JudicateMe Journal

JudicateMe

2020

EMERGING DARK WEB

Edited By:

1) **Saumya Tripathi**
(Editor-in-chief)
Saumya@judicateme.com,
Saumya.judicateme@gmail.com
+91 9044382618

2) **Harsh Sonbhadra**
(Student Editor)
Harsh.judicateme@gmail.com

EMERGING DARK WEB

By, Ashutosh Sharma
From Damodaram Sanjivayya National Law University, Visakhapatnam

INTRODUCTION

The Dark Web is a network of activities online that cannot be found on the Internet and cannot be accessed through the use of search engines. The concept of the Dark Web has existed in the US since the 1990s. The Department of Defense's two research institutes in the U.S. tried to create an anonymous network to secure the sensitive communications of spies[1]. In October 2013, the growth of the Dark Web did not catch the attention of the public until the arrest of "Dread Pirate Roberts", known as Ross William Ulbricht.

The Dark Web is a general term for the most planted corners of the web, where people can interact online without worrying about the watchful eye of the authorities. Typically, these sites are protected by encryption mechanisms such as Tor, which are used for "onion routers", allowing users to visit them anonymously. However, some sites do not trust Tor, such as password-protected forums where hackers exchange secrets, and even stolen credit card numbers can be considered part of the Dark Web.

People use the Dark Web for a variety of purposes: buying and selling drugs, discussing computer hacking techniques and selling hacking services, exchanging child pornography, and more.

It is important to remember that the techniques used to facilitate "dark web" activities are not fundamentally good or bad. Similar techniques can be used by drug dealers and child pornographers to conceal their identities from whistleblowers and decenter in oppressive rulers.[2]

WHERE DOES THE DARK WEB COME FROM?

[1] Aditi kumar and Eric Rosenbach, The truth about the dark web (sept. 2019) https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-web-kumar.html

[2] Timothy B. Lee, The dark web: what it is, how it works, and why it's not going away (Dec 31, 2014), https://www.vox.com/2014/12/31/7470965/dark-web-explained

The U.S. government has created a "dark web" to allow spies to exchange information anonymously.

U.S. military researchers developed a technology called the Tor (Onion Router) in the mid-1990s and released it to the public.

The reason was that they wanted to remain anonymous - it would have been more difficult to distinguish between government messages and spies if thousands of others had used the same system for many things. Tor now hosts about 30,000 hidden sites.

It's called an onion router because it uses onion routing technology - to encrypt websites using encryption layers. Most websites also host onions on the domain.[3]

HOW DOES THE DARK WEB WORK?

The Dark Web can only be accessed by unconventional browsers, especially TOR and I2P (of which TOR is the most popular)[4]. Tor provides anonymity by directing Internet traffic through a computer using other "TOR nodes" or browsers.[5] This traffic bounces through TOR nodes until it finally passes through the "exit node".[6] This essentially creates an “onion” or multi-layered anonymity. According to the Tor website, “Tor protects you by tricking your communications around a relay distribution network run by volunteers around the world: it prevents you from learning what sites you visit when you see an Internet connection, and which sites prevent you from visiting your physical location. "

In addition to benefiting the TOR browser, many users will use a virtual private network (VPN) and/or a virtual machine (VM) to facilitate additional levels of protective anonymity. These additional steps are not necessary to access the Dark Web but are considered the best practice by cybersecurity professionals who regularly engage in research activity on the Dark Web. Once the TOR browser (or its I2P equivalent) is installed on the user's a computer and network anonymity is enabled, the user needs to decide which dark web location they want to access.

---

[3] Jennifer Hale, What is the dark web? From drugs and guns to the Chloe Ayling kidnapping, a look inside the encrypted network (2 Aug 2019), https://www.thesun.co.uk/tech/2054243/dark-web-kidnap-chloe-ayling-encrypted-network-black-death/

[4] *ibid*

[5] "What The Heck Is A TOR Exit Node?", *Skeptical Science*, 2017, https://www.skeptical-science.com/science/technology/heck-tor-exit-node/

[6] The Tor Project, Inc, Torproject.Org, https://www.torproject.org/.

No search engine works on the Dark Web, so simple directories with address links are used to navigate the Dark Web. However, links directories are unreliable because addresses are constantly changing. Often the website shuts down overnight and will reopen at a different address the next day, as sites are compromised by hackers or law enforcement agencies. Navigating the Dark Web is notoriously difficult for new users. Regular users rely on other users' websites to address the information they already know.

DARK WEB CRIMES

Any type of crime with obscure transactions, including drugs, money, or even humans, can be committed on the Dark Web. The darkest corner of the internet is just a platform for numerous crimes, but here are some examples of dark web crimes:[7]

MURDER FOR IRE HIRE- This place is a market for the contract killing of Besa Mafia (and others like it).

BLACKMAIL / EXTORTION - A scam involves threatening to release conciliatory photos (even when there are no such photos) unless the victim states the amount of bitcoin.

[7] Findlaw's team, Dark Web Crimes, (May 15, 2019) https://criminal.findlaw.com/criminal-charges/dark-web-crimes.html

DRUG ILLEGAL DRUG SALES - The Silk Road is the most publicized example, but there are others.

ILLEGAL ARMS SALES - It is estimated that thousands of dollars worth of firearms are sold illegally on the Dark Web every month.

SEX TRAFFICKING - In 2015, the Office Fees of the New York County DA used an experimental Internet search tool to apprehend and prosecute the leader of the sex trafficking ring.

TERRORISM - ISIS and other terrorist groups use the Dark Web to recruit and plan attacks.

CHILD PORNOGRAPHY - An estimated 144,000 individuals in Britain alone were using the Dark Web to access child pornography in 2018.

BITCOIN AND ITS USES ON THE DARK WEB

Bitcoin, a cryptocurrency founded in 2009, is a decentralized digital currency that has promoted many national security threats, as well as raised awareness around the need for government intervention and regulation.

Bitcoin operates on a peer-to-peer (P2P) blockchain, an encrypted system of records for all transactions distributed on the

Internet free of human interference. Cryptocurrencies are considered highly volatile due to short-term value fluctuations. However, its value has risen sharply since its inception and as of March 2017, the total net worth has reached the US $17 billion.

Individuals can buy and sell Bitcoin through an online exchange such as Quadrigacx, which facilitates transactions between banks and the Bitcoin market. Virtually anyone can own Bitcoin as long as they can transfer funds online through their financial institution. Many of these online exchanges require less customer identification to process a request. Because the ownership of this cryptocurrency is unknown and not controlled by governments, it enables the possibility of the purchase and distribution of illicit goods, money laundering, and terrorist financing.

Historically, cryptocurrencies have been used as a tool to facilitate the sale of illicit goods on the Dark Web. Dark Web is a platform online platform operating on a P2P network of websites that act as an e-commerce hub for buyers and sellers to communicate and trade a variety of illegal and unregulated goods and services. This includes the illegal possession of firearms, explosives, hazardous chemicals, stolen identification information, killers, drugs, and many other types of goods.

Transactions between users can remain anonymous through crypto-currency encryption, the use of virtual private networks that can mask the IP addresses of buyers and sellers, and P2P networks of the Dark Web. Many of these dark web sites operate on voluntary servers all over the world and back up to other locations in different countries under the pressure of pushing the shutter. Almost everyone who has Bitcoin can get involved in buying and selling these illegal goods. The tools needed to access the web are tools such as a P2P network browser, and a virtual private network (VPN).

The Dark Web serves as a gateway for high-risk individuals to acquire deadly weapons, which could inevitably compromise national security. For example, if a high-profile terrorist group was able to obtain weapons-grade uranium (which is available on the Dark Web), they could eventually develop a nuclear weapon that could be used against the state. As sellers and buyers are anonymous, it is difficult for foreign regulators to track sales of these goods and services. This suggests that high-risk individuals, such as terrorists, may be able to sell illicit goods such as drugs to finance their operations, even if they are anonymous.

Bitcoin also poses a risk of money laundering and terrorist financing, as the inadvertent distribution of wealth can allow the transfer of funds between terrorist groups, organizations, and banks. Although the exchange has imposed fees on bitcoin transfers between online exchanges, this is rarely a deterrent as anyone can transfer funds from one exchange to another and then to their bank while remaining anonymous.

Many online bitcoin exchanges are not monitored and do not require customer identification, so it is difficult to track who and where the money was sent from. Bitcoin is also decentralized and operating globally, making it difficult to determine which body should be responsible for monitoring money laundering through Bitcoin, international or local.

There is a great deal of discussion on the pros and cons of the Dark Web and Bitcoin. However, the international organization must monitor the activities taking place to safeguard national security.[8]

USE THE FINANCIAL WEBSITE TO ENGAGE IN FINANCIAL AND ARMS SUPPORT

In December 2018, Israeli authorities filed criminal charges against a man named Ahmed Sarsour for trying to use the Dark Web to arm and finance terrorists in Syria.[9] According to court documents, Sarsour's actions included attempting to purchase explosives, hiring snipers, and providing financial support. Additional reporting by CNN shows that this is not just a separate phenomenon, but an emerging phenomenon. In September 2018, CNN reported that a TOR website called "SadaqaCoins" had been launched on the Dark Web, with the site's stated goal of "supporting the jihad by providing a secure platform between funding and project organizers."[10]

As the global conflict between free society and terrorism persists into the 21st century, terrorists and terrorist sympathizers around the world continue to adapt their methods in response to changes in national security tactics and the evolution of technology. At

[8] Thomas Phelan, Bitcoin and The Dark Web's Threat to National Security (April 10, 2017), http://natoassociation.ca/bitcoin-and-the-dark-webs-threat-to-national-security/

[9] "Kafr Qasem Resident Indicted For Financing And Purchasing Weapons For Terrorist On Dark Web", Deep Dot Web, 2018, https://www.deepdotweb.com/2018/12/01/kafr-qasem-resident-indicted-for-financing-and-purchasing-weapons-for-terrorist-on-dark-web/.

[10] "Crypto Crowdfunding Terrorists: Marketplace For Jihadist Crowdfunding Found On Dark Web", CCN, 2018, https://www.ccn.com/crypto-crowdfunding-terrorists-marketplace-for-jihadist-crowdfunding-found-on-dark-web/.

this stage, it is common knowledge that NATO and its allies have the technical advantage of being able to observe what would be considered "open" communications (e.g. telephonic communications, radio, surface web, etc.). Terrorist organizations have also begun to realize this and are shifting their communication techniques to technological means that provide high-name anonymity to use TOR.[11] In addition to changing communication techniques in anonymous media, national security professionals should also try to understand how terrorist organizations will use the Dark Web to achieve their violent and political objectives.

In the future, it makes sense that terrorists would benefit the Dark Web Markets to purchase content capable of carrying out their objectives. In addition to weapons and funding, enabling content such as forged identities, non-compliant communication devices, and forged documents, the ability to travel, secure communication, establish proof of residence, etc. can help facilitate terrorist organization targets. This is especially true when we think about the impact of how a potential terrorist could use this competent material to adopt.

Instead of a list of forged documents in most markets, various forged documents can be found that include forged: passports, driver's licenses, utility bills, tax forms, green cards, etc. In some cases, vendors have demonstrated on the Dark Web. Ability to sell legal identity documents as opposed to counterfeit documents. In 2017, a man who may have been on the Terrorist Watch List tried to obtain a legal passport from the Dark Web from a fake identity seller. The seller claims to be selling genuine passports from European countries, which he can obtain through his alleged links to "corrupt individuals" within the passport issuing agencies of these European countries. Conversation between seller and buyer-buyer In an online conversation, the seller strongly denied the purchase request, saying he believed the buyer was on the watch list.[12]

LEVELS OF WEB

Level 0 Web: Common Web

Level 1 Web: Surface Web

[11] Ashley Madison is a popular extramarital dating site. ("Lessons To Be Learned From The Ashley Madison Data Breach", Panda Security Mediacenter, 2017, https://www.pandasecurity.com/mediacenter/security/lessons-ashley-madison-data-breach/.)

[12] Weise, Elizabeth. "Terrorists use the Dark Web to hide," USA Today, 2017, https://www.usatoday.com/story/tech/news/2017/03/27/terrorists-use-dark-web-hide-london-whatsapp-encryption/99698672/.

Level 2 Web: Bergie Web

(Proxy required after this point…..)

Level 3 Web: Deep Web

Level 4 Web: Charter Web

Level 5 Web: Marianas Web

WHO WAS CHLOE AYLING?

Chloe Ayling is a 20-year-old British model who was lured to Milan by a notorious sex trafficking gang known as the 'Black Death Group'.

One of the mothers was abducted for six days in a distant Italian farmhouse after being led to Milan by fake promises of a photoshoot.

She was stuffed inside drugs and bags before being auctioned off on the Dark Web.

The Black Death Group is an obscure group linked to several cases of kidnapping and human trafficking.

Departments of the Internet claim to be notorious for using dark web pens to buy abducted women in Europe.

WHO IS ROSS ULBRICHT?

Ross Ulbricht was the man behind the Silk Road, the Internet's largest market for illicit drugs - hosted on the Dark Web.

The Silk Road was valued at 34.5m and had about 10 million anonymous customers. On the Silk Road, you could buy drugs, services (such as hacking into Facebook accounts), pirated content, fake passports, and more. You'll also be able to check each dealer's reviews and star ratings left by other customers.

Ulbricht was arrested by the FBI in 2013, who closed the Silk Road and convicted him of money laundering, computer hacking, conspiracy to misrepresent traffic documents and conspiracy to smuggle drugs.

CONCLUSION

The most effective way to combat illegal activities on the Dark Web is to search for illegal sites instead of illegal users. Under the appropriate legal authority, government hackers may place deanonymizing tools on the computers of users who access the site. If the government just shuts down the site, it will be replaced elsewhere. On the other hand, if implementers bring charges against users of an illegal site, prospective users who are considering illegal sites will be more reluctant to do so because of the risk of catching them. The final option would be for the government to try to break the tor, in other words, to identify each tor user. This, given the previous trend with

the Silk Road, is likely to become a stronger version of the service, thwarting government efforts. It will also destroy useful tools for legitimate users like disgruntled people.

Understanding the best implementation techniques is just the first step. The United States is constitutionally committed to protecting freedom of expression on the Internet in a way that many other countries do not. Some countries want to have complete control over traffic on the Internet. They see freedom of speech as a threat to their power and the Dark Web that enables dissidents to speak freely. The Internet, by its very nature, is an international network of computers. Enforcement jurisdictions are foggy at best, so the government will have to find ways to cooperate in establishing at least some mutually acceptable rules governing the Dark Web.

The discussion around the Dark Web is by no means over. Anonymous is a double-edged sword that must be handled delicately. As policy-makers move forward, they must closely monitor the evolution of the Dark Web and ensure that enforcement agencies successfully provide the Dark Web with police resources and legal assistance. To maintain a balance between the needs of users with privacy and the government's responsibility to prevent illegal activity, like all good policies, the Dark Web policy must be nuanced and thoughtful.