

## Daesh's affair with the dark web

By R. Mohan Babu

Terrorist groups have relied on propaganda to spread their extremist ideologies. Though propaganda is used to allure sympathisers from around the world, it is also a sharp political instrument that can influence the policies of global leaders. With the sophisticated facets of communications technology at terrorists' disposal, modern day terrorism has become more intense, unpredictable and highly dangerous. Jihadi recruits can reach out to the sympathisers by a single click on the computer. This serves to highlight as to how the communication media used for propaganda have changed over the last three decades.

When Al-Qaeda was found in the late 1980's, it spread propaganda via pamphlets, audio cassettes and video tapes sold in mosques and specialist shops.<sup>1</sup> The efforts were extensive but the number of followers Al-Qaeda managed to muster can stand nowhere near what Daesh has today. Daesh has just shifted the trend of spreading propaganda from mosques and main stream media in to cyberspace. Cyberspace being a boundary-less domain facilitates terrorists to find resources, recruit and spread ideologies using social media which thus makes it easy to launch multiple attacks at the same time.<sup>2</sup>

The vastness of cyberspace has allowed the terrorists to move from the surface web to the dark web. With both being part of the cyberspace, surface web is that part of the web where all the websites available are publicly indexed. In the late 1990's terror organizations used the surface web for hosting websites that published materials propagating anti-western sentiments and chatrooms which were used as a space for recruitment.<sup>3</sup> After the 9/11 attacks, when Al-Qaeda emerged as the world's most dangerous extremist outfit, such websites increased in numbers. It was in the late 2000s and early 2010s when social media applications were being exclusively used for recruitment and spreading propaganda materials. Post 2010, intelligence agencies around the world, started cracking down on jihadi sites in social media.<sup>3</sup> Intelligence agencies snooping around in the surface web hampered the process of jihadi recruitment and the increased the chances of getting caught, therefore the trend of using the dark net took hold.

Dark web is a network built on top of the internet that is purposefully hidden and hosts sites that are not publicly indexed by search engines like Google, Yahoo or Bing.<sup>4</sup> The primary reason for the shift into the dark parts of cyberspace is that the terrorists need anonymity.

---

<sup>1</sup>Burke, Jason. "How the changing media is changing terrorism." The Guardian. February 25, 2016. (Accessed July 09, 2017) at <https://www.theguardian.com/world/2016/feb/25/how-changing-media-changing-terrorism>.

<sup>2</sup>"Technology is a foundation of modern society,". "The Role of Technology in Modern Terrorism." INFOSEC Institute. February 3, 2016. (Accessed July 8, 2017) at <http://resources.infosecinstitute.com/the-role-of-technology-in-modern-terrorism/#gref>.

<sup>3</sup>"Another major aspect of activism ". "DARKNET TERRORISM." DARKNETT AND DEEP WEB. 2016. (Accessed July 08, 2017) at <https://renbargerdarknet.wordpress.com/darknet-terrorism/>.

<sup>4</sup>"The internet has become a". "What is the DARKNET?" OWL Cybersecurity. (Accessed July 08, 2017) at <https://www.owlcyber.com/what-is-the-darknet/>

Certain applications allow for the IP (Internet Protocol) addresses<sup>5</sup> to be masked providing an added layer of anonymity while browsing both the surface web and the dark web.

Sites on the dark web can be accessed by installing special software and browsers designed for the purpose.<sup>4</sup> The Dark web also dubbed as the Darknet is not a centralized domain but is scattered via servers throughout the world.<sup>6</sup> The most popular way to access the darknet is via the Tor browser (The Onion router) in which the darknet sites end with the “.onion” extension. Tor is a network of volunteer relays through which data traffic bounces around, hence adding anonymity to the user (i.e.), in layman’s terms data request cannot be traced because the client’s request and the server’s response makes data go through a system of connected Tor users which makes tracing impossible.<sup>6</sup>

The shift to the dark web was more explicit post the “November 2015, Paris attacks”<sup>7</sup>. A major platform for jihadi recruitment and radicalisation after the Paris attacks has been encrypted messaging applications like Telegram and Orbot. Since the intelligence agencies started tightening the screws, Daesh’s shift towards such applications is evident. The loophole in encrypted messaging platforms have been converted into jihadi chat channels, especially after Telegram started the concept of channels in September 2015.<sup>8</sup> Daesh cited severe constraints on the release of their propaganda material on the surface web as a reason as to why their Isdarat outlet (Daesh’s official website) was moved to the dark web.<sup>8</sup> The link to the “Isdarat channel” on the dark web site was indeed posted on Daesh’s telegram channel.<sup>9</sup>

Apart from recruitment and radicalisation, another key reason for terrorist’s migration to the dark web is terror funding. After its rise in 2014, Daesh generated most of its fund from seized oil fields in Iraq and Syria.<sup>10</sup> Early on, most of the donations came from wealthy Daesh sympathisers but once the formal banking channels were shut down, Daesh resorted to

---

<sup>5</sup>IP address is a unique address containing a string of numbers that helps identify a machine on a network.

See Unuth, Nadeem. "What IP Means and How It Works." Lifewire. March 17, 2014. Accessed July 2017. <https://www.lifewire.com/internet-protocol-explained-3426713>.

<sup>6</sup>Bischoff, Paul. "Guide: How to access the deep web and darknet." Comparitech. April 12, 2017. (Accessed July 08, 2017) at <https://www.comparitech.com/blog/vpn-privacy/how-to-access-the-deep-web-and-darknet/>

<sup>7</sup>The November 2015 Paris attacks was a series of bombings and shootings conducted at various locations in Paris by Daesh (ISIS) ...  
See more at <http://www.bbc.com/news/world-europe-34818994>

<sup>8</sup>Weinmann, Gabriel. "Terrorist Migration to the Dark Web." *Perspectives on Terrorism*(2016). (Accessed July 7, 2017) at <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/513/html>.

<sup>9</sup>SITE staff. "IS Shifts Propaganda Archive to the Dark Web." INSITE BLOG ON TERRORISM AND EXTREMISM. November 18, 2015. (Accessed July 09, 2017) at <http://news.siteintelgroup.com/blog/index.php/categories/jihad/entry/406-is-shifts-propaganda-archive-to-the-dark-web>.

<sup>10</sup>Charles, Brooke Satti. "ISIS. Are they Using Bitcoins to Fund Criminal Activities?" SecurityIntelligence. October 29, 2014. (Accessed July 10, 2017) at <https://securityintelligence.com/isis-are-they-using-bitcoins-to-fund-criminal-activities/>.

the use of cryptocurrencies, which makes the money transfers more anonymous and untraceable.<sup>10</sup>

Cryptocurrency is a type of virtual electronic currency that is used to buy both real and virtual goods. Bitcoin is the most widely used cryptocurrency. Bitcoins do not come under the purview of currency laws nor are they illegal.<sup>10</sup> Bitcoin wallets have reference numbers for each transaction and are traded by sharing an anonymous private identification number.<sup>10</sup> Since 2014, Daesh has posted instructions in its dark web site, on how to use the Bitcoin wallets to bypass intelligence agencies, therefore making the trace difficult.<sup>11</sup>

Daesh have successfully exploited the dark web and made it into the invisible cloak under which they recruit, train, receive funds and supply weapons. Monitoring the dark web is a daunting challenge for intelligence agencies. Cataloguing the sites on the dark web for semantic analysis and profiling dark web marketplace transactions that can help narrow down transactions of the same kind, can help bring out patterns that can lead to the culprits<sup>12</sup>. Although with these measures being said, the untraceable nature of cyberspace will soon push intelligence agencies to move towards developing deterrents in cyberspace. The necessity of this can be attributed to the fact that terrorists have become technologically proficient. Also, deploying proactive measures in the surface web would keep the terrorists locked up in the dark web thereby hampering their ability to communicate globally to a large target group. There is no fool proof plan that can be drafted, when it comes to cyberspace, information sharing and constant vigilance via a collective security apparatus must be formed with the cooperation and coordination of all the major intelligence agencies in the world

**(R. Mohan Babu is a student of Symbiosis School of International Studies MA (IS), 2016-18 batch)**

---

<sup>11</sup>Harman, Danna . "U.S.-based ISIS Cell Fundraising on the Dark Web" Hareetz. January 29, 2015. (Accessed July 9, 2017) at <http://www.haaretz.com/middle-east-news/.premium-1.639542>.

<sup>12</sup>Chertoff, Michael. and Simon, Toby. "The Impact of the Dark Web on Internet Governance and Cyber Security" CIGI, February, 2015. (Accessed July 9, 2017) at [https://www.cigionline.org/sites/default/files/gcig\\_paper\\_no6.pdf](https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf)