Inter Agency Paper

No. 17W
November 2015

Countering Cyber Extremism

Megan Penn, Joshua K. Miller and Jan Schwarzenberg

Arthur D. Simons Center
for Interagency Cooperation

Fort Leavenworth, Kansas

An Interagency Occasional Paper published by the CGSC Foundation Press

Countering Cyber Extremism

Megan Penn, Joshua K. Miller and Jan Schwarzenberg

Arthur D. Simons Center
for Interagency Cooperation

Fort Leavenworth, Kansas

InterAgency Paper No. 17W, November 2015

Countering Cyber Extremism

by Megan Penn, Joshua K. Miller and Jan Schwarzenberg

Megan Penn is the Director of Global Education with United Nations Association of the National Capital Area (UNA-NCA). Before joining UNA-NCA and Global Classrooms DC, she was a research intern at the Center for a New American Security in the Technology and National Security program, and a former curriculum specialist with UNA-NCA. Penn received a M.A. in Security Policy Studies from the George Washington University, Elliott School of International Affairs. She received a bilingual honours B.A. in International Studies from York University, Glendon College in Toronto, Canada. Penn has professional experience in business development, aviation, and has been published in Canada and the U.S. on cyber security policy, mobile technology and cybercrime.

Joshua Miller is a Foreign Affairs Officer on the Pakistan desk, in the Office of the Special Representative to Afghanistan and Pakistan at the U.S. State Department. Miller is a recent graduate from the Elliott School of International Affairs' Master's program, earning a degree in Security Policy Studies with concentrations in Transnational Security Issues and U.S. National Security Policy and Process. Miller earned his bachelor's degree at an American university in Switzerland.

Jan Schwarzenberg is currently an M.A. candidate in the Security Policy Studies program at the Elliott School of International Affairs, George Washington University, focusing on emerging transnational threats. A retired U.S. Navy Special Operations Officer, Schwarzenberg has worked exclusively in counter terrorism and counter insurgency, in both military and civilian positions, since the attacks of 9/11. This has included combat deployments in four different countries around the Middle East and Southwest Asia. Schwarzenberg holds undergraduate degrees in Political Science and Criminal Justice, studied in Italy for a year and a half, and has a Master's in Diplomacy and Military studies. He is also a graduate of the U.S. Naval War College, Joint Forces Staff College, and the National Defense University. He is currently a federal officer employed by the Department of Defense.

Questions about this paper and the InterAgency Paper series should be directed to the Arthur D. Simons Center, 655 Biddle Blvd., PO Box 3429, Fort Leavenworth KS 66027; email: office@TheSimonsCenter.org, or by phone at 913-682-7244.

Contents

Introduction

Violent extremist organizations have increased their online presence using the Internet to establish an online brand, communicate with members, and radicalize sympathizers. The regular use of online media, forums, and communications has altered the way that governments, non-governmental organizations (NGOs), and private companies must approach countering violent extremism online. Currently, U.S. policy is ineffective in countering cyber extremism. For example, law enforcement has poorly intercepted vulnerable sympathizers, and the government has utilized unsuccessful counter-messaging campaigns against violent extremist organizations. With U.S. law respecting the difference between merely accessing online extremist sites and doing so with the intent to do harm, there is a major gap in identifying and interdicting radicalized recruits who travel overseas to join violent extremist organizations or remain at home to commit jihad here versus those who are simply curious.

With U.S. law respecting the difference between merely accessing online extremist sites and doing so with the intent to do harm, there is a major gap in identifying and interdicting radicalized recruits...

This paper provides seven recommendations for countering violent extremism to the U.S. government, private companies who host these online platforms, and NGOs who provide an alternative voice and expertise to the issue. The U.S. government, NGOs, and communities all play a role in counter-messaging extremist organizations' online presence. While this paper touches upon a number of themes and recommendations for U.S. government policy on countering violent extremism, there are many more avenues that can be explored from private sector, law enforcement, and international perspectives.

First, the U.S. government should create stimulating counter-messaging campaigns with the assistance of third party groups, specifically those who have a connection to the violent extremist community. In the case of Islamic State of Iraq and Syria (ISIS), the State Department's Center for Strategic Counterterrorism Communications must work with Muslim influences abroad to develop strong partnerships and communication among involved communities.

Second, NGOs must be given more tools to counter violent extremism, as they provide an alternative, impartial voice and can often bring together parties that governments are unable to access. For example, Google Ideas' Against Violent Extremism has managed to bring together victims and past members of violent extremist organizations to discuss how to counter extremist ideology

stemming from terrorism, gangs, and supremacist organizations.

Third, communities are best situated to provide citizens with a strong counter-violent extremist message. Including them in counter-messaging campaigns builds trust, ensures grass-root involvement in countering extremist violence, and, most importantly, gives direct access to vulnerable persons.

Fourth, with violent extremists using cyberspace to spread their messages, there should be an equally strong counter-message online. This message can come from a number of groups and influential individuals, but it must be cohesive to be most successful as a counter-message campaign against the extremists.

Fifth, once vulnerable persons have been identified, their need to be rehabilitated is necessary to preclude an attack. The United Kingdom's Channel Project has been successful in this and should be adopted in the U.S.

Sixth, the private sector that owns the databases and platforms used by violent extremist groups should more proactively self-regulate to ensure customers are following the terms of use.

Lastly, the role of law enforcement in protecting national security is incredibly important in responding to this online and physical threat. Necessary legal authorities already exist but have not been used to their fullest capacities. Combining the PATRIOT Act with counter-terrorism authorities within Article 18 of the U.S. Code allows law enforcement to monitor both extremist websites and the persons entering them to uncover any potential violent plots.

Combining the PATRIOT Act with counter-terrorism authorities within Article 18 of the U.S. Code allows law enforcement to monitor both extremist websites and the persons entering them to uncover any potential violent plots.

Due to the complexity of countering violent extremism, a combination of these options should be utilized to address the varying needs of all stakeholders. Embracing a whole-of-government approach coupled with the private sector, NGOs, and community engagement is the most effective strategy to address this ever-evolving and challenging issue.

Background

Since 9/11, violent extremist organizations have employed one tactic in common despite their varying motivations: They use the Internet to communicate with other members, potential recruits, and sympathizers. Extremist forums and websites offer a significant amount of information to their recruits, including organizations' missions, doctrines, and histories. They allow extremist organizations to communicate intimate information about their causes and themselves to potential sympathizers. Extremists often highlight their enemies and justify violence against them, which motivates lone wolves to act. Through the personal maintenance of their online presence, extremists are able to liaise directly with their target audiences without their message being distorted by mainstream

media or government entities. The Internet has become a major source of radicalization for potential recruits. It has the advantage of reaching a global audience at minimal expense without the need to bring recruits to a central location for indoctrination. Thus, the use of websites and the Internet by extremists has fundamentally altered the methods in which governments, law enforcement entities, the private sector, non-government entities, and average citizens must address these threats with one another. This has created an expanding gap in contemporary society, necessitating constant change and adaptation to address the evolving threat.

Identifying the Challenge

The issue is how to counter violent extremist organizations that radicalize and recruit sympathizers via the Internet. Streaming extremist ideology over the Internet cannot be halted at the border, as it once might have been when a U.S. Customs officer was able to seize seditious material. Countering these organizations is achieved by counteracting the effectiveness of the extremist ideology by countering extremist messaging, preventing attacks within the U.S. inspired by the online ideology, and identifying and apprehending extremist sympathizers within the U.S.

The lone-wolf phenomenon represents the success of online radicalization. The lone wolf, inspired and instructed via the Internet, plans, prepares, and executes attacks in his or her home country while evading apprehension. As Clint Watts notes, while U.S. law enforcement has been notably successful in disrupting lone-wolf attacks, the marked rise in such attacks represents the greatest radicalization threat to the U.S.[1] The difficulty behind lone-wolf attacks lies in the fact that it is extremely challenging to detect and interdict. Major Nidal Hasan's attack at Fort Hood in 2008 and Anders Breivik's attack in Norway in 2011 highlight these challenges.[2] In fact, very few of America's accused extremists appear to have arrived at jihadism through adherence to radical scripture. Watts notes that while some extremists rigorously delve into ideological scripture, most pull their understanding of militant Islam disparately from the Internet.[3] Other contributing factors may also lie outside of ideological piety. Watts indicates the unique challenges the new generation of Americans currently face, including "the disease of being disconnected—a plight of depressed, socially isolated, and mentally vulnerable youth more connected virtually with society than physically."[4] A recent American Pediatrics Report substantiates Watts's claim; it indicates that many who grow up in the cyber era face challenges such as cyberbullying, social anxiety, severe isolation, and what doctors are now identifying as Facebook depression.[5] The troubling consequence of this phenomenon is that

...while U.S. law enforcement has been notably successful in disrupting lone-wolf attacks, the marked rise in such attacks represents the greatest radicalization threat to the U.S.

more adolescents may increasingly suffer from this issue, resulting in further radicalization and potential lone-wolf attacks in the name of a variety of extremist ideologies.

Review of Current Policies

While many European countries have developed sophisticated programs to counter violent extremism, the U.S. has a woefully underdeveloped counter-extremist capability. This can be attributed to the fact that the size of the extremist threat in the U.S. is significantly smaller relative to European allies.[6] The U.S. has significantly more law enforcement tools at hand and a larger security apparatus to address counterterrorism issues directly. The Federal Bureau of Investigation, for example, acknowledges extremism as a complex threat due to varying motivations, levels of expertise, and tactics. As a response, the Bureau has increased its number of agents by 40 percent and now allocates approximately half of its resources to counterterrorism and the remaining half to all other criminal activity. Between 2001 and 2011, the Bureau almost tripled its intelligence analyst workforce.[7] In spite of having a significantly larger law enforcement capacity relative to others, the U.S. has not emphasized or allocated a sufficient amount of resources to countering violent extremism. This has largely stemmed from America's interpretation of counter-violent extremism in general. The U.S. has been addressing the symptoms of extremism solely from a criminal perspective and not the root causes of its existence.

The U.S. has poorly developed a counter narrative and counter message against extremists in spite of addressing this issue for over a decade.

The U.S. has poorly developed a counter narrative and counter message against extremists in spite of addressing this issue for over a decade. In 2011, the U.S. developed the State Department's Center for Strategic Counterterrorism Communications (CSCC) [8] to fulfill this mission. While laudable in its efforts, the CSCC has displayed a significant degree of ineptitude in producing an effective counternarrative.[9] In fact, many acknowledge the body has actually assisted extremist elements in their recruitment efforts.[10] Arguably still in its infancy, the CSCC is vastly under resourced and forced to keep up with a myriad of extremist groups, which has exacerbated its failures.

As part of developing a greater counter narrative, the U.S. government has also poorly enabled NGOs to play a bigger part in such an effort. While the government has funded some programs in the non-profit sector, the quantity and frequency of such funding has been largely insufficient. The U.S. government has lost credibility in many regards by not using non-governmental entities, which has served to assist extremist groups in their efforts.[11]

Need for Change

While violent extremist organizations have used social media for communication and recruitment in the past, their online presence has increased recently in large part due to ISIS's relative success in using social media to recruit members from abroad. Until recently, the U.S. government has been slow to meet and bring counter extremist stakeholders together. The White House's Countering Violent Extremism Summit in February 2015 was originally scheduled for Fall 2014, but was continually delayed until the recent attacks in France.[12] During this time, foreign fighter recruitment by violent extremist organizations increased, requiring a reevaluation of the U.S. government's efforts to counter them.[13] Now is the time for creative new approaches that can be applied to numerous such organizations, not just ISIS, and these new approaches must include actors outside the U.S. government.

Countering extremist organizations online requires the participation and involvement of multiple entities. The government alone does not have the capability to combat these organizations, since private companies own the networks and platforms. Given that NGOs and non-profits often have more accessibility to countries due to their third-party and impartial status, there must be a partnership between these groups and local communities.

Countering extremist organizations online requires the participation and involvement of multiple entities.

Discussion

Many analysts focus only on militant Islam as the culprit for radicalization. Major Hasan had an active correspondence with Al Qaeda in Yemen;[14] Zale Thompson, who attacked four New York City police officers with a hatchet, had downloads from extremist websites advocating beheadings and attacks;[15] Alton Nolen, who beheaded a co-worker at an Oklahoma factory, was inspired by recent extremist activities in the Middle East;[16] and John Booker, who attempted to bomb Fort Riley, admitted he did so in support of ISIS.[17] The real fear, however, is the empowerment and encouragement given to lone wolves to stay at home and fight their war among us. The Al Qaeda and ISIS online magazines "Inspire" and "Dabiq" constitute a highly developed form of outreach. Both give cogent arguments to support the jihad, as well as detailed instructions for building homemade bombs. An initial response might be to shut down the websites espousing extremist ideology that advocate violence or describe how to make explosive devices. In the wake of the January 2015 Charlie Hebdo attacks, France enacted legislation enabling the government to direct Internet servers to shut down objectionable sites.[18] However, this is a futile and impossible task for numerous reasons. First, it is physically impossible to survey the entire Internet to uncover, identify, and then shut down websites being

used by extremist organizations. Trying to cover the entire Internet for objectionable sites is a commitment of manpower that does not exist and, as mentioned, has little return for the investment. Second, one IP address can contain hundreds of URLs held in reserve. As soon as one is shut down, it can be instantly replicated. Furthermore, as discovered with criminal organizations engaging in cybercrime, websites managed in foreign areas, especially those with lax law enforcement, are beyond the reach of U.S. authorities. Lastly, even if an individual site overseas can be traced and its location identified, it might only be a relay point bouncing or re-transmitting information originating elsewhere.

While the government holds the authority to respond and combat violent extremist organizations, they lack ownership of the technology and networks.

While the government holds the authority to respond and combat violent extremist organizations, they lack ownership of the technology and networks. In contrast, NGOs often have access to local communities and countries that establish beneficial communications and programs on the ground. Therefore, what is required is a partnership composed of government, NGOs, local communities, and the private sector. However, the authority, responsibilities, capabilities, and roles differ among these actors and must be taken into account to realistically create ways to counter cyber extremism. Thus, for a holistic approach to countering violent extremism, policy options must be broken into themes of counter messaging, intervention and rehabilitation, private sector self-regulation, and law enforcement.

Counter Messaging

Counter Messaging: U.S. Government

As noted, the State Department's CSCC's efforts have yielded marginal results in developing an effective counter narrative. The majority of the CSCC's efforts lie in the body's Digital Outreach Team, which attempts to counter extremists' messages in Arabic, Urdu, Punjabi, and Somali via social media platforms such as Twitter and Facebook.[19] However, the CSCC's counter messages are subjected to a reviewing process before publication. This delays the responsiveness of the government's message, which intuitively goes against the purpose of social media—real time communication and conversation. Unfortunately, government attempts at counter messaging will never be as stimulating—visually or otherwise—as extremist organization's messages due to agency restraints and capabilities.

There are, however, potential downsides to empowering third-party capacity-building programs. The government cedes control of crafting the counter message to a third-party entity, thus risking a

narrative that diverges from the government's interests, which the government has committed to funding.

Some initiatives at the State Department have had some visible successes in capacity building. The Department successfully worked with social media experts, including playwright Wajahat Ali, to provide social media training to key Muslim influencers abroad. Training sessions were held in Pakistan, the Philippines, Singapore, Malaysia, and Jakarta, where individuals were introduced to using social media tools such as Facebook, Twitter, and LinkedIn[20] to counter animosity and extremist ideology online by building bridges between communities.[21] The instructor of the workshop, as a respected scholar not affiliated with the government, commanded credibility. Additionally, these workshops were hosted in the participants' country, which enabled many of the indigenous population to attend. The promising results of these workshops and training sessions suggest the U.S. government should reallocate resources toward these initiatives.[22] A counter message from the government is important because of the authority it holds in the international community, however, it should not be the sole message used to counter violent extremism.

Counter Messaging: Non-Governmental Organizations

Founded in 2010, Google Ideas is a think tank using technology to address complex and intractable problems. In its first project, Google Ideas tackled radicalization by creating a network, Against Violent Extremism, made up of renounced religious extremists, gang members, neo-Nazis, survivors of attacks, NGOs, and business partners.[23] Google Ideas hosted a conference that helped to identify the common threads of extremists' experiences and connect these activists with potential funds. Ultimately, they commissioned research that highlighted how positive role models and personal relationships can keep individuals from entering extremist groups and can also facilitate their departure from those groups.[24] Given NGO's ability to circumvent bureaucratic malaise and be distanced from governmental interests, the U.S. government would greatly benefit from forums similar to Against Violent Extremism.

[Google Ideas] commissioned research that highlighted how positive role models and personal relationships can keep individuals from entering extremist groups and can also facilitate their departure from those groups.

While funding currently does exist for NGOs, the U.S. government has failed to fully utilize existing programs and opportunities to counter extremism. By committing more resources through indirect small-grant donations, these initiatives could produce effective grass root counterweights

to extremist messaging. Additionally, the government's indirect funding creates the necessary distance between the program and governmental influence, appropriating program oversight to the impartial NGO. The U.S. government must also cooperate with these organizations to create a unified counter extremism message. Lastly, the government must include NGOs as regular partners in its summits and conferences to take greatest advantage of their expertise in this area.

Foundations and private sponsors offer a unique and beneficial value in countering extremism. Lorenzo Vidino argues that these groups are "unencumbered by the vast bureaucracy that saddles government agencies, and so may have more ability to consider any requests for funding or capacity-building assistance on a case-by-case basis."[25] Moreover, foundations and private sponsors could also monitor the impact of their efforts more readily and choose to halt or expand funding as the situation dictates. Finally, Vidino asserts, private sponsors and foundations "...are in a position to side-step thorny issues of ideology by basing assistance on specific and defined program objectives such as de-radicalizing individuals already on an extremist path, providing online safety training, or fostering interfaith relations."[26]

Counter Messaging: Community Outreach

Radicalization is largely occurring at the local community level. Of the counter messaging options discussed, the most important method is the involvement of communities in deterring potential sympathizers and recruits. The government must connect with these communities and encourage local law enforcement to incorporate these communities into its strategies for countering violent extremism. These efforts create new role models that promote moderate religious teaching to counter extremist narratives. Furthermore, providing a platform for former extremists to describe their experiences within extremist organizations can deter others interested in supporting extremists. They can provide a counter voice to the radical messaging of extremist websites. The de-radicalized extremist is the perfect bridge to such communities. They are perfectly suited to actively counter extremists' messages while also uncovering active extremist recruiters in the community. They can serve as ambassadors to lay and religious leaders to diffuse the romantic allure of becoming an extremist.

The de-radicalized extremist is the perfect bridge...They are perfectly suited to actively counter extremists' messages while also uncovering active extremist recruiters in the community.

The risk in working with de-radicalized extremists is the potential for their ideology to function as a "conveyor belt" for radicalization and lay the ideological groundwork for subsequent violence.[27] There must be a unified counter extremism message. Without proper coordination and cooperation between these

communities and the government, members may become frustrated and jaded with the U.S. approach to countering extremism. Lastly, law enforcement must be willing to work with local communities to make de-radicalized extremists accessible to vulnerable groups.

Counter Messaging: Online

The use of online and social media platforms by third-party entities and individuals to counter extremism is largely underdeveloped. There have been attempts to fill this gap, but they are either too new to accurately judge their impact or have been unsuccessful in reaching their objectives. These attempts lack stimulation and cohesiveness, inadvertently provide avenues for extremist organizations to defend their ideology, often result in trivial arguments and discussions, and fail to grasp the audience's attention effectively or directly connect the user. One example is the State Department's Peer 2 Peer: Challenging Extremism program, which encourages college students to develop digital material to counter message extremists online, specifically through social media.[28] Another example is the State Department's #ThinkAgainTurnAway campaign on Twitter and Facebook, where the mission is to "expose the facts about terrorists and their propaganda."[29]

An effective online counter narrative may be better served through the notion of a "Dead Facebook," which would provide an avenue for viewers to remember victims of extremism, in effect humanizing them to an often-desensitized audience.[30] The ideal website would compile in one location all the quotes and imagery of the victims, the defectors who have recanted, model members of the community, and the moderate credible scholars in order to effectively provide a counter narrative. Highlighting extremists' connections to criminal enterprises could go a long way to denigrating extremists' appeal and credibility in the eyes of peers, followers, and sympathizers.[31] The Philippine government used this tactic after the Superferry bombing in 2004 that killed 116 persons.[32] In a coordinated media blitz displaying vignettes of the victims' lives and communicated through six languages, the government was able to generate widespread public support against the extremist groups responsible for the bombing.[33] As a result, extremists who had previously enjoyed free range of movement throughout the community were isolated in the central swamp areas.[34] Their bullying tactics were no longer effective in the face of the anger created by the images of the many youthful victims of their attack, accompanied by a surge of anonymous tips to the police hotline.[35]

Highlighting extremists' connections to criminal enterprises could go a long way to denigrating extremists' appeal and credibility in the eyes of peers, followers, and sympathizers.

Through the power of negative imagery, "Dead Facebook" exposes violent extremists' hypocrisy through quotes and pictures. Frank Cilluffo adds that these images must be accompanied with

a corresponding "push to highlight the human toll, measured in the hundreds and thousands of lives lost, that our adversaries have caused. Unless and until we capture and convey the lost dreams, hopes, stories, and opportunities, we will not have done justice to victims of terrorism and their survivors."[36] "Dead Facebook" can garner public support against extremism, while also undermining extremist recruitment among those who would not have been deterred otherwise. Having a multilateral institution such as the UN sponsor such an initiative would add great legitimacy and support to the website. In effect, the U.S. would be able to leverage its weighted position in the UN to shape the UN's role as a "forum and conduit for the exchange of facts and trends observed and emerging in the neighborhood and language(s) used in each United Nations Member state."[37]

While "Dead Facebook" provides a centralized platform for victims of extremist attacks, it requires incredible upkeep. It also requires users to actively access the platform, as they would any other social media website, to find information on the attack and its victims. However, hostile governments may find ways to restrict access to "Dead Facebook" if they do not believe the posted narrative, which would severely limit access to the stories of the victims.

Intervention and Rehabilitation

Part of the holistic approach to countering the overall effect of extremist ideology is to recover those individuals who have succumbed to its lure.

Part of the holistic approach to countering the overall effect of extremist ideology is to recover those individuals who have succumbed to its lure. In the United Kingdom, the Channel Project is designed to help identify these vulnerable persons before they commit an attack or are completely radicalized.[38] It brings together representatives and agencies, including law enforcement, intelligence, community leaders, and academic centers, each with specifically outlined duties. Channel uses three indicators to assess an individual's vulnerability: engagement with a group or ideology, intent to cause harm, and capability to cause harm.[39] These indicators allow Channel to assess vulnerable persons before they commit an act, identify them, and give them an option for rehabilitation compared to prosecution. Implementing a similar program in the U.S., one that includes community involvement and law enforcement, could be incredibly successful in identifying vulnerable persons and engaging with them before they participate in extremist behavior and actions. Furthermore, such programs build relationships and strengthen trust between the government and communities and, most importantly, allow communities to be involved in identifying socioeconomic factors of deradicalization.[40] Before Abdullahi Yusuf, a Somali American, was charged with attempting to join ISIS, the U.S. attorney in Minnesota met with community leaders.[41] Later,

Yusuf was sentenced to a program for troubled boys.[42] This example also showed that, "the journey on the path to terrorism does not have to end in handcuffs; it can end with a handshake."[43] If communities know radicalization is not an automatic jail sentence, they may be more forthcoming in identifying vulnerable youth.[44] This type of program, which allows for law enforcement intervention prior to an attack or an individual joining a violent extremist organization, does not currently exist across the U.S.[45]

However, test programs similar to the United Kingdom Channel Project have been implemented in select cities.[46] Unfortunately, these pilot programs are on an ad hoc, municipal level with little to no federal funding and have no central oversight. There are no state or federal standards in place to determine when to intervene or prosecute. This policy option recommends that the federal government fund state law enforcement and NGOs who have already established intervention programs and establish standards for such programs. Without this involvement, these pilot programs are sure to fail due to lack of accountability, resources, and intelligence.

These programs carry risk. One failure and the careers of those involved are over.[47] The fear of political backlash and public opinion could dissuade persons from future intervention programs.[48] Certainly, the most dangerous individuals should not be part of the program. Only those accused of minor, lesser offenses may be eligible. Those individuals who return to their extremist views and counsel others to turn away as well must be judged against those who did not return to extremism. Furthermore, there is a loophole for those who have broken no laws. Unlike at-risk minors and individuals under court orders, as in Yusuf's case, it is more difficult to intervene and rehabilitate those who are not threatened by legal reprecussions.[49]

The private sector could help counter extremism through greater self-regulation.

Private Sector Self-Regulation

The private sector could help counter extremism through greater self-regulation. The government lacks the authority and ownership of electronic networks and, therefore, is unable to enforce terms of use and existing laws. The Digital Terrorism and Hate Report, published every year by the Simon Wiesenthal Center, releases a report card that measures the proliferation of hate and terror online across the social media, blog, and website spectrum. In the 2013 report card, Facebook received a grade of A-, reflective in the fact that Facebook has taken tremendous steps to identify and eliminate digital hate on its platform. YouTube landed a C-, indicating it must significantly improve. The worst offender was Twitter, earning an F, showing the company's ineptitude in coping with the influx of users and their content.[50]

The biggest barrier to private company cooperation in countering violent extremism is incentive. Private companies would have to bear a number of costs. One is the financial burden in allocating more time, labor, and resources to address this issue. Smaller companies will find this challenging and may be forced to shut down the company completely if unable to combat and remove extremist users. Companies are also accountable to their shareholders. Companies will look to their profit margins before taking on causes that threaten business. While the company may gain a poor reputation if they are known for aiding extremist communications, they must also worry about the repercussions from violent organizations when their accounts are disabled. For example, after blocking ISIS accounts on Twitter, founder Jack Dorsey and CEO Dick Costolo were both threatened by alleged ISIS sympathizers.[51] These individuals have not actively chosen to engage in an "online war" with extremist organizations. They are simply holding customers to the company's terms of use and blocking accounts based on complaints. Under these threats, especially if carried out, private companies may find that removing extremist profiles from social media platforms is equally as dangerous as keeping them open. Removing these profiles also eliminates the ability for law enforcement to effectively monitor, track, arrest, and prosecute extremists. Although self-regulation would stymie extremist messaging and ideology reaching potential recruits and sympathizers, it is a delicate balancing act to increase profit, maintain the moral high ground, and contribute to effective law enforcement.

While suggesting that law enforcement monitor websites is good in theory, in reality, it is a source of frustration for those agencies that have already attempted to do so.

Law Enforcement: Monitoring Extremist Websites

While suggesting that law enforcement monitor websites is good in theory, in reality, it is a source of frustration for those agencies that have already attempted to do so. This frustration is both political and technical. The American political system is woefully slow in keeping pace with modern technology. Systems develop and advance faster than legislation can address new threats. Consequently, the U.S. is very slow in developing any effective means to counter incidents and burgeoning threats.

Added to this is confusion over which agency should take the lead in dealing with threats coming in via the Internet. Debates continue on whether there should be a new agency devoted solely to this activity or an oversight agency coordinating the activities of other agencies. Whichever, strong interagency coordination will be required. Building a case against any particular site could involve overseas communications, which would include the Central Intelligence Agency and the National Security Agency. Acquiring or making weapons and explosives would involve the Bureau of

Alcohol, Tobacco, Firearms, and Explosives. Visa and passport violations would involve the Department of Homeland Security's Immigrations and Customs Enforcement and the State Department's Diplomatic State Security. An obstacle to overcome is the reluctance at the agent/local office level to share information. Agreements and memoranda may exist at headquarter levels among agencies. However, as long as promotions and budget allocations are based upon successful performance, officers at different agencies will jealously guard information to ensure their own advancement.

Law Enforcement: PATRIOT Act and Pocket Subpoenas

The recommendation to allow extremist websites to remain functional in order to monitor them frequently raises constitutional questions such as privacy and free speech. These would be valid complaints if the websites were private and available only to members with a login or password. However, they are publicly available. Being publicly accessible means they enjoy no expectation of privacy. Consequently, no special authority is required to monitor them. It does, however, become a manpower intensive proposition to attempt to monitor all the sites managed by extremist groups.[52] As for an individual's privacy in entering the site, which is in itself not a prohibited activity, the fact that the site is in the public domain again removes any expectation of privacy. There is no difference between this activity and standing at a corner newsstand leafing through a pornographic magazine. There is no expectation of privacy for conduct in the public view.

The recommendation to allow extremist websites to remain functional in order to monitor them frequently raises constitutional questions such as privacy and free speech...

The activities of Islamic-based extremist groups in the Middle East falls under the foreign intelligence description in the Foreign Intelligence Surveillance Act.[53] Under the auspices of the PATRIOT Act, accessing a publicly available extremist website is sufficient grounds for law enforcement to conduct further investigation into an individual's background, communications, and finances to determine if that individual poses any risk to domestic security.[54] The point and purpose of such an investigation is to distinguish among those who are merely curious, the academic seeking the actual doctrines of such groups, and the impressionable person open to being swayed to adopt, promulgate, and perhaps act upon the doctrine. Combined with the PATRIOT Act authorities, warrants can be issued to gather further information.

An extension of this proposal further assisting law enforcement is a "pocket" subpoena. The Internal Revenue Service and Drug Enforcement Agency have validated this practice over the years in criminal investigations. While a criminal organization's activities may be developed enough for a subpoena to be issued, the location or persons to be searched may be unknown at the time of issuance.

Having the authority to search resting in an agent's "pocket," the names and locations can be filled in upon discovery in order to immediately execute the subpoena. Utilizing existing law enforcement tools, U.S. national security can be enhanced by moving counterterrorism efforts into the law enforcement realm, where existing laws are ready to be applied. However, based on the Church Committee findings in the 1970s, the courts have demonstrated a reluctance to extend the tools and assets of criminal investigations to counterintelligence investigations.[55] Furthermore, the concept of "pocket" subpoenas or even granting warrants, especially at the federal level, have different parameters in different parts of the country. That which is deemed an acceptable level of probable cause for a warrant in Chicago, for example, may not meet the court's comfort level in California or the Northeast. The increased scrutiny and inability for law enforcement to effectively counter extremist activities in one part of the country versus another may essentially create "safe havens" for extremist suspects.

Recommendations

Countering violent extremism online is not as simple as removing the websites and communication...

To counter violent extremism, the U.S. government should adopt the following policies: counter messaging from the U.S. government, NGOs, and community outreach; intervention and rehabilitation; law enforcement monitoring of extremist websites; and utilizing "pocket" subpoenas. Countering violent extremism online is not as simple as removing the websites and communication, as has been demonstrated above. These websites eventually resurface, and the extremists continue their communications and recruitment. Because countering violent extremism involves different legal authorities and abilities, combining all these options is critical. The U.S. government has the authority to implement all the aforementioned recommendations and provide oversight. In addition, many of these options can be cost-effective in nature and implemented with relative ease. Finally, no one program can achieve the desired end state on its own. All of the recommendations taken together, however, create a holistic, societal approach to countering the ideology of extremist organizations.

The extremist websites are only tools used for communication. Completely shutting them all down is impossible and does not increase domestic security as it does nothing to counter individuals who embrace extremist ideology. To ensure U.S. security, the goal is to identify and intercept or disrupt those who would do harm. For that purpose, it is far better to allow the sites to remain active while monitoring them to identify individuals who access the sites. Shutting

down the sites defeats that purpose, possibly forcing the adherents underground to seek more surreptitious means of communication. As former Congressman Phil English asserts, "Defense against this threat is like the Civil Defense Program during the Cold War. A free society should be able to patrol against any hostile intervention. A free society does have the right to identify risks and defend itself."[56]

While all recommendations should be implemented, given the complexity of countering extremism online, there are some that should have a greater focus and priority in American policy. Specifically, the U.S. government should focus on two particular areas: (1) strengthening programs that are working, and (2) working to prevent radicalization and domestic lone-wolf attacks.

...the U.S. government should focus on two particular areas: (1) strengthening programs that are working, and (2) working to prevent radicalization and domestic lone-wolf attacks.

Implementation

These policy recommendations are intended to work with and balance each other. They are not stand-alone policies, and one particular policy should not be the only focus. The policy recommendations should be implemented in two waves. The first wave establishes legislation and allows for the government to become comfortable with these new policies. The second wave begins midway through the first wave and builds partnerships with communities and organizations that lead to a cohesive counter message to violent extremist organizations. The first wave can be implemented immediately, allowing time for the second wave to be constructed and implemented. By the time the first wave begins to produce results, the second wave will be ready to implement its policies. This overlap will ensure a sustainable and seamless transition throughout the entire process. Metrics for success should also be taken into consideration during the implementation of policy.

Wave One: Immediate Implementation (30–90 days)

Monitoring extremist websites, PATRIOT Act, and pocket subpoenas: These law enforcement tools already exist; therefore, nothing needs to be implemented or funded. These tools have also been tested in the courts and, with some modifications, have proven to be both effective and within the bounds of acceptable jurisprudence. The difference is the need to use these tools in the relatively new arena of counter radicalization. This phase of countering violent extremism is aimed wholly at the domestic threat and is therefore the focus of law enforcement utilizing the tools mentioned above. Combined with the other recommendations, countering radical ideology becomes an all-encompassing policy.

Intervention and rehabilitation: While this policy requires funding, it is included in the first wave to standardize the program as a proactive step in countering violent extremism. This program,

funded by the federal government, will provide local and national law enforcement with the necessary tools and empower NGOs who are working on similar intervention projects. The Department of Homeland Security, in collaboration with the Countering Violent Extremism Program at the State Department, would be responsible for funding this recommendation. Congress would need to reauthorize spending in these departments to provide adequate financial resources to intervention and rehabilitation. Funding would call upon local and national law enforcement partnerships to monitor and intercept vulnerable persons. These partnerships would work with NGOs, such as the World Organization for Resource Development and Education, whose rehabilitation programs currently exist in the U.S. to encourage non-duplication in funding and program development.[57]

Wave Two: Short Term Implementation (60–120 days)

U.S. government counter messaging: Immediately drawdown the CSCC's Digital Outreach Team programs and focus on capacity-building programs. Instead of calling upon additional funding and other resources, the CSCC would transfer funding, personnel, and other necessary resources from the Digital Outreach Team programs to capacity-building programs.

Community outreach counter messaging: The FBI's Joint Terrorism Task Forces (JTTF) exist in every major city across the country, providing partnership opportunities for federal, state, and local law enforcement agencies as well as community outreach. These task forces, working with local communities and involving them in countering extremism messages, can build trust between the communities and law enforcement. Meeting regularly, these bodies are comprised of all federal law enforcement and intelligence agencies as well as local law enforcement officers from the state and municipal levels. The JTTF should coordinate with communities immediately. It is further suggested that to ensure a seamless integration of community messages, opinions, and ideas into U.S. government counter messaging policies, the CSCC and State Department's Countering Violent Extremism Program also become involved in community outreach. The Department of Homeland Security and the State Department should fund this policy, with additional spending authorized by Congress, as necessary to ensure policy success. Additionally, once trust has been established, the U.S. government can begin to encourage and empower credible figures in disseminating counter extremism messages at a grassroots level.

...once trust has been established, the U.S. government can begin to encourage and empower credible figures in disseminating counter extremism messages at a grassroots level.

NGO counter messaging: The government should include these organizations and parties in the broader countering violent extremism

discussion. Given that the capacity and resources already exist in a variety of NGOs, the U.S. government can begin encouraging participation immediately.

Measures of Success

No program can move forward without a means of measuring its progress. It is impossible to improve or amend a policy without knowing if it is currently meeting its goals. This paper's recommendations are intended to be implemented en masse, thereby achieving success by working together. If one program is successful but another fails, then the entire policy fails.

Consequently, countering extremists' use of the Internet to advocate violence is marked as successful when decreasing numbers of people access radical websites, fewer people conspire to commit violence, and more people participate in community programs that speak out against radical extremism. In other words, the moderate voices are ascending.

In summary, the anonymity of the Internet makes it equally accessible to both the guilty and the innocent. In combating the global threat of extremism, it is extremely difficult to determine which targets pose the largest threats, especially when some individuals may be curious, while others are very dangerous. As the number of extremists, their messages, and their networks have expanded to the Internet to spread rhetoric, inspire, recruit, and radicalize others, so must the strategies of the U.S. government, law enforcement, NGOs, and individual citizens in countering them. All of these voices must come together to diminish violent extremist organizations as a threat to national security. ***IAP***

As the number of extremists, their messages, and their networks have expanded to the Internet to spread rhetoric, inspire, recruit, and radicalize others, so must the strategies of the U.S. government, law enforcement, NGOs, and individual citizens in countering them.

Endnotes

1 Clint Watts, "Radicalization in the U.S. beyond al Qaeda," Program on National Security Foreign Policy Research Institute, August, 2012, p. 8.

2 David Johnston and Scott Shane, "U.S. Knew of Suspect's Tie to Radical Cleric," *The New York Times*, November 9, 2009, <http://www.nytimes.com/2009/11/10/us/10inquire.html?_r=0>, accessed on April 20, 2015; Raffaello Pantucci, "What Have We Learned about Lone Wolves from Anders Behring Breivik?" *Perspectives on Terrorism*, Vol. 5, 2011, pp. 5–6.

3 Watts, p. 9.

4 Ibid.

5 Ibid.

6 Lorenzo Vidino, personal interview, February 8, 2015.

7 Dana Janbek and Valerie Williams, "The Role of the Internet Post-9/11 in Terrorism and Counterterrorism," *The Brown Journal of World Affairs*, Vol XX, Issue II, Spring/Summer, 2014, p. 302.

8 U.S. Department of State, Center for Strategic Counterterrorism Communications, <http://www.state.gov/r/cscc/>, accessed on April 5, 2015.

9 Frank Cilluffo, personal interview, January 30, 2015.

10 Katherine Luggiero, "Countering ISIS Recruitment in Western Nations," *Journal of Political Risk*, Vol. 3, No. 1, January 2015.

11 Vidino.

12 Josh Gerstein, "White House Sets Delayed Anti-Extremism Summit," Politico, January 11, 2015, <http://www.politico.com/blogs/under-the-radar/2015/01/white-house-sets-delayed-antiextremism-conference-200891.html>, accessed on May 2, 2015.

13 "Islamic State Crisis: 3,000 European Jihadists Join Fight," BBC News Middle East, September 26, 2014, <http://www.bbc.com/news/world-middle-east-29372494>, accessed on October 15, 2014.

14 Johnston and Shane.

15 Jonathan Dienst, "Hatchet Attack on Cops was a 'Lone-Wolf" Act of Terror," NBC New York, October 29, 2014, <http://www.nbcnewyork.com/news/local/Motive-Hatchet-Attack-NYPD-Zale-Thompson-Ax-Queens-Motive-280312192.html>, accessed on May 2, 2015.

16 Holly Bailey, "A Beheading in Oklahoma," Yahoo News, October 10, 2014, <http://news.yahoo.com/oklahoma-beheading--terrorism-or-workplace-violence-184638839.html>, accessed on May 2, 2015.

17 Samantha Laine, "Fort Riley Suicide Bombing Plot," *Christian Science Monitor*, April 11, 2015, <http://www.csmonitor.com/USA/USA-Update/2015/0411/Fort-Riley-suicide-bombing-plot-Was-an-FBI-sting-operation-necessary-video>, accessed on May 2, 2015.

18 Nadia Prupis, "French Website Shutdown Law," Common Dreams, February 9, 2015, <http://www.commondreams.org/news/2015/02/09/french-website-shutdown-law-decried-attack-free-speech>, accessed on April 15, 2015.

19 U.S. Department of State, Center for Strategic Counterterrorism Communications.

20 Todd C. Helmus, Erin York, and Peter Chalk, "Promoting Online Voices for Countering Violent Extremism," RAND, 2013, p. 6.

21 Ibid.

22 Ibid.

23 Ibid., p. 7.

24 Ibid.

25 Vidino.

26 Ibid.

27 Helmus, p. 10.

28 Samara Tu, "CVE Fellows Develop Social Media Campaign to Combat Violent Extremism," START, March 30, 2015, <http://www.start.umd.edu/news/cve-fellows-develop-social-media-campaign-combat-violent-extremism>, accessed on May 2, 2015; "Students Counter Violent Extremism with Social Media," Arizona State University, April 10, 2015, <https://asunews.asu .edu/20150410-p2p-countering-extremism-program>, accessed on May 2, 2015.

29 Department of State, "Think Again Turn Away," <https://www.facebook.com /ThinkAgainTurnAway#_=_>, accessed on May 2, 2015.

30 Cilluffo, personal interview. The idea of "Dead Facebook" would not necessarily have to be owned or created by Facebook; it is merely a name used for the purposes of this paper since it is a commonly understood idea.

31 Ibid.

32 Former member of Joint Interagency Coordination Group for Combatting Terrorism, U.S. Pacific Command, personal interview, 2015.

33 Ibid.

34 Ibid.

35 "Arrest Made in 2004 Philippines Ferry Bombing," *USA Today*, August 30, 2008, <http://usatoday30.usatoday.com/news/world/2008-08-30-ferry-bombing-arrest_N.htm>, accessed on April 15, 2015.

36 Frank J. Cilluffo, "Countering Use of the Internet for Terrorist Purposes," United Nations Security Council Counter Terrorism Committee, May 24, 2013, p. 8.

37 Ibid., p. 9.

38 "Channel Duty Guidance: Protecting Vulnerable People from being Drawn into Violence, Statutory Guidance for Channel Panel Members and Partners of Local Panels," Government of the United Kingdom, Crown Copyright, 2015, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/425189/Channel_Duty_Guidance_April_2015.pdf>, accessed on April 15, 2015.

39 Ibid., p. 12.

40 William McCants, "The Foreign Policy Essay—Special Edition: First, Do No Harm," Lawfare, February 17, 2015, <http://www.lawfareblog.com/2015/02/the-foreign-policy-essay-first-do-no-harm/>, accessed on April 14, 2015.

41 Ibid.

42 Ibid.

43 Ibid.

44 The Brookings Institution, "Countering Violent Extremism: Improving Our Strategy for the Future," Event, Washington, DC, February 4, 2015.

45 William McCants, personal interview, February 24, 2015.

46 Ibid.

47 McCants, personal interview.

48 The Brookings Institution.

49 McCants, personal interview.

50 "Simon Wiesenthal Center's 2013 Digital Terror and Hate Report," *Christian Telegraph,* March 12, 2013, <http://www.christiantelegraph.com/issue18975.html>, accessed on April 15, 2015.

51 Polly Mosdenz, "ISIS Sympathizers Threaten Twitter Founder Jack Dorsey and CEO Dick Costolo over Blocked Accounts," *Newsweek,* March 2, 2015, <http://www.newsweek.com/isis-sympathizers-threaten-twitter-founder-jack-dorsey-and-ceo-dick-costolo-310615>, accessed on May 2, 2015.

52 J.M. Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," *The Brookings Project on U.S. Relations with the Islamic World*, No. 20, March 2015. In a study conducted by the Brookings Institution, it is estimated there are 46,000 pro-ISIS Twitter accounts.

53 Title II, Section 201, USA PATRIOT Act, 107th Congress, January 3, 2001.

54 Title II, Paragraph 215, USA PATRIOT Act.

55 Larry Klumb, telephone interview, January 31, 2015.

56 Phil English, personal interview, February 5, 2015.

57 McCants, personal interview.

InterAgency Paper Series

The ***InterAgency Paper*** (*IAP*) series is published by the Simons Center for Interagency Cooperation. A work selected for publication as an ***IAP*** represents research by the author which, in the opinion of the Simons Center editorial board, will contribute to a better understand of a particular national security issue involving the cooperation, collaboration and coordination between governmental departments, agencies, and offices.

Publication of an occasional ***InterAgency Paper*** does not indicate that the Simons Center agrees with the content or position of the author, but does suggest that the Center believes the paper will stimulate the thinking and discourse concerning important interagency security issues.

Contributions: The Simons Center encourages the submission of original papers based on research from primary sources or which stem from lessons learned via personal experiences. For additional information see "Simons Center Writer's Submission Guidelines" on the Simons Center website at www.TheSimonsCenter.org/publications.

About the Simons Center

The Arthur D. Simons Center for Interagency Cooperation is a major program of the Command and General Staff College Foundation. The Simons Center is committed to the development of interagency leaders and an interagency body of knowledge that facilitates broader and more effective cooperation and policy implementation.

About the CGSC Foundation

The Command and General Staff College Foundation, Inc., was established on December 28, 2005 as a tax-exempt, non-profit educational foundation that provides resources and support to the U.S. Army Command and General Staff College in the development of tomorrow's military leaders. The CGSC Foundation helps to advance the profession of military art and science by promoting the welfare and enhancing the prestigious educational programs of the CGSC. The CGSC Foundation supports the College's many areas of focus by providing financial and research support for major programs such as the Simons Center, symposia, conferences, and lectures, as well as funding and organizing community outreach activities that help connect the American public to their Army. All Simons Center works are published by the "CGSC Foundation Press."

The Simons Center
PO Box 3429
Fort Leavenworth, Kansas 66027
ph: 913-682-7244
www.simonscenter.org
facebook.com/TheSimonsCenter

CGSC Foundation, Inc.
100 Stimson Avenue, Suite 1149
Fort Leavenworth, Kansas 66027
ph: 913-651-0624
www.cgscfoundation.org
facebook.com/CGSCFoundation
LinkedIn.com >> CGSC Foundation, Inc.