Sustainable Security

Addressing the underlying drivers of global insecurity

Terrorists Turn Social Media into Antisocial Media

April 11, 2016 · by Gabriel Weimann · in Marginalisation. ·

In March 2016, Jaelyn Young, a 20-year-old student at Mississippi State University was accused of attempting to leave the United States and join the Islamic State (ISIS). She attempted to board a flight with Muhammed Dakhlalla and fly to Turkey with the intent to cross into Syria and join the terrorist group. Young, who pleaded guilty, was posting messages on Twitter about her desire to join the jihadist group, catching the attention of the FBI in May 2015. An agent posing as an Islamic State recruiter began corresponding with her and Dakhlalla. Young and Dakhlalla told the supposed recruiter they would help Islamic State "correct the falsehoods" about it in U.S. news media, such as reports that the group trades young girls as sex slaves. They also asked the recruiter whether ISIS would offer Koran classes in English, how they would be required to prove that they were Sunni Muslims, and what kind of military training Dakhlalla would receive.

Young and Dakhlalla are just two of many cases of the new trend of terrorists using the newest online platforms, commonly known as the "new media" or "social media." As several reports on online terrorism reveal (https://en.wikipedia.org/wiki/Terrorism_and_social_media), today 90 percent of terrorist activity on the Internet takes place using social networking tools. The growing attraction of social media for modern terrorists relies on the combined impact of several trends: the expansion of online social media and their advantages for terrorists, the virtual interactivity that terrorist propaganda and recruitment are using especially with the targeting of specific audiences ("narrowcasting") and the emergence of "Lone Wolf" terrorist whose virtual pack is found in the terrorist social media. ISIS managed to recruit thousands of foreign fighters, many of them from Western societies. Many of them were radicalized and recruited on Western online social media. Modern terrorism is turning social media into a powerful anti-social platform of hate, destruction, suicide and mass murder.

Terrorist Migration to Social Media

Terrorist use of online platforms is not new. After the events of 9/11 and the antiterrorism campaign that followed, a large number of terrorist groups moved to cyberspace, establishing thousands of websites that promoted their messages and activities. Many terrorist sites were targeted by intelligence and law enforcement agencies, counterterrorism services, and activists, who monitored th sites, attacked some of them, and forced their operators to seek new online alternatives. The relocation to social media followed. The main motivation to use Facebook and other social media was properly outlined by the terrorist themselves in a Jihadi online forum (https://www.wilsoncenter.org/publication/new-terrorism-and-new-media) calling for "Facebook Invasion":

> **This [Facebook] is a great idea, and better than the forums. Instead of waiting for people to [come to you so you can] inform them, you go to them and teach them! …[I] mean, if you have a group of 5,000 people, with the press of a button you [can] send them a standardized message. I entreat you, by God, to begin registering for Facebook as soon as you [finish] reading this post".**

Social media differentiates from traditional/conventional media in many aspects such as interactivity, reach, frequency, usability, immediacy, and permanence. They are comparatively inexpensive and easily accessible. They enable anyone to upload, download, share and access information. Social medi depend on new communication technologies such as mobile and web-based networks to create highly interactive platforms. The global spread of cellular phone with online access to social media made these platforms so widely accessed and used, even in the poorest places in the world. There are (http://wearesocial.com/uk/special-reports/digital-social-mobile-worldwide-2015) **3.42 billion** internet users, equaling **46%** global penetration, **2.31 billion** social media users, delivering **31%** global penetration, **3.79 billion** unique mobile users, representing **51%** global penetration and **1.97 billion** mobile social media users.

These trends were noticed also by Internet-savvy terrorists who quickly learned how to harness the new social media for their purposes. Increasingly, terrorist groups and their sympathizers are shifting their online presence from websites, chatrooms and forums to the newer platforms, the social media.

Image via Wikimedia Commons. (https://commons.wikimedia.org/wiki/File:Backlit_keyboard.jpg)

Today, all terrorist groups are present on Facebook, Twitter, Instagram, YouTube, Telegram and other online platforms. Terrorists are encouraging their audiences, followers and operatives to join social media and use them. Maybe most successful is the Sunni terrorist group ISIS, which launched a multi-platform online campaign, covering the entire range of social media. ISIS is using social media to seduce, radicalize and recruit. Since the summer of 2014, ISIS has opened numerous social media accounts for distributing its videos, audios and images via various channels and in many languages, thereby avoiding online censorship. As part of these intensive propaganda efforts, it has launched Al-Hayat Media, a new media branch specifically targeting Western and non-Arabic speaking audiences. ISIS has developed an effective online propaganda machinery. On various social media platforms, ISIS has released numerous videos, photos, texts and music promoting different sides of the militant group. On the one hand is its face of cruel, bloody terror such as of beheadings and burnings of hostages; on the other are more humane and friendly videos of ISIS fighters posing with Nutella jars and kittens. Some of propaganda items on social media are about ISIS providing governance, social justice, and new construction.

Going Dark: the Move to the Dark Web

Social media, useful and beneficiary as they may be for terrorists, also involve risks for them: they could be monitored, traced and found. Many of the terrorist websites and social media on the so-called Surface Web are monitored by counter-terrorism agencies and are often shut down or hacked. That led to a recent terrorist migration to the Dark Web. One can describe the Internet as composed of layers: the "upper" layer, or the Surface Web, can easily be accessed by regular searches. However, "deeper" layers, the content of the Deep Web, are not indexed by traditional search engines such as Google. The

deepest layers of the Deep Web, a segment known as the Dark Web, contain content that has been intentionally concealed. The Dark Web serves as Internet users for whom anonymity is essential, since they not only provide protection from unauthorized users, but also usually include encryption to prevent monitoring.

The Dark Web is quite appealing for terrorist groups: While they may lose a broad audience that is available on the Surface Web, they can exploit the obscurity of the Dark Web to further their goals. Following the attacks in Paris (November 2015), ISIS has turned to the Dark Web to spread news and propaganda in an apparent attempt to protect the identities of the group's supporters and safeguard its content from hacktivists. The move comes after hundreds of websites associated with ISIS were taken down as part of the campaign launched by the amorphous hacker collective Anonymous. ISIS' media outlet, Al- Hayat Media Center, posted a link and explanations on how to get to their new Dark Web site on a forum associated with ISIS. The announcement was also distributed on ISIS' Telegram channel, the encrypted communication application. The messages shared links to a Tor service with a ".onion" address, more commonly known as a website on the Dark Web. The ISIS site in the Dark Web contains an archive of the group's propaganda materials, including its documentary-style film, *The Flames of War.* The site also includes a link to the terrorist group's private messaging portal on Telegram. Telegram offers encrypted messaging, a slick, intuitive interface, and a big userbase: it hit 100 million active monthly users in February 2016.

At this stage, terrorist presence in the Dark Web is rather modest: when propaganda, radicalization and recruitment are the chief goals of terror groups, the reach of Dark Web is limited. Yet, terrorists are already applying the newest privacy-preserving mobile applications like Telegram and are using the Tor browser to hide what they are browsing on the open web from prying eyes. This growing sophistication of terrorist's use of the Dark Web presents a tough challenge for governments, counter-terrorism agencies and security services. DARPA, the Defense Advanced Research Projects Agency, believes the answer can be found in MEMEX (http://www.wired.com/2015/02/darpa-memex-dark-web/), a software that allows for better cataloguing of Deep Web sites. Envisioned as an analog computer to supplement human memory, the MEMEX (a combination of "memory" and "index") would poke around the Dark Web and also tune its knowledge to specific domains of interest. MEMEX was originally developed for monitoring human trafficking on the Deep Web, but the same principles can be applied to almost any illicit Deep Web activity. In 2014, an investigation of the source code in one NSA program called XKeyscore, (revealed by the Edward Snowden's leaks), showed that any user simply attempting to download Tor was automatically fingerprinted, essentially enabling the NSA to know the identity of millions of Tor users. The NSA source code also revealed some of the behavior which users exhibit can immediately be tagged or "fingerprinted" for so-called deep packet inspection an investigation into the content of data packages sent across the Internet, such as emails, web searches and browsing history.

However, there is another side to counter measures in the Dark Web which can serve terrorist communications and activities but also serves journalists, civil rights and democracy activists – all of which may be under threat of censorship or imprisonment. Thus, the alarming infiltration of Internet-savvy terrorists to the "virtual caves" of the Dark Web should trigger an international search for a solution, but one that should not impair legitimate, lawful freedom of expression.

Dr. Gabriel Weimann is a Full Professor of Communication at the University of Haifa, Israel. His research interests include the study of persuasion and propaganda, political campaigns, terrorism and the media, online terrorism and cyber-war. He is the author of nine books and over 180 scientific articles. His recent book, Terrorism in Cyberspace: The Next Generation, was published in 2015 by Columbia University Press.

Tags: Cyber security, Dark Web, Deep Web, ISIS, Islamic State, World Wide Web