Dark Web For Dummies
Terrorist Edition

The Dark Web: The anonymization platform of the year!

What happens on the Dark Web, stays on the Dark Web

I Don’t know what I’ve Been Told, Jihadist Forums Are Out Of Control

Craving online anonymity? The Onion Router is TORmendous for that

December 2019

Anna-Maria Brokalakis
The Components of The Web

**Surface Web:** The indexed part of the internet. It can be accessed by anyone in the public, via popular search engines like Google and Bing (Sabarinath 2019).

**Deep web:** the non-indexed, and largest, part of the internet; its contents are invisible to the public, as they cannot be found on conventional search engines. It can only be accessed with a direct access link, gateway software or encryption (Sabarinath).

**Dark web:** a sub-category of the deep web which is designed for user anonymity. Its tricky to trace the identity of the sites hosts on the dark web as their IP address details are hidden. Its contents can be accessed via encryption applications, like The Onion Router. (Sabarinath).
Jihadists and the web

The surface web has transformed into a globalized platform, meaning one can reach many users in one centralized space. It’s become an easy and efficient tool Jihadists use to conduct all their activities on, such as spread propaganda, recruit and train members, fundraise, communicate with each other and plan attacks.

Although the surface web started off as a one-stop-shop for jihadist propaganda, it’s become too risky for jihadists to participate on it. Governments have found the surface web as an opportunity to monitor, censor, track and store all Jihadist online activities. Terrorist-related content is regularly filtered out and deleted, the illegality of interacting with pro-terrorist content weakens the relationship between Jihadists and its supporters, and Internet Protocol (IP) addresses are used to track user’s whereabouts. For anonymity-seeking Jihadists, the surface web has become public to the point that their operations and agendas are in jeopardy.

IP Addresses

Gabriel Weimann, a Professor of Communications with an interest in the study of online terrorist activities, describes IP addresses (online addresses for a device) as vital for counterterrorist agencies. IP addresses allow them to track Jihadist online actions and approximate locations (Weimann 2016). With the data from IP addresses collected, agencies can spot relationships between multiple IP addresses in the same area, or addresses interacting with similar suspicious online activities. With governments tracking Jihadists and sympathizers every moves, one small mistake can lead to an arrest.

So, what do Jihadists use?

Jihadists now use The Onion Router as a gateway into the Dark Web.

Diving Deep Into The Dark Web

The Dark Web anonymizes a user’s IP address. By anonymizing an IP address, counterterrorist agencies no longer have a vital piece of information which would allow them to monitor and track Jihadists online actions. With this, Jihadists are able to disseminate their ideologies and sympathizers are able to interact with those ideologies, all under the agencies noses.

The anonymity of the Dark Web makes it a desirable hub for Jihadists to center their activities on.
The Onion Route Process

- Personal device
- Guard relay
- Middle relay
- Exit relay
- Destination
The Onion Router

An IP Address's route to anonymity and the key to accessing the Dark Web

The Onion Router

The Onion Router, Tor for short, is the most commonly used browser to access the Dark Web. Tor is a free-to-download browser that anonymizes one's IP address. It does this by bouncing traffic across three or more volunteered IP servers worldwide, encrypting the information in several layers. Since the data travels through multiple relays, it makes it furiously difficult to trace one's actions back to them. One downfall to Tor is getting to a desired online location. Since the data is no longer travelling straight from your computer to the destination, it becomes significantly slower to reach the desired destination. For those seeking to anonymize their online actions, waiting a little longer to load a Website is worth every second (Klosowski 2014). Tor is where the Dark Web .onion domain Websites can be accessed. These Websites and their contents are unindexed and only accessible to other Tor users because they are unindexed. This means they can't be searched for on popular search engines, making them invisible on the surface. With .onion domains, one must have the exact URL to access the Website (Klosowski). The links to the Websites can usually be found via word of mouth, or from the Sub Reddit, Deep Web. On the Deep Web Sub Reddit, users share links of lists of .onion URLs one can browse through.

A Message's Route Through Tor

When a Tor encrypted message, or the request to travel to a Website, is sent from your computer to the desired destination, it typically is decoded three times, with each server unlocking only one layer of the encryption. The more relays the data has, the more difficult it is to track your online actions (Wright 2015). This prevents those servers from knowing too much about the data. For example, the middle relay simply knows it was sent data from the guard relay and it must pass the data on to the exit relay. It's unaware of your device or where the data's final destination is going.

When each layer is decoded, the exit relay is then able to decode the last layer which will tell it where the message's final destination is to be sent. Finally, the message is sent to the Website you requested to travel to which is then able to be accessed.

How Effective is Tor?

Jerry Mickles, a graduate student in cyber security, explains that when law enforcement tracks an IP address to the computer in which the illegal crime was committed on, they are only locating the Tor exit relay (Mickles 1). In other words, it would take a lot of time and skill to trace back all three volunteer IP addresses to get to the original one. That is, if law enforcement officers identify that the IP address, what they seize is merely an exit relay. Therefore, Tor is highly effective in anonymizing one's identity.

To add, each relay used to send an anonymous message only knows the previous and next server. If counterterrorism agencies were to spy on a single relay, they'd have to try and work backwards until they got to the original server that sent the message. It'd be nearly impossible to track the traffic coming to a server as multiple other messages are coming from a variety of destinations. It'd be excruciatingly time-consuming to trace a single message all the way back to the original server it came from and would prove to be too inefficient to trace back the message.

The Onion Model

Visualizing the layers of an onion is an easy way to understand the Tor Process. When the data is sent off by your computer, it's encrypted in multiple layers. As each relay decodes a section of the code, a layer of encryption is peeled back.
Due to the affordance of anonymizing one’s IP address, many Jihadists migrate to the Dark Web to communicate amongst each other. A study conducted by Jialun Qin and his colleagues compared the surface Web communications between US, Latin American and Middle Eastern terrorists on the Web. Although Middle Eastern Jihadists strive to support the communications between them and their sympathizers, they seemed to have the lowest interactivity with their members (Qin et al. 85). The results, or lack-of results, of the study demonstrates that Jihadists have moved their communications away from the heavily monitored surface Web, over to the lucrative Dark Web. An event that exemplifies the lack of anonymity on the surface Web is the arrest of terror suspect Kevin Omar Mohamed. After vocalizing what seemed like a terrorist threat on Twitter and forwarding it to an ISIS fighter, his IP address was flagged and traced to his home in Whitby, Ontario. He was arrested after witnesses spotted him at the University of Waterloo. Evidence of a possible murder plot were found in an engineering locker (Bell & Russell 2017). This situation demonstrates the value IP addresses hold when tracking down Jihadists, and the inconvenience they become as missions can be intercepted. Contrastingly the Dark Web, via Tor, anonymizes ones IP address, meaning Jihadist actions and locations can’t be monitored. Without information on Jihadist’s IP addresses, their online actions can’t be intercepted, thus diminishing a Jihadist’s fear of being tracked and arrested. It also decreases the likelihood of jeopardizing their agendas. Telegram, a popular encrypted messaging app may seem to do just the same. In 2015, a schoolboy used Telegram to discuss the logistics regrading a planned attack at the Anzac Day parade in Melbourne. The only way the terror plot was intercepted was due to an unrelated arrest of the boy in which authorities looked through his phone and stumbled upon the messages (Daily Mail 2015). Although this represents the effectiveness of allowing Jihadists to communicate away from authorities’ radars, Telegram is flawed. After the 2015 incident, Telegram blocked 78 ISIS-related accounts, showing that although Telegram offers anonymity, it’s a public platform (CGTN America 2:09-2:11). Since it’s a public platform, it has user guidelines such as agreeing not to promote violence, post pornographic content or send spam, all of which are not monitored on the Dark Web. Therefore, not only does the Dark Web provide the assurance that Jihadist communications won’t be monitored and traced, but it also allows Jihadists to talk about anything and everything without fear that their content will be deleted.
Although Jihadists value communications between fellow Jihadists, they also hold a high standard in Jihadist-sympathizer relations. The affordance of anonymity provides Jihadists with the ability to disseminate their propaganda to current and future sympathizers on the Dark Web without fear of censorship. Jihadists can post anything from motivational statements to how-to instructions on bombs. Many documents are posted on the Dark Web and the only way agencies have been able to find these files is via access to the very device containing all the documents. Weimann reports that in 2014 a laptop owned by an ISIS member was stolen. Thousands of Jihadist propaganda that had been published to the Dark Web were found. Among the documents was an instructional document on making and attacking with biological weapons, which is hidden somewhere on the Dark Web (Weimann 200). In contrast, content like this wouldn’t survive long on the surface web until it’d be flagged and removed. As well, IP addresses would be collected and further monitored for future reoccurrences of Jihadist propaganda.

While the surface Web affords instant access to billions of possible recruits, the removal of terrorist accounts and content prevents terrorists from effectively disseminating their message. With the surge of terrorist-related content, platforms have upgraded their policies, placing stricter rules around what users can post. It’s been reported that Twitter has suspended over a million terrorism accounts and content on its platform. As a result, less Jihadist content is posted (Reisinger 2016). Thus, although Twitter was once a major platform used by Jihadists, it’s become one of the least preferred platforms due to the constant filtrations of the vary content that Jihadists use to recruit. Censorship makes it difficult for Jihadists to do any long-term persuading. As more surface Web censor terrorist-related content, the more likely terrorists are going to continue migrating away from social media platforms.

Without the barrier of censorship on the anonymous Dark Web, Jihadists are able to create an army of extreme sympathizers more efficiently. A concept explaining this is group polarization, which is commonly found in forums. The General Intelligence and Security Service highlights forums as one of the most popular methods Jihadists use to share their propaganda materials, connect with and reinforce ideologies with their sympathizers (General Intelligence and Security Service 6). Group polarization is like-minded users adopting a more extreme viewpoint about a topic by the time a group discussion is over (Isenberg 1986). So, Jihadist propaganda is likely to have a lasting influential effect on the potential and current sympathizers on forums. The most Jihadists expose users to Jihadist material, the more likely sympathizers are to continue participating in Pro-Jihadism interactions. In the long-term, it strengthens their extreme viewpoints as their ideologies are constantly being reinforced.

So, although the Dark Web doesn’t have nearly as many active users as the surface web does, the lack of censorship allows Jihadists to leave lasting influence on vulnerable supporters via the spread of propaganda. This yields a higher jihadist-sympathizer inactivity, creating an army of radical supporters.
Unlike the surface Web, the anonymity of the Dark Web provides those who want to vocalize their support for Jihadism with the voice to do so. Although the surface Web is deemed to be a place of free speech, many limitations are placed; consequences arise when failing to abide by these limitations. According to the United States Code, it's illegal for one to display or participate in any pro-terrorism actions or thoughts online (Doyle 2016). This proves that the surface Web isn’t as free as it’s thought to be. There have been many instances where sympathizers were arrested due to proclaiming their support for Jihadism on the Surface Web. For instance, 71 people were charged with associating with the Islamic State after an abundance of posts were created boasting about Jihadism. They were all arrested after their posts were flagged by the F.B.I. (Shane et al. 2015). Although Jihadists would reach a much larger audience via the surface Web, the illegality of the average user interacting with Jihadist content would prove to be too much of a risk for users to interact with. Not only that, social consequences like being disliked for having opposing views from family members would turn one off from displaying Pro-Jihadism views. This would yield a lower participant rate than expected, especially when attempting to convert those who are vulnerable, curious and prone to manipulation. Contrastingly, the Dark Web compensates for its significantly smaller population of users by providing anonymity.

Anonymity provides a user with true free speech. Since anonymity diminishes the fear of both the social and legal consequences of interacting with Jihadist content, all users are free to explore new behaviours. In a review of the effects of anonymity, Kimberly Christopherson, whom is in the field of psychology, describes the feeling of true free speech as an increase in aggressive online behaviour, the expression of anti-normative thoughts and opinions, and the interaction with other like-minded individuals (Christopherson 3041). Pro-jihadism users seek this sense of freedom to interact with the content Jihadists provide, to network with other like-minded sympathizers and share their own gruesome fantasies in Dark Web forums. These interactions create a safe community where everyone can participate in the conversation, no matter the topic at hand.

Re: Sympathizers on the dark web
As we can see, due to anonymity, the lack of restrictions on speech on the Dark Web proves to be the perfect environment to grow an overtly extreme army of sympathizers. Due to a hidden identity, users are free to support what they believe in without fear of scrutiny.
The dark web poses a great threat to national security. As Jihadists migrate all their activities to the Dark Web, counterterrorism agencies are losing access to leads that aid their investigations. Without IP addresses, agencies can’t track, monitor and look for patterns in Jihadist activities; they can’t intercept communications and possibly terrorist attack plots; and they can’t monitor the ever-increasing number of Jihadist sympathizers and recruits.

Though, the dark web isn’t exactly full proof. There have been major shutdowns of websites and arrests, with the most notable being the crack down of Silk Road, the eBay of drugs. Most of these arrests are followed after human error, as seen in the example of the boy who had his phone seized over an unrelated charge. When taking a look at Silk Road, an article from USA today explained that the F.B.I used weak spots in the layers of encryption Ross Ulbricht, the mastermind behind Silk Road, implemented. They used those points as entryways into hacking their way through to the primary servers (Leger 2013). Although this method seems to have worked, this was a single website dozens of members in the F.B.I tirelessly worked on in order to achieve their goal.

If agencies wanted to replicate the F.B.I’s methods, it would take an excruciatingly long time to repeat the process to an indefinite number of terrorist accounts. Not only that, websites and users are from countries all around the world. This poses an issue to the United States as these people are beyond their jurisdiction. Weimann points out if the United States decides to work with other agencies around the world, which would prove to be more time efficient, issues of cultural and legal differences would arise (Weimann 195). As of now, a legal, efficient and agreed method of cracking down on Jihadists on the dark web is far from complete.

Another issue with the lack of a plan amongst counterterrorism agencies is that technology is constantly developing. By the time a plan is made, the chances of new and improved security methods being implemented into Jihadist websites are high. Jihadist groups are working towards increasing their own security on their websites. Zaklina Spalevic and Milos Ilic highlight the methods that protect Dark Web web portals when suspicious activity is spotted. Hosts infect the user’s computer with a bug that allows them to track every move they make on it. This way, Jihadists can monitor a user’s purpose for coming onto the website (Spalevic & Ilic 79). With this method, it’d be difficult for agencies mining for information to go unnoticed.

.onion websites often tend to be deleted or inactivated by the host as they’re constantly changing location. This proves to be another challenge for agencies attempting to enter specific website because they’d then need to find the exact URL of the new destination. Without the exact URL, they’re unable to mine the new website.

Counterterrorism agencies are working tirelessly to crack down the notorious Dark Web. Unfortunately with the complexities of it, there doesn’t seem to be much hope for a solution any time soon. Until then, the Dark Web proves to be the hub Jihadists need in order to centralize all their activities on under the radar.