Homeland Security
Policy Institute
THE GEORGE WASHINGTON UNIVERSITY

Countering Use of the Internet for Terrorist Purposes

Statement of Frank J. Cilluffo

Before the United Nations Security Council Counter Terrorism Committee

May 24, 2013

Introduction

Committee Chairman Loulichky, distinguished representatives and observers, it is a privilege to appear before you today to speak to the challenge of countering use of the Internet for terrorist purposes. Your initiative in placing this important issue on the Committee's agenda for consideration and further potential action is to be commended. While different countries may employ different means and mechanisms that best correspond to the specific circumstances and conditions that prevail in each Member State, our fundamental goals and objectives are shared—namely to thwart terrorists and terrorism committed against innocent individuals and populations. Just as we must work together in the physical world to counter terrorist organizations that are transnational in nature and seek to exploit seams in international cooperation, so too must we join forces online since the Internet and the adversary's use of it knows no borders.

My remarks here today will proceed in two parts. The first will address the nature of the challenge and offer a framework for categorizing and thinking about the key issues in this area. The second part will propose some response options that may be invoked in whole or in part depending upon the specifics of the case that require remediation. Please note that these thoughts are presented to you in my individual capacity, as a private citizen who directs a university-based policy and research institute. As such, the below does not necessarily reflect the position(s) of the United States Government. In addition, the below is intended to build upon and complement the counterterrorism efforts that have already been undertaken by the United Nations, its Members, and other organizations at the national, regional, and international levels.

The Nature of the Challenge: Use of the Internet for Terrorist Purposes

Terrorists use the Internet for four fundamental purposes: (1) to facilitate tradecraft; (2) to convey "how-to" knowledge and online training; (3) to radicalize and recruit prospects; and (4) to engage in computer network attack. The Internet has figured prominently in an overwhelming number of cases of "homegrown" radicalization and terrorism plots, thus blurring the lines between foreign and domestic threats. According to the Congressional Research Service, since 9/11 there have been over sixty terror plots or attacks involving Americans on U.S. soil. Other countries are facing a similar challenge.

Tradecraft is the lifeblood of terrorist operations, and refers to the skills developed and honed through hands-on activity that supports terrorist aims and objectives. Tradecraft includes communications, fundraising, and targeting, to name just a few of the ends and elements that may be advanced through the Internet. Online pursuit of these activities allows our adversaries to reach new audiences, tap new resources, and reach ever-higher levels of lethality. From a "how-to" perspective, terrorists have used the Internet to share as well as improve their tactics, techniques and procedures. The range of "how-to" information that may be distributed and imparted effectively online includes ways to build and design weapons of various sorts—notably improvised explosive devices (IEDs), ways to evade law enforcement, conceal identities, etc.

The Internet is also a powerful tool for sharing and reinforcing aberrant attitudes and ideas. Online, in the dark corners of the Web—and increasingly on mainstream sites that have no barrier to access, in contrast to password-protected forums—charismatic figures who possess cross-cultural fluency (also known as "bridge figures") continue to attract the vulnerable and the curious with their fiery rhetoric and gruesome imagery.[1] These figures, whose narrative and ideology bridges countries and contexts, help pull in new recruits to the terrorist cause, to replenish the pool. Once the first steps down the path to radicalization are taken, online communities act as echo chambers in which members embolden and encourage one another in their violent extremist views. At some point however, the virtual merges with the physical reality—indeed the killer "app" of the Internet is people.[2] Note also that the cyber domain is akin to ungoverned and under-governed spaces in the physical world, such as the Federally Administered Tribal Areas (FATA) of Pakistan, parts of the Maghreb and large swaths of the Sahel, where the adversary finds a more hospitable environment in which to plan, plot, train, etc. Along with States and /or their proxies, terrorist organizations may invoke computer

[1] United States Senate, "Zachary Chesser: A Case Study in Online Islamist Radicalization and Its Meaning for the Threat of Homegrown Terrorism," A Report by: Majority and Minority Staff of the Senate Committee on Homeland Security and Governmental Affairs (February 2012) http://www.hsgac.senate.gov/imo/media/doc/CHESSER%20FINAL%20REPORT(1).pdf

[2] Homeland Security Policy Institute and University of Virginia Critical Incident Analysis Group Special Report, NETworked Radicalization: A Counter-Strategy (May 2007) http://www.gwumc.edu/hspi/policy/NETworkedRadicalization.pdf. Frank J. Cilluffo, Jeffrey B. Cozzens, Magnus Ranstorp, Foreign Fighters: Trends, Trajectories and Conflict Zones (October 2010) http://www.gwumc.edu/hspi/policy/report_foreignfighters501.pdf

network attack (CNA) techniques and methods to advance their aims.[3] CNA efforts may allow the adversary to enhance their own weapon systems and platforms, as well as stymie those of others. CNAs may also be deployed as a force multiplier to enhance the efforts and lethality of conventional attacks.

To achieve their primary objectives, terrorists have successfully used and exploited social media, in particular the following trio of platforms: Facebook, You Tube and Twitter. Needless to say, these platforms have played a very positive role in society at large. However, these three vehicles have also been invoked to advantage by a range of groups worldwide including the Afghan Taliban, Tehrik-i-Taliban Pakistan (TTP), and Somalia's Al-Shabaab, along with al Qaeda and its affiliates in the Arabian Peninsula and beyond. Notably each country may have its own native-language versions of the above-mentioned social media vehicles—such as FPS and Renren—which are, respectively (and loosely speaking), Russian and Chinese versions of Facebook.

There is no shortage of examples and anecdotes that demonstrate all of the above concepts and principles. One of the best-known illustrations may be al Qaeda's online publication and distribution via social media of its English-language "Inspire" magazine, which has contained articles such as "How to make a bomb in the kitchen of your mom." News reports and analyses of the Boston marathon bombing have suggested that the perpetrators used information from "Inspire" to devise and build their own improvised explosive devices (though the perpetrators may have received additional training as well). And for years, al Qaeda, its affiliates and other jihadists, plus Hezbollah and other terrorist organizations have distributed legions of martyrdom videos online in order to attract new recruits and inspire and re-energize those already in the ranks.

As cyberspace has emerged as a domain of its own alongside the traditional others of land, sea, air, and space, we have seen considerable contest online. One dimension of such competition is the war of words manifested in the Twitter feeds of the Taliban versus that of NATO's International Security Assistance Force (ISAF). The caustic banter exchanged in this forum may appear, at first, to be little more than mere "back and forth" between adversaries. Yet these exchanges served an important purpose from the Allied (NATO) perspective, and that is to rebut the falsehoods propagated by the adversary.

Note that the United Nations itself has been cited and challenged by the adversary in this context. For instance, Taliban tweets have called into question the credibility of United Nations Assistance Mission in Afghanistan figures reporting that the overwhelming majority of civilian casualties in that country were caused by the adversary (insurgents). NATO rightly pushed

[3] See, for example, Frank J. Cilluffo, "Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure," Testimony before the U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies (March 2013) http://www.gwumc.edu/hspi/policy/Meehan_Cilluffo%20Testimony%20March%202013.pdf

back hard on these Taliban misrepresentations in the Twittersphere, rather than leaving such false claims to stand, for others to take up and (wrongly) run with them.[4]

Similar attempts to use Twitter to exaggerate military successes on the physical battlefield and underplay adversary losses there, etc., have occurred in the Somalian context, where Al-Shabaab—which has formally allied itself with al Qaeda—has punched above its weight online. Shabaab has engaged in verbal battle with a range of parties, from the Kenyan Army (which moved into Southern Somalia in 2011 to stabilize the area bordering on Kenya) to individual terrorism analysts based in the United States and working in a private / nongovernmental capacity. When Shabaab posted a Tweet saying that it would kill certain hostages unless the Kenyan Government met Shabaab's demands, a private citizen in the United States flagged the post for Twitter as a violation of the terms of use of the service. Shabaab's account was then shut down thanks to timely enforcement of the service agreement. But Shabaab's voice later re-emerged on Twitter, only a week later, unfortunately. It continues unabated.

Shabaab has skillfully used the foreign fighters in its ranks to advantage, drawing on their cultural and linguistic fluency and Western education to communicate in a way that resonates with a much wider audience, globally, than would otherwise be the case. Alabama-born Omar Hammami (also known as Abu Mansur al-Amriki) is a prime example, though it appears that he ultimately came into conflict with Shabaab; and interestingly, that dispute also played itself out online as Hammami took his grievances and disillusionment live in a series of snappy Tweets.[5]

In its annual report on Digital Terrorism and Hate, the Simon Wiesenthal Center distinguished between and among various social media, assigning grades to each for how well or how poorly content about terror and hate was handled. Twitter fared the worst, based on the sheer volume of such content that is allowed to persist on the service. Terrorists can thus upload links and share dangerous "how-to" (and other) knowledge essentially unaccosted.

By comparison, the reports notes, Facebook "does a reasonably good job" of removing terror- and hate-related content upon notification thereof. You Tube falls somewhere in between. There, "an immense amount" of how-to material exists and persists, and in multiple languages to boot. To their credit, You Tube has instituted a "promotes terrorism" flag that allows users to flag videos for terrorist content; and Community Guidelines "draw the line at content that's intended to incite violence or encourage dangerous, illegal activities that have an inherent risk of

[4] Nick Paton Walsh, "Twitter is new battleground for NATO and Taliban in Afghanistan," CNN (November 18, 2011) http://www.cnn.com/2011/11/18/world/asia/afghanistan-twitter-war. Austin Wright, "U.S. Twitter war vs. Taliban flares," Politico (June 18, 2012) http://www.politico.com/news/stories/0612/77524.html. Ben Farmer, "Kabul attack: ISAF and Taliban press officers attack each other on Twitter," The Telegraph (September 14, 2011) http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/8763318/Kabul-attack-Isaf-and-Taliban-press-officers-attack-each-other-on-Twitter.html.

[5] David Smith, "Al-Shabaab in war of words with Kenyan army on Twitter," The Guardian (December 13, 2011) http://www.guardian.co.uk/world/2011/dec/13/al-shabaab-war-words-twitter. Associated Press, "Twitter suspends al-Shabaab account," The Guardian (January 25, 2013) http://www.guardian.co.uk/world/2013/jan/25/twitter-suspends-al-shabaab-account. Christopher Anzalone, "Al Shabab's Tactical and Media Strategies in the Wake of its Battlefield Setbacks," CTC Sentinel (March 27, 2013) http://www.ctc.usma.edu/posts/al-shababs-tactical-and-media-strategies-in-the-wake-of-its-battlefield-setbacks.

serious physical harm or death."[6] Nevertheless, it remains easy to enter a search term and, with very little effort, find videos of US soldiers being killed overseas—content which is expressly against the Community Guidelines, and certainly deeply concerning, especially for a US company to allow on their servers. Again as noted in the Wiesenthal Center's report, You Tube has removed some material—such as the noxious videos of Anwar al-Awlaki (now deceased), the Yemeni-American operational planner for al Qaeda in the Arabian Peninsula (AQAP) and jihadi theoretician, whose "sermons" sought to radicalize and recruit an ever-increasing pool into the service of al Qaeda and its aims. Generally though, these You Tube takedowns occurred only in the wake of substantial controversy and public attention directed toward that particular item. To this day, You Tube (plus Twitter, and to a lesser extent Facebook) continue to serve as platforms for entities like Hezbollah to communicate their message.

Finally, the Wiesenthal Center's report observes that some social networking vehicles, such as Tumblr and Instagram, remain comparatively little used to spread content of the type at issue, at least at this point and time.[7]

Options for Response: Countering Use of the Internet for Terrorist Purposes

In parallel to the four primary objectives that terrorists seek to achieve through use of the Internet, there are four major categories of response options for Member States and their counterterrorism communities as well as localities and nongovernmental organizations (NGOs) to consider, both from a nation-specific and multilateral perspective. These options are: (1) to monitor online activity and collect information and intelligence that will support counterterrorism efforts; (2) to shut down online activity that terrorist organizations engage in; (3) to undertake a substantial and multipronged initiative to push back on the terrorist narrative that underpins terrorist activity and support; and (4) to deny service and destroy terrorist cyber networks through computer network attack (CNA).

Monitoring and Collection

With regard to monitoring and collection, the key question is whether and how long to pursue the subject of interest who is under scrutiny. As in the physical world, the challenge is to determine when to string the adversary along and when to string him up instead. Online however, the challenge of striking the most productive balance between these two courses is magnified. On the one hand, there may be a wealth of opportunities to collect information about

[6] http://www.youtube.com/t/community_guidelines

[7] Jam Kotenko, "According to a New Report, Twitter is a Breeding Ground for Terrorism and Hate Speech," (May 10, 2013) http://www.digitaltrends.com/social-media/online-hate-statistics-up-by-30-percent-says-report-but-theres-a-new-app-designed-to-get-it-under-control/. Sara Carter, "Jihadists use US servers to spread terror message," Washington Guardian (May 16, 2013) http://www.washingtonguardian.com/web-jihad-inaction.

adversary intent and capabilities in a range of interactive forums on the Internet. Both Twitter and Facebook generate opportunities for network analysis and geo-location. Further, given the anonymity that the Internet affords, "honeypots" and other long-used techniques may be employed to elicit facts that may assist in preventing terrorist action of various sorts. On the other hand, care must be taken to conclude the monitoring phase before damage or harm (that outweighs any benefit gained) is actually incurred in the physical world.

Shutdown

The second option, to shut down terrorist activity online, should be exercised judiciously and only in circumscribed cases. It is important to emphasize this requisite level of care because this course bears significant implications for the cherished value that is freedom of speech. Indeed each response option has its own notable consequences for an array of fundamental values, which include privacy as well as human rights. In defined circumstances however, the costs of inaction may well exceed those of acting—even if doing so means impinging to an extent upon a fundamental freedom. In these particular cases, there exists a responsibility to act, including on the part of companies (especially Internet service providers).

Put another way, more could be done worldwide to suppress what is—but ought not to be—on the Internet. For instance, anything operational in nature that relates to a Foreign Terrorist Organization ("FTO" being a U.S. designation) should assuredly be shut down immediately. Internet Service Providers could also do more to monitor and take down content that violates the codes of conduct that govern their service environments; and naming and shaming could help push the ball forward. Timely response of this sort would make it harder for "joy surfers" to access the type of information at issue. Admittedly the "whack-a-mole" problem would render this solution imperfect because content taken down from one site may well simply reappear on another. Nevertheless, by pushing this type of content to the margins you do make it harder to find; and while there will still be those that put in the extra effort try to access it, these are probably individuals of greatest concern—and smoking them out by such means is itself a valuable exercise.

Pushback

The third option is to engage, specifically by providing a counter-narrative that dissects and de-legitimizes, disaggregates and de-globalizes, and de-glamorizes the adversary's narrative.

Efforts to counter and defeat the jihadist ideology have not yet been sufficiently robust, with the result that the terrorist narrative lives on, and continues to attract and inspire those who wish us harm. A sustained, comprehensive, integrated and effective effort to combat violent Islamist extremism is a crucial element of statecraft on counterterrorism. In the United States however, we are still struggling with how to handle English-language material that is targeting the homegrown, "do-it-yourself" jihadists—and this is undoubtedly a shortcoming. The Department of State's Center for Strategic Counterterrorism Communications (CSCC) is doing some good work though, and represents a positive development in this space overseas. Likewise, in the United Kingdom, the current multipronged "Prevent" strategy (notably the "refresh" of 2011) constitutes a serious attempt to challenge the ideology that supports terrorism and those who promote it.[8] Laudable initiatives also exist in other countries, such as Indonesia, where defectors—such as former Jemaah Islamiya (JI) leader Nasir Abas—are active in renouncing (the adversary) in both the physical and cyber world. Collectively, though, we all need to do more and hit back harder. Keep in mind that the homegrown threat is of increasing concern in all countries.

Five "D's" should guide the proposed counter-narrative effort:

Dissect and De-legitimize

The first step towards pushback is to dissect and expose the adversary's narrative, so as to properly understand and rebut it. Here the power of negative imagery (as in a political campaign) could be harnessed to hurt our adversaries and further chip away at their appeal and credibility in the eyes of peers, followers and sympathizers. A systemic strategic communications effort aimed at exposing the hypocrisy of our adversaries' words versus their deeds could knock them off balance, as could embarrassing their leadership by bringing to light their seamy connections to criminal enterprises and drug trafficking organizations. The increasingly hybrid nature of the threat presents additional opportunities in this regard as the proceeds of trafficking in drugs and arms plus kidnapping for ransom are used to finance terrorism.

Disaggregate and De-globalize

Brokering infighting between al Qaeda, its affiliates and the broader jihadi orbit in which they reside will damage violent extremists' capability to propagate their message and organize operations both at home and abroad. Locally administered programs are especially significant as many of the solutions reside outside government and will require communities and individuals policing themselves, including on social networking sites. As for governments, they may have a role to play in helping to magnify the voices of others who reside at the grassroots and possess the credibility and authenticity necessary to affect outcomes. We all could and should do more to drive wedges and foment distrust, including by exploiting points of conflict between local interests and the larger global aims of al Qaeda (and its ilk), and encouraging even more defectors.

[8] "*Prevent* Strategy" (July 2011) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf. See also "CONTEST: The United Kingdom's Strategy for Countering Terrorism" (July 2011) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97994/contest-summary.pdf

De-glamorize

Above all however, we must remember the victims of terrorism, with a more heightened and sharpened focus on this area than ever before. To date, an enormous amount of time and resources of every type—capital, human, technological, etc.—has been devoted to and expended upon kinetic efforts directed against the adversary. These measures, while indisputably crucial, have not been matched by 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.

Undertaking more and deeper efforts to pay tribute to their memory, such as through a type of Facebook for the deceased, is the right thing to do on multiple levels and would serve as a powerful tool for undercutting and undermining terrorist support and recruitment. Putting names to the faces that have been murdered by terrorist groups, and sharing the details of these lives that have been lost, is poignant and compelling and serves to highlight the meaninglessness of our adversary's so-called cause.[9]

Important work in this area has already been initiated by the United Nations as a whole as well as by individuals such as Carrie Lemack who founded the Global Survivors Network (GSN), an NGO that has done so much to amplify the voices of survivors of acts of terror and thereby help to thwart radicalization and build a powerful counter-narrative. Indeed the GSN grew out of the 2008 UN Symposium on Supporting Victims of Terrorism. The act of sharing these personal and painful stories and experiences is a true public service, and the Internet may be leveraged to positive effect to ensure the widest and most effective distribution of this vital information. GSN, for one, employed a range of means and technologies to get these stories out and into the hearts and heads of those who most need to hear them—but more NGO efforts are required along with Member-State support (financial and otherwise) for their efforts. Just as the adversary has used imagery to advantage, so too must we put a human face on the toll of terrorism.

A single, comprehensive and dedicated website that bundles in one spot all of the victims, all of the defectors (from the adversary) who have recanted, and all of the scholars who have issued fatwas against al Qaeda and its affiliates, would go a long way towards de-glamorizing and pushing back on the adversary's narrative.

[9] Frank J. Cilluffo, "The Future of Homeland Security: Evolving and Emerging Threats," Testimony before the U.S. Senate Homeland Security and Governmental Affairs Committee (July 2012) http://www.gwumc.edu/hspi/policy/Testimony%20-%20SHSGAC%20Hearing%20-%2011%20July%202012.pdf. Frank J. Cilluffo, "The Internet: A Portal to Violent Islamist Extremism," Testimony before the U.S. Senate Homeland Security and Governmental Affairs Committee (May 2007) http://www.gwumc.edu/hspi/policy/testimony5.3.07_cilluffo.pdf.

Deny and Destroy

The fourth response option is one of last resort, to be considered only in very limited circumstances, as it is to invoke computer network attack methods and tools in order to up-end our adversaries' efforts to use the Internet to further their own ends. In this regard, there are opportunities to turn to distributed denial of service (DDoS) techniques to disrupt websites, chatrooms, and social media, and deny terrorists their use. In addition, there exists the more pointed possibility of engaging in computer network attack to destroy enemy computers, routers, and hard-drives to collapse adversary networks.

Conclusion

As a general matter, response must be case-specific and grounded in context. Having said that, a mix of all four response options outlined above is likely needed in order to thwart the broad array of terrorist goals and purposes connected to use of the Internet. For any and all of the described response options to work in the most effective manner, moreover, a supporting network is required. For example, monitoring and collection are activities that are most productively pursued in tandem, with bilateral and multilateral partners. The Boston marathon bombing is a case in point, spanning as it did—and continues to do, in the post-incident investigation phase—from New England to the North Caucasus, and from Cambridge to Chechnya.

In this type of scenario, early and ongoing assistance between and among members of the international counterterrorism community is crucial to protecting and preserving the national security of each constituent country. Indeed the United Nations is perfectly structured and situated to play a valuable role by acting as a forum and conduit for the exchange of facts and trends observed and emerging in the neighborhood and language(s) used in each UN Member State. Likewise, the counter-narrative and the focus on victims of terrorism are other initiatives and endeavors where each and every UN Member State can and should join and contribute, so as to help make these efforts more than the simple sum of their parts.

Thank you again for the opportunity to appear before you today. It is a true privilege to have the chance to share thoughts with this distinguished Committee, whose mandate is so important to furthering national, regional, and international security. I look forward to trying to answer any questions that you may have and would certainly welcome your comments upon and reactions to the ideas and proposals raised above.

***Frank J. Cilluffo** serves as Associate Vice President at the George Washington University, where he directs the Homeland Security Policy Institute (HSPI) and co-directs the Cyber Center for National & Economic Security (CCNES).*