2015

Countering Islamic State Exploitation of the Internet

David P. Fidler
Indiana University Maurer School of Law, dfidler@indiana.edu

COUNCIL *on* FOREIGN RELATIONS

CYBER BRIEF

Countering Islamic State Exploitation of the Internet

David P. Fidler
June 2015

This Cyber Brief is part of the Digital and Cyberspace Policy program.

The use of social media and other Internet-enabled communications by the self-proclaimed Islamic State is pushing the United States and other democracies to react to the abuse of liberal freedoms by illiberal forces. A leading response—fostering more online speech against extremism—relies on the "marketplace of ideas" and raises few problems with respecting the right of free expression, but questions about its effectiveness persist. By contrast, content-based measures, such as taking down violent videos and suspending social-media accounts, generate concerns about free speech, as well as skepticism about the contribution such measures make in the fight against the Islamic State.

The U.S. government and companies can counter the Islamic State's online onslaught through policies anchored in important liberal principles, namely protection of free speech, transparency, and accountability. Such policies include two main steps:

- *Articulate substantive justifications for content-based measures.* Through a presidential policy directive, the president should identify when the U.S. government would request a company to implement content-based measures online to counter terrorism and extremism. Similarly, companies that control online content should specifically explain their policies for using content-based measures against terrorist and extremist communications.
- *Oversee the implementation of content-based measures.* The Privacy and Civil Liberties Oversight Board—an independent body established by Congress—should examine U.S. government requests to companies for implementation of content-based countermeasures. Companies should establish independent reviews of their use of content-based measures aimed at restricting terrorism and extremism.

BACKGROUND: TERRORIST USE OF THE INTERNET

Policymakers have long feared terrorists will exploit the Internet for propaganda, recruiting, fundraising, and cyberattacks. Although terrorists have not yet shown much interest or skill in cyberattacks, their use of the Internet to communicate led to expanded government surveillance, sanctions against incitement of terrorism, and efforts against extremist radicalization and violence. Countries also began to remove content and block accounts associated with terrorism. For example, in 2010, the United Kingdom opened a Counter-Terrorism Internet Referral Unit that, in cooperation with companies, addresses Internet activities that violate legal prohibitions against glorifying or inciting acts of terrorism.

The rise of the Islamic State has intensified the challenge. The Islamic State is more strategic online, demonstrates greater social media sophistication, and operates in cyberspace on a larger scale and intensity than previous terrorist groups. Its online propaganda is linked with radicalized individuals traveling to fight in Syria and Iraq or committing "lone-wolf" terrorism in the West.

Islamic State territorial gains, the influx of foreign fighters, the volume of its online propaganda, and extremist attacks in Paris converged to catalyze more policy action in 2015. In February, the U.S. government convened a summit on countering violent extremism, which discussed extremist use of social media. In April, the European Union established an Internet Referral Unit to address terrorist content on the Internet. In May, the French National Assembly adopted legislation that expanded the government's surveillance authorities to counter terrorist threats.

CHALLENGES TO EFFECTIVE COUNTERMEASURES

Principled, effective online countermeasures are difficult to design, implement, and evaluate. First, the Islamic State's propaganda can be viewed merely as a symptom of a bigger problem. Radicalization usually involves more than consuming extremist tweets. A 2013 RAND study

concluded that the Internet's relative significance in radicalization compared to offline factors "remains to be established." Further, the Islamic State's perceived battlefield successes—not its social media prowess—give its online activities more radicalization potential. Put differently, the Islamic State is more a "boots on the ground" than a "bytes on the net" problem. Thus, countering its online propaganda might have limited strategic value.

Second, countermeasures face challenges from liberal principles that are different from the impact of robust government surveillance on the right to privacy. The Islamic State's online efforts play out largely on social media, which does not require covert surveillance to monitor but does create incentives to target the content of communications with implications for free speech. Strict First Amendment requirements explain why Obama administration strategies for countering violent extremism do not include content-based restrictions for online activities. Similarly, the importance of free speech places demands on private-sector enterprises that implement content-based measures.

Third, content-based countermeasures create transparency issues. Removing online communications in democratic countries because of terrorist content happens mainly through corporate, not government, actions. Companies censor, block, or terminate accounts for communications related to terrorism that violate their policies. On one day in April 2015, for example, Twitter suspended ten thousand accounts associated with Islamic State extremism. However, without better transparency, the legitimacy of these activities is open to criticism, especially when companies act on requests from governments or in response to criticism from public officials and politicians. Governments should not outsource censorship to the private sector in order to avoid legal principles protecting free speech.

Fourth, demonstrating that countermeasures are effective against online terrorist activities is difficult. Counter-narrative measures seek to prevent radicalization by making individuals resilient against extremism, but, as the executive director of the nongovernmental Global Community Engagement and Resilience Fund observed, "It is always going to be hard to demonstrate the success of preventive work." U.S. government online counter-propaganda efforts aimed at blunting the Islamic State's appeal have been criticized as ill conceived and counterproductive.

In terms of content-based measures, the UK's online actions against terrorist content started in 2010 and, by March 2015, the UK had removed seventy-five thousand pieces of content from the Internet. Yet, the UK is a leading source of radicalized individuals traveling to fight extremist jihad with the Islamic State. Experts analyzing the Islamic State's use of Twitter identified possible benefits from Twitter's suspension of accounts associated with the group, but they hesitated to make strong policy prescriptions on such preliminary findings. Further, social media "body counts"—the number of Twitter or Facebook accounts suspended—have the same questionable value to policymakers as the number of Islamic State forces and weapons destroyed by military activities. These issues of effectiveness caution against believing counter-narrative and content-based measures can deliver significant strategic results against the Islamic State.

RECOMMENDATIONS

Despite long-standing policy concerns about terrorist use of the Internet, democracies were caught flat-footed when the Islamic State went "viral." Reactions to the extremist attack in Texas in May 2015, including Senate hearings on social media and terrorist recruitment, show how policymakers and companies are under increasing pressure to do something about the Islamic State's online activities. In this context, the priority for the United States is to craft an online counterterrorism strategy anchored in liberal principles that delivers legitimate and effective actions from the public-private collaboration needed to respond to this threat.

The U.S. government should clearly identify the strategic objectives of countermeasures against Islamic State online extremism. The objectives should reflect government, company, and Internet-user interests and values. Strategic thinking should not be binary in reflecting separate public and private realms, because extremists exploit the online space created by limitations on government power and the private sector's reluctance to police cyberspace. Online counterterrorism should be based on public-private collaboration regarding strategic ends and means.

In terms of ends, given the importance of free speech, clarity is needed most for content-based countermeasures sought and implemented by the U.S. government and U.S. companies. Through a presidential policy directive, the U.S. government should articulate when it would request that a company implement content-based countermeasures in the online fight against extremism and terrorism. In particular, the directive should identify when the U.S. government would ask companies to implement content-based countermeasures the government could not impose under the First Amendment. For example, the U.S. government has asked companies to remove extremist content, including requesting that social media sites take down the video of the beheading of an American journalist. Dissemination of videos recording such atrocities perpetuates violations of the victims' dignity and international humanitarian law. The U.S. government should be able to ask companies take down such videos on these grounds, which, in this example, would align with company policies against violent content.

Similarly, U.S. companies that control online content should review and explain more thoroughly their policies for content-based measures against terrorism and extremism. As pressure has mounted on companies, policies and practices appear to have shifted often without sufficient clarity about the changes. Clear and comprehensive articulation of company policies can help ensure they are anchored in liberal principles and are not the result of bending to the winds of political anger and frustration.

In terms of means, "trust but verify" applies to ensure transparency and accountability. U.S. government requests to companies for content-based countermeasures should be subject to oversight. The Privacy and Civil Liberties Oversight Board should review government requests, interact with the requested companies, and report its findings to Congress and the public. The U.S. government and companies should agree on how to disclose the number of government requests for content-based countermeasures related to terrorism and extremism.

Similarly, companies should establish independent, periodic reviews of their implementation of content-based countermeasures. Such mechanisms should include users of the services and civil-society, academic, and nongovernmental experts from relevant disciplines, including counterterrorism, and analyze representative samples of content-based actions aimed at terrorism and extremism against company policies and other considerations, such as the emergence of new communication technologies and services. To achieve consistency across companies, this process could be centralized in an academic institution, such as Stanford University or the University of California, Berkeley, with the proximity and capacities to organize the reviews.

These recommendations ground online counterterrorism activities in liberal principles reflected in the U.S. Constitution, international law, and the values of Internet freedom and subject these activities to transparency and accountability mechanisms. The approach is exportable to other democracies similarly struggling with the Islamic State's online offensive. Overall, the strategy seeks to ensure that online counterterrorism avoids the worst political outcome for a liberal democracy—public and private behavior that is unprincipled and ineffective.

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. Founded in 1921, CFR carries out its mission by maintaining a diverse membership, with special programs to promote interest and develop expertise in the next generation of foreign policy leaders; convening meetings at its headquarters in New York and in Washington, DC, and other cities where senior government officials, members of Congress, global leaders, and prominent thinkers come together with CFR members to discuss and debate major international issues; supporting a Studies Program that fosters independent research, enabling CFR scholars to produce articles, reports, and books and hold roundtables that analyze foreign policy issues and make concrete policy recommendations; publishing *Foreign Affairs*, the preeminent journal on international affairs and U.S. foreign policy; sponsoring Independent Task Forces that produce reports with both findings and policy prescriptions on the most important foreign policy topics; and providing up-to-date information and analysis about world events and American foreign policy on its website, CFR.org.

The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.

The Digital and Cyberspace Policy program aims to identify solutions to one of the world's most pressing challenges in the twenty-first century: keeping the global Internet open and secure in the face of unprecedented threats. Through briefings, reports, and the *Net Politics* blog, the program produces research and analysis on the politics of cyberspace. Cyber Briefs are short memos that provide concrete recommendations on topics related to online privacy, cybersecurity, Internet governance, and the trade of digital goods and services.

For further information about CFR or this paper, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, or call Communications at 212.434.9888. Visit CFR's website, www.cfr.org.