8

Inside the Dark Web

Gar LOVEJOY

Abstract: The Dark Web and its widely abused platforms are a major security concern for many governments today. The following paper will explore the evolving landscape and emerging threats found on the Dark Web. This article aims to provide context, and appropriate tactics that governments can employ in countering this new age of global terrorism and crime. As well as a comprehensive review of the tools and services associated with the Dark Web.

Keywords: Dark Web, Tor, Bitcoin, Hidden Wiki

Layers of the Internet

The misinterpretation of terms such as the surface web, Deep Web, and Dark Web has always been prevalent[333]. The websites we browse for our day to day activities only make up a small percentage of the actual internet, this is called the surface web. It is visible and accessible to common search engines such as Google and Yahoo. While estimates vary, many experts agree that the surface web comprises roughly only 4% of all online content[334]. This is known as the Iceberg theory, with the part below the surface being much greater then above. The Deep Web, the part of the internet which is not directly available, makes up about 96% of the World Wide Web. It consists of the parts which are not indexed or accessible

[333] "What Is the Darknet or Darkweb? – DarkOwl – Darknet Big Data." *DarkOwl*. Accessed July 23, 2019. https://www.darkowl.com/what-is-the-darknet.

[334] "Understanding the Deep & Dark Web," *Hackernoon,* 2019.

by any standard search engine. These are benign private databases such as online banking, medical records, government resources, subscription information etc. These databases are not available to the general public, they can only be accessed by a direct URL or IP address and require authentication.

The Dark Web on the other hand, also known as the Dark Net, is a subset of the Deep Web. It is the anonymous part of the Deep Web only accessible by special software and specific cyber connections. One cannot access the Dark Web without specialized encryption and obfuscation software known as Tor, or I2P[335]. The Dark Web is a collection of thousands of websites that use these anonymity tools. Sites that exist on the Dark Web exist on encrypted networks and cannot be found using traditional search engines[336]. The user must know where to find the site through directories such as the "Hidden Wiki" in order to type in the URL and visit. To visit a Dark Web site or "hidden service" that runs Tor encryption, the web user needs to be using Tor. This principle applies to I2P as well, the visitor must use the same encryption tool as the site. Although many people have never seen or used this software, it is freely available for download and can be installed in just a few minutes. This is your passport to the digital underworld. The identity and activity of Dark Web users stay anonymous and cannot be traced due to the multi layered encryption system. The Dark Web's encryption technology routes users' data through a large number of proxy servers operated by thousands of volunteers around the globe. This provides a secure channel where the client and server can communicate without being concerned of their identities. These anonymity tools, Tor being the most widely used and I2P a distant second, prevent network surveillance and traffic analysis. Due to the Dark Web's anonymous nature it has enabled a variety of illegal activities to take place. It provides a safe haven for terrorist communications as well as a vector for recruitment. It allows for terrorist networks and crime syndicates to utilize bitcoin and

---

[335] Eric Cole, *Online Danger: How to Protect Yourself and Your Loved Ones from the Evil Side of the Internet*. (New York: Morgan James Publishing, 2018).

[336] "The Dark Web: What Is It? How Does It Work? And How Do I Access It?" Cryptalker. July 04, 2019. https://cryptalker.com/dark-web/.

various crypto currencies for money laundering. It has become a delivery service for any crime imaginable, drugs, stolen goods, identity theft, child porn, human trafficking, hit men, weapons, explosives, uranium, hackers for hire, malware distribution, rootkits, botnets, and zero-day exploits[337]. The Dark Web has become a proverbial Amazon for crime. It is a major concern for governments and security agencies around the world, one whose impact on society and public policy will be explored in this paper.

History of the Dark Web

As stated earlier, the Dark Web is a collection of sites and resources that are deliberately hidden. Most sites on the Dark Web makes use of Tor, short for "The Onion Router", that acts as an overlay network providing online protection. Tor's powerful encryption and network of volunteers make it virtually impossible to find anyone's real identity when they access a site using it.[7] Tor was originally created by the NRL the Naval Research Laboratory in the 90s as a means for military personnel to communicate abroad anonymously. However, its original purpose was negated because only the US government at that time used the network. Runa Sandvik, a security researcher who worked on the Tor Project, explained that Tor was released to the public in 2002 because, "if you have this anonymity system and all traffic going into the system is the US Navy and everything popping out is the U.S. Navy then you're not that anonymous. By opening up this system to everyone, different groups of people can hide in a big crowd of anonymous Tor users"[338]. Tor makes all of its users look the same which confuses the observer and makes you anonymous. The more people who use the Tor network, the stronger it gets. Since the security of a single user is a direct function of the number of overall users, a large user base is vital. Smaller darknets are easier to hack and easier to de-anonymize. Very quickly due to its anonymous nature, TOR attracted

---

[337] Marc Goodman, *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*, (New York: Anchor Books, a Division of Penguin Random House, LLC, 2016).

[338] Michael Chertoff, "A Public Policy Perspective of the Dark Web." *Journal of Cyber Policy* 2, no. 1 (2017): 26–38. doi: 10.1080/23738871.2017.1298643.

thousands who wanted to use it for a variety of purposes – ranging from legitimate to highly illegal.

With regard to the legitimate reasons to use Tor or other similar services, it is important to keep in mind that the ability for users to email, surf the web, share content without giving away their IP address is critical if you reside in China, Russia, Iran, or other countries that control and surveil the internet. One could rely on Tor to mask their identity when visiting sites such as Facebook, YouTube, or the New York Times. Tor also protects users' data against corporate and government targeted mass surveillance. The Tor Project has already won several awards for the spread of freedom and democracy around the world. For example, in 2009 during the "Green revolution" protests in Iran and the 2011 "Arab Spring" in Syria, Tor was used as a means for dissident movements to collaborate but remain hidden in plain view[339] or is also increasingly being used by journalists to securely communicate with sources and whistleblowers such as those within the WikiLeaks community.

Even if Tor might have been originally developed for good, ironically within the US government, it should come as no surprise that given its powerful ability to facilitate clandestine communication, criminals, terrorists, and black hat hackers have adopted the tool in droves, enabling the creation of illegal marketplace services such as the Silk Road[340].

Illegal Marketplace

The Dark Web facilitates a wide variety of criminal transactions where a range of malicious actors – from drug and arms dealers to terrorists to hackers for hire leverage the secrecy and anonymity afforded by tools like Tor and I2P to facilitate conversation, coordination, and action[341]. A user on the Dark Web can buy drugs, guns, credit card numbers, various exploits, and just about

---

[339] Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press, 2014.

[340] Goodman, *Future Crime*, 2016.

[341] Kristin Finklea, "Dark Web," *Federation of American Scientists*, March 10, 2017, Accessed July 18, 2019. https://fas.org/sgp/crs/misc/R44101.pdf.

anything you can imagine. Anonymizing services like Tor enable these Dark Web sites that host illegal content to exist. A paper published in 2016 by researchers at Kings College attempted to quantify how much of Tor's hidden services were used for illegal activity. Researchers used the two most popular search engines on the Dark Web, Ahmia and Onion City. The scans returned a total of 5,205 live websites over a 5-week period within the Tor network. Out of which 1547, 28%, hosted illicit material (see table below)[342].

Table 8.1

Category	Websites
None	2,482
Other	1,021
Drugs	423
Finance	327
Other illicit	198
Inknown	155
Extremism	140
Illegitimate pornography	122
Nexus	118
Hacking	96
Social	64
Arms	42
Violence	17
Total	5,205
Total active	2,723
Total illicit	1,547

Classification of websites in Tor network, source: Daniel Moore & Thomas Rid, "Cryptopolitik and the Darknet," *Global Politics and Strategy*, 58:1, (2016), 7–38, doi: 10.1080/00396338.2016.1142085

A 2019 study, *Into the Web of Profit*, conducted by Dr. Michael McGuires at the University of Surrey, shows that things have become even worse. The number

[342] Daniel Moore & Thomas Rid, "Cryptopolitik and the Darknet," *Global Politics and Strategy*, 58:1, (2016), 7–38, doi: 10.1080/00396338.2016.1142085

of dark web listings that host illicit content has risen by 20% since 2016[343]. The definitions used by these researchers for illegal activities were as follows:

Table 8.2

Category	Details
Arms	Trading of firearms and weapons
Drugs	Trade or manufacture of illegal drugs, including illegally obtained prescription medicine
Extremism	Content espousing extremist ideologies, including ideological texts, expressions of support for terrorist violence, militant how-to guides and extremist community forums
Finance	Money laundering, counterfeit bills, trade in stolen credit cards or accounts
Hacking	Hackers for hire, trade or distribution of malware or DDoS capabilities
Illegitimate pornography	Pornographic material involving children, violence, animals or materials obtained without participants' consent
Nexus	Websites primarily focused on linking to other illicit websites and resources within the darknet
Other illicit	Materials that did not easily fit into the other categories but remain problematic, such as trade of other illegal goods and fake passports or IDs
Social	Online communities for sharing illicit material in the form of forums, social networks and other message boards
Violence	Hitmen for hire, and instructional material on conducting violent attacks
Other	Non-illicit content, such as ideological or political content, secure drop sites, information repositories, legitimate services
None	Websites which were either completely inaccessible or otherwise had no visible content, including websites which hosted only placeholder text, indicating that their operator had yet to generate indicative content

Categories of websites in Tor network, source: Daniel Moore & Thomas Rid, "Cryptopolitik and the Darknet," *Global Politics and Strategy*, 58:1, (2016), 7–38, doi: 10.1080/00396338.2016.1142085.

Some security and law enforcement experts privately estimate the vast majority of Tor's hidden services are unlawful. As you can see in Table 8.1,

[343] Moore & Rid, "Cyberpolitik and Darknet" 2016.

the rate of criminal adoption is far outpacing that of privacy activists[344]. As of 2017, Tor software had been download over 200 million times, and currently in 2019, it is being used by 3 million people daily. That means over 400,00 criminals are getting up and going to work on the Dark Web using Tor's hidden services. Silk Road was just one of dozens of online criminal super marketplaces. If you want to purchase drugs today on the Dark Web you can go to Empire Market. Or if you want to commit identity theft and buy credit cards, bank account numbers, from virtually every bank and country in the world, one would only need to go to Genesis Market[345]. If criminals and terrorists, for example, need to travel across international borders and establish new identities, they could buy a fake passport, or immigration documents from the BlackBooth Market. If someone wants to purchase weapons and explosives, such as handguns with silencers, Ak-47s, Bushmaster M4's, C4 explosives, NIJ level IV body armor, they would only need to access AlphaGuns or the EuroGuns market. Additionally, as we saw on Silk Road, assassinations are also just a click away on the Dark Web. Service providers such as Quick Kill and C'thulu have all advertised "permanent solutions to common problems"[346].

There have also been numerous sites on the Dark Web providing a sanctuary for merchants of child pornography[347]. Sites like Jailbait, and Lolita City have thrived. For example, one Dark Web site alone had over 27,000 registered pedophile members in its forums. All these illicit goods and services are offered for sale on the Dark Web. With the transactions on the Dark Web taking place using crypto currencies like Bitcoin, it makes it difficult for law enforcement to trace these transactions, identify suspects and gather evidence of criminality. Today, these marketplaces – driven by a "fully networked and anonymous criminal workforce"[348], drive tremendous profits, a trend that is only increasing.

---

344 Goodman, *Future Crime*, 2016.

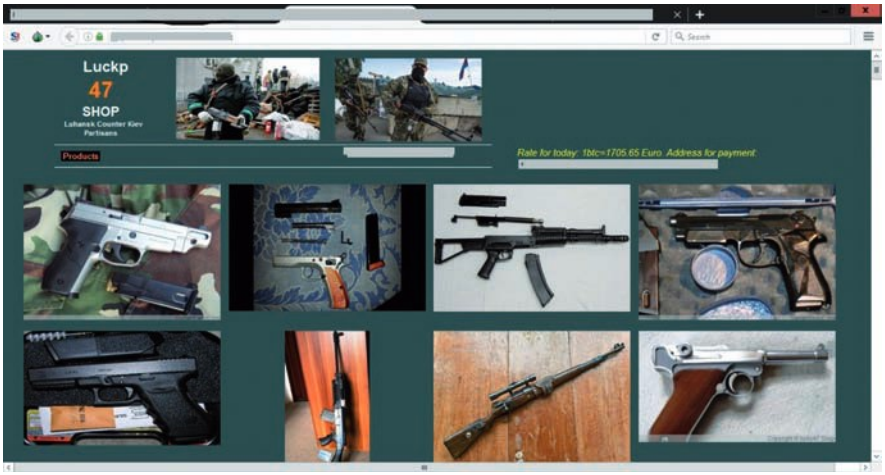
345 13 "Darknet Market List – Top 23 Deep Web Markets With Links & Status." *Dark Web Links | Dark Web Sites | Deep Web Links 2018*, July 18, 2019, https://www.thedarkweblinks.com/darknet-market-list/.

346 Goodman, *Future Crime*, 2016.

347 "Darknet Market List –Top 23 Deep." *Dark Web Links*, 2019.

348 Goodman, *Future Crime*, 2016.

Dark Web Gun Store



Source of the image: https://www.linkedin.com/feed/update/urn:li:activity:6487109320453472256.

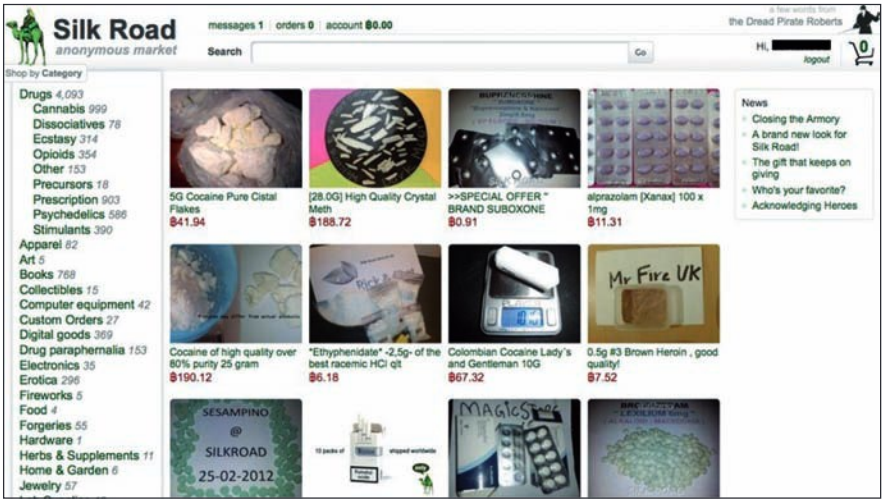
The Silk Road, "also known as the Amazon of drugs and vice," is one of the best-known examples of a successful and lucrative online criminal marketplace. Known as the first modern Darknet market[349], it was launched in 2011 and offered every possible illicit product imaginable, neatly presented by category with costumer reviews, high resolution photos, and descriptions. It offered, "stolen bank accounts, counterfeit currency, Ak-47s, armor piercing rounds, stolen credit cards, computer viruses, keystroke loggers, compromised Facebook accounts, tutorials with step by step instructions on hacking ATMs and other point of sale machines, child pornography, and even hit men for hire"[350]. Between 2011 and 2013, Silk Road processed more than 1.2 billion dollars' worth of transactions. Users on marketplaces like Silk Road use Bitcoin and other crypto currencies that are rooted in anonymity, making it extremely difficult for Law Enforcement to track. According to *Addiction* nearly 20% of drug users in the United States purchased narcotics on Silk Road. Even though Silk Road was eventually shut down and its owner arrested, ironically "the Silk Road bust was

[349] "Case 76: Silk Road (Part 1) – Casefile: True Crime Podcast." Casefile. February 11, 2018. Accessed July 18, 2019. https://casefilepodcast.com/case-76-silk-road-part-1/.

[350] Goodman, *Future Crime*, 2016.

the best advertising the Darknet markets could have hoped for[351]. In 2013 the number of listings offering illegal content for sale on the Dark Web appeared to have more than doubled in less than a year.

Silk Road Website



Source of the image: https://www.elheraldo.hn/mundo/607212-318/justicia-cierra-sitio-web-de-venta-de-drogas

Tor's most controversial property is its capability of creating hidden services such as Silk Road on its network[352]. This allows anybody running Tor the ability to create and host a hidden web service, "a virtually untraceable server hosted within the Tor network, simply by adding two short lines of code to a short configuration file"[353]. This allows circumvention of all known forms of content restrictions or surveillance. Neither the Internet Service Provider (ISPs) that route the traffic, nor law enforcement agencies, nor even the developers of the Tor project itself, have visibility into the

---

[351] Angus Crawford, "Dark Net Drugs Adverts 'Double in Less than a Year'," *BBC News*, July 31, 2014, Accessed July 19, 2019, https://www.bbc.com/news/technology-28242662.

[352] "The Dark Web: The Land of Hidden Services." *ICANN*. Accessed July 23, 2019. https://www.icann.org/news/blog/the-dark-web-the-land-of-hidden-services.

[353] Daniel Moore & Thomas Rid, "Cryptopolitik and the Darknet," *Global Politics and Strategy*, 58:1, (2016), 7–38, doi: 10.1080/00396338.2016.1142085.

hosted servers' location or the identity of its operator[354]. Unlike the human readable domain names that we are used to seeing on the surface web. com,.org,.net, these hidden services or Dark Web sites deal with domains that do not participate in the public DNS (Domain Name System) and are not recognized by ICANN (The Internet Corporation for Assigned Names and Numbers) they are always 16-character values prepended to the.onion top-level domain[355]. For example Silk Road's hidden domain name was silkraodvb5piz3r.onion. Users can navigate to these sites through directories, as stated prior, such as the "Hidden Wiki" which organizes Dark Web sites by category similar to Wikipedia. In addition, users can also browse the Dark Web with search engines such as Ahmia, Onion City or Grams which were patterned after Google where users can find illicit drugs, guns, counterfeit money and other contraband[356].

Terrorism

Crime is not the only reason to use Tor hidden services. A number of reports indicate that Al Qaeda, ISIS, Ansar al Sharia in Libya (ASL), Jabhat al-Nsura (JN), as well as other terrorist groups, use the secrecy and anonymity afforded by Tor and I2P encryption protocols. They use the Dark Web, "to communicate, recruit new members, raise funds, purchase arms, spread propaganda, and even plan operations"[357]. 25 Terrorists have started to recognize the advantages of the Dark Web and have begun to use its secret platforms. Many of the terrorists' websites or social media are shut down. With the decision by many governments to filter extremist content, it has resulted in jihadists looking for new online safe havens[358]. The conventional surface web is much too risky, for terrorists can be monitored,

---

354 Moore & Rid, "Cyberpolitik and Darknet" 2016.

355 "The Dark Web: The Land of Hidden Services." *ICANN*. 2019.

356 Finklea, "Dark Web," 2017.

357 "Going Darker? The Challenge of Dark Net Terrorism." *Wilson Center*, June 04, 2018, Accessed July 21, 2019, https://www.wilsoncenter.org/publication/going-darker-the-challenge-dark-net-terrorism.

358 "Going Darker? The Challenge of Dark Net Terrorism." *Wilson Center*, 2018.

traced, and found, in contrast to the Dark Web, where the decentralized and anonymous networks keep their identity and activity hidden[359].

Solid evidence of terrorist use of the Dark Web platforms was found in 2013. The NSA intercepted encrypted communications between Al-Qaeda leader Ayman-Al Zawahiri and Nasir Al-Wuhayasi, the head of AQAP. It was revealed that for about a decade the communication between leaders of the worldwide Al-Qaeda network was at least partially leveraged on the Dark Net[360]. Following the Paris attacks in November 2015, ISIS had completely 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[361]. The move came 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 even posted a link and explanations on how to get to their new Dark Net site on a forum[362].

Terrorists also use the Dark Web to obtain weapons. In the Paris attacks four of the assault rifles used had been originally purchased off the Dark Web from a vendor in Germany. Additionally, the weapon used in the 2015 Munich shooting rampage was also bought off the Dark Web. This illustrates the pervasiveness of arms dealing on the Dark Web[363]. With the sheer availability of weapons on these marketplaces, it is likely to facilitate a nexus between criminal arms dealers and terrorists, as it removes the need for a physical connection between vendor and buyer[364]. This is par-

---

[359] Gabriel Weinmann, "Terrorist Migration to the Dark Web." *Perspectives on Terrorism* 10, no. 3 (2016): 40–44. http://www.jstor.org/stable/26297596.

[360] "Going Darker? The Challenge of Dark Net Terrorism." *Wilson Center*, 2018.

[361] Weinmann, "Terrorist Migration to the Dark Web," 2016.

[362] "Going Darker? The Challenge of Dark Net Terrorism." *Wilson Center*, 2018.

[363] Paoli, Persi, Giacomo, Aldridge, Judith, Ryan, Nathan, Warnes, and Richard, "U.S. Weapons Are the Main Source of Illegal Arms on the Dark Web," *RAND Corporation*, July 19, 2017, https://www.rand.org/pubs/research_reports/RR2091.html.

[364] Nikita Malik, "How The Darknet Can Be Used By Terrorists To Obtain Weapons," *Forbes*, January 15, 2019, https://www.forbes.com/sites/nikitamalik/2019/01/15/how-the-darknet-can-be-used-by-terrorists-to-obtain-weapons/.

ticularly concerning given the fact that ISIS has called for simplistic attacks in the past such as vehicular attacks, and knives. This growing nexus raises the stakes quite a bit. It is possible now for self-starter terrorists, savvy enough to access Dark Net marketplaces, to obtain weapons and carry out significant attacks.

The Dark Web can also be used by terrorists for the clandestine transfer of funds, using virtual currencies like Bitcoin and Monero. This recent trend is one of the most alarming combinations of terrorism and the Dark Net capabilities[365].

In 2015 a Singapore based cyber intelligence company S2T uncovered concrete evidence that a terror cell, related to ISIS operating in the Americas solicited Bitcoin in its fundraising efforts[366]. One hacker group "Ghost Security" even went so far as to track the digital footprints of the perpetrators of the Paris attacks. They successfully uncovered a number of Bitcoin addresses belonging to ISIS. One of the accounts analyzed, contained over 3 million US dollars' worth of Bitcoin. The growing sophistication of terrorists' use of the Dark Web and crypto currencies presents a tough challenge for governments, counter terrorism agencies and security services[367].

Hackers for Hire

The Dark Web is also a sort of hackers' paradise. It is a black market of exploits. Hackers distribute malware, exchange attack methods, share known vulnerabilities in networks or software, and collaborate to breach tough cyber defenses[368]. Quite often the worst cyber-attacks are launched from the Dark Web. Take for example the Target breach of 2013. The malware BlackPOS, which was responsible for the massive invasion of Target's point of sale systems, was purchased off the Dark Web. This was one of the

---

365 "Going Darker? The Challenge of Dark Net Terrorism." *Wilson Center*, 2018.

366 Weinmann, "Terrorist Migration to the Dark Web," 2016.

367 "Going Darker? The Challenge of Dark Net Terrorism." *Wilson Center*, 2018.

368 Cole, *Online Danger,* 2018.

largest data breaches in history, with over 40 million credit and debit card numbers, along with 70 million records of personal information stolen[369].

Some of the most popular cyber exploits can be found on the Dark Web – fully packaged cyber-crime toolkits like SpyEye, Zeus, and Bugat[370]. These kits can be used for phishing campaigns, spam, fraud, DDoS attacks, and data theft. Network compromises and large-scale data breaches used to be spearheaded by highly skilled hackers. Now a days it does not take a sophisticated and carefully planned operation to break into IT systems. Hacking tools and malware that are available on the Dark Web, make it possible for amateur hackers to cause enormous damage[371].

Frighteningly enough, in the digital underworld, users can shop for zero-day exploits. As reported, "Zero-day bugs … have not yet been discovered by software and antivirus companies thus defeating common security measures without raising alarm"[372]. Zero-day exploits enable particularly stealthy and sophisticated attacks against specific targets, giving rise to what security researchers term APTs, advanced persistent threats. The likelihood of being detected in one of these attacks is effectively nil. Society today is faced with serious challenges emanating from this proliferation of open source cyber weapons. Marc Goodman, former member of the FBI cybercrime division warns, "The panoply of malware toolkits and millions of botnet zombies on the Dark Web are providing criminals and terrorists powerful tools of domination that can be used as offensive weapons, cash making machines or both"[373]. There are tools on the Dark Web available for download developed to attack industrial control systems and take power grids off-line. Goodman states that there are zombie botnets, like Storm Bot 2.0 for sale capable of generating 300 gigs per second of attack

---

[369] Finklea, "Dark Web," 2017.

[370] Goodman, Future Crime, 2016.

[371] Ivana Kottasová, "An Entire Nation Just Got Hacked," *CNN*. July 21, 2019, Accessed July 23, 2019, https://edition.cnn.com/2019/07/21/europe/bulgaria-hack-tax-intl/index.html.

[372] "Zero-day Vulnerability: What It Is, and How It Works." *Norton*, Accessed July 24, 2019, https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html.

[373] Goodman, Future Crime, 2016.

traffic, enough to "knock small countries offline." How long will it be before someone uses one of these "digital Molotov cocktails" and lobs it back at us with the intent of attacking our own critical infrastructure systems?[374].

The Role of Cryptocurrencies

One of the main enabling mechanisms of the Dark Web is cryptocurrencies like Bitcoin. Bitcoin is pseudonymous and difficult to trace. It is the standard currency of the Dark Web. Bitcoins are an uninsured and variable currency that was created in 2009[375]. They are stored in encrypted digital wallets. Bitcoins are designed to be very difficult to track back to the person who spent them. Each transaction is recorded in a public log, but only the wallet IDs are recorded, not the names of the buyer or seller.

Bitcoin can then easily be laundered through unregulated exchanges, such as those without KYC/AML procedures (Know-Your-Customer and Anti-Money Laundering) which avoids identity checks. In a report from 2016, researchers at the University of Technology in Sydney found that approximately 25% of bitcoin users and 41% of bitcoin transactions were associated with illegal activity[376]. The same report estimated that roughly $72 billion worth of bitcoin changes hands for illegal goods and services each year, with a majority of these transactions taking place on the Dark Web. The Center on Sanctions & Illicit Finance even published a memo that roughly 95% of bitcoin laundered from 2013 to 2016 originated from transactions made on Dark Web marketplaces such as Silk Road, AlphaBay and Agora.[377]45 In 2017 another research group CipherTrace reported that the amount of cryptocurrency laundered had tripled from 2016. One can assume by 2019 it is significantly larger. The level of anonymity is unrivaled by any other payment mechanism. Bitcoin's use of a wallet as the

---

[374] Ibid.

[375] Chertoff, "A Public Policy Perspective of the Dark Web." 2017

[376] 44 Tebba Von Mathenstien, "Cryptocurrency's Criminal Revolution." Medium. July 19, 2018. https://medium.com/s/story/cryptocurrencys-criminal-revolution-6dae3cdf630f.

[377] Von Mathenstien, "Cryptocurrency's Criminal Revolution," 2018.

sole identifier of an entity in a transaction makes analysis harder than with traditional financial institutions and instruments[378].

However, all is not lost, law enforcement agencies and data analysis firms are quickly adapting. Police forces around the world are getting faster, and more competent at flagging Bitcoin transactions linked to illegal activity. Bitcoin's underlying digital ledger technology the blockchain can also work against criminals and terrorists. It records which address sends and receive transactions including time and amount. Analytic firms and law enforcement agencies have developed databases and powerful sophisticated engines capable of blockchain analysis.

However just as law enforcement has adapted, so too has the adversary. Criminals are now turning in droves to bitcoin mixers known as tumblers. This refers to online third-party services which break down your coins into many different parts and mix those parts with other broken parts from other clients[379].A tumblers purpose is to mix one's funds with other users' money, obscuring the trail back to the fund's original source[380]. Even more concerning for law enforcement, is the shift criminals have taken, moving towards crypto currencies such as Monero, Zcash, and Dash that provide massive advantages over Bitcoin. Virtual currencies like Monero, have an increased focus on privacy. It encrypts the recipients blockchain address and generates fake addresses to obscure the real senders, it also obscures the amount of the transaction[381]. High privacy cryptos like Monero, eliminate law enforcements ability to trace transactions and identity suspects.

---

[378] "Cryptocurrency's Criminal Revolution." *Bitcoin Insider*, July 12, 2018, https://www.bitcoininsider.org/article/32485/cryptocurrencys-criminal-revolution.

[379] "What Is a Bitcoin Mixer (or Tumbler) and How Does It Work?" *Cryptalker*, July 17, 2019, https://cryptalker.com/bitcoin-mixer/.

[380] "Europol, EU Authorities Take down Crypto Laundering Site Bestmixer in First-ever Such Action" *Association of Certified Financial Crime Specialists*. A BARBRI, Inc. ACFCS. 2019. https://www.acfcs.org/news/453974/Europol-EU-authorities

[381] "Criminal Underworld Is Dropping Bitcoin for Another Cryptocurrency," *Gulf*, January 10, 2018, Accessed July 19, 2019, https://www.gulf-times.com/story/577660/Criminal-underworld-is-dropping-bitcoin-for-anothe.

Policing the Dark Web

Due to the threats lurking within, the Dark Web is fair game for the most aggressive intelligence and law enforcement techniques. Law enforcement agencies for years have been developing technology to infiltrate and deanonymize services such as Tor.

All the way back in 2002 the FBI put resources into developing malware that can compromise servers in attempt to identify users of Tor[382]. The FBI reportedly used a "computer and Internet protocol address verifier (CIPAV) to identify suspects who were disguising their location using proxy servers or anonymity services like Tor[383]. This technology allows Tor traffic to be flagged separately from regular internet traffic. This helps law enforcement agencies narrow down their search parameters during an investigation.

Police forces have been expending considerable resources in trying to unmask the uses of Tor. In 2014, it was revealed the FBI paid the SEI of CMU (Software Engineering Institute of Carnegie Melon) $1 million to hack Tor. This led to the arrest and prosecution of Silk Road 2.0 operators. Tor eventually patched this protocol vulnerability in mid-2014, but it demonstrated the law enforcement's reach. That same year DARPA (Defense Advanced Research Projects Agency) began conducting a research project called Memex. This was the development of a software that allowed for better cataloguing of Dark Web sites. Zetter shares, "It aimed to shine a light on the Dark Web and uncover patterns and relationships in online data to help law enforcement and others track illegal activity"[384].

Additionally, after the Snowden leaks, it was revealed that the National Security Agency (NSA) reportedly had a program called Xkeyscore. This showed that any user simply attempting to download Tor, was automatically

---

[382] Finklea, "Dark Web," 2017.

[383] Poulsen, Kevin. "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack." Wired. June 03, 2017. Accessed August 02, 2019. https://www.wired.com/2013/09/freedom-hosting-fbi/.

[384] Zetter, Kim. "DARPA Is Developing a Search Engine for the Dark Web." Slate Magazine. February 10, 2015. https://slate.com/technology/2015/02/darpa-memex-dod-agency-developing-a-search-engine-for-the-dark-web.html.

fingerprinted, essentially enabling the NSA to know the identity of millions of Tor users[385]. Tor is a high priority target for the NSA. The work of attacking Tor is executed by the NSA's application vulnerabilities branch, which is a part of the SID (systems intelligence directory).

Furthermore in 2015 the FBI employed the most extensive use of malware a US law enforcement agency had ever employed before. Targeting the world's most notorious darknet child pornography site. The FBI used a hacking tool, NIST (network investigative security technique), which exploited the Tor Browser. 95% of the code in Tor browser comes from Firefox with some modifications and some additions[386]. Court documents show that likely a piece of Flash or JavaScript that exploits a vulnerability in the Firefox based Tor browser was employed. Once law enforcement found the IP address to the physical server that hosted this illegal site and arrested its operator, instead of shutting it down, they ran the site for another 2 weeks on a FBI server as a watering hole. Any visitor to the site had the malware planted on their machine, making it an easy way for law enforcement to identify and prosecute them. Over 1500 Playpen users were arrested. Tor quickly applied a patch to the critical zero-day vulnerability. The operation however was legally controversial, it generated serious concerns about security research ethics, not to mention the right of not being unreasonably searched guaranteed by the US fourth amendment. The debate surrounding the Dark Web had just begun. Online anonymity is a double-edged sword that must be handled delicately[387].

Going Forward

This paper has shown clear evidence that the Dark Web is a major platform for global terrorism and criminal activities. The growing sophistication of terrorists' and criminal use of the Dark Web presents a tough

---

[385] "Going Darker? The Challenge of Dark Net Terrorism." *Wilson Center*, 2018.

[386] Inc. "Tor." Tor Project: FAQ. Accessed July 23, 2019. https://2019.www.torproject.org/docs/faq.html.en.

[387] Chertoff, "A Public Policy Perspective," 2017.

challenge for governments, counter terrorism agencies and security services in the future[388].

While countries like China and Russia have taken efforts to completely block access to Tor, these agendas compromise the ideals of a free and open society. Specific tactics for intervening on the Dark Web must be carefully considered. Dark Web policy, like all good policy, "must be nuanced and thoughtful in order to strike the balance between the needs of innocent privacy minded users and the government's responsibility to stop illegal activity"[389].

Governments have to employ appropriate tactics that stop illegal activity while also protecting innocent privacy minded users like those who live under repressive regimes. However, there is an obvious demand for illegal online marketplaces, so it is not an issue that will dissipate on its own. Law enforcement agencies and prosecutors around the world must undertake coordinated actions in targeting high value black marketplaces. This will overcome jurisdictional obstacles. The international community must promote cross-border information sharing, investigation and enforcement operations such as those during Operation ONYMOUS by Europol's European Cybercrime Centre, the FBI, the U.S. Immigration and Customs Enforcement's, Homeland Security Investigations and Eurojust. The operation resulted in 17 arrests of vendors and administrators running online dark marketplaces and more than 410 hidden services being taken down. Bitcoins worth approximately USD 1 million, EUR 180 000 euro in cash, drugs, gold and silver were seized. The dark market Silk Road 2.0 was taken down by the FBI and the U.S. ICE HIS, and the operator was arrested[390].

Government agencies need to solidify their policies on how to regulate the Dark Web within a legal framework. Consensus is important and coordinating regulations is vital. The combined capabilities of different government

---

388 Weinmann, "Terrorist Migration to the Dark Web," 2016.

389 Chertoff, "A Public Policy Perspective," 2017.

390 "Europol's 20 most noteworthy operations:, source: https://www.europol.europa.eu/about-europol/europol-20-years/europols-20-most-noteworthy-operations.

agencies can be effectively utilized towards regulating the Dark Web. The most appropriate tactics to employ are those that are narrowly focused like the FBI and Europol's take down of Playpen and Silk Road 2.0[391]. This allows for long term deterrence by looking for illegal sites instead of illegal users; government hackers can place deanonymizing tools onto the computers of users accessing the site, and future users who are considering accessing illegal sites will be more hesitant to do so in the future[392]. Tools and techniques must be continually developed in order to monitor and track the illegal activity. Cybercrime budgets must be increased. Law enforcement has to be able to recognize and deal with the various crimes on the Dark Web, whether it is enhancing security agencies ability to trace cryptocurrencies like Bitcoin through blockchain analysis with certain training and collaboration in both the private and public sector, or mapping Tor's hidden service directories through software like Memex. There is a need to develop NITs, hacking tools which maintain the privacy of the average Tor user, while unmasking the criminal on specific sites[393]. These methods and measures must be put in place in all security agencies. The cyber skills gap between authorities and the adversary must be closed.

Like Michael Chertoff the former head of DHS said, "us policy makers moving forward must monitor vigilantly the evolution of the Dark Web and ensure that enforcement agencies have the resources and legal support to successfully police the Dark Web"[394]. These widely abused platforms have to be fair game for the most aggressive intelligence and law enforcement techniques as well as for invasive academic research[395]. The line between utopia and dystopia is growing increasingly thin.

---

391 Chertoff, "A Public Policy Perspective," 2017.

392 Finklea, "Dark Web," 2017.

393 Chertoff, "A Public Policy Perspective," 2017.

394 Albamonte, Herman, "Illicit Trade in the Dark Web", Accessed August 25, 2019, https://medium.com/@hernan.albamonte/illicit-trade-in-the-dark-web-a734ee605340.

395 Moore & Rid, "Cyberpolitik and Darknet" 2016

Bibliography

Bitcoin Insider. "Cryptocurrency's Criminal Revolution." Bitcoin Insider. July 12, 2018. https://www.bitcoininsider.org/article/32485/cryptocurrencys-criminal-revolution.

"Case 76: Silk Road (Part 1) – Casefile: True Crime Podcast." Casefile. February 11, 2018. https://casefilepodcast.com/case-76-silk-road-part-1/.

Chertoff, Michael. "A Public Policy Perspective of the Dark Web." *Journal of Cyber Policy* 2, no. 1 (2017): 26–38. doi: 10.1080/23738871.2017.1298643.

Cole, Eric. *Online Danger: How to Protect Yourself and Your Loved Ones from the Evil Side of the Internet*. NY, NY: Morgan James Publishing, 2018.

Crawford, Angus. "Dark Net Drugs Adverts 'double in Less than a Year'." BBC News. July 31, 2014. https://www.bbc.com/news/technology-28242662.

"Criminal Underworld Is Dropping Bitcoin for Another Cryptocurrency." Gulf. January 10, 2018. https://www.gulf-times.com/story/577660/Criminal-underworld-is-dropping-bitcoin-for-anothe.

"Cryptopolitik and the Darknet." Taylor & Francis. https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085?scroll=top&needAccess=true#.

"Darknet Market List – Top 23 Deep Web Markets With Links & Status." Dark Web Links | Dark Web Sites | Deep Web Links 2018. July 18, 2019. https://www.thedarkweblinks.com/darknet-market-list/.

"Europol, EU Authorities Take down Crypto Laundering Site Bestmixer in First-ever Such Action" Association of Certified Financial Crime Specialists: A BARBRI, Inc. Company. ACFCS. 2019. https://www.acfcs.org/news/453974/Europol-EU-authorities-take-down-crypto-laundering-site-Bestmixer.io-in-first-ever-such-action.htm.

Finklea, Kristin. "Dark Web – Federation of American Scientists." March 10, 2017.. https://fas.org/sgp/crs/misc/R44101.pdf.

"Going Darker? The Challenge of Dark Net Terrorism." Wilson Center. June 04, 2018. https://www.wilsoncenter.org/publication/going-darker-the-challenge-dark-net-terrorism.

Goodman, Marc. *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*. New York: Anchor Books, a Division of Penguin Random House, LLC, 2016.

Greenberg, Andy. "Hacker Lexicon: What Is the Dark Web?" Wired. July 20, 2017.. https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/.

Inc. "Tor." Tor Project: FAQ. Accessed July 23, 2019. https://2019.www.torproject.org/docs/faq.html.en.

Kottasová, Ivana. "An Entire Nation Just Got Hacked." CNN. July 21, 2019. https://edition.cnn.com/2019/07/21/europe/bulgaria-hack-tax-intl/index.html.

Malik, Nikita. "How The Darknet Can Be Used By Terrorists To Obtain Weapons." Forbes. January 15, 2019. https://www.forbes.com/sites/nikitamalik/2019/01/15/how-the-darknet-can-be-used-by-terrorists-to-obtain-weapons/.

Mathenstien, Tebba Von. "Cryptocurrency's Criminal Revolution." Medium. July 19, 2018. https://medium.com/s/story/cryptocurrencys-criminal-revolution-6dae3cdf630f.

Paoli, Persi, Giacomo, Aldridge, Judith, Ryan, Nathan, Warnes, and Richard. "U.S. Weapons Are the Main Source of Illegal Arms on the Dark Web." RAND Corporation. July 19, 2017.. https://www.rand.org/pubs/research_reports/RR2091.html.

Poulsen, Kevin. "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack." Wired. June 03, 2017. https://www.wired.com/2013/09/freedom-hosting-fbi/.

Rumold, Mark. "Playpen: The Story of the FBI's Unprecedented and Illegal Hacking Operation." Electronic Frontier Foundation. September 28, 2016. https://www.eff.org/deeplinks/2016/09/playpen-story-fbis-unprecedented-and-illegal-hacking-operation.

Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press, 2014.

Staff, NPR. "Going Dark: The Internet Behind The Internet." NPR. May 25, 2014. https://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet.

"The Dark Web: The Land of Hidden Services." ICANN. https://www.icann.org/news/blog/the-dark-web-the-land-of-hidden-services.

"The Dark Web: What Is It? How Does It Work? And How Do I Access It?" Cryptalker. July 04, 2019. https://cryptalker.com/dark-web/.

"Understanding the Deep & Dark Web." Understanding the Deep & Dark Web – By. https://hackernoon.com/understanding-the-deep-dark-web-8e4cad356587.

"What Is a Bitcoin Mixer (or Tumbler) and How Does It Work?" Cryptalker. July 17, 2019. https://cryptalker.com/bitcoin-mixer/.

"What Is the Darknet or Darkweb? – DarkOwl – Darknet Big Data." DarkOwl. https://www.darkowl.com/what-is-the-darknet.

"Zero-day Vulnerability: What It Is, and How It Works." Official Site. Accessed July 20, 2019. https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html.

Zetter, Kim. "DARPA Is Developing a Search Engine for the Dark Web." Slate Magazine. February 10, 2015. https://slate.com/technology/2015/02/darpa-memex-dod-agency-developing-a-search-engine-for-the-dark-web.html.