National Security Program

Homeland Security Project

Countering Online Radicalization in America: Executive Summary

The Internet has revolutionized the way all of us communicate and do business. Its benefits to people everywhere have been enormous and will continue to drive progress in practically every area of life. At the same time, it should be recognized that, while being a force for good, the Internet has also come to play an important—and, in many ways, unique—role in radicalizing homegrown and domestic terrorists. Supporters of Al Qaeda, Sovereign Citizens, white supremacists and neo-Nazis, environmental and animal liberationists, and other violent extremist groups all have embraced the Internet with great enthusiasm and vigor. They are using it as a platform to spread their ideas, connect with each other, make new recruits, and incite illegal and violent actions.

We believe that this trend will continue and that future terrorist attacks against the United States and its interests will involve individuals who have been radicalized—at least in part—on the Internet. As a result, countering online radicalization should continue to be a major priority for the government and its Countering Violent Extremism (CVE) efforts.

The purpose of this report is to equip policy makers with a better understanding of how the Internet facilitates radicalization, in particular within the United States; an appreciation of the dilemmas and trade-offs that are involved in countering online radicalization within the United States; and ideas and best practices for making the emerging approach and strategy richer and more effective.

In doing so, this report builds on previous reports by the Bipartisan Policy Center's (BPC) Homeland Security Project, especially *Assessing the Terrorist Threat* (2010) and *Preventing Violent Radicalization in America* (2011).

The Strategy

In its 2011 counter-radicalization strategy and the subsequent implementation plan, the White House acknowledged that "the Internet has become an increasingly potent element in radicalization to violence," and promised to "develop a separate, more comprehensive strategy for countering and preventing violent extremist online radicalization and leveraging technology to empower community resilience." Nearly a year later, this still hasn't happened, and the report's first and most important recommendation is for the White House to complete its work on the strategy, make it public, and begin its implementation with alacrity.

In strategic terms, online radicalization can be dealt with in three ways:

Approaches aimed at *restricting freedom of speech and removing* content from the Internet are not only the least desirable strategies, they are also the least effective.

Instead, government should play a more energetic role in *reducing the demand for radicalization and violent extremist messages*—for example, by encouraging civic challenges to extremist narratives and by promoting awareness and education of young people.

In the short term, the most promising way to deal with the presence of violent extremists and their propaganda on the Internet is to *exploit, subject to lawful guidelines and appropriate review and safeguards, their online communications to gain intelligence and gather evidence* in the most comprehensive and systematic fashion possible.

Reducing the Supply

For reasons ranging from the political to the practical, approaches that are aimed at reducing the supply of violent extremist content on the Internet are neither feasible nor desirable. They also tend to conflict with the imperative of gaining intelligence that can be useful in pursuing terrorists and preventing terrorist plots.

Filtering of Internet content is impractical in a free and open society, taking down foreign-based websites should only be a very last resort, bringing prosecutions against propagandists often does more harm than good by publicizing their rhetoric, and relationships with Internet companies are more productive when based on partnerships, not confrontation.

The report's recommendations are as follows:

- Government should refrain from establishing nationwide filtering systems.
- Government needs to retain its capability for aggressive takedowns of foreign-based websites but only use it when doing so is absolutely essential to stop a terrorist attack and/or prevent the loss of life.
- The circumstances and legal framework governing the use of cyber-attacks need to be clarified.
- Prosecutions against violent extremist Internet entrepreneurs need to weigh the chances of success against the unintended consequence of drawing attention to their ideas and propaganda.
- Government should accelerate the establishment of informal partnerships to assist large Internet companies in understanding national security threats as well as trends and patterns in terrorist propaganda and communication.

Reducing the Demand

Much needs to be done to activate a virtual marketplace in which extremism, terrorism, and other bad ideas are drowned out by pluralism, democracy, and the peaceful means through which good ideas can be advanced.

The federal government can play a limited but positive role in helping to bring this marketplace about—for example, by helping to create awareness, convene relevant non-governmental actors, build capacity, and foster media literacy. While doing so, government needs to be realistic about its own role, the extent to which civic challenges to violent extremist ideologies can be engineered (especially on the Internet), and the time and resources that is required for them to become effective.

The report's recommendations are as follows:

- Government, in partnership with community groups, needs to continue to expand programs and initiatives that create awareness and spread information about online radicalization among educators, parents, and communities.
- Government should serve as an enabler, bringing together the private sector, foundations, philanthropists, and community groups to build capacity and to help potentially credible messengers—such as mainstream groups, victims of terrorism, and other stakeholders—to become more effective at conveying their messages. The forthcoming Internet strategy should spell out what the government will do and how success will be measured.
- The government's Internet strategy also needs to make clear what part of government will coordinate capacity building, engagement, and outreach efforts as well as what resources will be made available to support this task.

- The government should encourage school authorities to review and update their curricula on media literacy, consider violent extremism as part of their instruction on child-safety issues, and develop relevant training resources for teachers.

Exploiting Cyberspace

Rather than removing violent extremist content or trying to undercut the demand for it, a different approach for dealing with online radicalization is to take full advantage of violent extremists' and terrorists' presence in cyberspace and make maximum use of the information they are sharing with others.

This information can be used to gain strategic intelligence on terrorist groups' intentions and networks, on tactical intelligence on terrorist operations and the people who are involved in them, and on evidence that can be used in prosecutions.

Doing so is the most effective way of dealing with online radicalization in the short term, and government should pursue this approach more systematically. This, however, requires the clarification of existing laws and the creation of appropriate review and oversight mechanisms that will give domestic agencies more confidence to operate in cyberspace.

The report's recommendations are as follows:

- Government needs to review oversight procedures and clarify the legal framework under which domestic agencies are permitted to monitor, save, and analyze online communications.
- Government should increase the amount of online training offered to members of law enforcement and intelligence agencies, including state and local agencies.
- Given the rapidly changing nature of the online environment, government needs to periodically review the scope, sophistication, and appropriateness of the regulatory framework that governs data gathering and analysis in cyberspace, as well as the technological tools and capabilities that are used for doing so.

Arguably, the use of the Internet to radicalize and recruit homegrown terrorists is the single-most important and dangerous innovation since the terrorist attacks of September 11, 2001. This should remind us that dealing with online radicalization must not be a one-off effort. As the Internet keeps changing, so do the methods of those who want to use it to spread hate and incite terror.