# Exploring the Dark Web: Where Terrorists Hide?

Tuesday, February 5, 2019

***by Ghadah Alrasheed & Brandon Rigato***

One area that has not received adequate attention in the vast academic literature surrounding extremist movements and their use of the Internet is the Dark Web, whose websites are vaguely assumed to work as hubs for terrorists, drug-traffickers, and gangs. The structure, mechanisms, and impact of dark networks on terrorism is largely unknown for a variety of reasons, the main of which is the difficulty of collecting and accessing primary sources of data on the Dark Web.

Source: Reuters

The Dark Web is generally understood as a place for those seeking anonymity and invisibility when the surface web is too risky to use. This anonymity comes from the difficulty of finding who is behind the sites since, unlike other research browsers such as Google, the Dark Web sites are not indexed by search engines (Weimann, 2016a). One way to access them is through TOR (The Onion Router), a software originally developed by the U.S. Naval Research Laboratory "as a tool for anonymously communicating online" (Weimann, 2018, p. 3). The TOR Browser was later offered to the public as a free service to promote anonymous access to the internet, especially where online censorship or surveillance is high (Malik, 2018).

The Dark Web has sporadically made mainstream headlines. In 2015, it was linked to the hacking of the Ashley Madison database when the personal data of around 37 million clients were stolen and dumped in the Dark Web, including their e-mails, names, home addresses, and credit card information (Zetter, 2015). The technology has also been associated with the infamous WikiLeaks, Bitcoin, and illegal goods ranging from drugs to weapons sold on the infamous Silk Road (Gehl, 2016; Malik, 2018; Weinmann, 2018). Due to the history of organized crime linked with the Dark Web, Western security agencies have become greatly concerned with the potentiality of the Dark Web to be used by terrorist groups such as ISIS to propagate their narratives while remaining completely hidden from intelligence agencies, thus making it increasingly difficult to detect and arrest terrorism perpetrators or inciters of hate.

While being connected to a number of scandalous events, the Dark Web has received support and praise from organizations and companies such as Google, Human Rights Watch and the Electronic Frontier Foundation for the anonymity it provides (Gehl, 2016). Whatever the capacity or the efficacy of the

Dark Web in supporting illegal activities or being essential to political struggles, the Dark Web seems to have become infused with power and is symbolically seen as a source of primary effects.

Similar to previous technological developments, the novel anonymity and encryption features of the Dark Web have fuelled fears especially in relation to ideological and political violence. In a CNN article, titled as *Pentagon hunts for ISIS on the Dark Web,* Starr and Crawford (2015, May) state, "The U.S. believes ISIS and other potential terrorists are now using the most covert part of the online world to recruit fighters, share intelligence and potentially plan real world attacks.". A report prepared by the Defence and Security Accelerator, part of the UK Government's Defence Science and Technology Laboratory and Ministry of Defence (2018), warns of the threatening possibility of the Dark Net and encrypted technology to aid terrorists or criminals and jeopardize national security. The report, however, remains vague about how and when terrorists used the Dark Web to recruit or operate.

This article is a critical assessment of (scarce) academic research on the terrorist use of the Dark Web and "how" and "if" the Dark Web is used by terrorists as a dissemination or operation tool. It is important to note that there is a small number of resources that tackle the topic. Beside the lack of academic publications on the Dark Web, these resources are often inter-cited, feeding off each other. This gap in academic research on the Dark Web has shrouded the Dark Web in a cloak of mystery and discursively determined it as a place that can only accommodate dark activities. It has also allowed some confusion between the Dark Web and other end-to-end encrypted technology such as the Telegram and WhatsApp. Reviewing the literature on the Dark Web, the main definer of what the Dark Web is or how we can measure its impact is government and security think tanks. On the other hand, the Dark Web has not received much attention from independent academic disciplines and researchers.

Another form of disconnect between researchers studying the dark web is the literal and figurative use of the "dark web" in the field of terrorism. While there is the literal "dark web" that can only be accessed by downloading the TOR browser (Weimann, 2016), researchers such as HscinChun Chen (2012) and Abdullah bin Khaled al-Saud (2017) use the term "Dark Web" in a figurative sense, denoting online behaviours associated with the darker side of humanity such as organized crime and terrorism. What these academics are exploring is the "dark" activities in the regular web rather than the technical space of the Dark Web itself.

One study on the encrypted Dark Web was conducted by Nakita Malik in 2018, confirming that terrorists use the Dark Web to recruit, radicalize, gain material benefits and hide their communications and propaganda. The main evidence in the article for ISIS's use of the Dark Web as a propaganda hub was a single website found by the researcher Scot Terban via a message on the *Shamikh* forum (one of ISIS's websites on the regular web). Although this is clear evidence, it is not balanced by a systematic study of the Dark Web's content or a comparative study of such content in the open and Dark webs. The lack of evidence leads one to question the necessity or the practicality of Malik's proposal to found a governmental "regulatory body" to oversee the Dark Web (Malik, 2018).

In Malik's piece (2018), there is evidence of encrypted services such as the Telegram being used to send TOR links amongst ISIS members, as witnessed following the 2015 Paris attacks. However, there is no strong evidence of wide-spread adoption of TOR for mainstream distribution of ISIS propaganda, which is different technology than end-to-end encrypted services. This difference between the two technologies is well described by Dilipraj (2014):

> The conventional encryption softwares were able to encrypt the data payload but failed in hiding the header, whereas Tor is different from previous encryption softwares in a way that it cannot only encrypt the data payload but can also hide the header which is used for routing, thus, erasing the cyber footprint of any communication and creating more privacy, security and anonymity for its users (p.130)

In 2018, Gabriel Weinman published an article, according to which ISIS has turned to the Dark Web following the Paris attacks in 2015 when there was a massive takedown of ISIS accounts. This move, as Weinmann indicates, resulted in the creation of more than 700 Telegram channels. Similar to Malik's piece, there is an interchangeable use of the Dark Web and other encrypted technologies such as the Telegram. Therefore, it is not clear evidence of ISIS's increasing use of the Dark Web for recruitment and propaganda dissemination.

The findings of these studies are usually founded on empirically scarce ones. The only study that is based on rigorous analysis of the Dark Web's content is Moore and Rid's paper, which reveals a "near-absence of Islamic extremism on TOR hidden services" (Moore and Rid, 2016, p. 21). In their scan of hidden-services websites within the Tor network, Moore and Rid collected data through a website crawler and found 2,723 websites that met the criteria of containing illegal content. Among these, the researchers have found only a fewer than a handful of active Islamic extremist sites. While groups such as ISIS tend to use the internet for propaganda and internal communication, both uses have not stabilized on the Dark Web.  Moore and Rid explain that the reason that the Dark Web is not commonly used by ISIS mass-spreading of violence is because of the Dark Web's limited reach and its unsustainability as a way of communication.

The conclusion of Moore and Rid's study contradicts the work of many who suggest that the Dark Web is a safe haven for terrorists and an effective tool for their communications. While it is true that there is apparent and clear evidence of terrorists (like other criminals) utilizing the Dark Web for transfer of funds using the Bitcoin (Weinmann, 2018 & Malik, 2018), there is less consistent substation of the argument that the Dark Web is an ideological or discursive hotbed for terrorists and groups such as ISIS.

Robert Gehl refers this unreasonable fear of the Dark Web to moral panics associated with the internet over the past 35 years. We, similarly, argue that tech-deterministic understandings of new technologies in previous eras have constituted "a historical prior" that determines discourses and extends technological utopian/dystopian discourses to newer technologies. Discourses on the internet, therefore, tend to cluster around "liberating" or "threatening" rhetoric. It is not surprising to find such rhetoric recurring with the development of the Dark Web.

## *Works Cited:*

Abdullah bin Khaled al–Saud. (2017). The tranquility campaign: A beacon of light in the dark world wide web. *Perspectives on Terrorism, 11*(2), 58-64. http://www.terrorismanalysts.com/pt/index.php/pot/article/view/596

Chen, H. (2012). *Dark web: Exploring and data mining the dark side of the web.* New York, NY. https://www.springer.com/gp/book/9781461415565

Defense and Security Accelerator (2018). Future technology trends in security. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/728113/Future_trends_research_V6.pdf

Dilipraj, E. (2014). Terror in the Deep and Dark Web. *Air Power Journal* 9 (3), 121-140. http://www.academia.edu/9622433/TERROR_IN_THE_DEEP_AND_DARK_WEB

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the dark web social network. *New Media & Society, 18*(7), 1219-1235. Retrieved from https://www.researchgate.net/publication/280025737_Powerfreedom_on_the_dark_web_A_digital_ethnography_of_the_Dark_Web_Social_Network

Jardine, E., & Centre for International Governance Innovation (2015). *The dark web dilemma: Tor, anonymity and online policing*. Waterloo, Ontario: Centre for International Governance Innovation. Retrieved from https://www.cigionline.org/sites/default/files/no.21.pdf

Malik, N. (2018). Terror in the dark: How terrorists use encryption, the Darknet, And cryptocurrencies. The Henry Jackson Society. Retrieved from http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf

Moore, D. & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival: Global Politics and Strategy, 58*(1). Retrieved from https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085

Starr, B. & Crawford, J. (2015, May). Pentagon hunts for Isis on the secret internet. *CNN*. Retrieved from https://www.cnn.com/2015/05/12/politics/pentagon-isis-dark-web-google-internet/index.html

Weimann, G. (2018). *Going darker? the challenge of dark net terrorism*. Woodrow Wilson International Center for Scholars. Retrieved from https://www.wilsoncenter.org/publication/going-darker-the-challenge-dark-net-terrorism

Weimann, G. (2016a). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism, 39*(3). https://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546

Weimann, G. (2016b). Terrorist migration to the dark web. *Perspectives on Terrorism*, *10*(3), 40-44. Retrieved from https://www.jstor.org/stable/pdf/26297596.pdf?refreqid=excelsior%3Acf3e5132308f0aec803995af380c67e

Zetter, K. (2015). Hackers finally post stolen Ashley Madison Data. *Wired*. Retrieved from https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/

## *About the author*

**GHADAH ALRASHEED**

Ghadah Alrasheed is a postdoctoral researcher with the ALiGN Media Lab. She obtained a PhD in Communication from Carleton University with a dissertation titled "Tweeting Towards Utopia: Technological Utopianism and Academic Discourse on Political Movements in the Middle East and North Africa".

Ghadah Alrasheed is ALiGN researcher, writer, and editor.

**BRANDON RIGATO**

A PhD candidate in Communication at Carleton University, Brandon Rigato's research focuses is on extremism, radicalization and social movements, with a particular interest in right-wing and religious terrorism.

Brandon Rigato is ALiGN researcher and writer.

Tuesday, February 5, 2019 I Categories: Illuminate, Issue I: Exploring the Dark Web
Post tagged with Dark Web, Darknet, Deep Web, Google, Surveillance, technology, Terrorism
Share: Twitter, Facebook
Short URL: https://carleton.ca/align/?p=1689