Terrorist Migration to the Dark Web

by Gabriel Weimann

"Increasingly, we are unable to see what they [terrorists] say, which gives them a tremendous advantage against us." — FBI Director James Comey, December 2015 [1]

Abstract

The terms Deep Web, Deep Net, Invisible Web, or Dark Web refer to the content on the World Wide Web that is not indexed by standard search engines. The deepest layers of the Deep Web, a segment known as the Dark Web, contain content that has been intentionally concealed including illegal and anti-social information. The conventional Surface Web was discovered to be too risky for anonymity-seeking terrorists: they could be monitored, traced, and found. In contrast, on the Dark Web, decentralized and anonymous networks aid in evading arrest and the closure of these terrorist platforms. This paper reports some of the recent trends in terrorist use of the Dark Web for communication, fundraising, storing information and online material.

Keywords: *Internet; Dark Web; Deep Web; Terrorism; Al-Qaeda; Islamic State*

Introduction

Beneath the familiar online world that most of us know and use, a world of *YouTube*, *Google, Facebook*, and *Twitter*, lies a hidden network of sites, communities, and platforms where people can be anyone, or do anything they want. This is 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 or directing your web browser to a known website address. 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 can be defined as the portion of the Deep Web that can only be accessed through specialized browsers. A recent study found that 57% of the Dark Web is occupied by illegal content like pornography, illicit finances, drug hubs, weapons trafficking, counterfeit currency, terrorist communication, and much more.[2] Probably the most notorious example of these activities can be seen in The Silk Road website. In October 2013, the FBI shut down the first version of this drug market and arrested its owner Ross William Ulbricht. The Dark Web has been associated with the infamous WikiLeaks, as well as Bitcoin, said to be the currency of the Dark Web. Over its successful two-year run, The Silk Road made over US $1.2 billion in bitcoins. Of course, dissident political groups, civil rights activists and investigative journalists in oppressive countries have also been known to use the Dark Web to communicate and organize clandestinely.

To access material in the Dark Web, individuals use special software such as TOR (The Onion Router) or I2P (Invisible Internet Project). TOR was initially created by the U.S. Naval Research Laboratory as a tool for anonymously communicating online. It relies upon a network of volunteer computers to route users' web traffic through a series of other users' computers so that the traffic cannot be traced to the original user. Not all Dark Web sites use TOR (i.e., ".onion") addresses, but a TOR-enabled web browser can access virtually any site without revealing the user's identity. On the Dark Web, a visitor must know where to find the site in order to access it. A few search engines have been developed for the Dark Web, but they are limited in scope and usefulness.

Terrorist Interest in the Dark Web

Terrorists have been active on various online platforms since the late 1990s.[3] However, the Surface Web was discovered to be too risky for anonymity-seeking terrorists: they could be monitored, traced and found. Many of the terrorist websites and social media on the Surface Web are monitored by counter-terrorism agencies and are often shut down or hacked. In contrast, on the Dark Web, decentralized and anonymous networks enable evading arrest and the closure of these terrorist platforms. According to the London-based *Quilliam Foundation*, "The terrorist material reappears on the Internet as quickly as it is banished and this policy risks driving fanatics on to the 'dark web' where they are even harder to track." Moreover, "Islamist forums and chat rooms in English and French are still widely available, but...a large portion of more extremist Islamic discourse now takes place within the dark web."[4] "ISIL's activities on the Surface Web are now being monitored closely, and the decision by a number of governments to take down or filter extremist content has forced the jihadists to look for new online safe havens," Berton writes in her report on ISIS's use of the Dark Web.[5]

Following the November 2015 attacks in Paris, 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 *Operation Paris* (OpParis) campaign launched by the amorphous hacker collective Anonymous. ISIS's 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 *Telegram*, the encrypted communication application used by the group. Telegram is an application for sending text and multimedia messages on Android, iOS, and Windows devices. *Telegram* is so confident of its security that it twice offered a $300,000 reward to the first person who could crack its encryption. The messages shared links to a Tor service with a ".onion" address on the Dark Web. The site contains an archive of ISIS 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*. My earlier report on terrorists' use of the Dark Web revealed some early indications of the growing terrorist interest in the dark online platforms.[6] However, within several months, monitoring of online terrorism added new indications, new findings and new trends of terrorist presence in the Dark Web.

What are Terrorists Doing on the Dark Web?

A simple description of what terrorists do on the Dark Web would be, "more of the same but more secretly." However, that is only partially true. Terrorists are using the Dark Web as they have been using the Surface Web for several decades, but there are also new opportunities offered now to cyber-savvy operatives. Terrorists have used the Internet to provide information to fellow terrorists, to recruit and radicalize, to spread propaganda, to raise funds, and to coordinate actions and attacks. All of this activity, however, has now shifted to deeper layers of the Internet. Terrorist propaganda material, for example, is now stowed in the Dark Web. On 15 November 2015, two days after the Paris attacks, ISIS posted a message discussing their official *Isdarat* website, which archives propaganda and releases. The message contained links to a hidden Tor service with a ".onion" address, indicating the move of the *Isdarat* outlet to the Dark Web. The message declared: "Due to severe constraints imposed on the *#Caliphate*_Publications website, any new domain is deleted after being posted. We announce the launch of the website for "dark web." The online libraries of terrorist material led several Jihadists to suggest a "Jihadwiki".[7] In December 2015 an al-Qaeda group called the "al-Aqsa IT Team" distributed a manual entitled "Tor Browser Security Guidelines" for ensuring online anonymity while using Tor software. It offers step-by-step instructions for everything from downloading and installing the browser to steps for hindering geolocation and identification by counter-terrorism agencies.

Terrorists are now using the Dark Web also to communicate in a safer way than ever before. Although it has been long assumed that terrorist attacks are coordinated in a secret network, solid evidence has only been attained in 2013. In August 2013, the U.S. National Security Agency (NSA) intercepted encrypted communications between al-Qaeda leader Ayman Al-Zawahiri and Nasir Al-Wuhaysi, the head of the Yemen-based al-Qaeda in the Arabian Peninsula. The Institute for National Security Studies revealed that, for about a decade, the communication between leaders of the worldwide al-Qaeda network "apparently took place in a part of the Internet sometimes called deepnet, blacknet, or darknet."[8]

Recently, ISIS and other jihadist groups have used new online applications which allow users to broadcast their messages to an unlimited number of members via encrypted mobile phone apps such as *Telegram*. Since it went live on 14 August 2013, *Telegram* has seen major success, both among ordinary users as well as terrorists. But it was not until its launch of "channels" in September 2015 that the Terrorism Research & Analysis Consortium (TRAC) began to witness a massive migration from other social media sites, most notably *Twitter*, to *Telegram*.[9] On 26 September 2015, just four days after *Telegram* rolled out channels, ISIS media operatives on *Twitter* started advertising the group's own channel dubbed *Nashir*, which translates to "Distributor" in English. A recent ICT special report on *Telegram* revealed that "since September 2015, we have witnessed a significant increase in the use of the *Telegram* software (software for sending encrypted instant messages) by the Islamic State and al-Qaeda. In March 2016 alone, 700 new channels identified with the Islamic State were opened".[10]

While many of the channels have Islamic State affiliations, there are an increasing number of channels from other major players in the global jihadi world: these include al-Qaeda in the Arabian Peninsula (AQAP), Ansar al-Sharia in Libya (ASL) and Jabhat al-Nusra (JN) and Jaysh al-Islam, both in Syria. Al-Qaeda's Yemeni branch (AQAP) launched its own *Telegram* channel on 25 September 2015 and the Libyan Ansar al-Shari'ah group created its channel the following day. According to a TRAC report, membership growth for each discrete channel is staggering. Within a week's time, one single Islamic State channel went from 5,000 members to well over 10,000.[11] When asked about it, *Telegram*'s CEO Pavel Durov conceded that ISIS indeed uses *Telegram* to ensure the security of its communications, but added: "I think that privacy, ultimately, and our right for privacy is more important than our fear of bad things happening, like terrorism."[12]

Another safe communication application adapted by terrorists is the *TrueCrypt*. One of the ISIS members who was captured by French police in August 2015 revealed details about this program. Reda Hame, a Parisian IT specialist who traveled to Syria to join ISIS and fight was instead put through a rapid training course and sent back to France to carry out an attack. Hame provided details of his training to use *TrueCrypt*, an encryption application, and how, before returning to France, he was given a USB drive containing the program. The ISIS technicians also instructed Hame to transfer *TrueCrypt* from the USB key to a second computer once he reached Europe. *TrueCrypt* was launched in 2004 by Paul Le Roux, a programmer and a crime lord, who operated a global drug, arms and money-laundering cartel out of a base in the Philippines. Le Roux was arrested in Liberia on drug-trafficking charges in September 2012. But *TrueCrypt* is still active and backdoor-free, which explains why ISIS terrorists still use it for encrypted communications and file sharing.

Terrorists can use the Dark Web for fundraising, money transfers, and illegal purchase of explosives and weapons, using virtual currencies like Bitcoin and other crypto-currencies. For instance, "Fund the Islamic Struggle without Leaving a Trace" is a Deep Web page which invites donations for Jihad through transactions to a particular Bitcoin address. A PDF document posted online under the pseudonym of Amreeki Witness titled "Bitcoin wa Sadaqat alJihad," which translates to "Bitcoin and the Charity of Violent Physical Struggle," is in fact a guide for using the Dark Web for secretive financial transactions.[13] The weapons used for the deadly Paris attacks are now thought to have been purchased from a hidden Dark Web store, which,

according to official documents from the Stuttgart prosecutor's office, was a German Dark Net vendor under the username DW Guns.[14] Some reports revealed that the Dark Web has also become a medium for some terrorist organizations to sell on online black markets human organs (probably of their captives), as well as stolen oil or smuggled antiquities looted from ancient cities.[15]

In January 2015, the Singapore-based cyber intelligence company S2T uncovered concrete evidence that a terror cell, purporting to be related to Islamic State and operating in the Americas, is soliciting Bitcoin as part of its fundraising efforts.[16] The online message from the group's fundraiser, a man later identified only as Abu-Mustafa, declared: "One cannot send a bank transfer to a mujahid [someone engaged in Jihad] or suspected mujahid without the kafir [infidel] governments ruling today immediately being aware …A proposed solution to this is something known as Bitcoin …To set up a totally anonymous donation system that could send millions of dollars' worth of Bitcoin instantly…right to the pockets of the mujahideen, very little would be done [against it]".[17] Another example comes from Indonesia where a Jihadist group collected donations, both from national and international donors, through Bitcoins on the Dark Web. Furthermore, getting a stolen identity from the Dark Web, they hacked a Forex trading website to whip the points of the member. From these series of cybercrimes, the terrorist group collected US $600,000.[18]

The Challenge of Dark Web Terrorism

Terrorists flying drones to spread highly radioactive material over a civilian area: this is part of the nightmare scenario that U.S. President Barack Obama urged world leaders to consider as they debated better ways of controlling nuclear material. Speaking to a group of 50 heads of state and foreign ministers in Washington, D.C., in April 2016, President Obama described how a terrorist group had bought isotopes through brokers on the Dark Web. In March 2016, the French Interior Minister, Bernard Cazeneuve, argued that the Dark Web is being used extensively by terrorists. In a meeting of the National Assembly, he said that those who have been responsible for the recent terrorist strikes in Europe have been making use of the deep web, communicating through encrypted messages.

The growing sophistication of terrorists' use of the Dark Web presents a tough challenge for governments, counter-terrorism agencies, and security services. There is an urgent need to develop new methods and measures for tracking and analyzing terrorist use of the Dark Web. Thus, for example, the American Defense Advanced Research Projects Agency (DARPA) believes the answer can be found in MEMEX, a software that allows for better cataloguing of Deep Web sites. Providing clear evidence that shows the Dark Web has turned into a major platform for global terrorism and criminal activities is absolutely crucial in order to provide the impetus for the necessary tools to be developed to counter it. 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 February 2015, a special report entitled "The Impact of the Dark Web on Internet Governance and Cyber Security" presented several suggestions regarding the Dark Web.[19] The report states that "in order to formulate comprehensive strategies and policies for governing the Internet, it is important to consider insights on its farthest reaches—the Deep Web and, more importantly, the Dark Web." It also notes that "While the Dark Web may lack the broad appeal that is available on the Surface Web, the hidden ecosystem is conducive for propaganda, recruitment, financing and planning, which relates to our original understanding of the Dark Web as an unregulated space."

Finally, it is necessary to remember that the Dark Web also serves journalists, civil rights advocates, and democracy activists—all of whom 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 to combat illegal and nefarious activities, but one that should not impair legitimate, lawful freedom of expression.

About the Author: **Gabriel Weimann** *is a Full Professor of Communication at the Department of Communication at Haifa University, Israel. His research interests include the study of media effects, political campaigns, persuasion and influence, modern terrorism and the media. He published nine books and more than 180 academic articles in scientific journals. He received numerous grants and awards from international foundations and was a Visiting Professor at various universities including University of Pennsylvania, Stanford University, Hofstra University, Lehigh University (USA), University of Mainz (Germany), Carleton University (Canada), the American University (Washington, D.C.), the NYU branch in Shanghai (China) and the National University of Singapore. His books include Terror on the Internet (2006) and Terrorism in Cyberspace: The Next Generation (2015).*

Notes

[1] In the FBI's director's testimony to the Senate Judiciary Committee.

[2] Moore, Daniel. & Rid, Thomas. 2016. "Cryptopolitik and the Darknet", *Survival*, 58:1, 7-38. Accessed April 30, 2016; URL: http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085

[3] Weimann, Gabriel. 2006. *Terror on the Internet.* Washington, D.C.: United States Institute of Peace; Weimann, G. 2015. *Terrorism in Cyberspace: The Next Generation*. New York: Columbia University Press.

[4] Hussain, Ghaffar and Saltman, Erin Marie, 2014. "Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter It". A special report by *Quilliam*, May 2014; accessed October 1, 2015.URL: http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/jihad-trending-quilliam .

[5] Berton, Beatrice, 2015. "The dark side of the web: ISIL's one-stop shop?". Report of the European Union Institute for Security Studies, June 2015 accessed March 1, 2016. URL:http://www.iss.europa.eu/uploads/media/Alert_30_The_Dark_Web.pdf .

[6] Weimann, Gabriel, 2016. "Going Dark: Terrorism on the Dark Web", *Studies in Conflict & Terrorism* 39, 195-206. URL: http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546 .

[7] SITE Intelligence Group. 2014. "Jihadist Suggests Creating "Jihadwiki"".URL: https://news.siteintelgroup.com/Jihadist-News/jihadist-suggests-creating-qjihadwikiq.html .

[8] The Institute for National Security Studies (INSS), 2013. "Backdoor Plots: The Darknet as a Field for Terrorism", September 10, 2013.URL: http://www.inss.org.il/index.aspx?id=4538&articleid=5574 .

[9] TRAC. 2015. "Massive Migration to Telegram, the new Jihadist Destination", *TRAC Insight,* November 4, 2015.URL: http://www.trackingterrorism.org/chatter/trac-insight-massive-migration-telegram-new-jihadist-destination .

[10] International Center for Counter-Terrorism (ICT), 2016."The Telegram Chat Software as an Arena of Activity to Encourage the 'Lone Wolf' Phenomenon", May 24, 2016. URL: https://www.ict.org.il/Article/1673/the-telegram-chat-software-as-an-arena-of-activity-to-encourage-the-lone-wolf-phenomenon .

[11] TRAC. 2015. "Massive Migration to Telegram, the new Jihadist Destination", op. cit..

[12] Cited in the *Washington Post*, November 19, 2015.URL: https://www.washingtonpost.com/news/morning-mix/wp/2015/11/19/founder-of-app-used-by-isis-once-said-we-shouldnt-feel-guilty-on-wednesday-he-banned-their-accounts/ .

[13] The document is available online; URL: https://alkhilafaharidat.files.wordpress.com/2014/07/btcedit-21.pdf .

[14] Reported in numerous news outlets. See, for example, *Fox News*. URL: http://www.foxnews.com/world/2015/11/27/germany-arrests-man-reportedly-suspected-selling-guns-to-paris-attackers.html

[15] Wimmer, Andreas and Nastiti, Aulia, 2015. "Darknet, Social Media, and Extremism: Addressing Indonesian Counterterrorism on the Internet", *Deutsches Asienforschungszentrum Asian Series Commentaries,* Vol. 30. URL:https://www.academia.edu/20813843/DARKNET_SOCIAL_MEDIA_AND_EXTREMISM_ADDRESSING_INDONESIAN_COUNTERTERRORISM_ON_THE_INTERNET .

[16] "U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests", *Haaretz*, January 29, 2015; URL: http://www.haaretz.com/middle-east-news/.premium-1.639542 .

[17] Cited in "Supporter of Extremist Group ISIS Explains How Bitcoin Could Be Used To Fund Jihad", *Business Insider*, July 8, 2014; URL: http://www.businessinsider.com/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7

[18] Wimmer and Nastiti, 2015, op. cit.

[19] Chertoff, Michael. and Simon, Tobby. 2015. "The Impact of the Dark Web on Internet Governance and Cyber Security"; URL: https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf