studies shed light on the particular ways that terrorists use the internet and underscore the importance of law enforcement intervention into online criminal activities. However, an ongoing challenge for researchers and policymakers engaged in preventing and countering violent extremism (CVE) is how to proactively address the role of the internet and social media in the context of violent extremism before criminal activity has occurred. To respond to that challenge, two broad policy approaches have emerged. One approach advocates for online content removal and account suspension in order to reduce the supply of non-criminal but potentially extremist content. The European Commission recently instituted content-flagging

Cartels

ORG's Vision

Remote Warfare: Lessons Learned from Contemporary Theatres

mechanismsmodelled after an initiative by the British government's Counter Terrorism Internet Referral Unit. Outside of government, technology companies also have taken steps to remove terrorist content. In December 2016, social media companies announced their own cooperative efforts to use hashing techniques to quickly identify and take down extremist images and content that violate terms of service agreements. In their latest annual transparency report, Twitter suspended around 636,000 accounts between August 2015 and December 2016 for promoting extremist content.

Research studies that have assessed whether content removal and account suspension efforts work to curb the propagation of violent extremist messages suggest promising outcomes. For instance, a report from the George Washington's Program on Extremism found that "over time, individual users who repeatedly created new accounts after being suspended suffered devastating reductions in their followers." While ISIS users quickly learn how to overcome account suspensions and restore some followers, the study suggests these actions to reestablish followers have only "limited benefits" once a suspension has occurred.

Yet, as technology companies like Twitter, Microsoft, and Facebook become more effective at detecting extremist content with tools that recognize unique "fingerprints" of extremist content, terror groups have also become more agile in how they use the internet to facilitate their work. Terrorism researcher Audrey Alexander describes how attempts to limit terrorist content online have pushed extremists away from public platforms and to encrypted tools like WhatsApp, Telegram, and ProtonMail. Indeed, Telegram now "appears to be the top choice among both individual jihadists and official jihadist groups." The covert nature of these platforms poses significant barriers to

researchers and authorities seeking to understand, track, and measure the terrorist threat.

Another method for combatting online violent extremist content suggests creating counter narratives to refute terrorist claims. The idea is to craft messages that will appeal to vulnerable individuals to persuade them that violence is not the answer. To explore this approach, the U.S. government has sponsored an initiative along with support from Facebook that known as the Peer to Peer: Challenging Violent Extremism program to engage young people, who may be most vulnerable to violent extremist messages, to create credible counter message for their own peers. Since the program launched in 2015, over 5,000 students have taken part. The 2016 winning team from Rochester Institute of Technology developed an awareness campaign called “Ex-Out Extremism” to “open people’s eyes” to violent extremism and to encourage them to take a stand against it. While initiatives like Peer to Peer typically reach broad audiences, foster educational engagement and increase public awareness, researchers have pointed out that continued work is needed to understand what can inoculate or prevent radical ideologies from taking root in the first place.

A more targeted approach for reaching at-risk individuals online has been piloted at Jigsaw, Alphabet’s technology incubator focusing on geopolitical challenges, to redirect users from ISIS propaganda to curated YouTube videos that credibly debunk ISIS recruiting themes. Similarly, the Institute for Strategic Dialogue conducted a pilot study to direct individualized online intervention services to those demonstrating affinity to violent extremist groups through their online activities. The results found that intervention messages that reached at-risk individuals were “highly likely” to cause behavior change, either

by prompting radicalizing individuals to change their privacy settings or to send direct messages to the intervenors for more engagement. While these results are based on a very small sample, directed intervention programs may offer options for providing “off ramps” to individuals at critical points.

The value of partnerships

Whether intervening online to remove content and suspend accounts or developing credible counter messages or intervention options, effectively addressing violent extremism will require innovative partnerships inside and outside government. To this end, in 2016 the United States government launched an interagency task force to address countering violent extremism with representation from both security and non-security agencies along with engagement from civil society groups. While these multidisciplinary partnerships are challenging bureaucratically, they underscore the need for developing networked approaches to emerging security challenges. Similar cooperative agreements might span across national boundaries, not only for the purposes of information sharing between law enforcement officials, but also to include cooperation, such as the recent announcement by the Netherlands and Kenya to build a comprehensive partnership around a range of security related issues including deradicalization efforts.

Although some have suggested that there is little evidence that terrorism prevention works, there is a small but growing literature providing support for the application of prevention science to the problem of violent extremism. Without question, more attention is needed for rigorous assessment of these programs, especially with regard to evaluating the effectiveness of online campaigns. To fill this gap, the RAND Corporation recently released an evaluation toolkit for countering violent extremism, which includes

guidelines for assessing programs' social media metrics. The London-based Royal United Services Institute has published a guide to CVE program design and evaluation, which provides guidance for articulating relevant impact measures. Ultimately, these resources, coupled with innovative public and private sector partnerships, will contribute to preventing radicalization to violence both online and offline.

Tackling online radicalization will undoubtedly be a major security priority for policymakers in the future. Following the deadly May 22, 2017 bomb explosion in Manchester, leaders of the G7 convened in Taormina, Italy to reaffirm their efforts to counter terrorism and violent extremism. In a statement, members underscored several areas for continued engagement, not only through traditional counterterrorism measures like "knowledge-sharing" and cutting off "sources and channels of terrorist financing," but also through technology sector engagement "to substantially increase their efforts to address terrorist content" and well as civil society engagement to promote "alternative and positive narratives rooted in our common values." The future war against online extremism may prove to be a long and difficult one, but it is a fight that must be won.

Image credit: Andres Eldh/Flickr.

Dr. Susan Szmania has served in government and academic positions addressing violent extremism. She is currently a senior research analyst at the U.S. Department of Homeland Security in the Office for Community Partnerships. In this capacity, she leads the research and analysis line of effort on the U.S. government's interagency Countering Violent Extremism Task Force. Prior to this work, Dr. Szmania was a senior researcher at the University of Maryland's National Consortium for the Study of Terrorism and

Responses to Terrorism, and she served in government positions at U.S. Embassies in Sweden and Spain to implement programs to counter violent extremism. She received her Ph.D. in Communication Studies from the University of Texas at Austin in 2004.

Matthew Conway has served in various research capacities focusing on conflict and extremism, both independently and with two London-based think-tanks. He is currently a research adviser for the Department of Homeland Security's Office for Community Partnerships, where he focuses on Countering Violent Extremism research. He received his Master's in Conflict, Security and Development from King's College London in 2015 and his Bachelor's in Political Science and International Studies from the University of Wisconsin-Madison in 2013.

Share this page

Contact

Unit 503
101 Clerkenwell Road London
EC1R 5BX
Charity no. 299436
Company no. 2260840

Follow us

Useful links

Login
Contact us
Sitemap
Accessibility

Email us

020 3559 6745